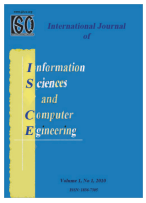
Information Sciences and Computer Engineering, Vol. 1, No. 2, (2010) 15–20

PHARUS

International Journal of
Information Sciences and Computer Engineering

journal homepage: http://www.ijisce.org



SMS Based Microcomputer Control System (MCS) for Computer Automation and Security

Awodele Oludele*, Adamo David, Kadiri Kamal-Deen, Orekoya Morolake

Department of Computer Science and Mathematics, Babcock University, Ilisan-Remo, Ogun State, Nigeria

***Abstract*– This paper presents a cost-effective solution that provides a means of controlling microcomputers remotely and also enables computer security against intrusion when an authorized computer user is absent. The system is based on SMS technology and provides an ideal solution to computer users and system administrators who are not always at the computer's immediate location but need to carry out basic computer operations and prevent unauthorized access. The Microcomputer Control System (MCS) is built with mobility in mind such that it would provide remote access to a microcomputer while providing security. Hence, this paper proposes a system that allows users to control their computers ubiquitously and also provide security on detection of intrusion by the use of SMS/GSM technology.**

1. Introduction

In an environment where most of the valuable and sensitive information is stored on computers, computer and data security is of paramount importance. Proper measures therefore have to be taken to prevent intrusion. In addition, there is a need to automate basic computer tasks so that the user can take advantage of current technology such that leaving the immediate location of the computer does not completely isolate an authorized user from the computer. As mobile phones have developed rapidly, several attendant services such as the Short Messaging Service (SMS), Multimedia Messaging Service (MMS) and others have been implemented in order to add to the usefulness of mobile phones.

Since the first Global System for Mobile Communications (GSM) network started operation in 1991, more than 100 countries have adopted the standard. Over 20 million subscribers of GSM networks are now offered worldwide coverage, outstanding voice quality over a whole range of operating conditions, and a variety of value-added services. These services include voice mail, call handling facilities, call line identification, and SMS [1]. SMS in particular is widely used in communication, and more recently has been leveraged to provide several services like airline ticketing, banking services, commercial services like Share and Sell (an added service provided by MTN Nigeria), where subscribers can easily share and/or sell airtime, and several others [2].

2. The Need for SMS Based Remote Microcomputer Control

In developing countries, the level of internet availability is low and quite expensive. Even in places where an Internet connection is available, the speed and reliability of such a connection is often below par. Since most remote PC control solutions are internet based, their effective use in such environments is severely limited.

The SMS based Microcomputer Control System (MCS) not only allows computer users and/or system administrators remotely carry out specific computer operations but also provides security against intrusion. This is done by sending messages to a pre-registered number upon detection of intrusion, or responding to a request sent from an authorized user to lock the computer.

Presently, the use of computers for important tasks and storage of sensitive information is considerably high and more and more individuals and corporations are employing computers that perform time-sensitive tasks and store critical information such that they have to be monitored and administered at all times irrespective of geographical location. With remote computer access and control, users can now conveniently monitor a computer and interact with it in various ways, but this convenience cannot be achieved if the user does not have access to a reliable, high speed Internet connection. This tends to limit the usability of a remote access system.

SMS stands for Short Message Service. It is a mobile technology that allows for sending and receiving text or even binary messages to and from a mobile phone [3]. With an SMS based computer control system, monitoring and control can be achieved at all times. This is as a result of the ease of accessibility that comes with the use of a mobile phone. Therefore, to achieve an effective remote control and monitoring (security) system for a microcomputer, irrespective of Internet connection availability, an SMS based microcomputer control system is needed.

3. Existing System Overview

A number of remote PC access and control software already exist. These systems enable computer users gain remote access to their workstations via an Internet connection or through an existing wireless or wired network. One of such systems is Virtual Network Computing (VNC) and its numerous variants. Although, VNC and similar systems provide remote access to a user's desktop and even allow remote mouse and keyboard interaction, these systems are highly dependent on high-speed internet connections or networks. They are therefore not very applicable

*Corresponding author:
Email addresses: delealways@yahoo.com, Ph: +23 47037355385

in situations where a reliable high-speed Internet connection or some other non-GSM network is unavailable.

TweetMyPC is an open source development project that uses the Twitter network to relay command messages to a PC. It requires a valid Twitter account, set up for this particular purpose, and from there checks the feed of the control account every minute. Anytime the feed account twitters the following commands: Shutdown, Restart, or Logoff, *TweetMyPC* performs the command on the computer being controlled. A Mac version called *TweetMyMac* also exists for the same purpose. Although this is quite convenient, it is still dependent on the availability of an Internet connection on the computer being controlled and from the remote control device (which may be a mobile phone). This internet connection is necessary to access the Twitter network and may not be readily available.

Remote PC/microcomputer control systems exist that function via Bluetooth technology. However, this system is only applicable within the range of a Bluetooth connection and is therefore geographically limited.

Generally, most remote PC/microcomputer control systems operate via an Internet connection or some other form of non-GSM network connection that may not be readily available to the average user, especially in third world countries, or may be limited by distance. Furthermore, most of these systems do not provide intrusion detection functionality.

4. Related Work

This section provides a general overview of similar works that employ SMS technology in remote control and monitoring of systems.

In [4], a system for effective and more efficient control of systems in "intelligent" buildings, using a GSM network, specifically SMS and MMS messages for communication between an administrator and the system, is proposed. The system is especially useful in cases when there is no 24 hour presence of staff in the controlled building.

In [5], the use of wireless and mobile technologies in remote virtual experimentation as part of a mobile education laboratory scenario is explored. A mobile learning system is developed and deployed over the GSM network based on a traditional client-server architecture. Mobile phones, PCs or PDAs communicate with the server side in the form of a mobile connected to a PC or a microcontroller that runs the experimental setup. Students can conduct experiments by issuing predefined commands and then communicate with the server via SMS.

Another example of an SMS based remote monitoring and control system is the one described in [6]. The paper explores the applicability of a short message service based control system in civil telemetry applications. The paper goes ahead to present some experimental and theoretical evaluations on energy consumptions, cost and efficiency in case of applications requiring small amounts of data exchanging.

In [7], an SMS based wireless control system for automating appliances and security is considered. The paper investigates a cost effective solution that will provide controlling of home appliances remotely and will also enable home security against intrusion in the absence of the home owner.

Seixas & Palmer [8] describe the conception of an electronic system for alarm monitoring and remote command devices through a GSM mobile network using the short messaging service (SMS). The system was developed as a low cost solution based on a common mobile phone and Intel 8751 microcontroller. The system is intended for device state monitoring in a residence, for sending alarms and also for remote command of equipment, by using simple messages in a mobile, through a GSM network.

5. The Proposed SMS Based Microcomputer Control System (MCS) Overview

The microcomputer control system is based on GSM technology which would be used for the transmission of SMS from one location to another. SMS technology is used for ubiquitous access to the computer and for enabling security breach control.

The system is made up of two subsystems. The microcomputer control subsystem enables the user to carry out basic computer operations remotely whereas the security alert subsystem provides remote security monitoring. When the user is away, the microcomputer control system locks the computer in such a way that no interaction with the desktop can be initiated with mouse or keyboard. The system has the ability to respond to SMS from a specific cell number to carry out a basic operation on the computer such as shutting down, hibernating and locking the computer. Furthermore, the system has a security alert system which allows the automatic generation of an SMS, upon detection of an intrusion attempt, thus alerting the user against a security risk.

5.1. Features of MCS

The characteristics of the proposed system include remote controlling of a microcomputer, intrusion detection and system security. The MCS enables a user or administrator lock a computer such that access can only be granted by entering a password. In order to enter a password, the user or administrator would have to be physically present at the computer's location. The system alerts users about attempts to breach security. The user gets alerts anywhere through SMS/GSM technology thus making the system location independent. Intrusion detection is a feature that is conspicuously absent in most existing remote PC control systems. The MCS also provides secure access via SMS through a preconfigured number and a corresponding PIN. The wireless nature of the system ensures ease of use, portability and flexibility. GSM technology provides the benefit of the system being accessible in remote areas irrespective of distance from the actual system. This eliminates the issue of distance limitation in the case of Bluetooth-based systems and also alleviates the issue of lack of a readily available high-speed internet connection. In cases where a phone is used, the system can generate SMS alerts concerning low battery levels, charging status and signal strength. The system is generally simple, scalable and extensible.

5.2. Working

A PC/microcomputer has the MCS installed on it. The microcomputer control subsystem is responsible for enabling access to the computer from any location where a GSM signal exists and the second subsystem, which is the security alert subsystem, is

responsible for security intrusion detection. These two subsystems work on GSM technology for the transmission of instructions from sender and receiver.

The GSM modem is a plug and play device and is attached to the PC/microcomputer. This modem communicates with the PC via a USB port. The GSM modem enables/disables SMS capability.

The cell phone is a mobile device that communicates with the GSM modem. The mode of communication is wireless and is based on GSM technology. This mobile device would have a Subscriber Identification Module (SIM) card and a GSM subscription. The cell number of this SIM card is registered on the system. The user would transmit instructions via SMS and the system would respond as appropriate.

5.3. Methodology

- Program starts up as a background process upon system startup.
- When the program is executed, GSM hardware tests are run in order to check if the GSM modem is available. If the modem is available, the system will activate it. If the hardware tests fail, the program is terminated.
- After activation, the modem/phone will be tested for SMS capability. If the modem or phone does not have this capability, the user is alerted and the program terminates.
- If the modem/phone has SMS capabilities, then a serial communications port would be opened and the GSM hardware will allow transmission of SMS.
- The system will then connect and after a connection has been established, the system would be ready to receive instructions in a specified format from a predefined cell phone number and a corresponding Personal Identification Number (PIN) and generate SMS alerts concerning intrusion attempts in situations where the user has previously locked the computer.
- SMS will be silently ignored if cell number is not authorized or other authentication fails.

5.4. System and Software Design

The system is made up of hardware and software components.

5.4.1. Hardware

The MCS consists of the following basic hardware components:

PC: This unit contains the software components such as the MCS through which the computer is controlled and security is monitored.

GSM Modem: This is a hardware component that enables the system to send and receive SMS to and from the system. Communication with the system takes place via a USB port. A cell phone can also be used in place of a GSM modem.

Mobile Device: A mobile phone containing an appropriate SIM card with a specific cell number would be necessary for the user to communicate with the computer. This device communicates with the GSM modem via radio frequency. The mobile user transmits SMS using this device.

5.4.2. Software Design

Input Design . As shown in figure 1, user input is sent as text messages that strictly adhere to a specified syntax. Immediately the microcomputer receives the message, it processes it and an appropriate response is sent to back to the user. If the number is not authorized or some other authentication procedure fails, the microcomputer silently ignores the message. Below are some of the input operations which can be sent to the computer:

1. Shutting Down/Hibernating/Restarting the Computer

To shut down, hibernate or restart the computer remotely, a user has to send:

shutdown|hibernate now|[time in seconds] [PIN]

A user can decide to shutdown the computer immediately by using the *now* command or shutdown the computer after an elapsed period of time (specified in seconds). When the SMS arrives, the application checks a database to verify that the PIN code corresponds with the preregistered phone number. If authentication completes successfully, the command is carried out and the shutdown process is started on the computer. The sender then receives a message of confirmation in the form:

shutdown process successfully initiated at [time]

2. Executing a File or Script

To execute a script or file that exists on a particular location on the computer, a user has to send:

execute now|[time in seconds] [path_to_file] [PIN]

If authentication is successful, and the script or file is executed successfully, the system responds with a confirmation message in the form:

Execution instruction successfully initiated

3. Locking the Computer

Locking the computer involves preventing access to the operating system's interface until an appropriate password has been entered. In order to do this remotely, the user has to send:

lock now|[time in seconds] [PIN]

If the command is successfully executed, a confirmation message is sent back to the user in the form:

Lock procedure successfully initiated

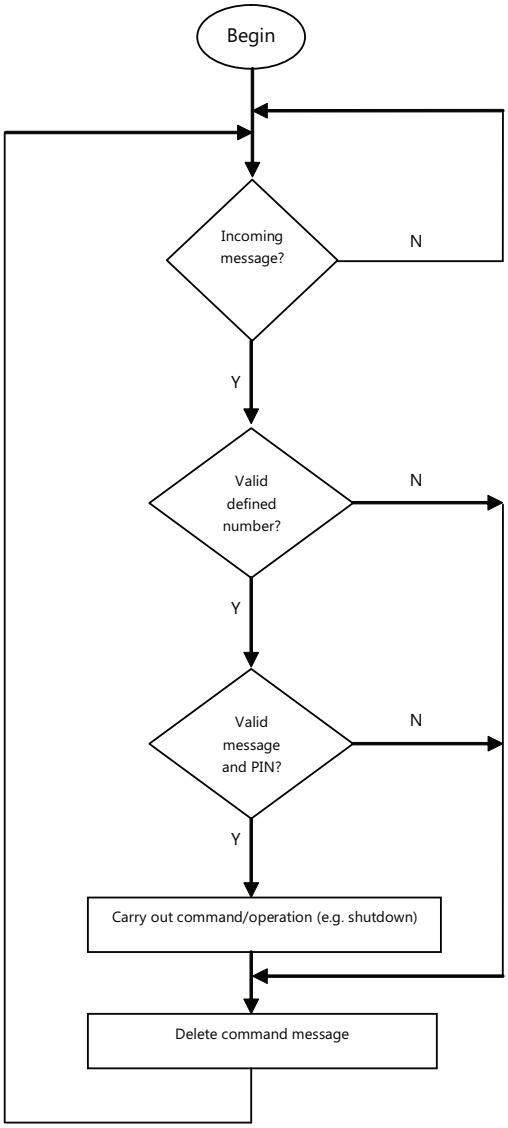
4. Get List of Processes Running on the Computer

This functions like a remote task manager. In order to get the list of processes/programs running on the computer, the user has to send:

getprocesslist [PIN]

If this command is executed successfully, the system returns the list of processes/programs currently running on the computer along with their process ids.

A command can be sent to *kill* a particular process based on the on the process id. In order to do this, the user has to send:



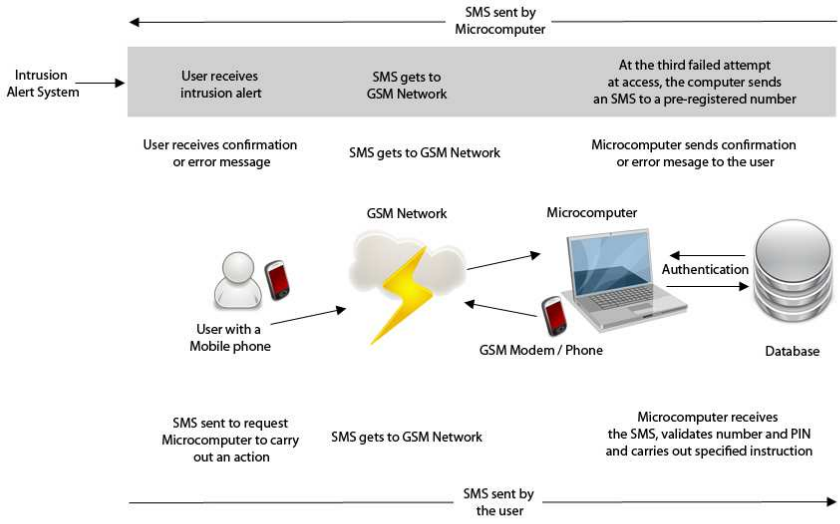


Fig. 2. System Model.

kill [process_id] [PIN]

On successful execution of this command, a confirmation message is sent back in the form:

Process successfully terminated

Intrusion Alert. When the microcomputer has been locked, and a specified number of failed attempts have been made at entering a password, the system generates an SMS alert and notifies the user of the attempted intrusion. The SMS alert would be of the form:

Intrusion attempt detected at [time]. Please take precautionary measures.

Error Handling. Like almost any other system, there exists the possibility of errors. Error handling is an integral part of a good system since errors are more often than not likely to occur in situations that require user input. There is always the possibility of users sending SMS instructions to the microcomputer in the wrong format. A feedback mechanism is therefore implemented to inform users of their errors.

6. SMS Security Issues

SMS technology is a convenient means of transferring small amounts of information from one point to another. However, it has a number of security issues.

SMS messages can be intercepted quite easily. The cost of intercepting an SMS message is lower than in voice communication. It is easy for an operator to scan all SMS going through their network for keywords, and this is often done. Scanning does not need to be done with the consent of the operator. Devices for GSM wiretap can be bought on the black market [9].

Unlike a phone call, an SMS can exist on a cell phone long after the information has been sent. After a call has been completed, the information transferred is not persistent. Therefore, if a user forgets to delete an outgoing SMS, it will be present on the mobile device until it is deleted. A person who has access to the mobile device can have access to these SMS. This is also a concern if the mobile device is stolen.

In general, for SMS messages to be a reliable and secure means of communication, a number of requirements must be fulfilled.

1. They must be secured against interception by a third party.
2. They must be secured against modification.
3. The sender of the message must be clearly identified.
4. Saved messages must be protected from reading when the phone is in the wrong hands.

7. Advantages of SMS Based Remote Microcomputer Control

The advantages of SMS based remote microcomputer/PC control arise from the advantages of SMS technology. These include:

- Convenience – SMS technology is easy to use and learn and can be accessed easily when needed.
- Accessibility – instructions can be sent to the microcomputer to be controlled and monitored from any location provided there is the existence of an active GSM network.
- Portability – a microcomputer can be controlled and monitored from any GSM phone that supports SMS. Considering the fact that most GSM phones support SMS, the system is therefore highly portable.
- Saves Time – an SMS based remote monitoring and computer control system saves time as the user is not required to gain access to an internet connection or make an dedicated connection to the computer to be controlled as opposed to a Bluetooth-based system or an Internet based system.
- Cheaper – SMS services are generally cheap and are sometimes provided for free (at least for certain periods) by service providers. Furthermore, most service providers do not charge users for receiving SMSs.
- Mobility – User and/or system administrators are more likely to have their phones with them at all times than they are likely to physically be in front of their computers. An SMS based system therefore enables them have ubiquitous access to the computer to be controlled and monitored.

8. Limitations of an SMS Based Microcomputer Control System

The limitations of the proposed system stem from the basic problems that SMS technology still faces. Several identified limitations [2] are:

- The length of SMS message is 160 characters and this poses a limitation. Therefore, messages need to be constructed within this character limit.
- SMS technology does not guarantee set transmission times or guaranteed delivery of the message and this may result in the delay of some messages or even total message loss.
- Not all networks have full coverage and some locations maybe protected from electromagnetic radiation, thereby preventing users from getting a signal.
- As ubiquitous as mobile phones seem to be, not all individuals possess a mobile phone.
- Delay of transmission of SMS by the GSM operators and intra and interconnection delays and traffic between GSM operators.
- The SMS based feedback mechanisms are limited by the SMS tariff of the network in use and the current amount of minutes on the GSM Subscriber Identification Module (SIM) that the system employs. Therefore, if the SIM does not have minutes, the feedback mechanism would not work.
- The SMS capabilities of devices differ. Some devices can receive only 140 characters per message while others can support concatenations of SMS messages.

9. Conclusion and Future Work

This paper has focused on introducing a low cost, secure, ubiquitously accessible, and remotely controlled solution for automation of basic computer operations and security. The approach discussed in this paper achieves the goal of controlling microcomputers remotely using the SMS-based system.

GSM technology has proved to be a capable solution for remote control and security and is cost-effective when compared

with other alternatives such as an Internet connection; especially in this environment where having a reliable high-speed Internet connection is a tough thing to achieve. A fundamental level of microcomputer control and remote monitoring has been implemented. The system is extensible and many computer operations can be automated by writing batch scripts and scheduling them to be executed upon receiving a particular SMS instruction.

References

[1] G. Peersman and S. Cvetkovic, "The global system for mobile communications short message service," *IEEE Personal Communications*, June 2000.

[2] E. R. Adagunodo, O. Awodele, and O. B. Ajayi, "Sms user interface result checking system," *Issues Informing Science and Informing Technology*, vol. 6, 2009.

[3] E. R. Adagunodo, O. Awodele, and S. Idowu, "Sms banking services: A 21st century innovation in banking technology.," *Issues in Informing Science and Information Technology*, vol. 4, 2007.

[4] V. Obradovic, J. Karisik, and B. Odadzic, *Wireless Communication with Intelligent Buildings using GSM Network.* 15th *Telecommunications Forum.* 2007.

[5] A. Y. Al-Zoubi, A. A. Tahat, and O. M. Hassan, *Mobile Virtual Experimentation Utilizing SMS. Proceedings of the Fourth IASTED International Conference Communications, Internet and Information Technology*. 2005.

[6] B. Ciubotaru-Petrescu, D. Chiciudean, R. Cioarga, and D. Stanescu, *Wireless Solutions for Telemetry in Civil Equipment and Infrastructure Monitoring.* Retrieved from from http://www.bmf.hu/conferences/saci2006/ciubotaru.pdf.

[7] M. H. S. Khiyal, A. Khan, and E. Shehzadi, "Sms based wireless home appliance control system (hacs) for automating appliances and security," vol. 6, pp. 887–894, 2009. Retrieved from http://iisit.org/Vol6/IISITv6p887-894Khiyal592.pdf.

[8] M. Seixas and J. Palma, *Remote Alarm and Command System for Residential Domotics through GSM-SMS*. Retrieved from http://www.aedie.org/9CHLIE-paper-send/312-seixas.pdf.

[9] "Security of sms communication." Retrieved January 15, 2010 from http://www.circletech.net/download/en/press0305.pdf.

Dr Awodele Oludele is presently the Head of the Department of Computer Science and Mathematics, Babcock University, Ilishan-Remo, Ogun State, Nigeria. His research areas are Software Engineering, Data Communication and Artificial Intelligence. He has published works in several journals of international repute.

Adamo David Jr is a final year undergraduate student of Computer Science as Babcock University, Ilishan-Remo, Ogun State, Nigeria. His areas of interest include Database Technologies, Software Engineering, Software Development and Human Psychology.

Kadiri Kamal-Deen is a final year undergraduate student of Computer Science at Babcock University, Ilishan-Remo, Ogun State, Nigeria. He is especially interested in Database Design and Business Management.

Orekoya Morolake is a final year undergraduate student of Computer Science at Babcock University, Ilishan-Remo, Ogun State, Nigeria. Her areas of interest include Software Development and Database Design.