International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 2, February, 2012

Encrypted IP Voice Call Communication on Android through Sip Server on 3G GPRS

Saruchi Kukkar
Department of CSE/IT, Lovely Professional University (India)

ABSTRACT

In today's scenario there are many voice transmission techniques available in cellular communication, but they do not allow to exchange data in a secured manner due to the challenges involved in the analog mode of communication as it is more prone to eavesdropping and noise interference.

VoIP (voice over internet protocol) is a one of the best technology available for voice communication which has the potential to completely rework the world's cellular systems. VOIP works by converting analog voice signal into digitized data but it still cannot solve the problem of security of digitized data travelling through communication links.

Using encryption techniques this digitized voice data is transformed into cipher text form on third generation GSM data or GPRS servers in android platform which results in a better encrypted voice speed and clarity.

Keywords: *Voice Over Internet Protocol, GPRS, Android, Encrypted IP voice call*

1. INTRODUCTION

Technology has improved and advanced exponentially and with it, the pros & cons have also affected. In today's era, cellular communication owns a sensitive and vital part in our lives. The security aspect in voice transmission has become important concern.

Voice calls which travel through Analog signals and use them as carrier have a very high tendency of getting eavesdropped or interfered.

1.1 Need of Secured Voice Communication

Any voice communication is threatened by 2 biggest risks. One is, when someone is listening to our conversation behind our shoulder. The other and very dangerous risk is, someone listening to it over the wire at the time when it is getting transmitted. First risk can be avoided by being agile and alert during the communication but the causes of Second risk are beyond our control because, physically we would never know who is listening to our conversation.

Secured voice communication plays a very important role in our day to day life. The need of secured voice communication can be anticipated in the following situations:-

- Sensitive situations like National defence wherein during emergency situations, secret codes like missile unlock or lock code, the army's position code are conveyed. If these codes are hacked during communication by enemy, severe, unimaginable threats can be thought for national security.

- Secured communication needed at different government or ministerial levels like budget planning, terrorists attack information and plan to avoid it etc.

- Secure communication can be thought of when there is a conversation happening between a company's top management personnel when they discuss about the profits and future plans of the company.

- When a person convey his account number, PIN number to even someone in the family. Suppose, someone listens to debit card or PIN number during the call conversation, one can imagine of serious consequences. Secured communication happens at different government or

- ministerial levels like budget planning, terrorists attack information and plan to avoid it etc

- Suppose, A calls B, the call will pass through several hops or devices before landing on the recipient's handset. If someone eavesdrop on call in any of the intermediate servers, both will never know who is doing it and where. And now-a-days, eavesdropping mechanisms are so advanced that they always snoop on the wire from where the call travels and the moment the call connects, the device catches the conversation. Such kind of devices is generally used by the anti- terrorist organizations to eavesdrop or hack terrorist communication

1.2 VOIP (Voice Over Internet Protocol)

The technique for making a phone call using the Internet is referred to as Voice over Internet Protocol (VoIP), because it uses TCP/IP for delivering voice information. The VOIP converts voice signal into digitized data and compresses it. The compressed, digitized voice signal is broken up into IP packets. The packets are sent out across the internet the same as any other IP packets, using the internet's TCP/IP protocol. The IP voice gateway takes the voice packets, combines them, uncompresses them, converts them back into original form.

1.3 Encrypted IP Voice Call

VOIP works by converting analog voice signal into digitized data packets. The packets are sent out across the internet the same way as any other IP packets, using the internet's TCP/IP protocol The Internet is a notoriously insecure network. Anything send across internet can be easily snooped upon. This is of particular concern when highly confidential information, such as corporate data and credit card numbers, is transmitted across the Internet. Another related concern is that it can be difficult to know whether the person sending the information, is really who he says is he.

Several ways have been developed to solve these problems. At the heart of them is Encryption, it is technique of altering information so to anyone other than the intended recipient it will look like meaningless garble. When the recipient gets the information, it needs to be decrypted that is, turned back into the original message by the recipient, and only by the recipient.

In the Encrypted IP voice call this digitized voice data is transformed into Ciphertext form using encryption techniques. Hence, the encrypted voice call is very secured as compared to VOIP.

1.4 GPRS

GPRS is a packet based communication service for mobile devices that allows data to be sent and received across a mobile telephone network. It is an overlay of GSM. It works for both voice and data services. It combines mobile access with internet protocol based services, using packet data transmission that makes highly efficient use of radio spectrums and enables high data speed.

It is an open mobile platform that was developed by Google. It is based on linux operating system and all of its applications written in JAVA. Android phones typically come with several built-in applications and also supports third party programs. Developers can create programs for Android SDK software development kit using java and run through Google's "Davlik" virtual machine which is optimised for mobile devices.

2. SIGNIFICANCE

- This can benefit the users to communicate with each other through digitized voice data which is free from any noise or interference in comparison to its analog variant and carries more clarity.
- The best part of this communication will be it can be done from geographically any independent location.
- It will enable the users to communicate with each other in an encrypted fashion which will enhance the security and confidentiality of the communication.
- The most significant part is it support the newest generation of the mobile handset called SmartPhones which run on an advanced hardware and latest mobile operating system from Google called Android.

3. OBJECTIVES

- Users will be able to communicate effectively, speedily and most importantly, securely, thereby enhancing the privacy and confidentiality of mobile communication.
- Implementing voice encryption on third generation GSM data or GPRS servers which would in turn result in a better encrypted voice speed and clarity.
- The configuration and usage of proxy server (SIP / Asterisk) through defining call routing and handset registration mechanisms.
- It will enable the users to communicate with each other in an encrypted fashion.

4. METHODOLOGY

4.1 Formulation of the Hypothesis

Users wish to communicate with each other in a secured fashion but the mode of communication available, does not allow them to exchange data in a secured manner due to the challenges involved in the analog mode of communication as it is more prone to eavesdropping and noise interference.

Furthermore assumption that users would be using an advanced level of mobile operating systems and third generation networks which will empower them to control the security of communication at their will.

4.2 Research Design

Research design specifies the logical structure of a research project and the plan will be followed in its execution.

Suppose A want to communicate with B through secured voice communication. A and B must have android based mobile handsets with J2ME (proposed) application installed on it which is responsible for encrypted voice communication.

- The mobile handsets need to be registered at SIP server.
- When A calls B the application installed on mobile handsets will convert it into encrypted data.
- The encrypted data will travel through GPRS channels.
- The SIP server will route the call to the registered recipient B.
- The application installed on B handset will perform the decryption process.

Step 1: Voice communication can occur in 2 ways namely:

- Wi-Fi (without the SIM card in Android handsets)
- GPRS (with SIM card in Android handsets). In the proposed work GPRS mode will be used.

Step 2: There would be 1 SIP server (Asterisk) and minimum 2 Android handsets. The handsets need to be registered at SIP server.

Step 3: The SIP server will be installed and configured on a system which will remain in an ON state and connected to the internet at all times.

Step 4: The Android application which will be developed needs to be installed on all the handsets which are registered in the SIP server and wish to communicate with each other using encrypted IP voice communication.

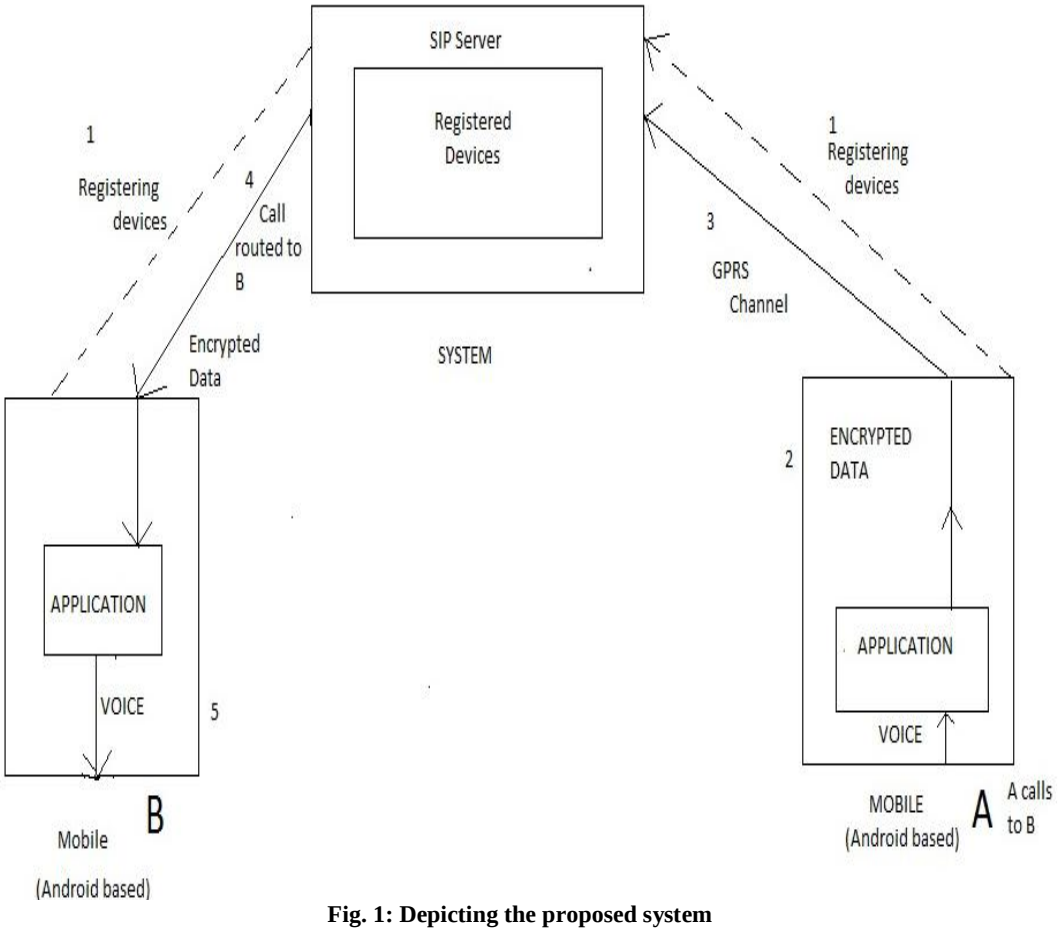

Fig. 1: Depicting the proposed system

Step 5: The dialler will launch the Android application on his/her handset and dial the receiver's number. The dialling interface will be developed for the Android application. Once the call is made, the request will go the SIP server wherein the recipient's number will be checked and the call will be routed on its handset.

Step 6: Once the recipient receives the call through the same Android application and the dialler starts the conversation, all the digitized voice data will first be encrypted on the dialler's handset by the application and then sent to the SIP server for routing to the

recipient's handset. Logically, every handset will be assigned a numeric no. in the SIP server during configuration through which it will become identifiable.

Step 7: Once the recipient receives the call through the same Android application and the dialler starts the conversation, all the digitized voice data will first be encrypted on the dialler's handset by the application and then sent to the SIP server for routing to the recipient's handset. Logically, every handset will be assigned a numeric no. in the SIP server during configuration through which it will become identifiable.

Step 8: The digitized voice data will travel in an encrypted fashion through the GPRS medium. The Android application will also have the capability that the recipient's may turn ON/OFF the decryption feature. That is to say, if the recipient turns ON the decryption feature, he will listen to the original, decrypted voice. Else, the encrypted thing which could be a beep, non-understandable words, silence etc.

4.3 Tools

4.3.1 Android 2.2 SDK

It is an open mobile platform that was developed by Google. It is based on linux operating system and all of its applications written in JAVA.

4.3.2 J2ME

Stands for Java 2, Micro Edition. It is a version of java used for developing applications for the devices which have limited processing power in storage capabilities like Mobile Phones, Wireless Devices, Pagers.

4.3.3 SIP SERVER (Configuration)

It will be installed and configured on a system which will remain in an ON state and connected to internet at all times. It is basically call router/ switcher from one android device to another. During the configuration of SIP server, mobile handsets have to be registered.

4.3.4 Android 2.2 Based Mobile Handsets Connected through GPRS

4.4 Analysis

- In the proposed work, GPRS mode is used. It is feasible to use this mode for voice encryption because voice is digitized and can travel through data channels.
- Voice Encryption is feasible as voice is converted into data packets and then any Encryption algorithm used for data can be applied for voice.
- The Android application which is need to be installed on mobile handsets can be developed using J2ME

REFERENCES

[1] Nor Shahinoza kamal Basah Ivar Jorstad, Do van Thuan Tore Jonvik & Do van Thanh (2011), "A mobile service Architecture for improving Availability and Continuity", IEEE.

[2] Ahmad Ali Habeeb, Mohammed A Qadeer and Shashir Ahmad (2007),"Voice communication over GGSN, SGSN, IEEE.

[3] Angelos D. Keromytis (2011)," A Comprehensive Survey of Voice over IP Security Research", IEEE

[4] Roy Chaoming Hsu, Cheng-Ting Liu, Wen-Ping Huang, Jun-Jay Yang, "An Embedded Software Approach for the Development of SIP-Based VoIP Server", Proceedings of the 11th Asia-Pacific Software Engineering Conference.

[5] Tuneesh, Lella and, Ricard (2007),''Privacy Of Encrypted Voice-Over-IP",IEEE

[6] Mohammed A Qadeer, Robin Kasana and Sarvat Sayeed (2009)", Encrypted Voice Calls with IP enabled Wireless Phones over GSM CDMA /WI-FI Networks", International Conference on computer engineering and Technology

[7] Chia –Hui Wang, Mei-Wen Li, and Wanjiun Lian (2003)," A Distributed Key-Chnaging Mechanism for Secure Voice over IP (VOIP) SERVICE ", IEEE.

[8] Kaldan R, Meirick I and Meyer M(2002), "wireless Internet access based on GPRS", IEEE

[9] Phone Lin Yi-Bing Lince (2001),"Channel allocation for GPRS", IEEE.

[10] Goode, AT&T Labs and Weston (2002), "Voice Over Internet Protocol ",IEEE

[11] Stallings W (2007),"Network Security and Cryptography, Pearson Education", New Delhi.

[12] Theodere D. Rappaport (2008),"Wireless and mobile Communication", Pearson Education", New Delhi

[13] Emmanuel Seurre, Patrick Savelli, Pierre-Jean Pietri(2003), "GPRS for mobile Internet", Artech House