

**Design and Implementation of Distributed Real-time Security System
via Mobile Technology**

Dhuha Basheer Abdullah

Prof.dhuha_basheer@uomosul.edu.iq

Wael W. Mahmood

College of Computer Sciences and Mathematics

University of Mosul, Mosul, Iraq

Received on: 08/01/2012

Accepted on: 19/04/2012

ABSTRACT

In this paper, a distributed real time security system for monitoring and remote control on building and protecting it from unauthorized entering is designed and implemented. This system is based on the transfer of signal in real time when there is a breach and image of an unauthorized person to enter the building to the mobile phone of the person who is responsible for the security of the building.

The real time system consists of three main parts, the first one is the computer with an electronic circuit connected via the serial port. The designed electronic circuit contains the Microcontroller for reading sensors connected to ports of the building (G1, G2, and G3) and processing the signals. Also, there is a monitoring camera to capture an image when registering a case of breach. The program in the computer receives signals from the three ports and uses a fixed real time algorithm for scheduling signals and gives them priorities according to the importance of ports, then sends signals to the second part of the system. The second part of the system consists of a server on the Internet which receives signal and image of the breach, stores it in a database system and then transferring it in real time to the third part. The third part consists of several mobile phones to achieve the principle of distribution for this system, each mobile phone will be responsible for a single port in the building, while there is one mobile phone responsible for all ports which belongs to the person who is responsible for the building security. Each mobile phone contains three programs, the first program would receive a signal of the breach and give the alarm, the second program displays picture, and the third program sends a control signal.

Keywords: Real Time, monitoring, microcontroller, GPRS, Scheduling, Multithreading, security.

تصميم وتنفيذ نظام زمن حقيقي موزع امني باستخدام تقنية الهاتف النقال

وائل محمود

ضحى بشير عبد الله

كلية علوم الحاسوب والرياضيات، جامعة الموصل

تاريخ قبول البحث: 2012\04\19

تاريخ استلام البحث: 2012\01\08

المخلص

تم في هذا البحث تصميم وتنفيذ نظام امني للمراقبة والسيطرة عن بعد على بناية وحمايتها من الدخول غير المخول، يعتمد هذا النظام على نقل إشارة عند حصول حالة خرق وصورة للشخص غير المخول من الدخول إلى البناية للهاتف المحمول للشخص المسؤول عن أمن البناية.

تتألف منظومة المراقبة والسيطرة من ثلاثة أجزاء رئيسية، يؤدي كل جزء من هذه الأجزاء مهمة معينة، إذ يتألف الجزء الأول منها من جهاز حاسوب مع دائرة إلكترونية تربط عن طريق المنفذ التسلسلي مع جهاز الحاسوب، وتم تصميم الدائرة الإلكترونية بحيث تحتوي على المتحكم المصغر (Microcontroller) لغرض قراءة المتحسسات التي تربط على منافذ المبنى (G1, G2, G3) ومعالجة الإشارات الناتجة منها، فضلاً عن وجود كاميرا مراقبة لالتقاط صورة عند تسجيل حالة خرق. البرنامج في الحاسوب يستلم الإشارات من المنافذ الثلاثة، و يستخدم خوارزمية ثابتة للوقت الحقيقي وتجدول هذه الإشارات وتعطيها أسبقيات حسب الأهمية للمنافذ، ثم ترسل الإشارات إلى الجزء الثاني من المنظومة، أما الجزء الثاني من المنظومة فيتألف من خادم على شبكة الانترنت يحتوي على برنامجين، الأول يقوم باستلام إشارة الخرق والصورة وتخزينها في

قاعدة بيانات المنظومة والبرنامج الثاني يقوم باستلام إشارة سيطرة من الهاتف المحمول وإرساله إلى الحاسوب فضلاً عن وجود موقع الكتروني يسمح للشخص المسؤول عن أمن المبنى من الاطلاع على آخر صورة تم التقاطها من خلال اسم مستخدم وكلمة مرور، في حين يتألف الجزء الأخير من عدة هواتف محمولة لتحقيق مبدأ التوزيع (Distribution) لهذا النظام، وكل هاتف محمول يكون مسؤولاً عن منفذ واحد في المبنى، في حين هنالك هاتف محمول واحد تصله جميع حالات الخرق هذا الهاتف يعود للشخص المسؤول عن النظام الأمني. ويحتوي كل هاتف محمول على ثلاثة برامج، البرنامج الأول يقوم باستلام إشارة الخرق ويعطي جرس إنذار والبرنامج الثاني يقوم بعرض الصورة والبرنامج الثالث يقوم بإرسال إشارة سيطرة. **الكلمات المفتاحية:** الزمن الحقيقي، المراقبة، متحكم مصغر، الجدولة، متعدد المسالك، أمني

1. Introduction

The applications of real-time provide reaction or response to an external event in a predictable way of its delaying time. The applications of real-time need a high speed computing power, and cover a wide range of tasks with different reliability of time [1 and 8]. The real time applications may have many properties, in some cases it is possible to have some of the strict and critical tasks that must be carried out within its time boundaries, others require a large input and output of data [6]. Some of the tasks can be run out with lower priority or without the need for the concept of time in general. The successful implementation of real-time application lies in the ability of the programmer to determine the application requirements at every stage of the program's progress very carefully. Some of the resources and the importance of real-time are only used when they are needed so that the application does not become exaggerated [11].

The idea of wireless communication means never use "wire" and provides various communication services to users everywhere: at home, in the car, plane, ship, institutions and at the universities ... etc. On the other hand, providing the same services and features offered by telecommunications, For example, the wired computer networks is used such as (LANs) and (MANs) and (WANs) and then the wireless networks came (WLANs), which are commercially known as Wi-Fi (WiFi) and then (WiMax) came [9].

The wireless communications are classified into directed and in-directed communication.

- 1 – The directed radio communications use a directed antenna for example the mobile phone network, and the use of these antennas have many benefits.
- 2 – The In-directed telecommunications, for example, the Ollvizione broadcasting and broadcast where there is one central tower in the city broadcasting a signal in all regions and in a high ability for comprehensive coverage of the city.

The communication with Internet in a wireless way via mobile phone is considered one of the greatest technical innovations [3], which makes it possible to access the Internet and takes advantage of all its services via mobile phones and laptops. Wireless communication is an old idea started with Morris signals, however, these signals were often lost in wave disturbances and the obstruction primary for using wireless communication to connect with Internet is the high cost of communication and the slow speed of data transfer which contains mostly texts, images, audio and video clips [2].

Mobile phone can be used in several ranges in which the person who is in somewhere can get a warning message from the mobile phone to inform him about, for example, a slump in the shares, prices of a particular company that gives instructions for the device to enter to the Finance affairs who shall mobile phone instantly open the Web site to deal with stocks on the Web and then sell some or all of the shares to reduce the value of the loss, or ask the person from the mobile phone service booking airline tickets and who buys a ticket to travel to a specific region, or ask the person from the

mobile phone to guide him to the nearest coffee shop to sit until the date of travel, before heading to the airport.

There are many buildings vulnerable to looting and theft during the absence of security officials on them without the ability to detect criminals and thwart their attempts and there are also many shortcomings in the existing regimes to resist the robbers, especially those experienced or in the weakness of the used systems and their inability to overcome all the means that can be used by thieves, especially those with skills, so this system takes into account all the things that provide the greatest possible protection against this common threat, especially in our local difficult environment.

1.1 Related Works

Thesis submitted by (Jean-Paul Kouma) at the Umea University in 2006 represents the real implementation of protection systems that rely on the principle of real-time by knowing of recognized faces. System has a set of cameras placed at certain strategic points in the home such as the door or window, etc., the goal of the system is to detect intruders via the image that will be picked up at the moment of penetration and then sent it to the user via the multimedia service in the mobilephone.[7]

The researcher (Kamil Cetin) in 2006 at the Dokuz Eylul University Section Electronics engineering / Izmir / Turkey, designed an intelligent system controls home through phone lines. This system contains control panel and sensors. The circuit of the (Microcontroller) controls the electric devices and observations received from home, the telephone lines were used because of their presence in almost every house from which data is send and received. [4]

The researcher (Ibrahim Geha) in 2007 [5]at the American University / Beirut, designed a system to monitor and address any of emergency situation, in this system, cameras are linked with essential programs via the serial communication protocol. The system contains a program for detecting faces that work automatically in emergency situations. The system contains three key features to ensure the protection of the building or home:

- 1 – The detected device of thumbprint to make sure the persons authorized to enter.
- 2 - Thermal and electrical sensors.
- 3 - A program that is used to monitor as interface for the user.

A group of researchers (Malik Sikandar Hayat Khiyal) and others in 2009, designed a system focuses mainly to control the applications in home remotely to protect home when the persons are outside home. The system relies on a mobile phone and SMS service, this system uses wireless technology and it is also used to solve the problems faced by homeowners in their daily lives, the system is used to protect home from unauthorized entering and to control other applications within home by using the SMS service via a GSM technology. [10]

1.2 Contributions

This paper presents some of the contributions which are:

- 1- Design and implementation of the Interfacing between the computer and optical sensor via design and building an electronic circuit containing a Microcontroller to transmit signals and processing them from sensors to the computer.
- 2- Design software in the computer to control the Interfacing containing the Microcontroller and storage the case of breach, and transmit the signal to the Web Site within a GSM network in accordance with the principle of real time.
- 3- Development of real-time algorithm to transmit the signal and determine the importance of the port according to the supported priorities.

- 4- Use of the (GSM) and Global Packet Radio System (GPRS) service, to transfer the signal of the breach from the website to a group of mobile phones and the achievement of the principle of distribution via designing embedded programs in these mobile phones for this purpose.

2. System Outlines

In this work, a distributed real-time security system by using a mobile technology is designed and called as (Distributed Real-time Security System "DRTSS"); this paper discusses the detailed work of the distributed real-time security system from the moment when the breach occurs until the arrival of a signal to the mobile phones of the persons responsible for the security of the building. When a case of breach is recorded, the port in which the breach occurred is specified to give a signal to the person responsible for it, and there is one mobile phone had received all the records signal of the breach. This power is given to the person responsible for the security of the building as a whole, the basic units of the system illustrated in Figure (1).

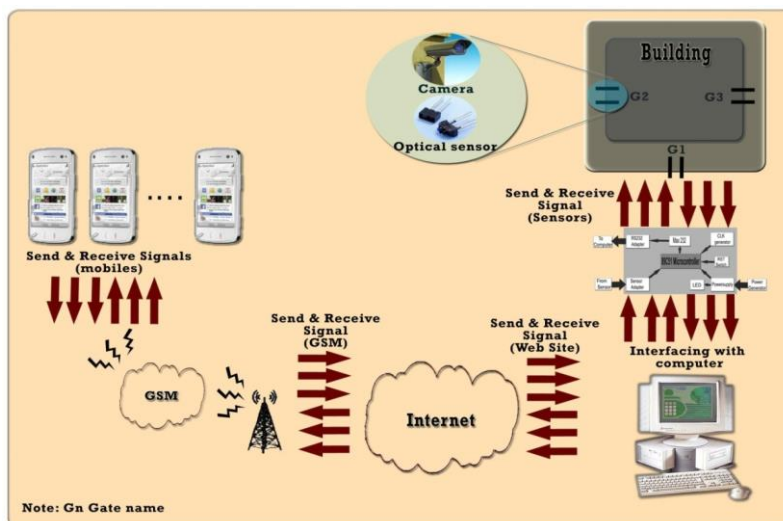


Figure (1) Units of a DRTSS System.

Figure (1) illustrates the basic units to design a distributed real-time security system via mobile technology. The work of the system is based on the presence of peripheral sensors that may be optical or kinetic or thermal ... etc.(in this work, Optical sensor had been used). Figure (1) details the work of the system from the moment of the breach until the arrival of the signal to the mobile phones and it also represents the shares that are in the opposite direction, the ability of the person responsible for a port in the building to send a control signal to take a particular procedure (for example, close a door or a window) after a case of breach. It can also be noted that each port is indicated by encoded as (Gn), where (n) represents the sequence in the port building. The interface with the computer enables the user of the distributed real-time security system to use eight or more ports when using the (Multiplexer).

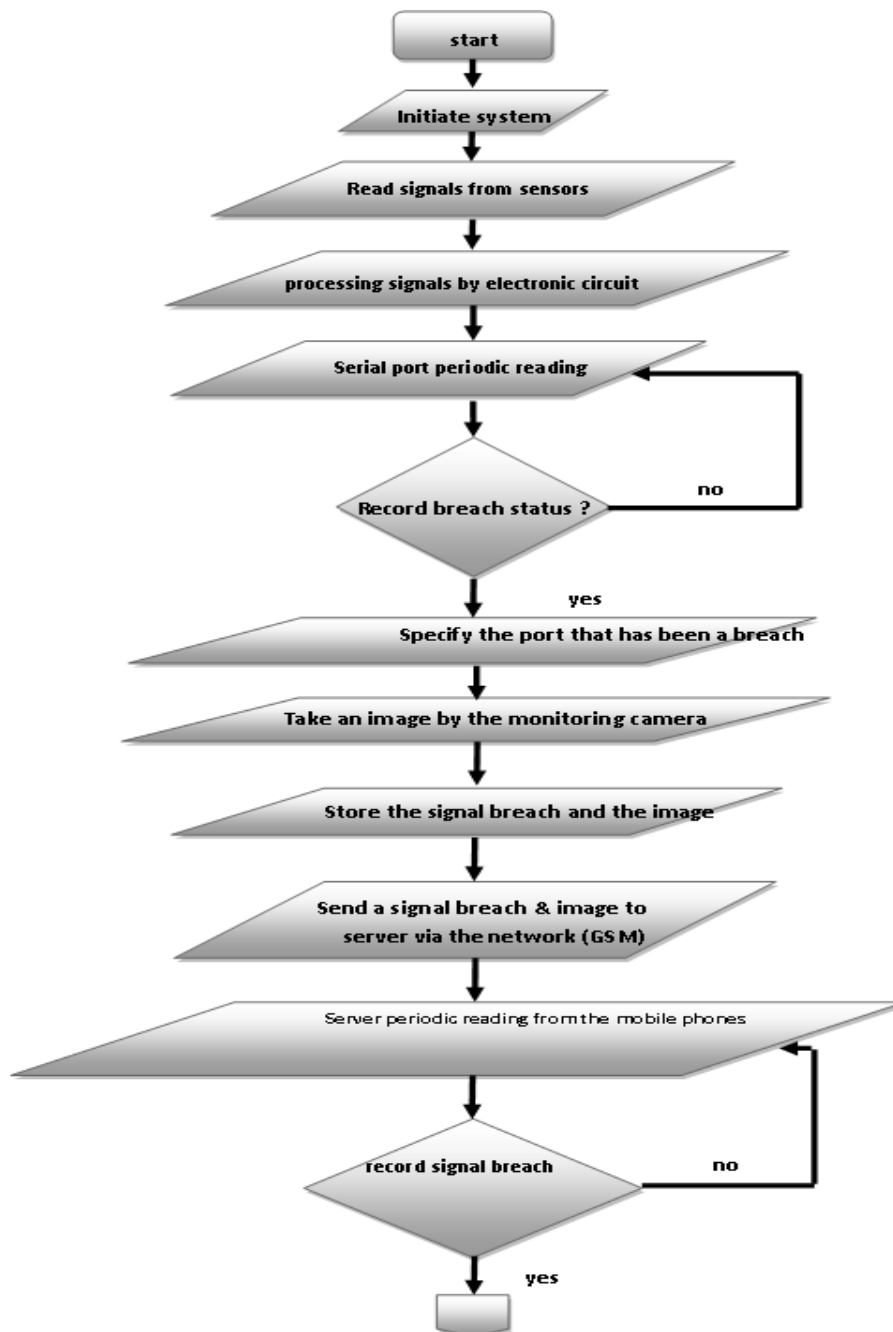
This system also contains a computer to store and send the signal when the breach occurs to the server that is considered as an intermediate part until the arrival of the person responsible for the port where the breach is occurred, the work of a distributed real-time security system can be illustrated in diagram (1).

3. General Structure of DRTSS

The distributed real-time security system consists of several units, or parts work in linkage and flowing with each other to achieve the idea of working, and here is an explanation for each unit.

3.1 Interfacing

The interface which contains a microcontroller to process signals works as a link between sensors and computer. To link several sensors with serial port, we use the Microcontroller because of the absence of serial ports to connect more than two or three sensors to the computer at one time.



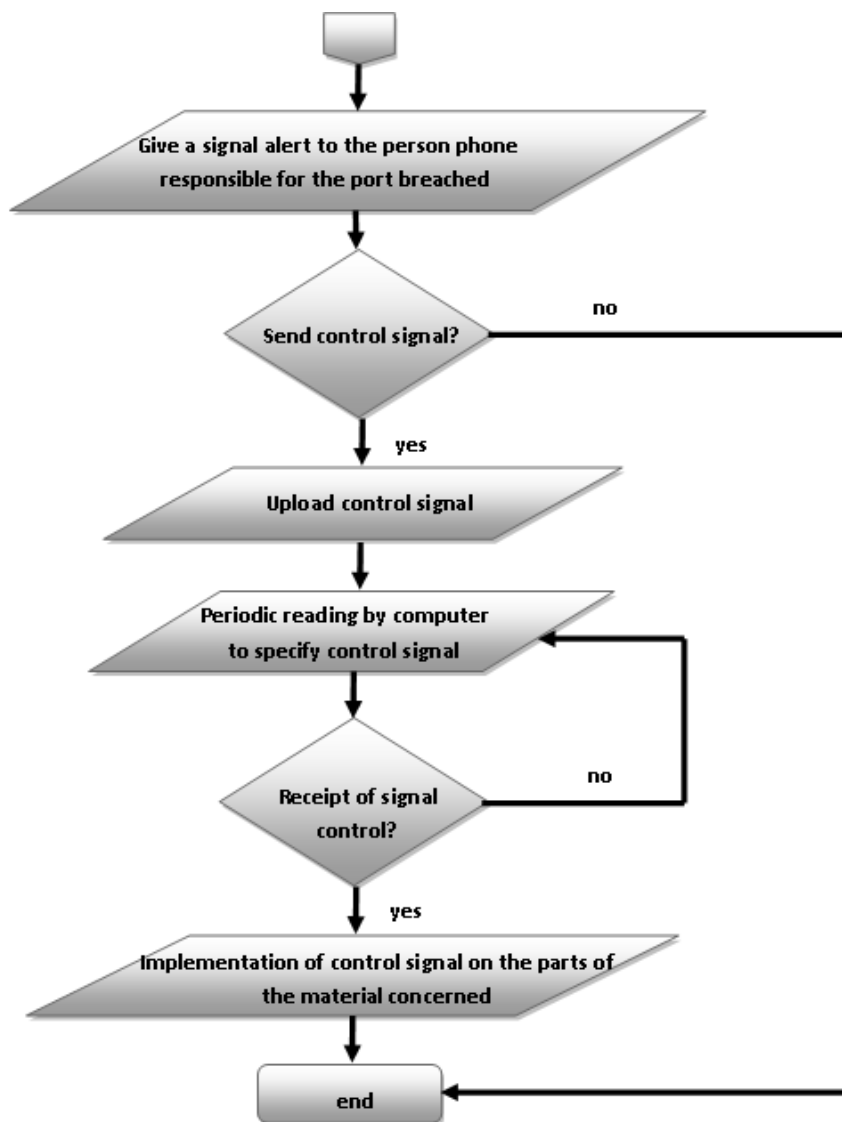


Diagram (1) Distributed Real-time Security System Work

3.1.A Design of Electronic Circuit Used as an Interface

An electronic circuit was designed in order to read value of more than one sensor and to send the data to the computer via the serial port by using the Microcontroller 89C51. The program projected on the microcontroller is designed for the continuous reading from the sensors (three sensors are used in this system to read the signals from three ports (G1, G2, and G3)) and converted it into one signal to be sent to the computer via the serial port, the signals stream from the sensors to the computer is shown in Figure (2), and Figure(3) shows the core units of the electronic circuit designed as an interfacing.

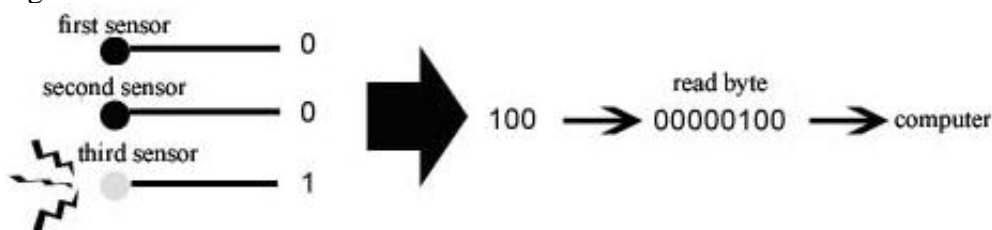


Figure (2) : Signals Stream from the Sensors to the Computer

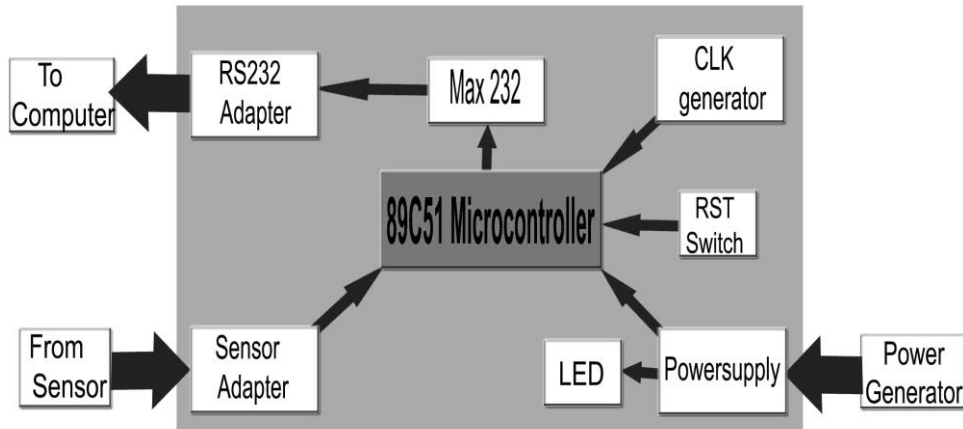


Figure (3): The Core Units of the Designed Electronic Circuit (Interfacing)

The work of microcontroller is to give each sensor (1 bit), setting the bit when the sensor senses signal, and the (0) value when the sensor is not sensing. Then, the readings had been collected and placed in a single byte and sent to the computer via the serial port. Figure (4) shows the waveform that is expected to read (1 byte), and the values of start and stop bit represent the beginning of transmission and the end of the transmission of each byte. The direction of transmission begins with (Least Significant Bit).

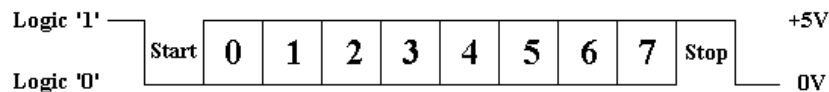


Figure (4) Serial Port Reading

3.1.B Interfacing Units

1. Integrated circuit (MAX 232)

The signal resulted from the microcontroller needs to transform operation to higher voltage (5 volts). The voltage required to deal with (RS-232) is (10 volts), therefore we use the integrated circuit (MAX 232) for the conversion of (5 volts) to (10 volts).

2. Serial port adapter (RS-232)

The serial port adapter is used for linking the designed electronic circuit to computer via (Com-to-Com) cable.

3. Sensors adapter

The designed circuit for connecting eight different sensors can be distributed to multiple ports in the building. The eight sensors have been replaced by eight keys (Dip Switch) each one represents a separate sensor, for the purpose of ease of application.

4. Pulse generator (CLK Generator)

In the circuit of pulse generator related to microcontroller, a Crystal with a particular frequency is used (11.0592 MHZ) and this frequency is the only one that can be obtained at a frequency of sending and receiving (Baud Rate) compatible with the standard specifications of the serial port.

5. Reset circuit (RST Circuit)

The circuit of zeroing is used to restart the Microcontroller.

6. Power Supply

The electronic circuit is supplied with a capacity equal (5 volts), via the use of capacity emerging from the port (USB).

7. Microcontroller

An integrated electronic chip to a large degree of complexity was developed, so it was obtained the so-called microcontroller which is an integrated electronic chip useless without a program stored in its memory in order to read it and the implementation of its instructions, respectively. So there is an integrated electronic chip called the Microcontrollers that contain all that is needed by mini-controller to work in reliability higher, and microcontroller takes more than a form or type, depending on the number of Pins and the company manufactured it.

In this type of microcontroller, there is no need to define the function of each pole of the poles of the window which is already in use whether it is input or output but the process of writing is directly done to the pole of this window and also the process of reading might be done from this pole after the implementation of the instruction of the writing to it, but we should pay attention that the time of scanning program is very fast (less than (1 ms) for a program of 1000 instructions) the pole must be given the pole time to settle the case of the output before its use as an input again (this is possible when we use it as output and input together), otherwise, there will be an error in reading the pole in order to read the value that was previously entered.

3.1.C Streamline the work of the electronic circuit

Figure (5) shows the overall design of the Electronic circuit required to read more than one sensor at a time where the sensors are linked via the port (P2) for the microcontroller, and as mentioned before, eight sensors can be linked via the Serial Port at the same time. Capacitors size (10µf) were used, diagram (2) shows the data stream in the program projected on the microcontroller.

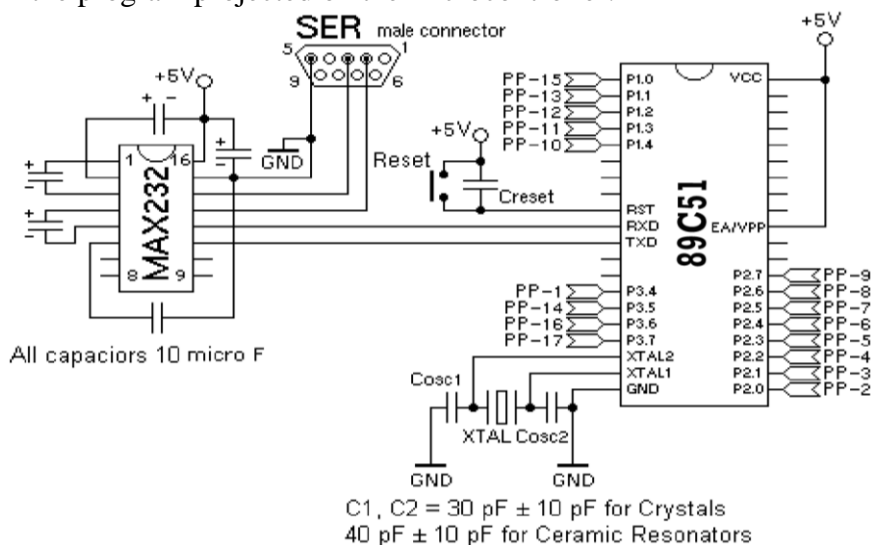


Figure (5) Design of the Electronic Circuit

3.2 Computer

Computer side contains a program that works automatically in the case of unauthorized entering. The computer controls the data that is read from the serial port, as well as controlling the camera linked over the (USB) port. When the disclosure of the case of unauthorized entry, the program stores the image (Algorithm (1)) and the time and date of the breach in a database, then the program will send the breach signal and the image to a server. The work of the program on the computer is illustrated in the Algorithm (2).

The program in the computer starts to work by opening a channel of communication with the serial port, an error message is provided if it cannot provide a channel to connect to the serial port. After that, the program creates contact with the monitoring camera by sending signal to the monitoring camera to see if a monitoring camera is ready to work, otherwise it will be given a letter of no ability to create access to the camera by giving a letter for this purpose. After that, the program that depends on real time algorithm starts to work by periodically reading the data coming from the serial port to indicate the status of building ports if they are safe or to give a signal in the case of breach. In the case of a breach, the program gives an order to the monitoring camera to capture an image to determine the identity of the hacker, and then stores the time and date of the case of a breach in a database as well as to store the image.

After storing the data for the case of a breach and the image in the database, the program puts the data of breach in the file type (Text), and then upload it to the server side. Using user name and password for authorization to change the files (to add or delete) on the server-side.

Algorithm (1) image capturing from camera

Step 1: Wait signal to capturing the image.
Step 2: Specify the Frame Rate per second.
Step 3: Does the camera in standby mode? If yes go to step 4; else go to step 5.
Step 4: Capture image and save it in BMP extension, go to end.
Step 5: print Error message.
Step 6: end.

Algorithm (2) the controlling program in computer

Step 1: Open connection with serial port.
Step 2: Periodically reading from the serial port.
Step 3: If breach status is recorded, go to step 4, else go to step 2.
Step 4: Send signal to capture the image.
Step 5: Save image and the date of breach.
Step 6: Open connection with server.
Step 7: Send the breach signal and image to the server.

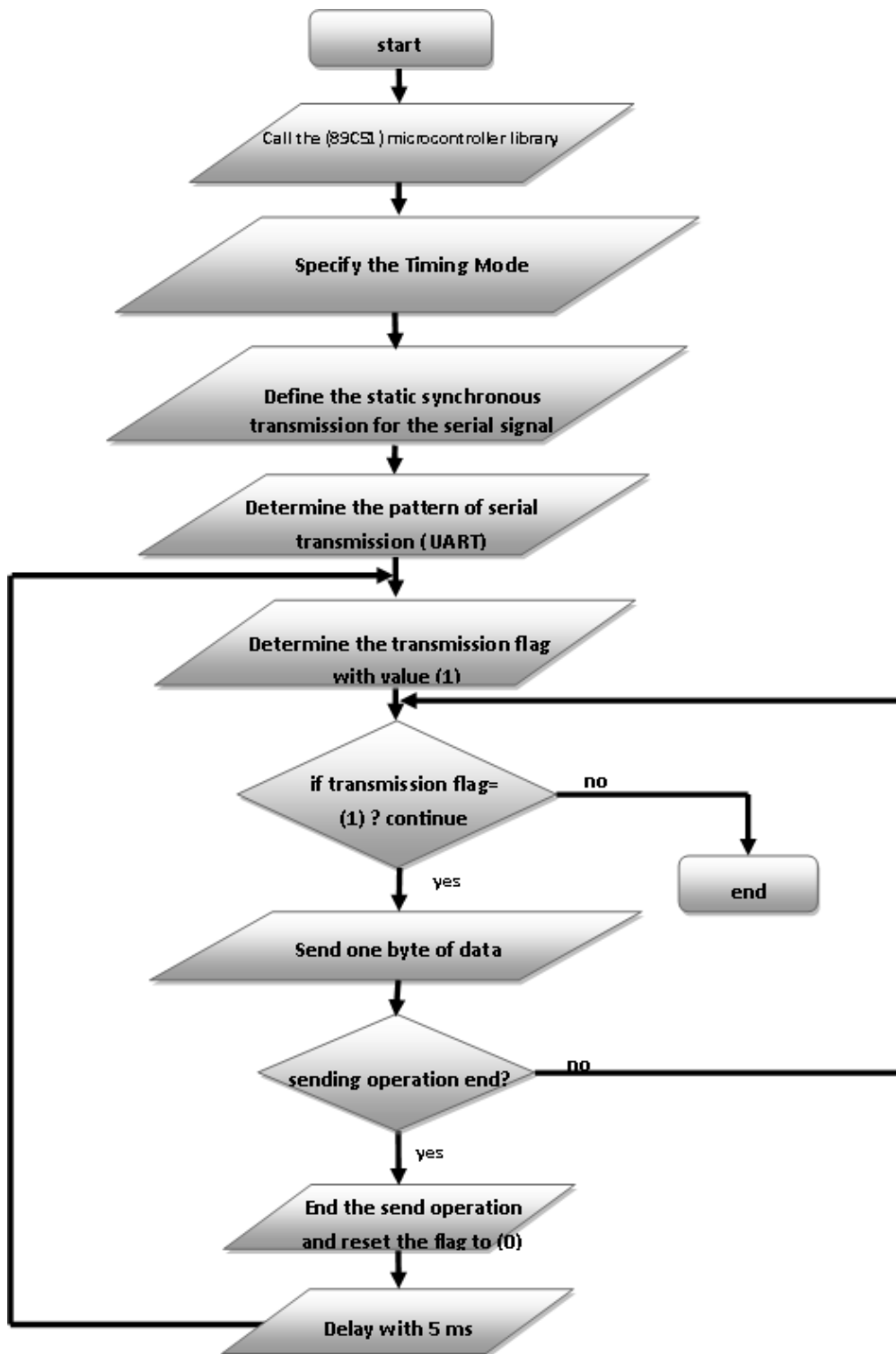


Diagram (2) Microcontroller Program

3.3 Real Time Algorithm

Values of sensors have been read from the serial port and then these values are scheduled depending on the real-time algorithm by identifying the importance of each port in the building. If the building contains three gates (G1, G2, and G3) and the gate (G1) was of a higher importance, and when if there was a breach in more than one gate at the same time, the real-time

algorithm used in this work will give a higher priority to the gate (G1). The real-time algorithm depends on Rate Monotonic (RM) policy to determine the priorities for the ports of the building and in according to the importance. The algorithm (RM) is considered (Static Algorithm) to determine the priorities, algorithm (RM) is based on the period in determining the priority, each (Job) which is periodically carried out has a higher priority over the rest of the jobs if the job has a period less than the rest of the jobs.

Algorithm (RM) is applied in the distributed real-time security system by considering each reading for the port inside the building is Job, while (Period) represents the time of the last read until getting a further reading of the same port (table 1). The time lines for scheduling these jobs (gates) are shown in Figure (6). The scheduling of sensor gates on these time lines for the designed system algorithm depends on Execution times and Periods values. The job for reading sensor gate (G1) is executed every 4ms (period = 4ms), the job for (G2) is executed every 5ms and for G3 every 20ms.

Table (1) Period and Execution Time for Building Gates

Jobs	Period	Execution time
G1	4 ms	1 ms
G2	5 ms	2 ms
G3	20 ms	5 ms

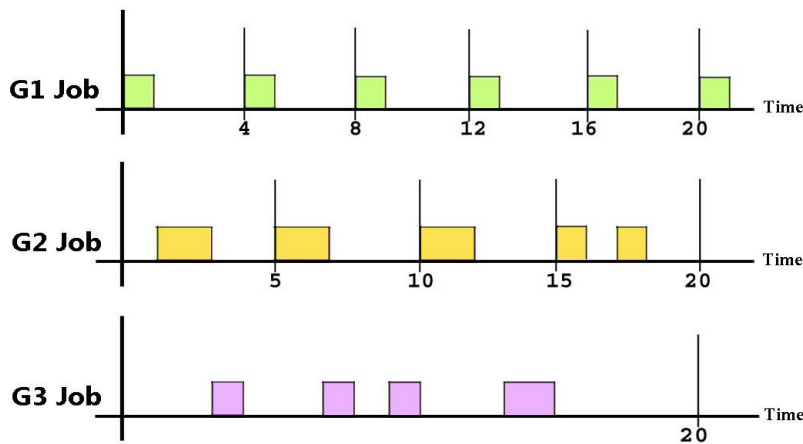


Figure (6): Time Lines for Scheduling Gates Jobs.

3.4 Web Site

After the signal of the breach is sent from the computer to the Internet, there must be a server works as (Buffer) to the signals data which is a Web site hosted at the site (Freehostia) under the name (<http://aliwael.freehostia.com>) hosting data that is sent from the computer and put it in a text file under the name (Status.txt). The website and the computer are linked by a program written in a (Perl) language and at the form (CGI Program) loaded to a server. Site design is done via the use of languages (HTML, Java Script, PHP). The function of the server is to store signals and image. The person responsible for the security of the building has property to access the site and see the latest updates by entering a user name and password, limited powers have been granted to the peoples responsible for the gates of the building and absolute

power is granted to the (building administrator security) in which he can notice the status of all the gates of the building. Program is configured by using a (Perl) language in the form (CGI Program) to coordinate the interaction between mobile phones and the server where the mobile phones read periodically the stored data in a text file under the name (Delay.txt) and give an alarm in case of an authorized entry. Figure (7) shows the strategy of public work in terms of server and its location within the distributed real-time security system.

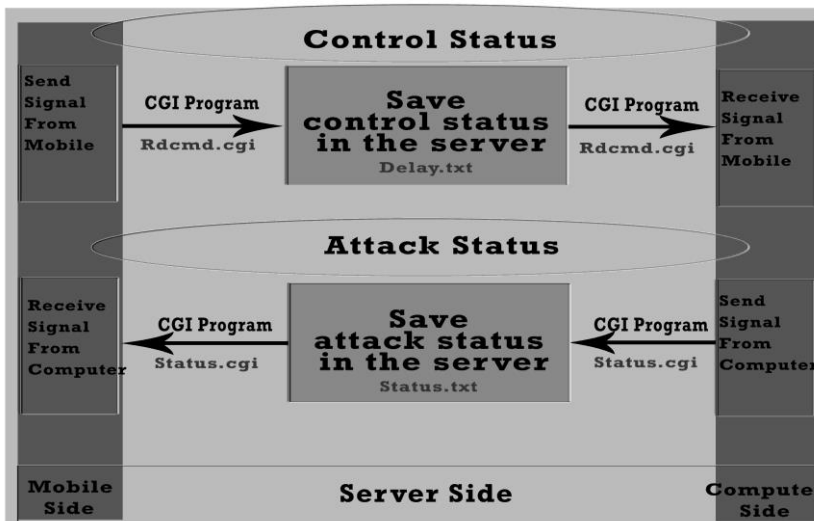


Figure (7) Business Strategy for the Server-side

3.4.A Server Program (Status.cgi)

The program has been assigned (Perl) language, it is an assistant program to open a channel of communication between the server and the computer, algorithm 3.

Algorithm (3) Status.cgi server program

- Step 1: Read a series of data sent from the computer.
- Step 2: Open the (status.txt) text file to store a breach signal.
- Step 3: write the breach signal in the text file.
- Step 4: Close the text file.
- Step 5: end.

3.4.B Server Program (Rdcmd.cgi)

It is also considered one of the assistance server software that allows the mobile phone to send a control signal to the computer after making sure that the process of breach is occurred, and the Algorithm (4) shows the work of the program.

Algorithm (4) Rdcmd.cgi server program

- Step 1: Open (delay.txt) file text.
- Step 2: Write the breach signal on the file text.
- Step 3: Close the file text.
- Step 4: end.

3.4.C Site Management Program

This program is used for managing and designing the site. The program is limited to authorized persons to enter the site and access the information on the system

by using user name and password. Each person responsible for the port inside the building is given a user name and password which made him able to follow up the case of port and see the last image is being captured, and the person responsible for the security of the building has full right of access to information for all ports of the building.

3.5 Mobile Station

A mobile phone is the end station of the distributed real-time security system, which receives the signal of the breach from the server-side and then alerts the mobile phone's owner via an alarm and displays the sequence of the port at which the breach occurred on the screen of the phone.

The principle of (Multithreading) has been adapted in the program of mobile phone, this led to the parallel and synchronization implementation. It also gave the possibility to expand the program by adding an additional thread.

3.5.A Distribution on mobile phone

The information of the ports has been distributed on more than a mobile phone where each phone receives a signal of a single port, so the principle of (Distribution) is implemented for this designed system. There is also a one mobile phone of the person responsible for the building (building security director) receives all the signals of a breach to all ports.

3.5.B Controlling from mobile phone

Using distributed real-time security system a person responsible for the security of the building and via the mobile phone can send a control signal by the server to the computer to do a particular procedure (the process of the control in the computer depends on the signal output via the serial port only for the lack of the physical equipment that can take a specific process such as locking a door or window) to keep the building and at the same time making a particular procedure until the arrival of the owners of the building or contact the emergency, and the pictures are considered as a visible evidence of the person penetrating even if he escapes. Algorithm (6) shows mobile program that performs this task. The General Packet Radio Service (GPRS) should be effective in the mobile phone and activated by selecting the access point (according to the contact company) and activate the service from the company because the process of transferring data from the Web Site is only done via the Internet connection from a mobile phone. A mobile phone for each person responsible for the port in the building consists of three programs written in Java minute (J2ME) language that is appropriate to write programs for small devices (Smart Devices). The programs are:

3.5.B.1 Mobile Phone First Program (Activate The System)

The function of this program is to activate the system via the establishment of a connection to the server. The program receives the signal of the breach from the Web site via the server software and then gives an alarm when the case of breach occurs and shows the sequence of the port on the screen and Algorithm (5) shows the structure of the first program of the mobile phone.

For establishing the connection, we have to specify the communication variable and the variable of data receipt, put the value (Null), and then specify temporary storage for incoming data and server address.

Algorithm (5) structure of first program in mobile phone

Step 1: Initial mobile screen.
Step 2: Create connection to the server (<http://aliwael.freehostia.com>).
Step 3: read the text file that contains a breach signal by contacting with (<http://aliwael.freehostia.com/status.cgi>).
Step 4: If breach status is recorded, go to step 3, else go to step 5.
Step 5: Any Exception ?, if yes go to step 2, else go to step 6.
Step 6: Close connection.
Step 7: end.

3.5.B.2 Mobile Phone Second Program (View Image)

This program is used to show an image of the hacker, and it could be used after a breach. It is optional, not compulsory for the person responsible for the port in the building. The program works by opening a channel of communication to the server and then displays the image on the screen of the mobile phone via the creation of the screen to display the image and determine the dimensions of the screen to ensure a clear view of the image. Algorithm (6) shows the structural image view in the mobile phone.

Algorithm (6) Second program to show image

Step 1: Initial the mobile screen.
Step 2: Specify screen resolution.
Step 3: Create connection and download image from (<http://aliwael.freehostia.com/pic.bmp>).
Step 4: Any Exception ?, if yes go to step 3, else go to step 5.
Step 5: Show image.
Step 6: Close connection.
Step 7: End.

3.5.B.3 Mobile Phone Third Program (Sending Control Signal)

This program is used to send control signal after a case of a breach. It is optional and not compulsory for the person responsible for the port in the building. This program works by using the assistant program (Rdcmd.cgi) for the server. This program opens the text file (Delay.txt) for the purpose of writing and specifying the type of control signal. Algorithm (7) shows the work of the third program to send a control signal.

Algorithm (7) Third program to send control signal

Step 1: Initial mobile screen.
Step 2: Create connection with (<http://aliwael.freehostia.com/rdcmd.cgi>).
Step 3: Open (delay.txt) file text to write in it.
Step 4: Any Exception ?, if yes go to step 3, else go to step 5.
Step 5: Close connection.
Step 6: End.

3.5.C Close the communication

The process of closing the communication is done in several cases, including:
i- **Causes from the software:** an exception occurs in the program, such as damage in the communication for several reasons, including weakness in the communication network or interruption of the service in the network.

ii- **Causes of hardware:** damage occurs in any of the physical parts, such as the server stops working because of a certain malfunction.

The process of closing the communication is summarized in several steps: In the beginning, the value (Null) is placed in a contact variable (c) and the variable of data receipt (is) and then the (classes) which are responsible for stopping the program of the mobile unit is called for and these classes are (Destroy (), Stop (), Pause ()) that lead to the end of the program.

The update process of the data in the mobile phone takes place only in the case when a change in values occurs, when there is a difference between reading with its predecessor, and the speed of the drawing the implementation of the program on a mobile phone depends totally on the specifications of the mobile phone and the speed of its processor.

4. System Implementation

The Software has been divided into two programs on the computer.

4.A The first program: sending a breach signal to the server

The program is designed to carry out a monitoring of the outlets for a building Figure (8) shows the main interfacing of the system, a setup file of the computer program is configured. The person responsible for the security of the building installs the program.



Figure (8) Main Interfacing of the System

The main interface of the program contains buttons to (Start System) and (Stop System) and (Reset System), until the person responsible for the security of the building activates the system, to restore the system to normal. The main interfacing of the system contains also (Video Box) to convey the coming image from the monitoring camera. The image coming from a monitoring camera can be controlled by the choice (camera) in the main menu, which contains the following options:

- 1 - Start Camera.
- 2 - Stop Camera.
- 3- Reset Camera.

4.B The second program: receives the control signal from the server

The second program downloads a text file under the name (Delay.txt) from the server periodically, this file contains the control signals sent from the mobile phone, the program reads the file (Delay.txt) and depends on the value that is contained, the control of the port in which the breach occurred is done. The lack of physical parts in which the control can carry out (such as locking a door or window), (LED) has only been lighting

via the serial port to indicate an access control signal to the port that the breach occurred.

Before activating the system, the electronic circuit that is designed to connect more than one sensor must be linked to one serial port that is shown in Figure (9), the electronic circuit designed is linked to the serial port of the computer, and a monitoring camera is linked across the port (USB), then the person responsible for the security of the building can activate the system by clicking on the button (Start System).

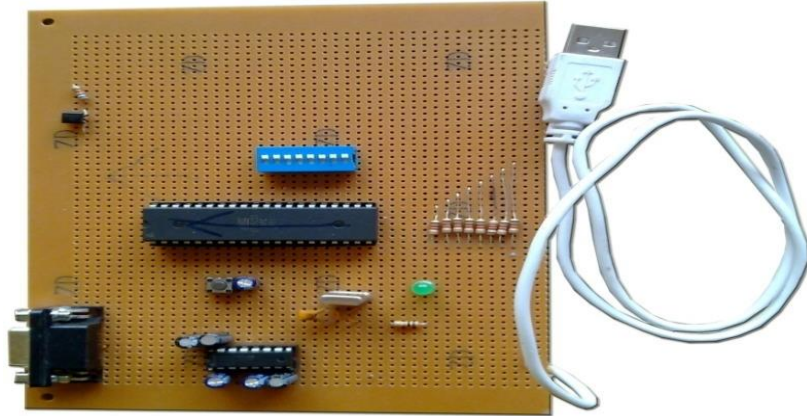


Figure (9): Board of the Designed Electronic Circuit.

4.1 Website Programs Implementation

The website of the system works in two directions the first one represents internal workings of the site, which contains assistant programs for the server and the second represents the interface of the site that enables people responsible for the security of the building to access the information of the system via the using of a user name and password.

4.1.A The first trend: assistance program for the server-side

1- Server Program (Status.cgi)

(Status.cgi) is an assistant program to open a channel of communication between the server and the computer, the program provides a channel of communication between the server and the computer when a case of breach occurs, the work based on the Algorithm (3).

2- Server Program (Rdcmd.cgi)

With the assistance of the mobile phone to send a control signal to the computer after making sure of a breach of the process and his work is based on the Algorithm(4).

4.1.B The second trend: the website

A second trend represents the visible part of the prior user of the system, which is a Web site that is designed with languages (PHP, JavaScript, HTML) which enable the persons responsible for the security of the building to access the information of system via the using of a user name and password, we can access the data of the ports through website and by entering the website address ([Http://aliwael.freehostia.com/web.html](http://aliwael.freehostia.com/web.html)) as in Figure (10), which shows the general form and the external appearance for the site.

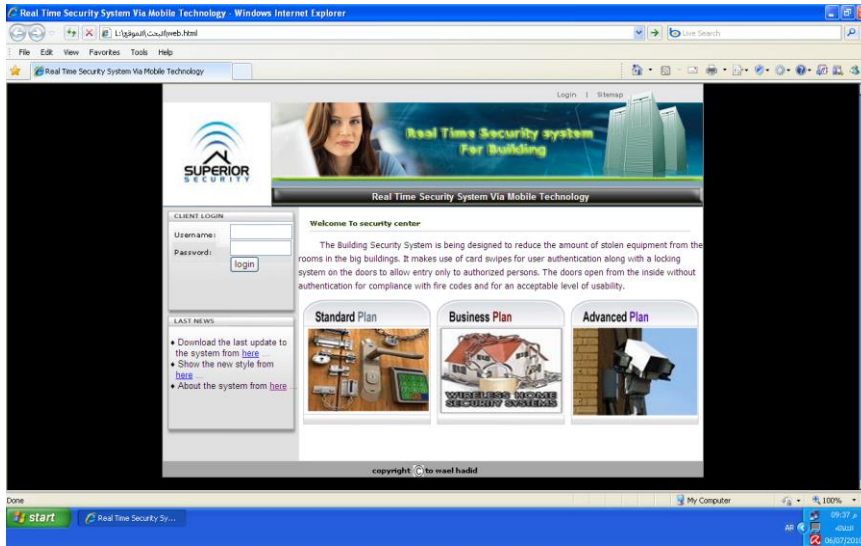


Figure (10) External Appearance for the Web Site

4.2 Mobile Programs Implementation

A mobile phone contains three programs as shown in figure (11).

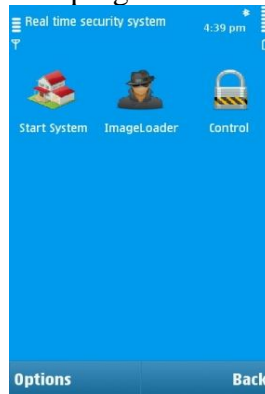


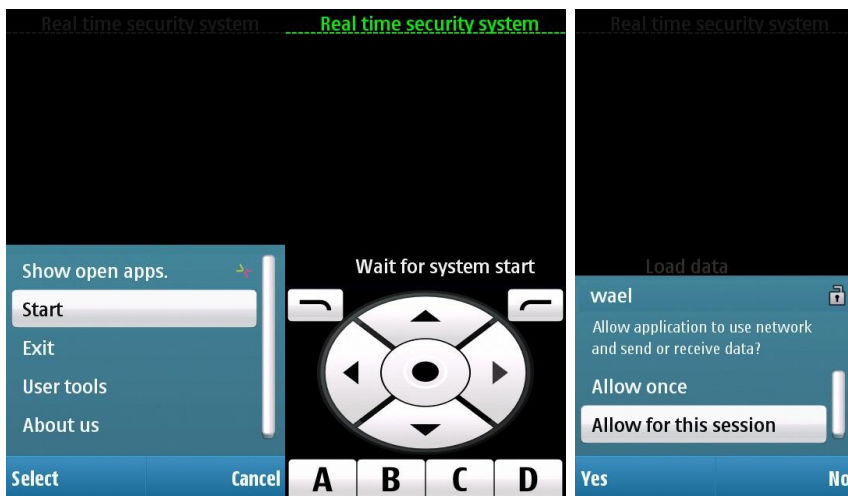
Figure (11) Mobile Phone Programs

4.2.A First program

The first program is to activate the system via creating of a connection to the server, this program still working on a mobile phone if the system was activated. The program receives a breach signal from the website via the server program and then gives an alarm when a case of a breach occurs and shows the sequence of the port on the screen. It contains:

- 1 - **Run:** This selection is used to start the system and create the connection and read data from the server. When press it, observe the appearance of an interface that asks the user of the mobile phone to connect with internet as in Figure (12) and this command turns to (Stop) in the case of activating the system, and when press it, the system stops and the connection with internet cuts off.
- 2 - **Stop:** This selection appears instead of the selection of (Start) after start the system to allow the mobile user to stop the connection and then stop the system working.
- 3 - **Exit:** This can be used to give a mobile user the option to exit from the program.
- 4 - **User Tools:** This selection contains a set of collection of settings that includes determining the period of sequence of each data coming to the mobile phone and sent to the server that means determine the period of reading.

5 - **About Us:** This represents the identification of the system designer and the type of release.



a-Wait for system start b-Server connect c-Wait to start

Figure (12) First Mobile Program Implementation

4.2.B The second program (view image)

This program is used to show a picture of the person (hacker). This program is used after a breach. It is optional but not compulsory for the person responsible for the port in the building. The program works by opening a channel of communication to the server and then displaying the image on the screen of the mobile phone via the creation of the screen to display the image and determine the dimensions of the screen to ensure a clear view of the image. Figure (13) shows the display image in the mobile phone.

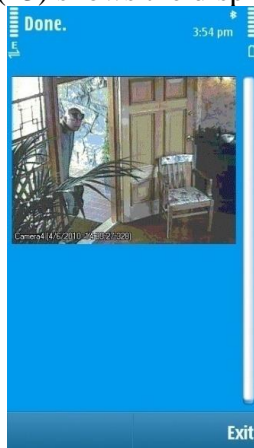


Figure (13) Image Display

4.2.C The third program (to send a control signal)

This program is used to send control signal after a case of a breach. It is optional, but not compulsory for the person responsible for the port in the building. This program works via assistant program (Rcmd.cgi) for the server which opens the text file (Delay.txt) for the purpose of writing and specifying the type of control signal.

5. Discussion

The DRTSS system was implemented and tested by using different issues of the Nokia mobile phone. The system was practically implemented by sending a signal of

the breach and the image successfully to the mobile phone in its real time and the signal has been read and the image has been displayed by the person responsible for the security of the building, a control signal was also delivered from the mobile phone and received by the computer for the purpose of control of part of the building. The response time of the system is calculated to transfer the breach signal from the moment of the breach until the signal reaches to the mobile phone of the person responsible for the concerned port in the worst conditions and placing it in the variables related to it, in according to the following equation:

$$RSTC = TGC + TCS + TSM$$

- **RSTC**: response time of the system.
- **TGC**: time it takes to transfer the signal from the sensor port to a computer.
- **TCS**: time it takes to transmit the signal from the computer to a server.
- **TSM**: time it takes to transfer the signal from the destination server to the mobile phone.

$$RSTC = TGC + TCS + TSM = 1 + 3 + 2 = 6 \text{ second.}$$

This response time (6 second) is obtained by using mobile phone of type Nokia 97 and Internet with speed (256 kilo byte) in best cases. The longest delay time between system portions is (12 seconds) at best case and less than (25 seconds) in the worst case by relying on less efficient and performance devices. The system was also tested on various types of Nokia mobile phones in different times. Figure (14) shows different response times for various Nokia mobile phones while Figure (15) shows Nokia 97 response times in different times.

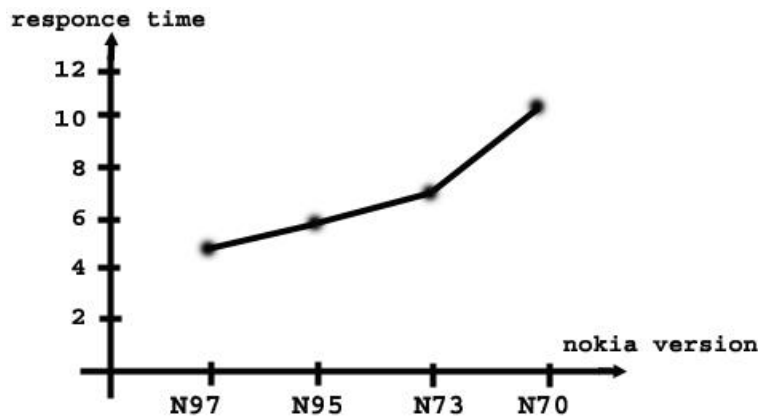


Figure (14): Different Response Times for Various Nokia Mobile Phones

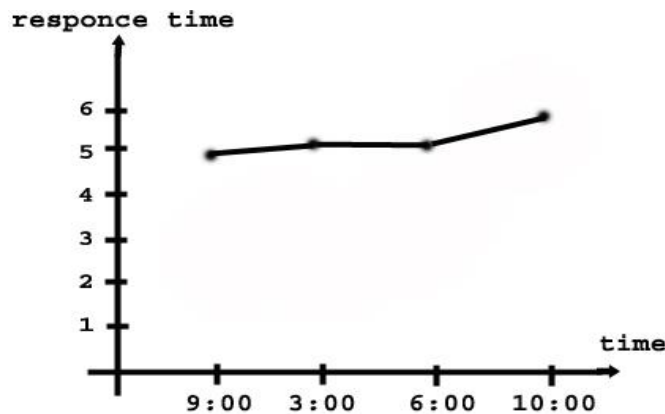


Figure (15): Nokia 97 Response Times in Different Times.

6. Conclusions

In this paper, a system for monitoring and controlling building in terms of security has been designed and implemented, via placing sensors at all ports of the building as well as the presence of monitoring cameras that capture an image if the case of breach occurs, and then send it to mobile phones. During the work, we conclude the following: -

- 1 - The use of website that designed on the server provides quick and easy way to observe the state of the system and view the recorded data without the need to use a mobile phone.
- 2 - The use of the electronic circuit designed for the purpose of transferring of the parallel signals to sequential signals helps to be used with the serial port in the absence of a parallel port in the computer, and eight sensors can be linked and then monitoring the eight ports in the building.
- 3 - Mobile phone programs used depending in its performance on the type of device used, specifications, type of operating system equipped with it, and the real-time algorithm used in the system. The use of an independent program and dispensing browses attached to devices help to improve the performance of the system and the rapid exchange of data.
- 4 - The transfer of the signals to the server is only done in the case when there is a change in the values of the signals this will reduce the cost and congestion of the network.
- 5 - Using the principle of (Multithreading) in the mobile phone has led to a parallel implementation. It also gave the possibility to expand the program by adding an additional thread.

7. Future Works

Some points to be future work are :

- 1 – Use Sockets technology provided by Web servers and communicate with server special ports, this will keep communication open between system portions and to abandon the technology of (CGI), which require a call to the program and implemented them at every communication operation and exchange of data or information.
- 2 - One can improve the performance of the monitoring system by using image compression and data encryption to give the nature of privacy and security of exchanged data by using the methods of protection that are available including the Protocol (HTTPS) (HTTP with Security) and other technologies.
- 3 - Using Bluetooth technology to exchange data between sensors on the one hand and between the computer and mobile phone on the other hand.

REFERENCES

- [1] Al-bazaz D. B., 2004, "Design and Implementation of Real Time Software for Multitask system", Phd., College of Computer and Mathematics Sciences, University of Mosul.
- [2] Al-Hafith B. M., 2006, "Design and Implementation of Control and Monitoring System Through Mobile Phone Using GPRS", Msc., College of Engineering, University of Mosul.
- [3] Alheraish A., W. Alomar, and Abu-A-Ela M., 2006, "remote PLC System Using GSM Network with Application to Home Security System", department of Electrical Engineering, King Saud University, Riyadh, Saudi Arabia.
- [4] Çetin Kamil and Sahin Özge, 2007," VOICE INTEGRATED HOME AUTOMATION AND SECURITY SYSTEM THROUGH TELEPHONE LINE", Dokuz Eylül University, Faculty of Engineering, Department of Electrical & Electronics Engineering, 35160, Buca, Turkey.
- [5] Geha Ibrahim, Elie Kfoury, and Jaafar Ashraf,2007 ," An Advanced Home Security System", American University of Beirut , Department of Mechanical Engineering, Beirut, ing01, Lebanon.
- [6] Jane W. S., ,1993, "A prototyping Environment for Real Time Systems", Department of Computer Science, University of Illionios, Japan.
- [7] Kouma Jean-Paul, 2006, "Intelligent Home Security System", Applied Physics and Electronics, SE-901 87, Umea university, Sweden.
- [8] Liu Jane W. S., 2000, "Real Time Systems", United state of America.
- [9] Sharma A., 2003, "Design of Wireless Sensor Network for Building Management System", Research Project, Master of Science in Electrical Engineering, University of California at Berkely , USA.
- [10] Sikandar Malik and etc, 2009, "SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security", Issues in Informing Science and Information Technology Volume 6, Pakistan.
- [11] Xie Tao, Qin Xiao and Lin Man, 2006, " Open Issues and Challenges in Security-aware Real-Time Scheduling for Distributed Systems", 801 Leroy Place, Socorro, New Mexico, 87801, USA.