A vertical handover mechanism with security services for mobile applications

Juan A. Vargas Enríquez [1] and Arturo Díaz Pérez[2]
[1] Instituto Tecnológico de Cd. Victoria,
Blvd. Emilio Portes Gil # 1301 Pte. C.P. 87010
Cd. Victoria, Tamaulipas
Jvargd@itcv.edu.mx
[2] CINVESTAV, Unidad Tamaulipas
Laboratorio de Tecnologías de Información
Parque Científico y Tecnológico TECNOTAM
Km. 5.5 carretera Cd. Victoria-Soto La Marina
Cd. Victoria Tamaulipas, México
Paper received on 26/08/10, Accepted on 15/09/10.

Abstract. A mechanism, called vertical handover, for changing networks on mobile devices is presented. Particularly, we explain how to do such changes in cell phones owning Wi-Fi controllers. The proposed mechanism enables applications accessing the Internet on a cell phone to automatically switch between WLAN and GPRS networks. Additionally, in order to assess the performance of the handover mechanism, it is presented an application that transfers data through a secure channel via Internet from a cell phone to a desktop computer that acts as an application server. The secure channel provides confidentiality, integrity and authentication services. The tests conducted showed that the handover mechanism makes network changes in the three possible scenarios: GPRS to WLAN, GPRS to WLAN and WLAN to WLAN.

1 Introduction

Currently the use of the cell phone is not just limited to making phone calls. According to a survey conducted in the United States by America On Line in 2006 [1], 8% of the users use their cell phone to access the web, and 7% use it to send email. The integration of Wi-Fi to the cell phone has become decisive when it comes to accessing the Internet due to its low cost and higher data rates compared to GPRS (General Packet Radio Service) of GSM (Global System for Mobile communications). The number of cell phones with a Wi-Fi interface is growing. According to the report "Wi-Fi Component forecast and Vendor Share" of the 2005 [2], in 2009 most of the Wi-Fi chips had been installed in cell phones. On the other hand, wireless networks are widely available in offices and public places such as hotels, airports, malls and schools [3]. The integration of these technologies is needed in order

©E.Cuatecontzi Cuahutle, A.Cortés Fernández,
J. F. Ramírez Cruz, J. H. Sossa Azuela. (Eds.).
Advances in Intelligent and Information Technologies.
Research in Computing Science 50, 2010, pp. 249-259

to allow mobile devices to roam seamlessly between WLAN and GPRS networks, a process called vertical handover [11].

In this paper we propose a vertical handover mechanism between WLAN and GPRS networks for mobile devices. In order to evaluate the performance of the handover mechanism it was developed an application in the health care area for patient monitoring. The application for services in the area of health consists of a cell phone with Wi-Fi interface and a sensing device, the system monitors the patient's vital signs and sends this information to a medical facility through the GPRS network or through a wireless network if available. Handover events occur when the patient enters or leaves the coverage areas of wireless networks. We also propose a security mechanism to provide authentication, data integrity and confidentiality services in order to establish a secure communication channel [12] between the cell phone and the application server.

The remainder of this paper is organized as follows. In section 2 the system architecture is presented and a description of the modules that comprises is given. Section 3 discusses the implementation of the architecture. Section 4 discusses the security services implemented. Sections 5 and 6 discuss the performance of the system and the analysis of results. Section 7 presents the conclusions drawn.

2 System architecture

The proposed architecture for patient monitoring system is shown in Fig. 1. The architecture follows the client server model, where the client is the application that runs on the cell phone and the server is the application server for Internet communications.

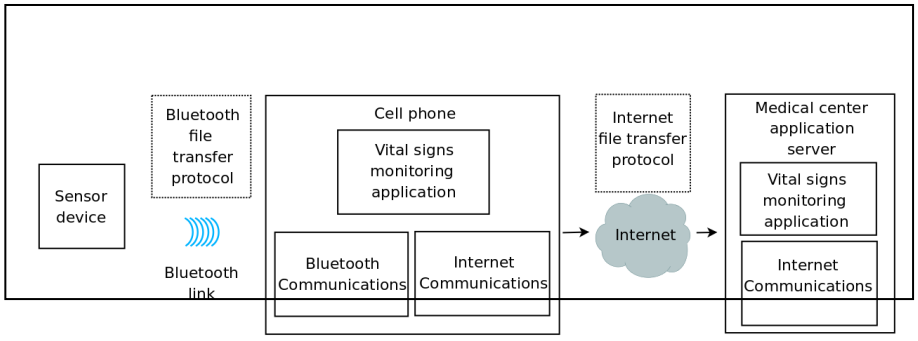

Fig. 1. Vital signs monitoring system architecture

The client architecture consists of three modules which are described below.

- Bluetooth file transfer module: The function of this module is to transfer data stored in the internal memory of the monitor device to the cell phone.
- Data display module: The function of this module is to present in the cell phone data received from the monitor device.
- Internet file transfer module: The function of this module is to transfer the data file from a cell phone to the application server providing the security services of authentication, confidentiality and integrity. This module also provides the handover mechanism to make the automatic change between GPRS and WLAN networks.

The server architecture consists of four modules which are described below.

- Internet file transfer module: This module receives the data file sent from the cell phone using the developed file transfer protocol. This module also performs two other functions, the first one is to respond to authentication requests from clients and the second one is to provide session keys that require both client and server to provide integrity and confidentiality services.
- Data display module: The function of this module is to present to staff in the health care facility the data received from the monitor device.

3 Communications

The system for monitoring vital signs performs a transfer of information from the monitor device to the application server; this transfer is done through two different types of networks, Bluetooth and Internet. To make this transfer of data reliable two communication protocols are used one for Bluetooth and one for Internet.

3.1 Bluetooth file transfer

Transferring data via Bluetooth interface requires the implementation of a file transfer protocol for two reasons. Firstly, the vital signs monitor device has limited computing capabilities and has only a basic implementation of RFCOMM transport protocol. Secondly, the communications via Bluetooth present frequent errors [13] and need an error recovery mechanism additional to that provided by RFCOMM. When messages are lost or when communication errors occur, the error recovery mechanism of the protocol stops completely the file transfer to enable the cell phone

and the monitor device to synchronize again. Once the devices are synchronized, the file transfer is resumed from the beginning.

3.2 Internet file transfer

To make the file transfer between cell phone and the application server through the Internet a protocol was developed over the TCP/IP protocol. The Internet transfer protocol keeps the state of the transfer, in this way a mechanism for more efficient error recovery can be added. If the file transfer is interrupted, it resumes at the point where it was stopped. This error recovery scheme is necessary because of interruptions in the data transfer can occur more frequently in this protocol. The commands in this protocol are shown in Table 1.

Table 1. Commands of the Internet file transfer protocol

Commands issued by cell phone	Answer from server
SEND_FILE	COMMAND_RECEIVED
RESEND_FILE	Last data block received
EOF	EOF_RECEIVED
Data block	BLOCK_RECEIVED

The command SEND_FILE tells the application server a client (cell phone) wants to start a transfer session to send a file to the server.

The command RESEND_FILE is issued by the cell phone and tells the server that the file transfer failed, it also tells the server that the file transfer is going to restart at the point it was interrupted.

3.3 Vertical handover GPRS/WLAN

The vertical handover process has been extensively addressed in the formal literature and several solutions have been proposed.

In [4] Salkintzis discusses the motivations for integrating WLANs with 3G cellular networks and presents an outline for a tightly coupled architecture between WLAN and GPRS networks.

In [5] it is proposed a hybrid architecture to support vertical handover between an IEEE 802.11 network and an UMTS network (Universal Mobile Telecommunications System), which incorporates SIP (Session Initiation Protocol) and mobile IP protocol.

In [6] it is proposed a scheme of vertical handover between WLAN and GPRS networks based on routing. In addition, it is presented a model for the handover decision, which reduces the latency time of handover procedure.

In an article by Song et al [7] it is proposed a hybrid coupling scheme to support interworking between UMTS and WLAN networks, which differentiates the data paths based on the type of the traffic. For real-time traffic a tightly coupled network architecture is chosen. For non real-time traffic the loosely coupled network architecture is chosen.

In this paper, it is presented a mechanism called *vertical handover*, which allows changing networks on mobile devices, particularly cell phones that have Wi-Fi interface. The proposed mechanism enables applications accessing the Internet on a cell phone to automatically switch between WLAN and GPRS networks without restarting the data transmission from scratch. The algorithm used in the process of searching the best Internet access network is shown in Fig. 2. If there are any available wireless networks, the one with the greatest signal strength is selected, otherwise GPRS is chosen as Internet access point. The developed handover mechanism considers 3 scenarios in which there may be a network change as shown in Fig. 3:

Network change GPRS to WLAN: The network change occurs when the signal strength of the WLAN network reaches a minimum value of -75 dBm, this value was determined by tests that were performed.

Network change WLAN to GPRS: As explained before, the minimum signal strength to establish a connection is -75 dBm, when the signal strength falls below this value is considered that the cell phone is out of range of the wireless network and the handover mechanism proceeds to close the connection and makes the switch to the GPRS network.

Network change WLAN to WLAN: When the cell phone moves away from the WLAN to which is connected, the WLAN signal will be lost eventually, when this happens the handover mechanism will change the access network to the WLAN that has the strongest signal.

3.4 Handover during file transfer.

The use of a handover mechanism for file transfer is necessary so the transfer service can properly handle the loss of the network signal in use, or availability of another network with better features. The purpose of the vertical handover module is to provide the best access network to the Internet during the file transfer. The handover module is independent of the transfer protocol, is placed in a lower layer and is responsible for providing the best available communication network. The error recovery mechanism used by the file transfer protocol is initiated in the cell phone and can resume an interrupted transfer from the point of interruption.

During a file transfer several network changes may occur, these changes however occur only under two circumstances when the signal is lost or when a better network is available, in either case the handover mechanism is invoked in the same way. When the lost of the network signal that is being used in the cellular phone is detected, the transfer protocol responds with the error recovery mechanism, this in turn invokes the handover module to provide the new best communication network. When the cell phone sets the transfer session with the server, it checks if there is any

transfer in progress reviewing the value of the variable that stores the number of last block sent, if this is different from zero means the file transfer was not completed and a RESEND_FILE command is issued. When the server receives the RESEND_FILE command, sends in response to the cellular phone the number of the last block received. When the cellular phone receives the number of last block, the file transfer is initiated from the next block. The protocol performs all these operations through a series of messages exchanged between the cell phone and the application server as shown in Fig. 4.

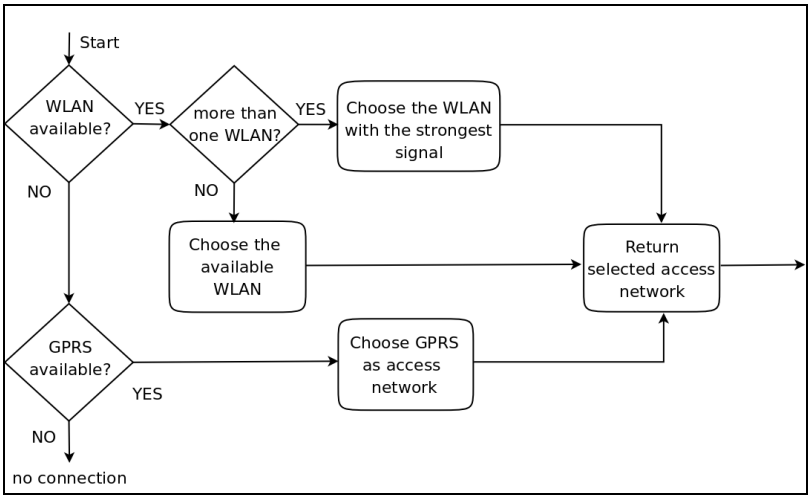

Fig. 2. Flow chart for selection of Internet access network during handover

4 Security Services

Beside the handover module, the security services module provides authentication, confidentiality and integrity services [8] to applications placed in the upper layer.

The mechanism of distribution of session keys is responsible for distributing between the client and server the session keys that are required for data encryption. In addition, the protocol for the management of session keys performs the authentication function. Under this scheme the application server acts as a distribution center of session keys and simultaneously authenticates the mobile phone at the start of a transfer session. The implemented authentication is performed only in one way, the application server authenticates the mobile phone but the cell phone does not authenticate the application server. The process of distribution of session keys assumes that both client and server share a secret key previously distributed in some way. In these implementations the life time of a session key was set in one day.

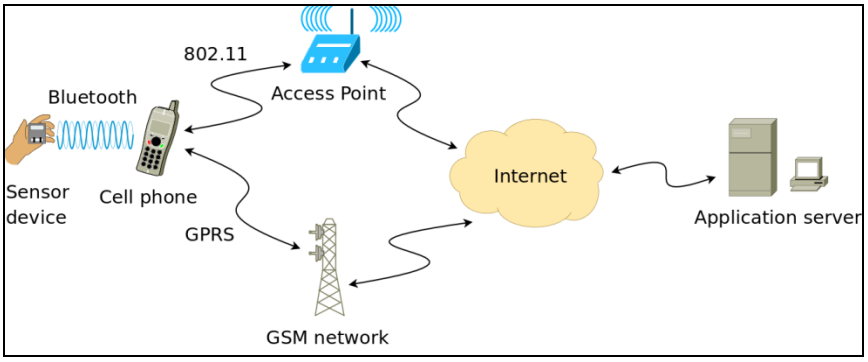

Fig. 3. Patient monitoring system scenario

Confidentiality is implemented using symmetric key cryptography. The encryption algorithm used is AES with a key of 128 bits [9]. The confidentiality service is deployed on both ends of the communication channel. However, in this application, the data only flows from the client to the server but not vice versa. Therefore the cell phone encrypts the data file before sending it to the application server using a 128 bits session key that was previously distributed during the set up of the transfer session. After the transfer of the data file is completed in the application server, the data file is decrypted using the session key to restore it to its original condition.

The integrity service is provided using the SHA-1 hash function [10]. Once the data is encrypted and transferred from the cell phone to the application server, the integrity service is implemented by calculating the SHA-1 hash function of the original data file, the digest that generates SHA-1 function is then sent to application server. In the application server, the integrity service is implemented after the data file and its corresponding digest are received from the cell phone, the data file is first decrypted and then SHA-1 function is calculated, then both digest are compared, the one that was received and the one that was calculated in the application server, if both digests are equal that means that the file was received fine, and an acknowledgment message is sent to the cell phone, if they do not match that means the file was corrupted during transfer, in this case the application server does not return any acknowledgment message and the cell phone sends the data file again.

5 Functionality testing

The client application was installed on a Nokia N91 cell phone, this cell phone has Bluetooth, GPRS and 802.11 (Wi-Fi) communication interfaces, the server application was installed on a desktop computer with Linux operating system. There were also two wireless networks available, both were registered as Internet access

points in the configuration of the cell phone. Authentication to access the wireless networks was done using MAC address filtering. Three tests were conducted to test the handover mechanism during the change of communication network, from WLAN to GPRS, from GPRS to WLAN and from WLAN to WLAN. In each test an image file in jpeg format was sent from the mobile phone to the application server.

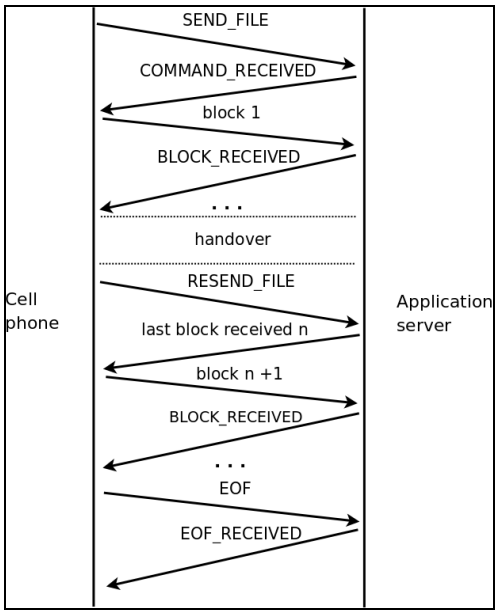

Fig. 4. Message exchange during handover

6 Performance testing

To assess the performance of vertical handover mechanism 15 tests were carried out; the performance was measured in categories such as time of handover, transfer time and file encryption and decryption time, and power consumption.

The handover time is the time it takes for the application on the mobile phone to make a change from one type of network to another. It is measured from the moment the current connection with the application server is closed until the connection is opened with the new selected network. The average times for the three possible scenarios of network change are shown in Table 2.

Table 2. Handover time in seconds

Handover type	Average time	Standard deviation
WLAN/GPRS	18.69 s	9.10 s
GPRS/WLAN	3.76 s	0.97 s
WLAN/WLAN	1.25 s	0.14 s

In the encryption tests conducted it was found that the average rate of encryption is 47.89 KB/s with a standard deviation of 1.4 KB/s, showing that the rate of encryption is kept more or less constant regardless of the size of the file being encrypted. Similar results were obtained for decryption, the decryption rate averaged 50.00 KB/s with a standard deviation of 2.29 KB/s, it was observed that the rate of decryption is slightly higher for files whose size is greater than 2 MB.

To determine the time of a file transfer and the data transfer rate when using a WLAN, six files whose sizes ranged from 128 KB to 5 MB were transferred from cell phone to the application server.

To determine the overhead imposed by security services to the file transfer it was performed the same procedure as in the previous test but the time measurements were taken considering the time involved in making the operations of authentication, file encryption and hash function calculation. The results of this test are shown in Table 3.

Table 3. File transfer times and data transfer rates using a WLAN

	128 KB	256 KB	512 KB	1 MB	3 MB	5 MB
Average transfer time in seconds	1.08	2.00	2.93	4.48	11.97	19.94
Average transfer time with security services	3.83	7.30	13.62	25.70	74.66	125.61
Overhead % due to security services	354.60	365.00	464.80	573.60	623.70	629.90

To determine the time of file transfer and the data transfer rate when using a GPRS network, six files whose sizes ranged from 4 KB to 256 KB were transferred from cell phone to the application server. The sizes of these files were smaller than those of the same test for WLAN because the nominal transfer rate of GPRS is only 150 KB/s, transferring files over 1 MB would be slow as well as costly. The average transfer times and transfer rates with and without considering the time added by the security services is shown in Table 4.

Table 4. File transfer times and data transfer rates using GPRS

	4 KB	8 KB	32 KB	64 KB	128 KB	256 KB
Average transfer time in seconds	20.74	44.41	159.58	287.8	519.42	905.65
Average transfer time with security services	21.39	44.70	163.26	288.38	519.61	921.74
Overhead % due to security services	1.03	1.01	1.02	1.00	1.00	1.01

To determine the battery life for data encryption, the battery was fully charged and then a 1 MB text file was encrypted repeatedly until the battery ran out. At the same time the percentage of battery use was recorded periodically. It was found that an average 776 MB of data can be encrypted with a fully charged battery. The process for determining the power consumption is similar for decryption. The tests showed that energy consumption is slightly higher for decryption. It was found that on average of 749 MB of data can be decrypted with a fully charged battery.

The test of power consumption of data transfer was only carried out through a WLAN because doing this test through GPRS was impossible due to economic constraints. As in previous tests the battery was fully charged and a text file of 1 MB was sent repeatedly from the cell phone to the application server until the battery ran out. It was found that an average of 580 MB of data can be transferred with a fully charged battery.

7 Conclusions

The vertical handover platform works as a separate module that can be used by any application that accesses the Internet from a cell phone. The integration of the handover platform to different applications is feasible as demonstrated by the development and implementation of the system for monitoring vital signs. However, the handover mechanism developed is suitable mainly for applications tolerant to transmission delays.

Tests showed that the handover mechanism successfully performs network changes in the three possible scenarios. This system, as demonstrated by tests, is capable of transferring information from the cell phone to the application server on scenarios of network change, ensuring the integrity and confidentiality of the information.

References

1. How americans use their cell phones, http://www.pewinternet.org/pdfs/PIP_Cell_phone_study.pdf
2. Wi-Fi component forecast and vendor share 2005, http://www.strategyanalytics.net/default.aspx?mod=ReportAbstractViewer&a0=2480
3. Smith, R.: Wi-Fi Home Networking, pp. 16--19. McGraw-Hill, (2003)

4. Salkintzis, A.K.: Interworking between WLANs and third-generation cellular data networks. Vehicular Technology Conference, 2003, 3:1802--1806, (2003).
5. Good, R., Ventura, N.: A multilayered hybrid architecture to support vertical handover between IEEE802.11 and UMTS. IWCMC 2006, pp. 257--262, (2006)
6. Rong-Hong Jan, Wen-Yueh Chiu.: An approach for seamless handoff among mobile WLAN/GPRS integrated networks. Computer Communications, 29:32--41, (2005)
7. Jee-Young Song, Hye Jeong Lee, Sun-Ho Lee, Dong-Ho Cho.: Hybrid coupling scheme for UMTS and wireless lan interworking. International Journal of Electronics Communications, 61:329--336, (2007)
8. Rodríguez-Henríquez, F., Saquib N.A., Díaz-Pérez, A., Kaya Koc, C.: Cryptographic Algorithms on Reconfigurable Hardware, pp. 8--9.wblock Springer, (2006)
9. NIST. Announcing the ADVANCED ENCRYPTION STANDARD (AES), November 2001.
10. NIST. Announcing the SECURE HASH STANDARD, August 2002
11. Apostolis K. Salkintzis. Interworking between WLANs and third-generation cellular data networks. Vehicular Technology Conference, 2003, 3:1802{1806, 2006.
12. Stallings, William.: Cryptographic and Network Security Principles and Practices, pp. 11--14,353. Prentice Hall (2005)
13. Houda Labiod, Hossam A__, and Costantino de Santis. Wi-Fi Bluetooth ZigBee and WiMax, page 104. Springer, 2007