Design and Implementation of Controlling and Monitoring System Based on Wireless VPN

Siraj Qays Mahdi
Electrical and Electronics Techniques Collage, Foundation technic/ Baghdad
Email: siraj_qays@yahoo.com.

Received on: 16 /5 /2012 & Accepted on: 6 /9 /2012

ABSTRACT

The work presented in this paper was concerned to design a new remote control and monitoring system, which can be used for controlling the electrical devices at college/office and monitoring the clients' status by using the Virtual Private Network (VPN). The system is consists of server and multi clients and utilize VPN for establish a secret communication within internet network or enhanced wireless network. The server employed for controlling the remote devices which inherent with clients through serial interface. The interface circuit was designed to connect the serial port with the devices which are consisting of (Max238, UART, and CD4060) to complete the functions of interface. There are 8 pins for data output, which can produce up to 256 different control signal statuses. The mechanism of monitoring operation was achieved through executing two function: firstly, the files transfer (image or text) between sever and clients; secondly, monitoring the client status through server computer. For more security a new wireless enhanced network was built to implement the Virtual Private Network (VPN) which consists of four power nano station (5GHz) to establish transfer information for distance up to 35 Km. PPTP (Point to Point Tunneling Protocol), IPSec. (Internet Protocol Security) was configured to give secret authentication for virtual private network. Visual basic language was used to implement the frameworks (GUI) and socket connection.

Keywords: VPN, Socket, Wireless Network, Serial Interface, UART.

تصميم وتنفيذ نظام السيطرة والمراقبة المستند على الشبكة اللاسلكية الظاهرية الخاصة

الخلاصة

العمل المقدم في البحث يهتم بتصميم نظام ألسيطرة والمراقبة عن بعد، والذي يستخدم للسيطرة على الأجهزة الكهربائية في الكلية /المكتب وكذلك مراقبة حالة حاسوب الزبون باستخدام الشبكة الظاهرية الخاصة . يتألف النظام من خادم وعدة زبائن ويتم استخدام الشبكة الظاهرية الخاصة لتأمين الاتصال السري ضمن شبكة الانترنت أو شبكة لا سلكية محسنة. يوظف حاسوب الخادم

https://doi.org/10.30684/etj.31.2B.4
2412-0758/University of Technology-Iraq, Baghdad, Iraq

للسيطرة على الأجهزة البعيدة المتأصلة مع حواسيب الزبائن من خلال التوصيلة المتسلسلة. تم تصميم دائرة التعشيق لربط المنفذ المتسلسل مع الأجهزة والتي تتألف من (Max238, UART, and CD4060) لإكمال وظيفة التوصيلة. توجد ٨ مسامير لإخراج البيانات والتي يمكن أن تنتج بحدود ٢٥٦ إشارة سيطرة مختلفة. إلية عملية المتابعة أنجزت من خلال تنفيذ وظيفتين: الأولى، نقل الملفات (الصورية أو النصية) بين الخادم والزبائن. ثانيا، مراقبة حالة حاسوب الزبون من خلال الخادم. لزيادة الأمنية، شبكة لاسلكية محسنة تم بنائها لتنفيذ الشبكة الظاهرية الخاصة والتي تتألف من أربعة محطات إرسال (5GHz) لتأمين نقل البيانات لمسافة بحدود ٣٥ كيلومتر. بروتوكول قناة الاتصال وبروتوكول الانترنت السري تم تشكيلهم لإعطاء التحقق السري للشبكة الظاهرية الخاصة. استخدمت لغة فيجوال بيسك لتنفيذ الواجهات واتصال المقبس.

INTRODUCTION

Computer networks are typically a shared resource used by many applications for many different purposes. Sometimes the data transmitted between application processes is confidential, and the application users would prefer that others not be able to read it [1]. A VPN is an example of providing secret connection and controlled connectivity over a public network such as the Internet. VPN utilize a concept called an IP tunnel-a virtual point-to-point link between a pair of nodes that are actually separated by an arbitrary number of networks [2].

The key that distinguish Virtual Private Network (VPN) from the general network is that VPN adopts tunnel technology. The data packets are encapsulated and transmitted after they are encrypted by the tunneling protocol, and ensure that the data packets' confidentiality and integrity when they across the public network. The basic process of tunnel technology is that the data at the interface of source local area network and public network (data of data link layer or network layer) can be encapsulated into a transmission data formats at the public network as the load [3]. At the interface of local area network and public network, the data will be encapsulated and removed the load.

A Virtual Private Network (VPN) provides a secure communications mechanism for data and other information transmitted between two endpoints [4]. VPN tunneling protocol has four categories: point-to-point tunneling protocol (PPTP), the Layer 2 Tunneling Protocol (L2TP), the network layer tunneling Protocol: IP Security Protocol (IPSec) and the Protocol for sessions traversal across firewall securely (SOCKS v5) of the session layer [5].

Design a new remote control and monitoring system using VPN has became an important research which can be used in the modern Laboratories to control the experiments equipments and monitoring the students' results and exchange the resources between them. In addition for achieving it in factories which need for Supervisory control.

Many researchers were introduced for design a system for controlling the devices using PIC microcontroller or LAN network.

[Hassan A.], describe a distributed home monitoring and control system using microcontroller as device controller. A host computer act as master and client manages the activities of the microcontroller by instructing them to control their respective devices and collecting data from them [6].

[Zhang Y, et al.], describe a necessary system to monitor and control remotely the devices in scattered unattended machine rooms. The remote monitoring and controlling system are designed based on SNMP and TCP/IP which used mainly intranet [7].

[Wijetunge S., et al.], a general purpose controlling module is designed with capability of controlling and sensing the devices simultaneously. The communication between the controlling module and the remote server is done using Bluetooth technology [8].

This paper was implemented by depending on virtual private network instead of the traditional network (LAN, MAN) to avoid the penetrating by comparing with the previous researches. And new enhanced wireless network was built to achieve the virtual private network, in addition to use (PPTP & IPSec.) protocols to increase the authentication and to insure data transfer between nodes.

ARCHITECTURE OF THE PROPOSED SYSTEM

The purpose of this work is building a virtual private network between server and multi clients through a public infrastructure network. The server was responsible for controlling the devices inherent with clients through serial port; the monitoring was accomplished with through the secret data transfer between server and clients. The construction of public network was enhancement for occurring intranet with a large extent and depended on wireless technologies, such as IEEE 802.11 and IEEE 802.16 (which reach up to 35 kilometer) , the proposed network was shown in Figure(1).

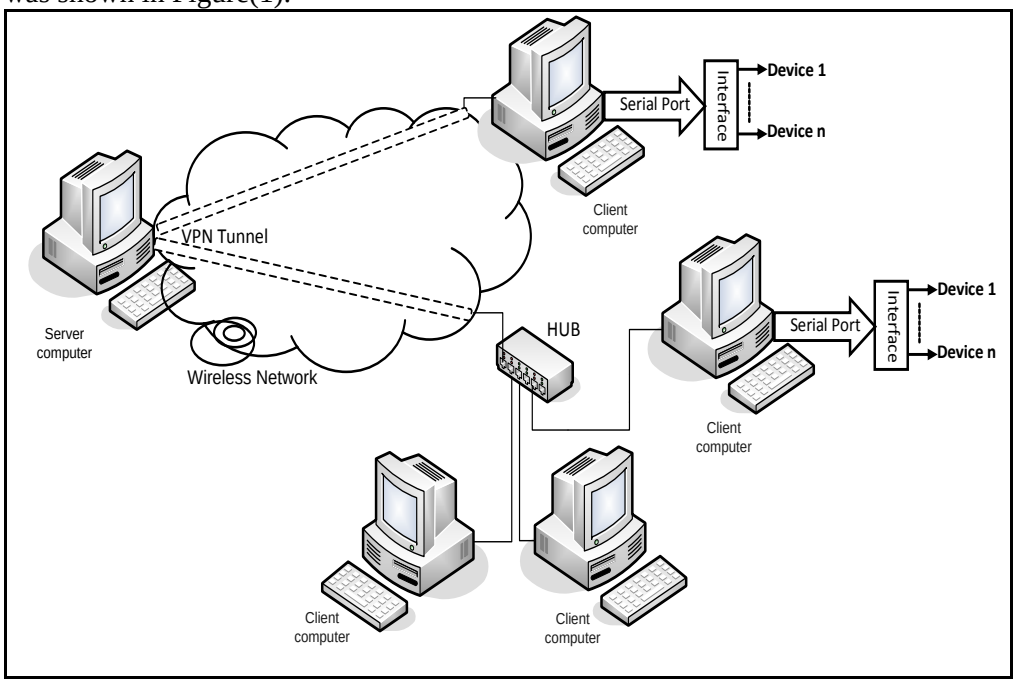

Figure (1) The proposed network.

The block diagram of the control system is shown in Figure (2), where the server send the control command through network by using software applied for

this purpose, the client receive this command and analyze it using another software and insert the signal to the device through serial interface.

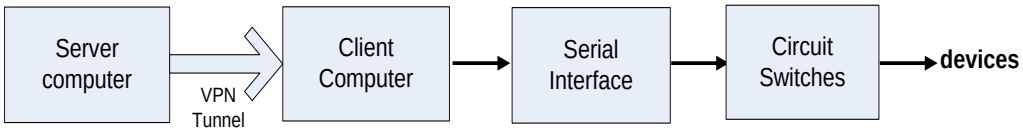

Figure (2) Block diagram of control system.

VPN CONNECTION

A VPN is a private network that is constructed within a public network infrastructure such as internet or intranet to make remotely access in addition to secure tunnel depend on PPTP (point to point tunneling protocol) was built between server and clients. The standard configuration in the server and clients are explaining in the following steps [9]:

The VPN configuration in server computer:

1. Create a new connection.
2. Set up an advance connection: in order to make other computer able to connect it.
3. Accept incoming connections: allow other computer to connect to this computer.
4. Allow virtual private connection.
5. Identify the names with its password for each client which needs to connect with its computer server.
6. Identify the protocol (TCP/IP) and specify the address range of computers (clients) which connect with its computer (server).
7. Finish the connection wizard.

The VPN configuration in each client:

1. Create a new connection.
2. Connect to the network at my work place.
3. Allow virtual private network connection.
4. Identify the name of server will connect to it.
5. Identify the public IP address of server.
6. Finish the connection wizard.

The different steps was lead to make a private tunnel between each client and server, but the server is very complicated configuration than other because contain all the names and password of clients that authorized for connection with server in addition to contain a packet of IP address which limited the size of network and to avoid the collisions.

When the connection of VPN between server and client was established which depended on public IP of server, the protocol TCP/IP and IPX/SPX protocols

insured for dealing with the rule of VPN connection. In addition to PPTP was open tunnel between two nodes (server and client).

IP security system structure referred to as IPSec. is a group of cryptography based security of open network security protocol; it combines several security technologies to form complete system. Through data encryption, authentication and integrity check technology. It ensures the reliability of data transmission privacy and confidentiality [9]. A group of numbers was selected for each client computer to achieve the protocols of IPSec. under windows XP environment as shown in Figure (3), which consist of IP Encapsulating Security Payload (ESP) and key management protocol.

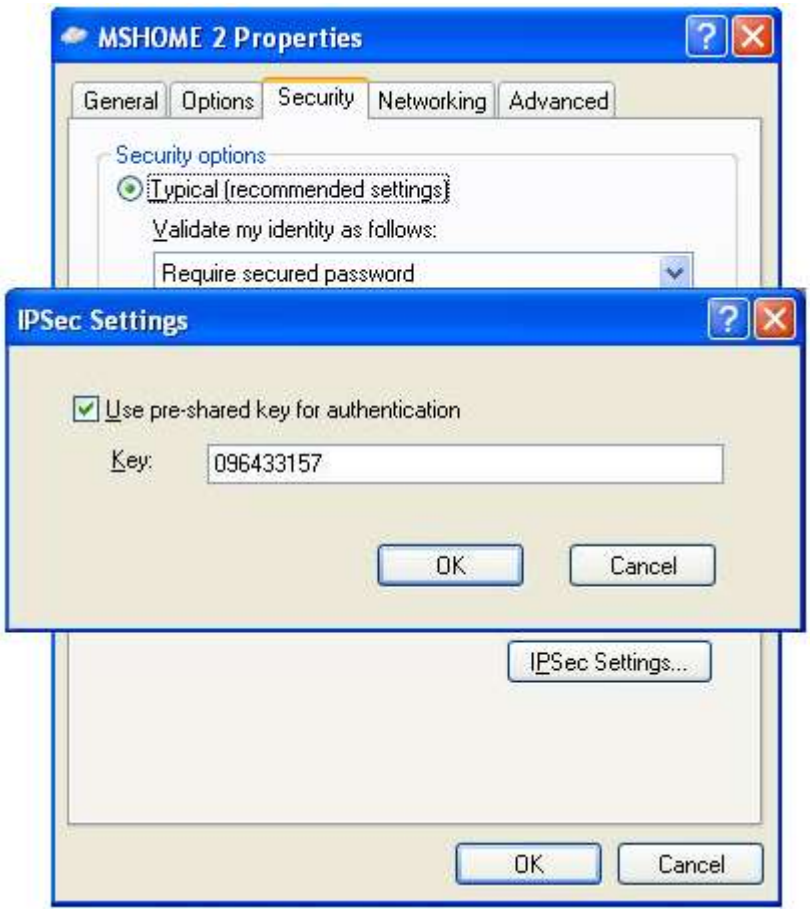

Figure (3) Pre shared key of IPSec.

Two types of networks can be used for implementing the virtual private network:

1. Internet: is widely used for this application. Therefore when implement VPN; the real IP (internet protocol) is used to establish the connection between server and clients. All clients was used the real IP to establish connection with the server and used class A to give IP address for each client.

2. Wireless network: New wireless enhanced network architecture was built for obtaining a large and secret network for this application comparing with traditional wireless network and MAN (Metropolitan Area Network). This type of network was classified within Intranet. The proposed architecture as shown in Fig. (4) which consist of four power nano stations (5GHz) , these power nano stations configured as follow:
   - First power nano station configured as Access point (AP).
   - Second power nano station configured as Station.
   - Third power nano station configured as Access Point (AP).
   - Fourth power nano station configured as Station.

These power nano stations used to build network which establish the monitoring and data transfer operation for any node. Therefore, each access point and station completes a separate network and achieving the routing path between networks through router device.

The router was configured to ensure the gateway for each network, and each computer installed with IP address. These IP address was selected within class C which can be obtain a maximum 254 computers for each network instead of the IP address within class A to avoid the interfusion.

For server: IP= 192.168.11.1 } Net1 Mask Net=255.255.255.0

For client1: IP=192.168.12.10 } Net 2 Mask Net=255.255.255.0

For client2: IP=192.168.12.11 Mask Net=255.255.255.0

(And follow for the rest clients).

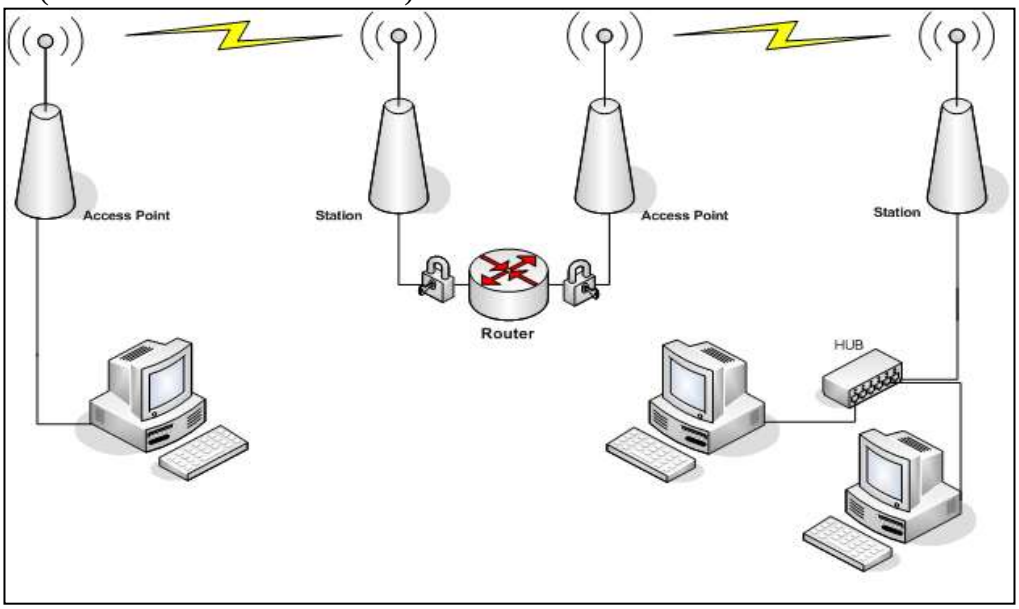

Figure (4) the proposed wireless network architecture.

NETWORK SOCKET PROGRAMMING

A network socket is an end point of an inter-process communication flow across a computer network. The communication between computers is based on the Internet Protocol (IP). The socket must build in each computer in network (server and clients) to allow application programs to use network for control and data transfer. The socket address is the combinations of an IP address and port number to initialize the physical connection [10]. The port no. (1000) was selected for clients and server to establish the connection between them. The socket connection for server and clients was illustrated in Figure (5).

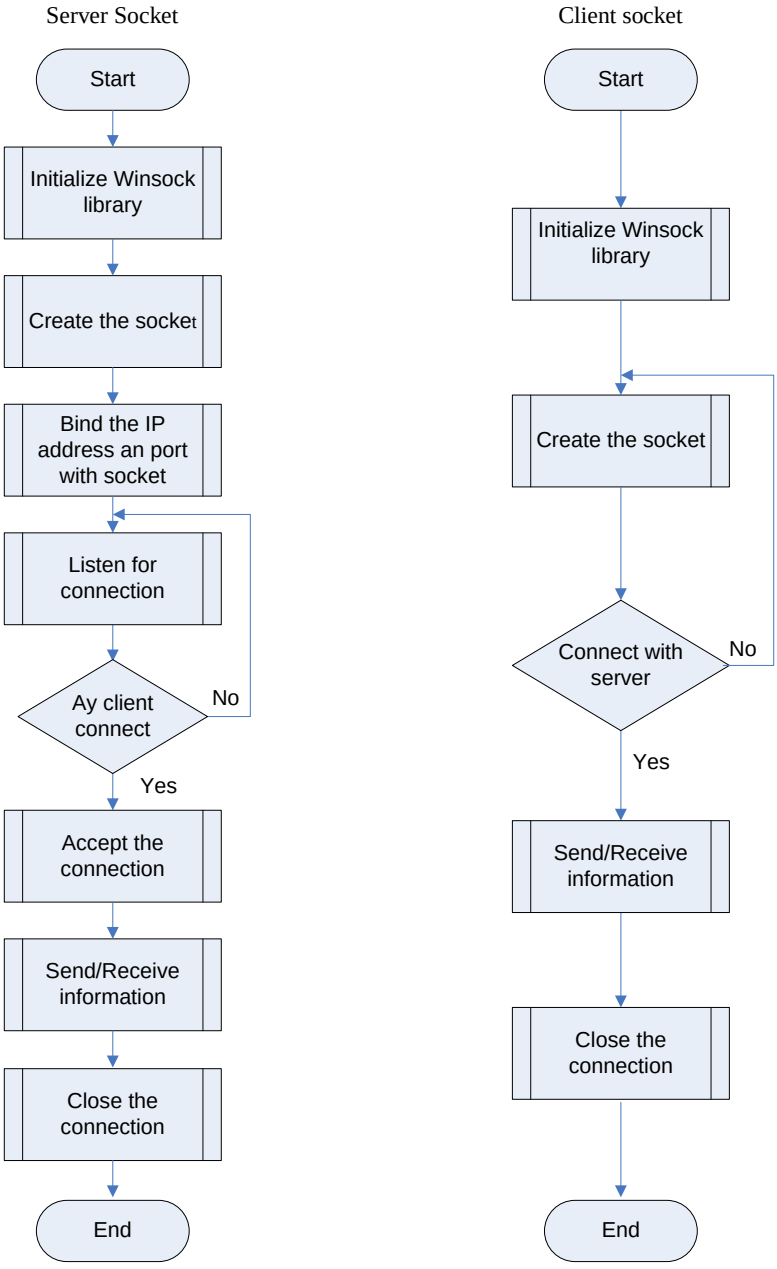

Figure (5) Flowchart for server and client socket connection.

DESIGN THE INTERFACE CIRCUIT

The interface circuit was used to make communication between client and devices to control it. The RS232 serial interface was employed for making the interface which was a bidirectional asynchronous serial communication interface for distance about 20 m. The RS232 is 9 pin D-type male connector. The function of each pin and its location was illustrated in Table (1) [11].

Table (1) Function of RS232 pins [11]

Pin	Bit	Function
1	DCD	Data Carrier Detect
2	RD	Receive Data
3	TD	Transmit Data
4	DTR	Data Terminal Ready
5	GND	Ground
6	DSR	Data set Ready
7	RTS	Request to send
8	CTS	Clear to Send
9	RI	Request indicator

The client connects with the devices through serial interface. Figure (6) shows the serial interface built as hardware part which consists of:

- Max238
- UART
- CD4060

The RS232 interface was dealing with (-10V) for logic (0) and (10V) for logic (1) comparing with driver circuits for devices interface which was dealing with TTL voltage as (0V) for logic (0) and (+5V) for logic (1). Therefore, Max238 (IC) was used for converting the RS232 voltage to TTL voltage and vice versa [11].

The Universal Asynchronous Receiver/Transmitter (UART) was used for expanding RS232 port to 8 bit for input and output instead of one bit for transmitting (TD) and one bit for receiving data (RD) and other handshake bits [11].

The clock input to the UART is generated by a circuit using CD4060 and a 2.4575MHz crystal for giving a baud rate about 9600.

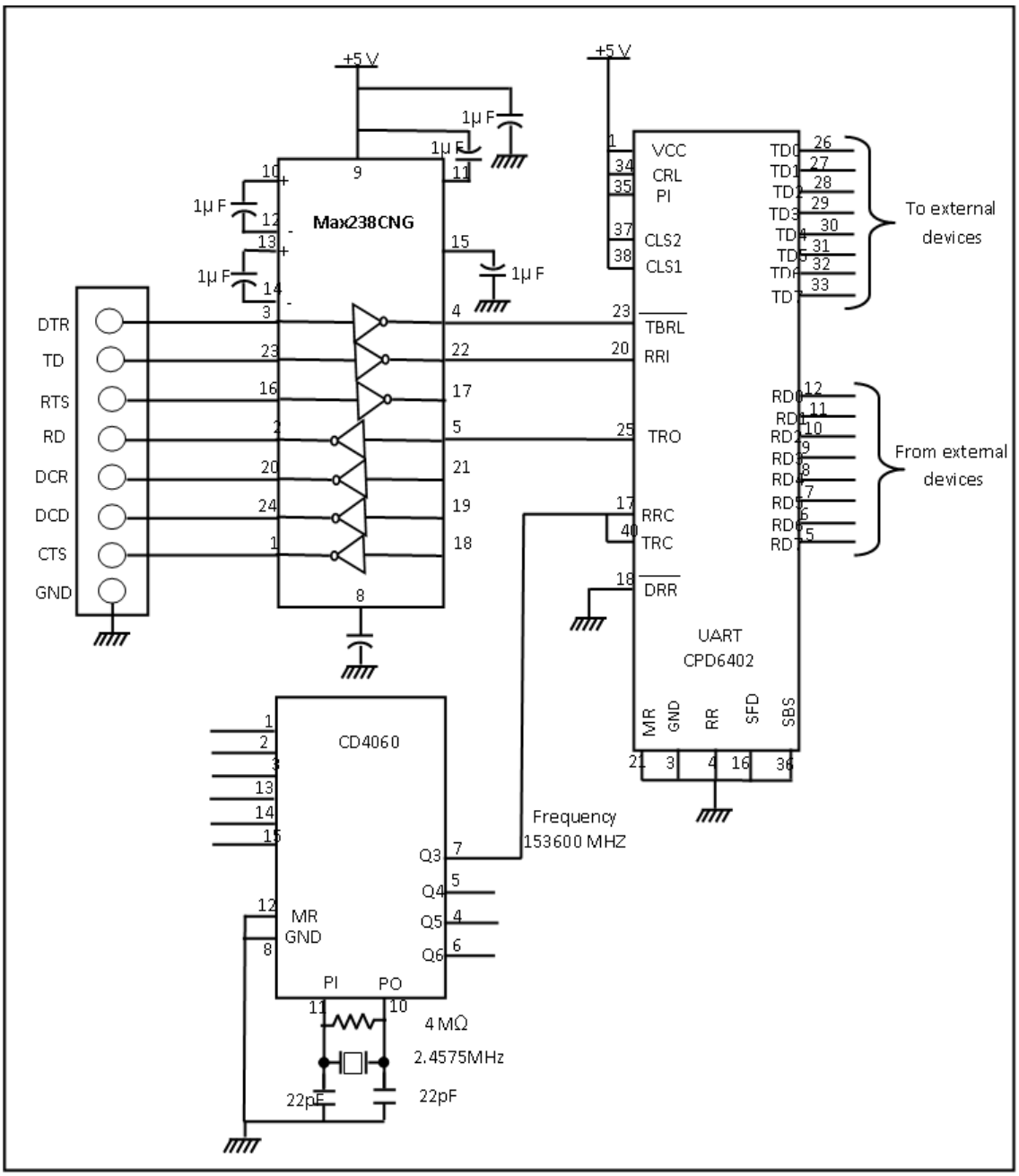

Figure (6) the schematic circuit for serial interface.

The 8 pins output of UART are TTL levels outputs. This namely, it put output 0 to 0.8 DC voltage logically 0, and 2.4 to 5 DC voltage logically 1. According to this behavior the output of UART can produce 256 different control signals (after connected it with decoder). Each external pin connected with driver circuit which consists of (D flip flop, transistor switch BC108 and Relay 24 volt) as shown in Figure (7).

The controlling operation was achieved through sending a message which contains the number of pins according to the selected device from the server to the selected client.

The client analyzes the received message, and then sends the number of pin to port (3F8 h) to switch on or off the selected devices. For example, if want to set pins (TD0) & (TD1) to logic 1. Therefore, the output value must be 1+2=3 and use (OUT &3F8, 3) command.

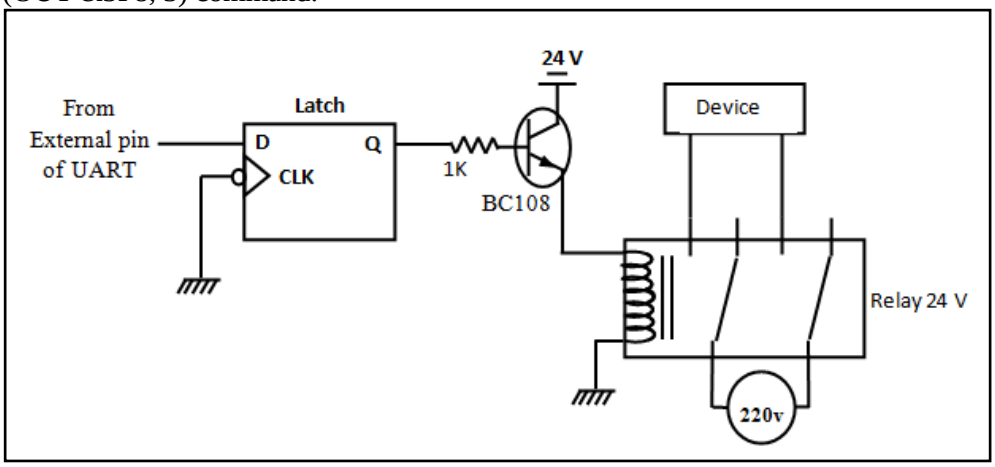

Figure (7) The driver circuit.

MONITORING OF THE SYSTEM

The operation of monitoring was accomplished through executing two functions:

- File transfer between clients and server.
- Monitoring the status of client.

1. The mechanism of transfer file (text, image) from server to client and vice versa was achieved after specify the file name through (Free file) command for searching in hard disk. The binary form one of the types for dealing with files as binary. Therefore a binary command used to convert the file to binary and save it in variable (s), it is necessary to measure the length of file (LOF command), then divide the file which stored in variable (s) to frames depended on the length of file using (space (LOF(s))/ size) command. The size depend on frame size which about 4K byte.

   After specify the number of frame, the command (SendData.wsk) used for sending the frames through Winsock.

   Before the frames transmit, the transmitter (server or client) send a message contain the name of file without the extension of it.

When the receiver computer receive a message, open a new file and using command (Put(s)) to save the frames progressively and then save the file in default folder (C:\\ my folder).

2. Monitoring the status of client was accomplished through capture the image of desktop for client repeatedly and sends it to server.

   When, the server send a message to client for monitoring it, the client capture the desktop image (25 images per second) by using (Keybad_event) command and timer. The timer contain interval (1000 part per 1second). Therefore, when need to send 25 image for 1 second, the interval must be (1000/25=40). This lead to send 25 images for desktop to the server at 1 second. When the (Keybad_event) command execute, the image will be save it, and put in frame then send it to the server.

   The 25 images were selected per 1 sec. because the movie was appearing about 25Frm/s.

   At the server computer, it loads the picture using (Load Picture) command and views it in (View Box).

IMPLEMENTATION OF THE PROPOSED SYSTEM

The implementation of the control and monitoring system was achieved using visual basic language (Ver.6) and depending on the VPN. The system consist of three clients will be connected with the server for testing. When the client1 connect with server, the status will be change to connect as shown in Figure (8).

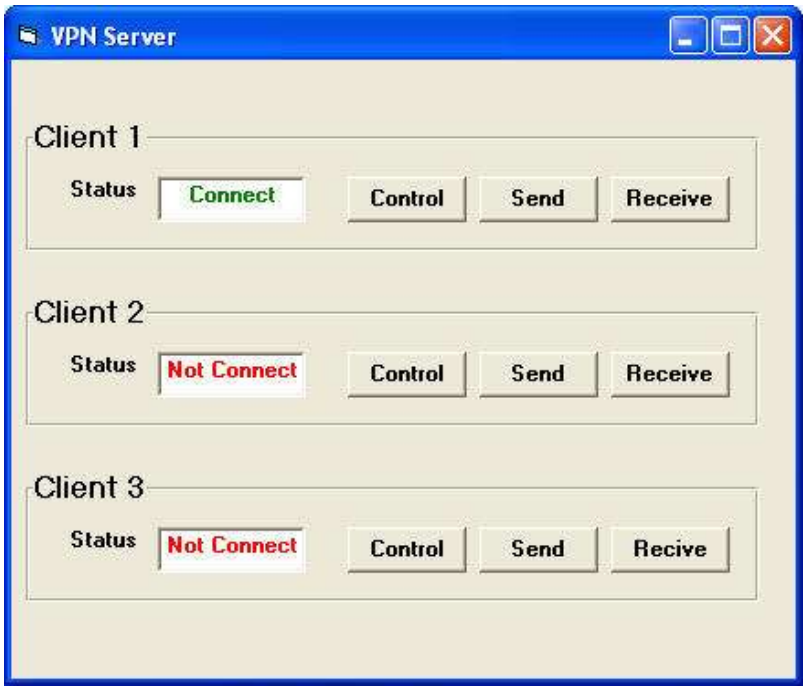

Figure (8) GUI for server.

The server can be control the devices which inherent with client. Therefore, when press on the control command for client1 a new GUI window is appear to select the device as shown in Figure (9).

When, selecting device1 check box, the server will send a message contain number (1) to the client1. The client1 will analyze the received message and change the status of device to switch ON for completing the matching status between server and client1 as shown in Figure (10).

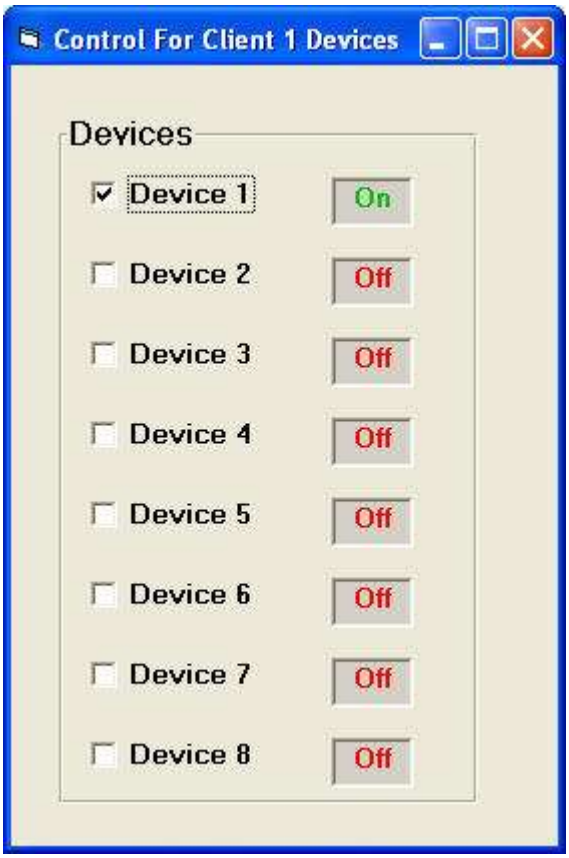

Figure (9) GUI for client1 control in server.

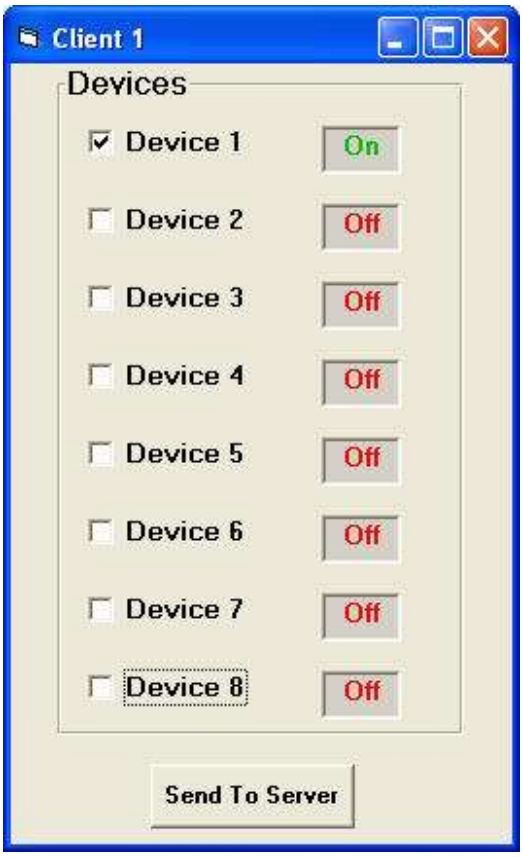

Figure (10) GUI for client1.

At least 8 devices can be connected with serial interface of each client. For example, alight is connected with client1. Therefore, when select the device 1 on the control command, the light became turn on as shown in Figure (11).

The operation of sending file from server to any client was accomplished through specify the client and then press the send command to write the name and type of file such as image in the path window as shown in Figure (12).

The sending of file was depending on the mechanism for converting it to the binary form after searching it in the hard disk to load it.

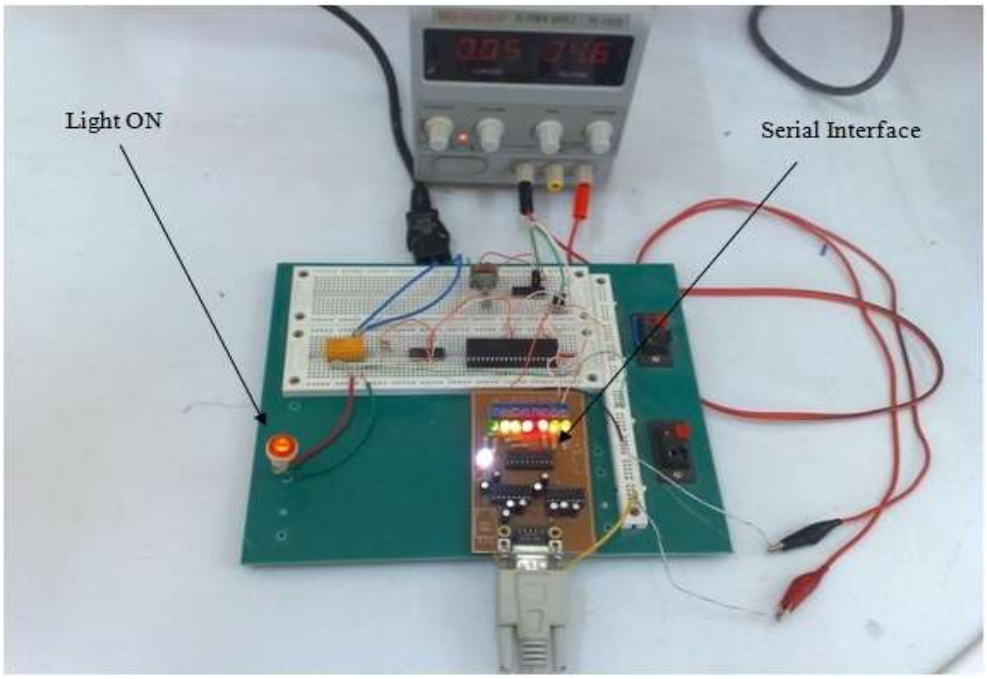

Figure (11) Overall control system and light on.

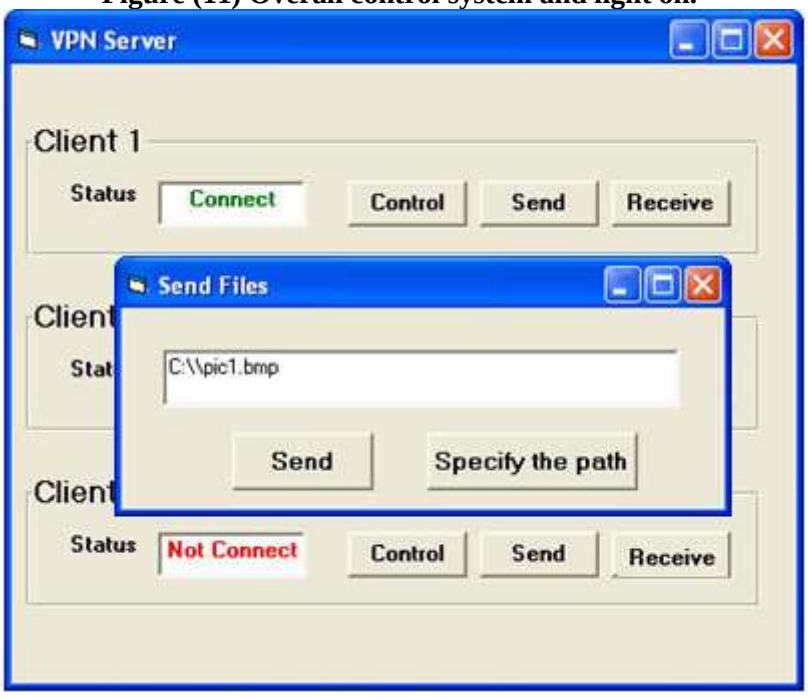

Figure (12) The file path.

Figure (13) will appear after pressing the receive command, which is illustrate the state of client1 through sending the picture of desktop with file to the server about 25 pictures at 1 sec. for monitoring the status of it and depended on the mechanism of monitoring.

Figure (13) the status of client.

CONCLUSIONS

1. Wireless VPN is secret network more than traditional network according to use tunnel protocol and using user name and password for each client computer in addition to less cost than internet because don't use real IP.
2. VPN was achieved within routing network. Therefore, don't implement the VPN within local network.
3. The serial interface can be transfer data up to 20m and controlling up to 256 devices which inherent for each client.
4. DDR pin(18) in UART must connected with logic (0) to continue receive data from serial port, and the DTR continuous change from (high to low to high) for outputting data.
5. The baud rate of serial transfer was depending on CD4060 IC and the size of file limited the no. of frames which send between server and clients.
6. The file sending operation from node to another node is very complex. Therefore, the file must convert to binary form and dividing it into frames for facilitating sending it.
7. The number of frames which was divided from the file (e.g. image) through the programming depended on the size of file and frame together.
8. The network load can be reducing it through minimizing the size of frame.

REFRENCES

[1].Kosta Y., Dalal U. and Jha R., "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)", International Conference on Recent Trends in Information, Telecommunication and Computing, IEEE, 2010.

[2].Eason G., Kebreua V., Constantinescu B. and Pierre S., "A New Security Approach for WLAN" pp. 1801-1804, May 2006.

[3].Wu J. "Implementation of Virtual Private Network based on IPSec Protocol", ETP International Conference on Future Computer and Communication, IEEE, 2009.

[4].SUN S. "The advantages and Implementation of SSL VPN", IEEE, 2011.

[5].Jaha A., Shatwan F. and Ashibani M., "Proper Virtual Private Network (VPN) Solution", The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, IEEE, 2008.

[6].Artail H. "A Distributed System of Network-Enabled Microcontrollers for Controlling and Monitoring Home Devices", IEEE, 2002.

[7].Yongliang Z., Yong X., Jun X. and Jiang Z., "Design of Remote Monitoring and Controlling System for Unattended Machine Room", Fourth International Conference on Intelligent Computation Technology and Automation, IEEE, 2011.

[8].Wijetunge S., Witetunge U., Peiris G. and Samarasinghe A., "Design and Implementation of Bluetooth based General Purpose Controlling Module", IEEE, 2008.

[9].Riehard D., "Fully configured of Cisco VPN", Beijing: Posts & Telecom Press, 2007.

[10].Wang Y., Xing Y., "Transition of Socket applications from IPv4 to IPv6", 2nd International Conference on Computer Engineering and Technology, IEEE, Vol. 6, PP. 75-78, 2010.

[11].An P., PC Interfacing using Centronic, RS232 and Game ports, Newness, 1998.