Voice over Wireless LAN and analysis of MiniSIP as an 802.11 Phone

Khurram Jahangir Khan <iw02_jkh@it.kth.se>
Ming-Shuang Lang <lang_esther@hotmail.com>
Royal Institute of Technology (KTH)

Report submitted for course 2G1325 Practical Voice over IP (VoIP): SIP and related protocols
29th June, 2004

Contribution:
Section 1-3: Ming-Shuang Lang
Section 4-5: Khurram Jahangir Khan
Abstract and Section 6-8: Together

Abstract

Voice over IP over Wireless LAN (VoWLAN) is getting great attention from the industry and the products for VoWLAN deployment are emerging rapidly. Although technologies for carrying voice in IP networks have been advancing for years, carrying voice over wireless networks introduces new challenges. For end users, the performance of VoWLAN phones (802.11 phones) are of great importance. The purpose of this document is to discuss the general issues in Voice over WLAN and to compare the features and functions of the 802.11 phones available in the market today. Reasons causing the degradation in performance of 802.11 phones have also been discussed briefly. To understand these issues, tests were conducted to use MiniSIP (A SIP based soft phone developed at KTH and provide enhanced security features based on MIKEY and SRTP) as an 802.11 phone and the analysis of the results of the testing is described in detail towards the end of the paper.

Keywords

VoIP, WLAN, 802.11 phones, SIP, MiniSIP, Handoff, Access Points, MIKEY, TLS, RTP

Acknowledgement

We would like to express our sincere appreciation here to:

Professor G. Q. Maguire Jr., who guided us throughout the effort and gave us very useful ideas from time to time.

Johan Bilien, who contributed so much time in helping us with MiniSIP compilation and other difficulties we encountered with Linux.

Erik Eliasson, who developed MiniSIP at KTH, and this gave us opportunity to work

The many People in TS Lab, who kindly provided us with the equipment we needed and cared about our progress.

Table of Content

1. Introduction

Voice over IP (VoIP) introduces voice into the packet switching world, which brings the convergence of packet and circuit networks. Today with VoIP, we can make economical long distance calls. Wireless Local Area Network (WLAN) gives freedom to the people from the wired network connections and hence users now can enjoy greater mobility. Recently, many people begun to show interests in delivering voice over WLAN, which promises further mobility to users. Years of experience with wireless LAN has made this technology quite mature. However, the introduction of voice into WLAN has brought new challenges. The WLAN industry is working hard to enable 802.11-based networks to accommodate the technical characteristics of VoIP.

VoIP over WLAN (VoWLAN) as technology enables IP voice to be sent over an (802.11) WLAN. New types of devices, such as various 802.11 phones have emerged. With the proliferation of both VoIP and WLANs, we are going to see more products of this type and it is predicted that this technology will be widely deployed in enterprises as well as in homes.

In this paper, we will first give some background about the development of VoIP and VoWLAN. Then we will discuss the features and performance of 802.11 phones. In order to understand our testing and results, some background knowledge about SIP and MiniSIP is also addressed. Following this a description of how we carried out our testing with MiniSIP and the results are analyzed. Finally, we present our conclusions and our suggestions for future work.

2. Voice in an IP World

The packet switching technology that is widely used for data communication was not designed for real time content delivery, e.g. voice. But packet switching has advantages over circuit switching as is used by normal voice systems, such as the PSTN (Public Switching Telephone System). In circuit switching, a ‘circuit’ is maintained for the whole duration of the conversation, thus, a large part of the telephone network resource is wasted at any given time. In contrast, using data networks to deliver voice not only avoids the need for two separate systems for data and voice, but also makes better use of the network’s resources. For these reasons, VoIP was introduced and has gained great popularity.

2.1. VoIP

Many companies now use VoIP in their IP data networks. It often works with a help of an IP PBX (Private Branch eXchange), which translates between data and analog telephones. In order to send voice via IP networks, the H.323 protocol was developed by ITU (International Telecommunications Union). H.323 is actually a suite of protocols that provides specifications

for real time, interactive videoconferencing, data sharings and audio applications (see Table 2.1). A full implementation of H.323 requires a lot of overhead and with increasing network resources has some unneeded functions. Meanwhile, IETF (Internet Engineering Task Force) developed the Session Initiation Protocol (SIP) for IP telephony. SIP is a more streamlined application layer protocol. It takes advantage of existing protocols to process VoIP. Compared with H.323, it's smaller yet efficient. SIP is described further in section 4 of this document.

Video	Audio	Data	Transport
H.261	G.711	T.122	H.225
H.263	G.722	T.124	H.235
	G.723.1	T.125	H.245
	G.728	T.126	H.450.1
	G.729	T.127	H.450.2
			H.450.3
			RTP
			X.224.0

Table 2.1: H.323 Protocol Suite

VoIP not only provides the same voice functions as traditional telephone systems, but operates over IP networks; it also adds new voice communications services. For example, 'follow me' services enable a user to have his phone calls find him regardless of his location. With increasing VoIP deployment, the benefits are obvious. VOIP leverages existing data networks, saving the cost of building and operating a separate voice network. Voice traffic can often run on the data networks "for free", i.e. at zero incremental cost. It also saves significantly on long distance calls by routing VoIP calls through data networks. VoIP can provide more flexibility in operations and new services. It can also enhance productivity by allowing integrated voice.

2.2. Voice over IP over WLAN (VoWLAN)

VoIP over WLAN refers to the provisioning of IP voice services across wireless LANs, usually 802.11-based (also known as voice over Wi-Fi). A VoWLAN system works by translating a (PBX) telephone call to IP packets and sends these IP packets over an 802.11 WLAN. 802.11 phones or softphones[4] will reassemble those packets and output the audio to the user. The reverse path is similar, but without the synchronous timing of a telephone network.

[4] Software based IP phones are usually installed on a PC, giving the PC a full range of phone capabilities, including call forwarding, conference callings, and integration with Microsoft Outlook for automatic phone dialing. Softphones may work alone or in conjunction with an IP PBX.

This technology can bring people many benefits. It has all the advantages of VoIP systems along with greater mobility. Mobility usually means increased productivity since it also reduces the cost for deployment of wired phones.

Just as when introducing voice to IP networks, VoWLAN has the same problems as VoIP regarding deployment. Some characteristics of wireless networks cause additional difficulties. Generally speaking, there are several major issues need to be solved before this technology will be fully accepted.

(1) Latency-induced VoIP performance degradation as users roam. This latency is usually caused by re-authentication required when associating with a new access point. ITU recommends that the total latency in a voice call should not exceed 150 milliseconds. In VoWLAN practice, it's agreed that the delay of roaming and authentication needs to be kept under 50 milliseconds. 802.11r working group has been founded to address fast roaming among access points.

Some vendors have made some progress in keeping such delay low. For example, Aruba Wireless Networks announced its new secure voice module for its AirOS WLAN switch, which centralizes state information about each user. It eliminates the need for access points to talk to one another but at the cost of using the central Aruba switch. It keeps inter-AP (Access Point) handoff times to 10 milliseconds. Inter-switch communications is via the Mobile IP protocol and their handoff delay is only 20 milliseconds.

(2) Lack of QoS (Quality of Service) mechanisms. In order to keep the real time features of voice traffic, voice packets should be assigned higher priority then normal data packets to maintain the quality of voice. In this sense, QoS is needed. Currently, there is no standard way of doing this. However, IEEE (Institute of Electrical and Electronics Engineers) is developing a QoS standard called 802.11e and it's expected to be finalized this year. There are two intermediate standards for QoS developed by vendors. One is the SpectraLink Voice Priority Protocol (SVP) [25, 26] from SpectraLink. It's an open standard for 802.11b networks. The other is from Symbol Technologies [25]. Many other vendors in the industry support these two standards.

In 802.11e, two different types of QoS are provided. One is prioritized QoS, which uses priority tagging to place different types of traffic in different queues. Although voice gets priority treatment, it cannot get a reserved bandwidth as it is not guaranteed that low priority frames will always wait until all higher priority frames are transmitted, so in order to provide better service to streams with higher priority, a reserved bandwidth may be helpful.

The other one is called parameterized QoS, which effectively reserves a certain amount of bandwidth for a certain stream [1].

(3) Today, VoIP handsets have less security than other data devices. This may leave the network vulnerable to potential spoofing.
Security measures for data may introduce more latency than voice can tolerate, so a special mechanism for voice should be developed. These can be achieved either on application layer through SRTP and MIKEY (see section 5) or on the data link layer with 802.11i. 802.11i is a task group that aims to enhance security that is stronger and better suited to wireless voice. 802.11i developed algorithms for confidentiality, data integrity, and data source authentication. It also includes a protocol for mutual authentication and key management [1].

(4) Limited number of voice calls. Because of the capability of access points for handling calls simultaneously, the number of calls is limited. Currently, when the number of calls reach 30, an access point becomes overloaded, thus the quality degrades. With 802.11a, 802.11g and 802.11h standards coming into the picture, this problem will be solved to some extent.

(5) Rapid drain of handset battery. Current wireless IP phone products usually have 20 hours stand-by battery duration and several hours' talk time (see Table 3.1: Summary Data Sheet of Several 802.11 Phone Products). To achieve true mobility, low power is one of the key point, since users expects long battery life. This should be improved in the future by adding sleep mode to the 802.11 phones. Moreover, low power required low power consumption of each component of a phone, so power saving may involve carefully design of every part.

(6) Insufficient support for video on WLANs. Most products today support only 802.11b WLAN (see section 3, 802.11 Phones). 802.11b's 11Mbps data rate translates into 4-5 Mbps of real throughput. Video requires lots of bandwidth, usually between 128kbps to 2 Mbps [27], so video now is still restricted on WLANs. On an 802.11a WLAN, the 54 Mbps data rate translates into 20Mbps to 25Mbps of real throughput and even this may not be enough when many users share the bandwidth. Many WLAN vendors are developing solutions to support IP Multicast on the WLAN through QoS to improve this.

Although VoWLAN has these problems, it has bright future. As a survey of 358 businesses by IDC[5] this March, 10% of users with WLAN infrastructures are running some voice over them, and another 50% say they are considering it while this may indicate potential interest in pre-

[5] www.idc.com

standard solutions [2]. VoWLAN would appear to have broad market. Currently, it's mainly deployed in vertical markets, such as health care, education, manufacturing, distribution and retail. With the decreasing of cost for deployment and the introduction of new products and services, VoWLAN will surely be accepted more widely.

3. 802.11 Phones

802.11 phones fall into two major types: hard phones and soft phones. Hard phones look exactly like mobile phones, but give you connectivity to WLAN with VoIP capability. Major manufacturers include Cisco, SpectraLink, Symbol Technologies, etc. Wireless softphones are software that is installed on PCs (Personal Computer), laptops, PDAs (Personal Digital Assistant), or other devices for voice communication in wireless LAN environments.

The basic components of a WLAN IP phone [8]: Usually, the digital signal processor (DSP) is the heart of a newer WLAN IP phone unit. It is responsible for the voice-over-packet (VoP) processing functions. It is used for low-bit-rate codecs, such as G.729 and G.723, as well as for echo cancellation and tone generation. A CPU (Central Processing Unit) is used for control and signaling. Supplementary services such as call-hold, mute, call-transfers and conferencing are also provided via this microprocessor. A wireless LAN module offers support for the various versions of 802.11, often including a, b, and g, and QoS via wireless multimedia extensions and 802.11e.

Table 3.1 lists products from major manufacturers. Molta, et al. [9] report on their testing and comparison of the performance of different products.

Manufacturer	Cisco	SpectraLink	Symbol Tech.	TeleSym	Vocera
Model	Wireless IP phone 7920	NetLink	NetVision	SymPhone (softphone)	Wireless communications badge
Target Market	Enterprise, work in conjunction with Cisco Call Manager and APs	Office (e340); Harsh environments. (i640)	Enterprise	Enterprise	Health care
Call control protocol	Cisco Skinny Client Control Protocol; Cisco Survivable Remote Site Telephony (SRST) V2.0+	H.323; Cisco Skinny Client Control Protocol (SCCP)	H.323 v2, optional: SCCP, MiNET, Nortel's voice-over-IP	SIP, H.323	
Codecs	G.711a, G.711u, G.729a	G.711, G.729ab	G.711, G.729a		
Wireless access protocol	802.11b	802.11b	802.11b	802.11b	802.11b
Network Features	Cisco Discovery Protocol, auto VLAN configuration, SNMP, DHCP	DHCP, SNMP	DHCP		

RF Channels	Up to 14		3-11		11
Frequency range	2.4-2.497 GHz	2.4-2.4835 GHz	2.4-2.486 GHz		2.4-2.4834 GHz
Coverage	15-300m indoors		75.5m indoors, 300m outdoors		
Security	Cisco LEAP, IEEE 802.1x, WEP 40/128 bit	WEP 40/128 bit, Cisco Fast Secure Roaming	WEP 40/128 bit, Kerberos V5		WEP 64/128 bit, CKIP; Cisco LEAP
QoS	SCCP and VLAN	SpectraLink Voice Priority (SVP)			
Battery Life	1440mA Li-ion: 3.5 talk time, 21hr standby; 1960mA Li-ion battery: 4.25 hr talk time, 30 hr standby	4hr talk time, 80hr standby	7.2v 800mA Li-ion: 3hr talk time, 20 hr standby	N/A	660mA Li-ion: 2hr talk time, 44hr standby; 800mA LI-ion: 2.5 hr, 53 hr
Output Power (peak)	100mW	100mW	60mW		75mW-100mW
Weight	135 grams	E340: 117 grams; i640 168 grams	154 grams		< 56 grams
SW update	TFTP	TFTP			
Price[6]	$595	e340: $399 i640: $599	$580		

Table 3.1: Summary Data Sheet of Several 802.11 Phone Products

From Table 3.1, we notice:

- All products run over 802.11b, but no product supports 802.11a/g yet. This may restrict deployment of services such as streaming video.
- Interoperability is a problem too, since some vendors adopted proprietary solutions. For example, Cisco phones are only compatible with their own access points. Another example is proprietary QoS solutions, such as SVP mentioned above. However, Cisco has taken a step forward by supporting 802.11e pre-standard in its products.
- Prices are still high. This restricts wireless IP phones to enterprises. Additionally an enterprise will only be willingly to adopt wireless IP phones when there is great need for them. For example, mobile phones are forbidden in some environments, such as some parts of a hospital. Note that low cost phones do not mean a low cost VoIP system. It's also dependent on voice servers and gateways.
- SIP is not supported by all these products, even it's been especially developed for voice calls setup in IP networks.

[6] Prices here are taken from [9].

- Easy to use/configure. Most products have a friendly user interface, which helps to configure phones. For firmware updates, TFTP (Trivial File Transfer Protocol) is often used and the process is automatic.
- Battery life is similar for all the products. It's much shorter compared with mobile phones, especially the standby hours. All components need to be optimized for low power consumption, because it directly affects talk time and standby time. At the moment the phones lack a sleep mode, so they drain batteries quickly. Meru Networks announced its sleep-mode drivers this March, which can double the talk time [10].
- Market focuses on enterprises. Market penetration has begun with vertical markets, specifically: health care, education, distribution, and retail.

Reliability is an important quality of a phone, yet it's hard to evaluate. We have no access to these products in market. For an evaluation of these products, see [9]. In our tests, we installed a softphone called MiniSIP (see section 6, MiniSIP) on our laptops. With the SIP server in our department, we then tried to call from the laptops connected to the WLAN in Forum building (see section 7.3 Testing Scenarios). From the testing, we tried to collect data for basic analysis such like delay and packet loss. We felt the performance is quite good. The delay is imperceptible except a handoff occurred (see section 7.4).

One feature vendors are working on is to have wireless IP phones also support cellular wireless technologies, such as CDMA (Code-Division Multiple Access) and GPRS (General Packet Radio Service). The goal and benefit are easy to see. Users can use a single phone to get both wireless VoIP service and cellular service. A handoff between cellular and WLAN occurs when users leave the coverage of cells or access points. This idea is very appealing, because the cost of handling calls placed from a given area using WLAN is a tenth the cost of using cellular [11]. Besides, we have all experienced the degradation of a cellular call inside a building. Thus WLAN can be used to improve cellular coverage inside buildings.

As to the services a wireless IP phone can provide, they are nearly all those you would expect from a mobile phone plus some additional networking capabilities; peer-to-peer dialing, speed dialing, pre-dialing, call conference, authentication, DHCP, RF & Battery level indication, local phone book, selectable ring melodies, call hold, call waiting, call transfer, call forwarding, call mute, redial, key lock, etc. One service that needs to be improved is the advanced location service for use with services such as E911.

We believe more companies will adapt to VoWLAN in the years ahead. First, because the advances in VoWLAN technology will improve the performance of the entire VoWLAN systems; second, more and more WLANs will be designed with carrying voice traffic in mind, which will push VoWLAN products to wider acceptance; third, more vendors will introduce the products, so that prices will be lower. In the following sections, we will introduce our testing of

MiniSIP. In order to understand the testing, basic knowledge of SIP and MiniSIP are covered first.

4. SIP

As we discussed earlier in section 2.1, for voice traffic to be carried over an IP network, there are two major call control protocols, H.323 and SIP. In this section we will introduce the reader to SIP in some more detail.

SIP is an application layer signaling protocol for session establishment developed by the IETF and defined in RFC 3261 [3]. The main functions of this protocol are to establish a session, modifying the session, and terminate it when the call is to be finished [3]. The sessions can be established with single or multiple participants. SIP is a simple text based protocol similar to HTTP (Hyper Text Transfer Protocol) and follows the client-server architecture. The transport protocol for SIP can be Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) or Stream Control Transmission Protocol (SCTP). Because of its simplicity, it is scalable in terms of the number of sessions and compatible with different protocol architectures. These are the reasons that SIP is becoming the industry standard for Voice over IP applications and products.

According to RFC 3261 [3], there are five types of services that SIP offers,

User Location	To find the location of the end system for communication.
User Availability	To find if the called party is willing to communicate.
User Capabilities	To negotiate and determine the media capabilities, e.g. a voice codec that is supported by both calling party and the called party.
Call (session) Setup	Ringing and establishing call parameters at both called and calling party.
Session Management	The transfer and termination of the calls.

4.1. SIP Components

SIP basically has two components [4, 5],

1. SIP User Agents
2. SIP Network Servers

The User agent is the component in the end system and consists of two parts:

(a) The client element called User Agent Client (UAC) used for call initiation;

(b) The server element called the User Agent Server (UAS) that is used to answer calls.

The SIP servers' functions include resolving the name and providing user locations, as end users usually don't know the IP address or the hostname of the called party. Following are several examples of SIP servers:

Registrar server The registrar server receives Register requests from the users. The Register request associates the user's SIP address called a SIP URI (Uniform Resource Identifier) with the current machine where they are located. This association is stored by the Registrar in the Location Service (LS).

Proxy Server Users send their SIP requests to the Proxy Server, which forwards the requests to the next hop proxy server or to a proxy server close to the called user. The proxy server can also modify and add information in some parts of the SIP requests if required. A Domain Name System (DNS) Server can be used to find the location of the Proxy server.

Redirect Server The Redirect server receives the request from the clients, but unlike Proxy Servers, it does not forward the request to another server or the user. Rather, it sends back a response to the calling user with the information about the destination.

4.2. SIP Addresses

SIP users are recognized by SIP addresses called a SIP URI. The SIP URI looks like an email address i.e. username@somedomain where the first part is the username or a phone number and the second part is the domain name or the network address [6]. An example of a SIP address would be "sip:khurram@ssvl.kth.se" where khurram is the username and ssvl.kth.se is the domain name. SIPS is the secure SIP URI introduced in RFC 3261 [3] and it requires that a secure mechanism is used between the user agent and the domain the user is contacting.

4.3. Session Description Protocol (SDP)

SIP is not meant to provide services and it should be used with other protocols for providing the services and media related information e.g. the types of codecs, and other media parameters. For this purpose, SIP uses Session Description Protocol (SDP) [7], which conveys the information about media streams in multimedia sessions. The media related information such as type of media (video or voice) and type of codecs, etc. is transmitted in a simple textual format called the SDP body and is added to the SIP INVITE messages when a call is initiated. This informs the called party about the session parameters acceptable by the calling party. Adding the SDP body to the SIP INVITE message avoids generating

unnecessary traffic and reduces the call setup time. The reply from the called party describes their session related capabilities [7].

5. Security in SIP

As we can see from the introduction above, an IP network might not be reliable for voice calls. In case of a circuit switched network, there is a dedicated path and all the voice traffic goes via that path for the duration of the call. So there are fewer chances that the traffic will be interrupted on the way or that someone will eavesdrop the call. On the other hand, if the voice traffic is going over a packet switched networks, the traffic travels in the forms of packets and they can take different paths to reach the destination. On the way, the traffic can pass through many gateways over which the sender or receiver has no control and it is quite possible that someone is listening to the traffic and recording the voice. (This is actually not quite different from today's voice networks which use fibers, switches etc. belonging to others.) This makes packet switched networks for voice traffic more vulnerable and less secure. As mentioned earlier, SIP is especially designed for voice on IP networks, so it is important that SIP provides some level of security.

There are two important points here. Firstly, as SIP is a signaling protocol for VoIP and it carries the information about the identities of the called user, the list of the calls, etc. and it is possible that a user does not want this information to be disclosed to a third party, there must be some way to protect the SIP messages from being intercepted and decoded on the way to the destination. The second and more important issue is to protect the actual voice traffic from being tapped by an unwanted person or machine [15]. To overcome these two issues, SIP messages as well as the RTP (Real Time Protocol) data, i.e. voice content should both be encrypted and secured from end-to-end. The encryption of RTP traffic can be done either on Application layer using Secure Real time Transport Protocol (SRTP) [16] as well as on the network layer using Encapsulated Security Payload (IP ESP) [15, 17]. At the same time keeping the SIP messages and the media information both private and intact is very important [18].

Authentication is another very important factor in SIP. The user should be authenticated before being registered by Registrar Server, e.g. Registrar should make sure that the user who is registering as khurram@ssvl.kth.se is actually the user named khurram and not someone else. Additionally, the authentication between client and server should be mutual. Thus, a user should be able to authenticate the Registrar. This will prevent registering with a fake registrar. Moreover, before sending the INVITE message to a SIP Proxy server, the Proxy server should require the user agent to be authenticated and the user agent can also ask the Proxy server to authenticate itself to the user [15, 18].

There are other Security issues in SIP as well, for example to reduce the risk of a Denial of Service (DOS) attack. If a Proxy server faces a DOS attack, it could become unavailable for the legitimate SIP clients [18].

We have discussed some of the security threats and how SIP can handle these concerns. But it is very important to note that if the SIP client is using a wireless network, then the security concerns are even greater. As in this case, the attacker does not need physical access to the network and the traffic can be sniffed in the air between the user and the Access Point.

6. MiniSIP

MiniSIP[7] is a SIP user agent which is developed by Erik Eliasson at KTH, Stockholm, Sweden. It is a SIP based soft phone, which works under LINUX. MiniSIP can work both on the iPAQ (tested on an HP iPAQ h5550 PDA [15]) and on a workstation/laptop running Linux. MiniSIP can be installed on an iPAQ running LINUX with Wi-Fi support and can be used as an 802.11 phone. MiniSIP also supports multiple CODECs and this feature makes it very useful for both high and low quality connectivity. This paper describes in Section 7 how tests were performed to evaluate the performance of MiniSIP as an 802.11 phone.

The security features in MiniSIP were added by using MIKEY (Multimedia Internet KEYing) as the key management protocol by Johan Bilien [15] and SRTP implemented by Israel M. Abad Caballero [19].

Let us have a closer look at the security features added by these. In MiniSIP, Mutual Authentication between the users is provided by the MIKEY support with the help of a key exchange. This key management is added to the INVITE message. The authentication of the user to the Registrar Server and by the Registrar to the user utilizes Transport Layer Security (TLS). One way this can be done is if the Registrar Server has a certificate installed on it and is presents this certificate to a user; the user verifies it through some Certificate Authority; once this is done, the user has to authenticate itself to the Registrar and this can be done with the help of a username and password. This TLS support in MiniSIP is possible only if the Registrar Server also supports TLS. The same method can provide authentication of a user to a Proxy Server and the other way, again if the Proxy Server has TLS support. This has not been tested by use. Hop by hop authentication between the Proxy Servers is also possible through TLS.

Another security measure that is provided by MiniSIP is securing the SIP messages themselves as a user might not want this information to be disclosed to others. This feature is

[7] http://www.minisip.org/

also achieved with TLS using Public Key Infrastructure (PKI). Encryption for the media information is provided in MiniSIP by SRTP. In this case, MIKEY provides the key for SRTP.

7. Testing

One of the main goals of this study was to perform some tests on MiniSIP and to evaluate its performance as a SIP phone. In this chapter we will describe the different test scenarios and explain to the reader how testing was performed and what parameters were used to evaluate its performance.

7.1. Resources

We used two MiniSIP clients in our testing. The first client machine form now onwards will be referred to as “Host A” had the following specifications:

Dell D600 Laptop with Pentium M 1.4 GHz with 256 MB Ram
Operating System: RedHat Linux 9.0
MiniSIP Version 0.1 with LibMIKEY Support
WLAN Card: Orinoco Silver WLAN card

The other Minisip Client Machine from now onwards will be referred to as “Host B” had the following specifications:

Dell C600 Laptop with Pentium lll 750 MHz Processor, 128 MB Ram
Operating System: RedHat Linux 9.0
MiniSIP Version 0.1 with LibMIKEY Support
WLAN Card: Orinoco Silver WLAN card

We used Labtec Axis 712 USB headsets with a built-in microphone for generating the voice and listening to it.

The following SIP addresses were used to conduct the testing on MiniSIP clients.
Host A: kj@ssvl.kth.se
Host B: khurram@ssvl.kth.se

The address for the Proxy Server was “sip.ssvl.kth.se”.

Wireless Network: The tests were conducted on Stockholmopen.net’s [20] Public Access Points which is an Operator Neutral network in the Forum Building at IT-University at Kista, Stockholm.

Wired Network: A hub with 10Mbps Ethernet ports was used for monitoring the traffic on the wired Network. The main reason for using the hub was to replicate all the traffic on all the

ports for capturing and monitoring. This hub was connected to the wired Network of IT-University on the 8th floor of Forum Building at IT-University, Kista.

Voice Traffic: It is important to note that calls were generated from both sides on a random basis and music was played mostly from one side (as usually one person speaks at a given time during a phone conversation).

7.2. Monitoring

There were two types of monitoring that were done during the tests.

7.2.1. RTP Traffic

We used Ethereal 0.10.4 [21] on a laptop running in Microsoft Windows 2000 as the monitoring tool. We used the analysis tools provided with ethereal to analyze data. During our testing, we captured only UDP packets, because the RTP packets we were interested in are carried by UDP. We set the filter before capturing as:

udp port 32776 and port 1045

The port numbers are chosen randomly by the MiniSIP at the beginning and will be incremented by 1 with each call if MiniSIP is not restarted.

When capture stops, we decode all these UDP packets as RTP. Then by choosing Statistics->RTP->Show All Streams, we usually could see the two streams for the call. Choosing one stream and clicking Analyse, shows the delay and jitter between two consecutive packets. Note that the delay given here is not the time a packet spent in the air, but rather the difference between arrival times [24]. The jitter calculation in ethereal follows the RFC standard for RTP. The Analysis also summarizes “maximum delay”, “total packets received”, “number of lost packets”, “loss rate” and “sequence errors”. As the “average delay” and “average jitter” were of interest, we saved the Stream Analysis as .csv files and then open with Microsoft Excel and used the “AVERAGE” function to calculate average values.

7.2.2. Observing Hand-Offs on Wireless Network

To find out the effect of handoffs for a roaming MiniSIP client, we followed an unusual method explained in the following section. Please note that the handoff results in the analysis are with reference to Host A which was moved back and forth between two AP. In some cases, Host B was also moved but no handoffs results were found out for that.

For our handoff experiments, the mobile MiniSIP client (i.e. Host A) was moved between two Access Points i.e. AP-1 and AP-2. NetStumbler 0.4.0 [22] was used to find out the channel number for the two Access Points. After finding out the channel numbers for the two APs, two

monitoring stations Monitor-1 and Monitor-2 running AiroPeek Version 2.0 [23] were setup. The machine Monitor-1 was configured to scan the channel using AiroPeek where AP-1 was working and Monitor-2 was configured to scan the channel in which AP-2 was working. In the AiroPeek software, two different filters were setup. The first filter was set up to make sure that the two monitoring machines accepted traffic only from the roaming MiniSIP user (i.e. Host A); this was achieved by configuring a filter to receive only that traffic which has a source MAC address of the MAC address of Host A. The second filter has been configured to receive only the "802.11 reassociation request" packets. Now consider the scenario when Host A moves from the AP-1 to AP-2, as soon as it leaves the coverage area of AP-1 and starts entering the service area of AP-2, it will send a reassociation request packet to associate with AP-2 and this is the approximate time when the handoff will occur. The average time for the handoff that was found in our tests was in the range of 150 msec to 500 msec depending on the load on the wireless network. While estimating the number of packets dropped due to a handoff, the handoff interval was assumed to be up to 1000 msec. It was quite possible that by following this method of finding handoff events, we might or might not find the correct time when the handoff exactly occurred; so this assumption was made. Moreover, it was noticed that in some cases, many packets were dropped either 500 to 700 msec before or after the re-association request packet was sent.

7.3. Testing Scenarios and Results

Tests were conducted for three different scenarios as described below.

1. Host A on the wireless network and Host B on the wired network
2. Host A and B both on the wireless network
    a. Host A roaming and Host B stationary
    b. Both Host A and Host B roaming
3. Host A and B both on the wired network

For each Scenario, two different types of calls were made,

1. Three Insecure Calls in which MiniSIP did not offer any security or encryption.
2. Three Secure Calls in which MiniSIP offered Security using a Pre Shared Key which was already defined in both the MiniSIP clients.

Thus a total of 6 calls was made for each scenario (the number of calls varied in few cases for some experiments).

The average duration of the calls was approximate 3 minutes. Initially it was decided to make calls with 3 different durations (3 minutes, 5 minutes and 10 minutes) but due to practical problems that we faced and a shortage of time, the call duration was kept to 3 minutes. The

calls were made both during the busy hours when there are many users on the network as well as late in the evenings.

In the following sections, we will explain each scenario, then the test results for each will be discussed.

7.3.1. Host A on Wireless Network and Host B on Wired Network

In the first scenario, Host A was connected to WLAN and Host B was attached to the wired network as shown in Figure 7.1. Host A roamed between two Access Points and the time at which handoff occurred was found out using the method described in section 7.2.2. It can be seen from Figure 7.1, that two monitoring Machines are being used with each scanning in a different channel (according to the channel of the respective AP). On the wired network, a third monitoring station running Ethereal was used to monitor the RTP traffic.

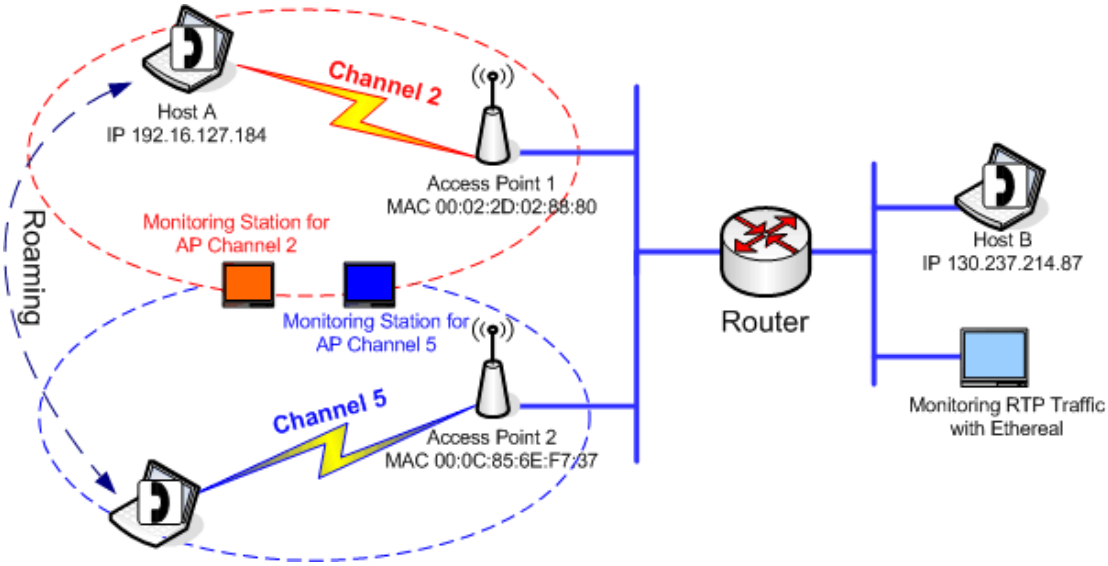

Figure 7.1: Hybrid Scenario, Host A roaming on wireless network, Host B on wired network

In the above figure, channel 2 is shown in red color and channel 5 is shown in blue color and the 2 monitoring machines have the matching colors. Moreover, the coverage area of the two APs is also shown according to the color of channel in which they are working. Please note that Host A and Host B were in different IP sub-networks, so they were connected through a router. Following is the analysis of the calls with details.

Insecure calls

A total of 4 calls were made for this scenario and the results of these calls are shown below.

Date: 6/3/2004 **Location:** Forum 6th floor, IT-University												
AP1: 00:02:2D:02:89:37 **AP2:** 00:02:2D:02:88:80 **Roaming Node A**: 192.16.127.237 **Fixed node B**: 130.237.214.87												
Call No.	**Start Time**	**Duration** (Sec)	**Total Packets Expected**	**Total Pckts Lost**	**Total Packets Received**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Avg. Jitter** (Sec)	**Handoffs**	**Packet lost of Handoff**
1	15:24:01	438	21849	113	21205	0.517	77	0.0207	1.0436	0.0018	6	3
2	16:10:26	359	17561	32	17529	0.182	28	0.0099	1.0282	0.0023	7	1
Date: 6/2/2004 **Location:** Forum 6th floor, IT-University												
AP1: 00:0C:85:6E:F7:30 **AP2:** 00:02:2D:02:88:80 **Roaming Node A**: 192.16.127.237 **Fixed node B**: 130.237.214.87												
3	18:47:23	150	7226	7	7219	0.097	5	0.0209	1.0436	0.0022	2	4
4	19:52:56	317	15106	14	15092	0.093	12	0.5221	1.0441	0.0331	3	5

Table 7.1: Results for the insecure calls for Hybrid scenario

Secure Calls

Four calls were made and table 7.2 below shows the analysis of these calls.

Date: 6/3/2004 **Location:** Forum 6th floor, IT-University												
AP1: 00:02:2D:02:89:37 **AP2:** 00:02:2D:02:88:80 **Roaming Node A**: 192.16.127.237 **Fixed node B**: 130.237.214.87												
Call No.	**Start Time**	**Duration (Sec)**	**Total Packets expected**	**Total Pckts Lost**	**Total Packets Received**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Avg. Jitter** (Sec)	**Handoff**	**Packet lost of Handoff**
1	15:34:21	159	7607	9	7598	0.12	8	0.021	3.0439	0.0024	3	1
2	15:39:56	166	8108	18	8090	0.22	17	0.0206	1.0246	0.0021	4	1
Date: 6/2/2004 **Location:** Forum 6th floor, IT-University												
AP1: 00:0C:85:6E:F7:30 **AP2:** 00:02:2D:02:88:80 **Roaming Node A**: 192.16.127.237 **Fixed node B**: 130.237.214.87												
1	20:50:14	220	10244	24	10220	0.23	21	0.0216	1.0317	0.0108	2	5
2	21:34:53	288	13524	24	13500	0.18	22	0.01	1.0433	0.0012	2	3

Table 7.2: Results for the secure calls for hybrid scenario

Special case: In this case, relatively a long call was made and the Host A was moved around in 6 APs with 9 handoffs to observe the quality of voice and to see if more packets are dropped. Host B was connected to the fixed network. In this case, we were not interested in finding out the time at which handoffs occurred, but rather in the sound quality as stated above. Please note that only insecure call was made. The results about this case are shown below in table 7.3.

Date: 6/3/2004 **Location:** Forum 6th floor, IT-University **Roaming Node A**: 192.16.127.237 **Fixed node B**: 130.237.214.87											
Call No.	**Start Time**	**Duration** (Sec)	**Total Packets Expected**	**Total Pckts Lost**	**Total Packets Received**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Avg. Jitter** (Sec)	**Handoffs**
1	16:23:21	271	13147	453	12694	3.445653	167	0.0214	1.7408	0.0031	9

Table 7.3: Results for the insecure call for hybrid scenario, Special case

It might be interesting for the reader to note that the packets loss rate in this case is around 3.44 percent as compared to previous cases in which the loss rate was below 0.5 percent. Moreover there has been a significant increase in the sequence errors too.

7.3.2. Host A and Host B both on Wireless Network

Host A and Host B were connected to different provider networks on WLAN. Both users were placed in different networks intentionally to involve a router in between them. Moreover, it was made sure that both the users do not get connected to the same AP, rather they were placed in different APs to involve more than one wireless hop for the voice traffic. In this setup, there were two sub scenarios described in the following sections.

7.3.2.1. Host A roaming and Host B stationary on wireless network

In the first sub scenario, Host A was moved between two APs back and forth and the time span for handoffs was found out using the two monitoring stations concept. The other user, i.e. Host B was kept stationary. A third monitoring station running Ethereal was used to monitor the RTP traffic. This is shown in the figure 7.2 below.

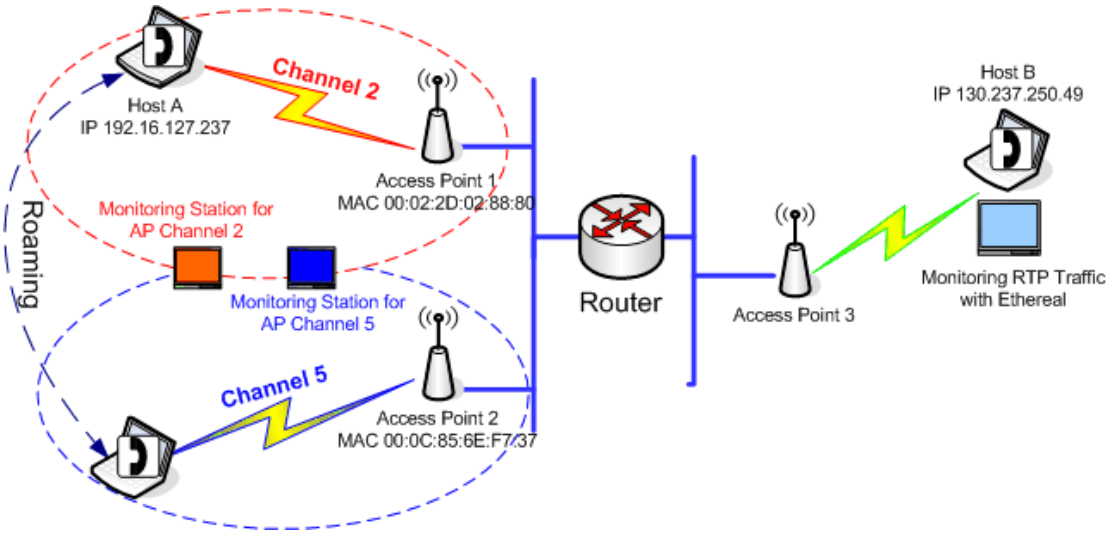

Figure 7.2: Host A roaming on wireless network and Host B stationary on wireless network

Again two types of calls were made, insecure calls and secured calls as described below.

Insecure Calls

3 calls were made in this case and table 7.4 below shows the analysis.

Date: 6/3/2004 **Location:** Forum 6th floor, IT-University												
AP1: 00:02:2D:02:89:37 **AP2:** 00:02:2D:02:88:80 **Roaming node A:** 192.16.127.237 **Fixed Node B**: 130.237.250.49												
Call No.	**Start Time**	**Duration** (Sec)	**Total Packets expected**	**Total Pckts Lost**	**Total Packets Received**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Avg. Jitter** (Sec)	**Handoff**	**Packet lost of Handoff**
1	17:02:59	111	5147	17	5130	0.3303	15	0.0218	0.9588	0.0032	3	0
2	17:06:37	86	3970	12	3958	0.3023	10	0.0219	0.0946	0.0033	2	1
3	18:12:54	84	5471	12	5459	0.2193	12	0.0207	0.091	0.0017	0	0

Table 7.4: Results for the secure calls for wireless network scenario with one host roaming

It is quite possible that the handoff events were not recorded accurately in this case as it seemed that very few packets were dropped due to handoffs.

Secure Calls

We made 3 calls for this scenario and the analysis about the traffic is shown below in table 7.5.

Date: 6/3/2004 **Location:** Forum 6th floor, IT-University												
AP1: 00:02:2D:02:89:37 **AP2:** 00:02:2D:02:88:80 **Roaming node A:** 192.16.127.237 **Fixed Node B**: 130.237.250.49												
Call No.	**Start Time**	**Duration (Sec)**	**Total Packets expected**	**Total Pckts Lost**	**Total Packets Received**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Avg. Jitter** (Sec)	**Handoff**	**Packet lost of Handoff**
1	17:13:52	157	7658	30	7628	0.3917	27	0.0206	1.0309	0.0016	3	0
2	17:19:09	175	8447	20	8427	0.2368	18	0.0204	0.1586	0.0018	4	0
3	18:49:21	210	10067	38	10029	0.3775	31	0.021	2.5746	0.0027	7	1

Table 7.5: Results for the secure calls for wireless network scenario with one host roaming

Similar to the last case, very few packets were dropped due to handoffs in this scenario. Table 7.5 shows that out of 3 calls, only one packet was dropped of handoff. This might be due to the reason that the handoff events were not accurately recorded (probably the clocks of the monitoring stations were not exactly synchronized).

7.3.2.2. Both Host A and Host B roaming on Wireless Network

Both Host A and Host B were connected to the wireless network and both were moving in this sub scenario. Host A was moved between two APs and handoffs were observed only for this user as it was not easy to find them out on both sides. Host B was also roaming between different APs. Like in all the scenarios, a monitoring machine running ethereal was used to observe the RTP traffic. This is shown in below in figure 7.3.

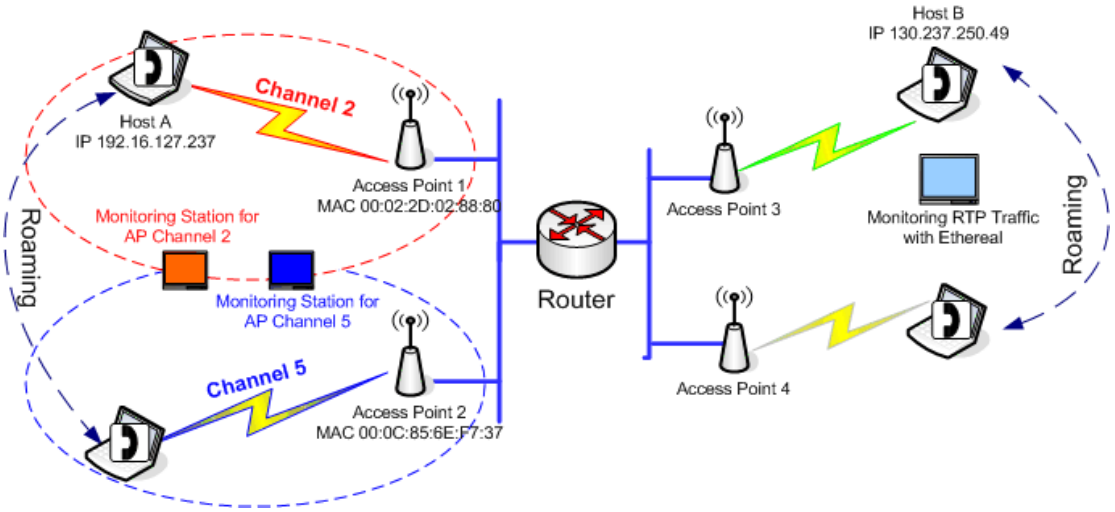

Figure 7.3: Both Host A and Host B roaming on wireless network

Insecure Calls

2 calls were made without security features and the data was analyzed in both directions i.e. from Host A to Host B and in the opposite direction. This is shown in the column “Direction” in table 7.6 below. There were some interesting and strange observations in this scenario.

Date: 6/3/2004 Location: Forum 6th floor, IT-University

AP1: 00:02:2D:02:89:37 **AP2:** 00:02:2D:02:88:80 **Roaming node A:** 192.16.127.237 **Roaming Node B:** 130.237.250.49

Call No.	Start Time	Duration (Sec)	Direction	Total Packets Expected	Total Pckts Lost	Total Packets Received	Loss Rate (%)	Seq. Error	Avg. Delay (Sec)	Max. Delay (Sec)	Avg. Jitter (Sec)	Handoffs	Packet lost of Handoff
1	18:16:12	206.802	A --> B	9546	6365	3181	66.7	13	0.6501	135.78	0.0064	3	1
No packets received between 18:17:16 and 18:19:32 and 1 handoff occured, Number of RTP packets dropped = 6359													
			B --> A	10152	6788	3364	66.9	51	0.0614	135.81	0.0026	Unknown	Unknown
No packets received between 18:17:16 and 18:19:32, Number of RTP packets dropped = 6726													
2	18:27:42	164	A --> B	7593	2767	4826	36.4	10	0.0341	60.104	0.0041	4	1
No packets received between 18:29:06 and 18:30:07 and 2 handoffs occurred, Number of RTP packets dropped = 2760													

			B --> A	8022	3039	4983	37.9	68	0.033	60.079	0.0025	Unknown	Unknown
No packets received between 18:29:06 and 18:30:07, Number of RTP packets dropped = 2948													

Table 7.6: Results for insecure calls for wireless network scenario with both hosts roaming

As shown in table 7.6, in both the calls, the wireless network seemed to be unavailable and several packets were lost during that period.

Lets analyze call no. 1 for the packets from Host A to Host B. The call duration was 206.802 seconds, and ethereal showed that 9546 packets were expected, but total packets received were 3181 and 6365 packets were lost. The actual sequence errors were just 13. The maximum delay encountered was 135 seconds, and during this delay, 6359 packets were lost. Before this loss, the last packet received had a sequence number 2851 and the next packet had a sequence number 9211. The average value of jitter was 6 msec. The behaviour in opposite direction was similar but the average value of jitter for the traffic in this direction was 2 msec.

Similar results were observed for call no. 2 as well.

Secure Calls

3 calls were made in this scenario and table 7.7 below shows the analysis of the calls.

Date: 6/3/2004 Location: Forum 6th floor, IT-University													
AP1: 00:02:2D:02:89:37 **AP2:** 00:02:2D:02:88:80 **Roaming node A:** 192.16.127.237 **Roaming Node B:** 130.237.250.49													
Call No.	**Start Time**	**Duration** (Sec)	**Direction**	**Total Packets Expected**	**Total Pckts Lost**	**Total Packets Received**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Avg. Jitter** (Sec)	**Handoffs**	**Packet lost of Handoff**
1	17:25:57	218	A->B	10638	3339	7299	31.39	39	0.0299	66.43	0.0017	5	3
No packets received between 17:27:26 and 17:28:32 and 2 handoffs occurred, Number of RTP packets dropped = 3316													
			B->A	9549	3103	6446	32.5	74	0.0337	66.41	0.005	Unknown	Unknown
No packets received between 18:17:16 and 18:19:32, Number of RTP packets dropped = 2999													
2	17:38:02	268	A->B	12982	6692	6290	51.55	45	0.0426	135.1	0.0027	8	0
No packets received between 17:39:16 and 17:41:31 and 4 handoffs occurred, Number of RTP packets dropped = 6698													
			B->A	12460	6651	5809	53.38	157	0.046	135.2	0.0047	Unknown	Unknown
No packets received between 17:39:16 and 17:41:31, Number of RTP packets dropped = 6418													
3	18:43:17	159	A->B	5656	2100	5656	37.13	97	0.0283	40.71	0.0023	4	1
No packets received between 18:44:18 and 18:44:59 and 1 handoff occurred, Number of RTP packets dropped = 2010													

			B->A	5706	2112	5706	37.01	83	0.028	40.71	0.0021	Unknown	Unknown
No packets received between 18:44:18 and 18:44:59, Number of RTP packets dropped = 2012													

Table 7.7: Results for the secure calls for wireless network scenario with both hosts roaming

It was observed that in each call in this scenario, the wireless network was unavailable similar to previous scenario.

No other calls (other than this scenario where both the hosts were roaming in wireless network) experienced these longs periods without any packets being forwarded or received. We do not know whether the packets were lost.

7.3.3. Host A and Host B both on Wired Network

In this scenario, both Host A and Host B were connected to Wired Network keeping them in different networks. This is shown below in figure 7.4.

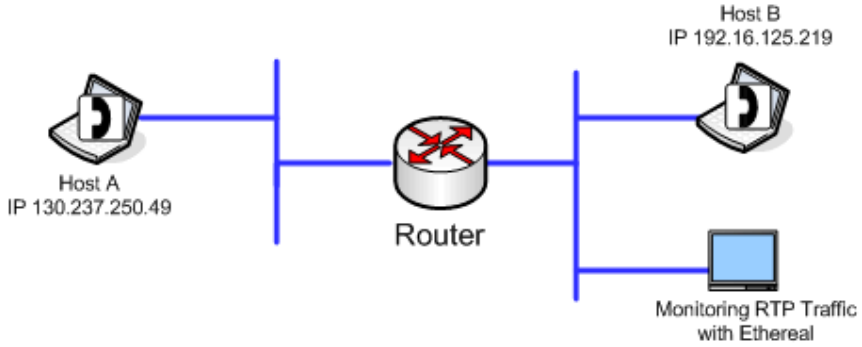

Figure 7.4: Both Host A and Host B on wired network

Insecure Calls

For this scenario, 2 calls were made their results are shown below in table 7.8.

Date: 6/1/2004 Location: Forum 8th floor, IT-University											
Node A: 192.16.125.196 **Node B:** 130.237.15.25 **Call from node B to node A, Insecured calls**											
Call No.	**Start Time**	**Duration (Sec)**	**Total Packets expected**	**Total Packets Received**	**Total Pckts Lost**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Pkts lost by max. delay**	**Avg. Jitter**
1	21:32:35	180	8861	8821	40	0.451	35	0.0204	0.141	6	0.00173
2	21:44:02	253	12499	12414	85	0.68	56	0.0204	0.2203	10	0.00046

Table 7.8: Results for the insecure calls for wired network scenario

Secure Calls

In this scenario, we made 6 calls and table 7.9 below shows the results of these calls.

Date: 6/1/2004 Location: Forum 8th floor, IT-University **Node A:** 192.16.125.196 **Node B:** 130.237.15.25 **Call from node B to node A, Secure calls**											
Call No.	**Start Time**	**Duration (Sec)**	**Total Packets expected**	**Total Packets Received**	**Total Pckts Lost**	**Loss Rate (%)**	**Seq. Error**	**Avg. Delay** (Sec)	**Max. Delay** (Sec)	**Pkts lost by max. delay**	**Avg. Jitter**
1	21:54:01	300	14978	14811	167	1.115	133	0.0203	0.22	10	0.00064
2	22:24:39	256	12640	12516	124	0.981	124	0.0205	0.0719	1	0.00055
3	22:32:31	225	11211	11135	76	0.6779	76	0.0203	0.0498	2	0.00043
Date: 6/3/2004 Location: Forum 6th floor, IT-University **Node A:** 130.237.250.49 **Node B:** 192.16.125.219 **Call from node B to node A, secured calls**											
4	19:36:07	207	10367	9954	413	3.9838	397	0.0208	0.0757	2	0.00366
5	19:40:42	157	7716	7371	345	4.4712	332	0.0214	0.531	1	0.00288
6	19:45:54	180	8994	8683	311	3.4579	298	0.0208	0.0757	2	0.00244

Table 7.9: Results for the secure calls for wired network scenario tests

7.4. Observations

7.4.1. Discussion

There were few assumptions and observations that were made after analysing the data collected from the tests explained below.

7.4.1.1. Comparing average jitter value

The average jitter was calculated for each call in all the scenarios (see section 7.3). Here we have calculated the average jitter value for each scenario and a comparison is shown in the graph below (figure 7.5). This was found to be the highest in the hybrid scenario and the lowest when both hosts were on wired network

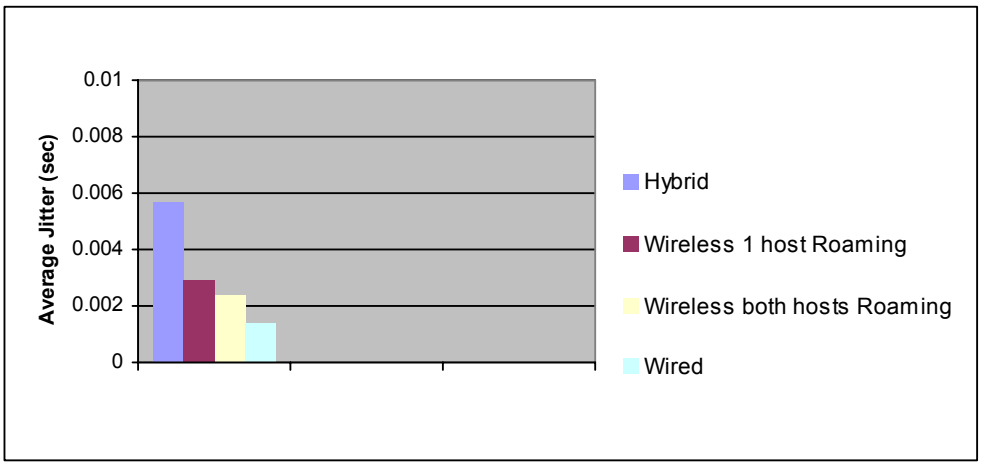

Figure 7.5: Graph for the average jitter

7.4.1.2. The loss rate comparison

The packet loss rate for each call was calculated (see section 7.3). In this section, the loss rate for each scenario has been compared as shown below in the graph.

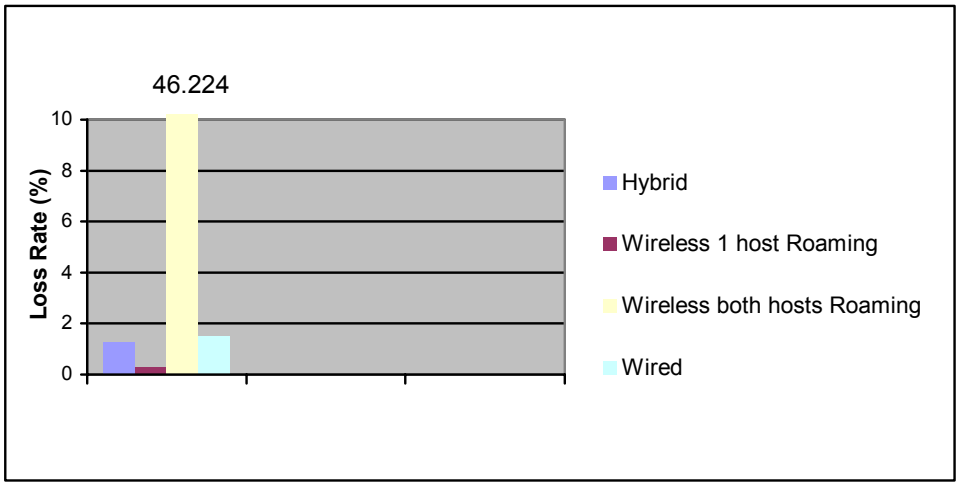

Figure 7.6: Graph for the loss rate

The above graph (figure 7.6) shows that the loss rate for the third scenario (both hosts roaming in the wireless network) was very extremely high as compared to other scenarios. This is due to the reason that the wireless network was unavailable during every call for a certain period of time for this specific scenario and no packets were received by the hosts (see section 7.3.3.2). The loss rate for the packets on the wired network was high too.

7.4.1.3. The sequence errors comparison

RTP packets with sequence errors for each call were calculated (see section 7.3). The following graph (figure 7.7) shows the average number of RTP packets with sequence errors for each scenario.

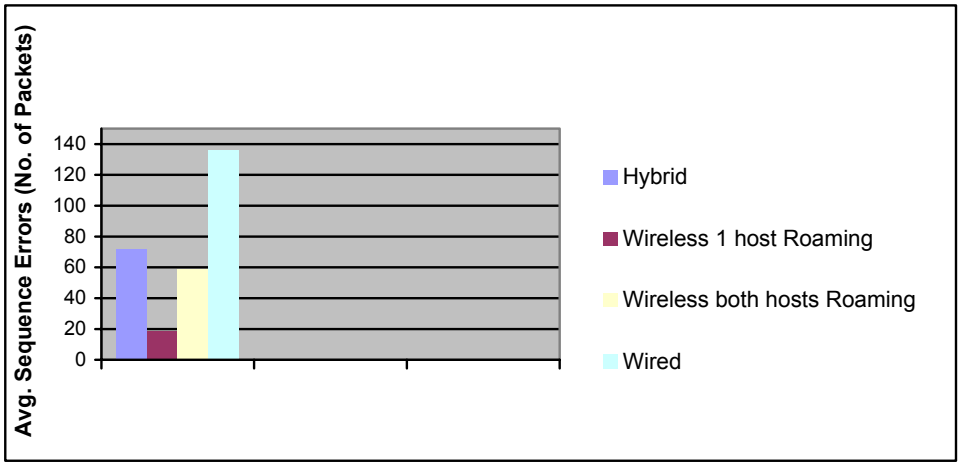

Figure 7.7: Graph for the average sequence errors

In some cases, the RTP packets were retransmitted by the sender and the receiver got duplicate packets. Such RTP packets with the same sequence number at the receiver side were counted in the sequence errors by Ethereal.

7.4.1.4. The average delay comparison

The average delay for each call in all the scenarios was measured (see section 7.3). We also calculated the overall average delay for every scenario and this is shown in the graph below (figure 7.8). The delay was found to be the highest in case when both the hosts were connected to wireless network and were moving.

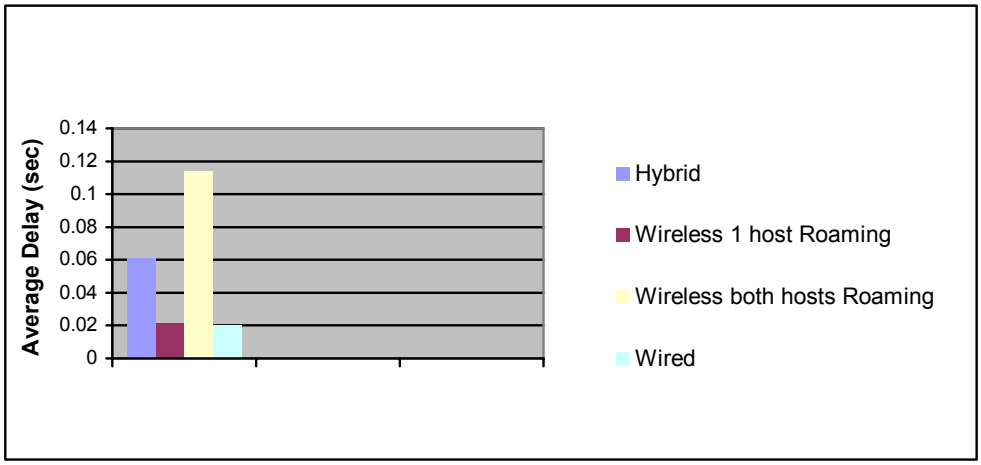

Figure 7.8: Graph for the average delay

7.4.1.5. The Maximum delay comparison

The maximum delay for every call in all the scenarios was measured through Ethereal (see section 7.3). The Average for the maximum was also calculated for each scenario and is shown in the graph below (figure 7.9).

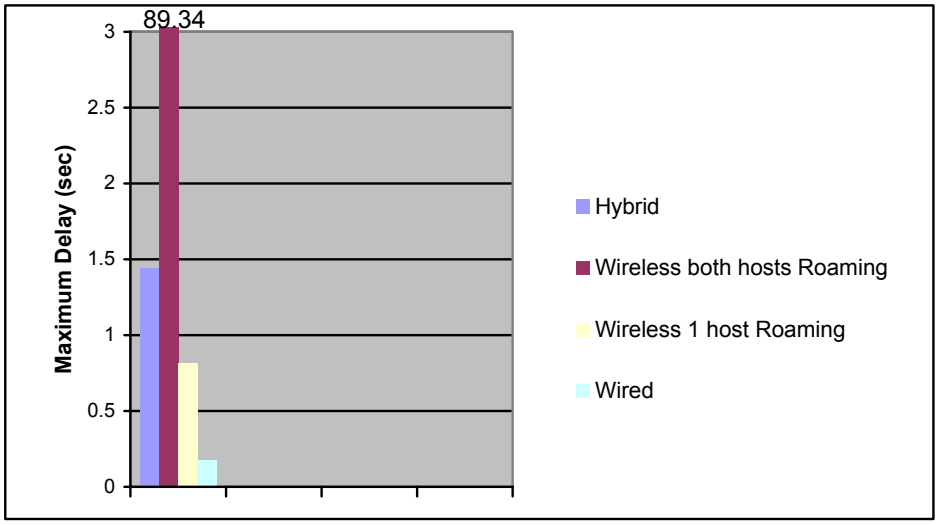

Figure 7.9: Graph for the average maximum delay

This value is the highest in case when both hosts were moving in the wireless network during a call due to the reason that there were no packets received for every call in that scenario for some duration (see section 7.3.3.2).

7.4.2. Problems met in the testing

We would like to report the troubles we encountered in our testing here. We hope it can help others doing similar test.

1. Ethereal Software

1.1 Delay calculated by analysis tools of ethereal indicates the delay between two consecutive packets. But due to the RTP standard, delay means the time spent while a packet travels from source to destination.

1.2 In order to get handoff information, we first thought of capturing 802.11 raw packets with ethereal, but for the current version (v 0.10.4.0), in Windows, the data cannot be dissected; in Linux, libpcap should be utilized. Also note that this can only be done while the wireless card is in monitor mode, and name resolving feature should not be selected accessed (as it slows down monitoring).

2. Data Collected

2.1 At the first, we use ethereal to capture the UDP packets only on one side. When we did our analysis, we found the data loss in one direction (from the side where the monitoring machine is on to another node) was always 0. This was obvious when we realized that we connected the monitoring machine and test node to the same subnetwork connected by a switch, resulting in rather 'perfect' network.

3. MiniSIP Crashing

During our tests, we faced a very weird problem with some APs on the 8th floor of Forum Building at IT-University, Kista. We started doing the tests around this area and during the start of this week; the network administrators upgraded these APs. After the upgrades, MiniSIP started crashing every now and then depending on which side initiated the call. The MiniSIP client on the fixed network crashed more often if call was initiated from this side. The error occurred in the other direction as well but not that often.

The error message that we received was "Resource Temporarily Unavailable". It seemed that a lot of packets were corrupted as the UDP checksum was not correct. There was no problem when both hosts were connected to the wired network and when tests were conducted on wireless network on another floor (6th floor, Forum Building). For more information about the problem, see Appendix C.

4. Headset problem with mandrake.

Mandrake hangs whenever a USB headset is connected to it. This prevents us from using Mandrake Linux for our tests.

8 – Conclusions and Future Work

8.1 – Conclusions

As we mentioned in section 2.2, VoWLAN faces new challenges. From our testing, we can see:

- When users roam, it does introduce greater latency. When we did tests in which both nodes were wireless, in one scenario, we let one node roam, in another scenario, we let both nodes roam. In the latter one, we observed greater delay.

- Voice on wireless networks is less reliable than on wired networks. From our testing, we noticed that the performance (delay, packet loss, etc.) on wired networks were better than on wireless networks.

- We observed that there was a slight disruption in the sound when an handoff occurred for the node connected to the wireless network during a call.

- It was observed that adding security features to a call did affect the performance of MiniSIP and the sound quality was the same as in case of an insecure call. Moreover, inconsequential differences were noticed in the number of packets dropped, sequence errors, average delay and average jitter while comparing the insecure and secure calls.

8.2 – Future Work

Some interesting recommendations for the future work are described here.

- Limited by time, we haven't done all the testing we planed. For example, in our testing, although we enabled security mechanism in some scenarios, we had no time to examine how strong the mechanism is. As it's usually thought that wireless headsets are less secure, future work to check the strength of MIKEY in MiniSIP will be very interesting. Also, the tests should be performed both during the busy hours and in the evenings when there are fewer users on the network and the results should be compared.

- Due to limited resources, the traffic was monitored only at one host. It will be interesting if the tests can be done by monitoring the traffic at both the nodes and monitor all the traffic.

- As described in section 7.3.2.2 when both the nodes were roaming in wireless network, the network was temporarily unavailable for sometime and no packets were transmitted or received, it will be interesting to monitor the status AP using Simple Network Management Protocol (SNMP) to verify if AP is working properly during this period.

- The method to find the handoff event (described in section 7.2.2) might not be accurate. This should be improved while doing the tests in future.

- It might be interesting to capture and analyze the SIP packets too besides the RTP traffic. Moreover, in future, if the tests are conducted, the monitoring should not be limited to RTP traffic only, rather all the traffic should be monitored and later analyzed. It can be helpful to reach some interesting conclusions.

- In future, the same tests can be performed by running MiniSIP on iPAQs. The comparison of the performance of MiniSIP on the iPAQs and the laptops will be very exciting.

- The testing could be done in future with more load on the network such as video.

9 – References

[1] Susan Breidenbach, VoWiFi standards situation, Network World, May 3, 2004. < http://www.nwfusion.com/research/2004/0503vowifiside.html> (May 22, 2004)

[2] Susan Breidenbach, 'Howdy, pardner! PBX, WLAN and handset makers step together to choreograph voice-over-wireless solutions', Network World, May 03, 2004. <http://www.nwfusion.com/research/2004/0503vowifi.html> (May 23, 2004)

[3] RFC 3261 'SIP: Session Initiation Protocol'. <http://www.ietf.org/rfc/rfc3261.txt?number=3261> (May 26, 2004)

[4] G. Q. Maguire Jr., '2G1325/2G5564 Practical Voice Over IP (VoIP): SIP and related protocols, Spring 2004, Period 3', Lecture notes. <http://www.imit.kth.se/courses/2G1325/VoIP-2004.pdf> (May 20, 2004)

[5] Rakesh Arora, 'Voice over IP: Protocols and Standards'. <http://www.cse.ohio-state.edu/~jain/cis788-99/ftp/voip_protocols/index.html#3.-Session-Initiation-Protocol(SIP)> (May 20, 2004)

[6] RFC 2543 'SIP: Session Initiation Protocol'. <http://www.ietf.org/rfc/rfc2543.txt?number=2543> (May 22, 2004)

[7] RFC 2327 'SDP: Session Description Protocol'. <http://www.ietf.org/rfc/rfc2327.txt?number=2327> (May 22, 2004)

[8] Irvind S. Ghai and Ashley Johnston, 'Wireless LAN IP Phones: Simplifying Communications?', Texas Instruments Voice-over-IP Group. <http://www.newtelephony.com/print/othervoices/791.html> (May 28, 2004)

[9] Dave Molta, Frank Bulk, and Sean Ginevan, 'VoWLAN:POISED FOR TAKEOFF', MobilePipeline, October 30, 2003. <http://www.kinetowireless.com/news/industry_articles/vowlan_takeoff.html> (May 29, 2004)

[10] Irvind S. Ghai and Ashley Johnston, 'Wireless LAN IP Phones: Simplifying communications?', Texas Instruments Voice-over-IP Group, April 29, 2004. < http://www.newtelephony.com/othervoices/#leadhjb> (May 12, 2004)

[11] Tim Greene, 'Wi-Fi VoIP will take time to mature, say vendors', Network World Fusion, March 30, 2004. <http://www.nwfusion.com/news/2004/0330voipwifi.html> (May 10, 2004)

[12] 'RTP: Some Frequently Asked Questions about RTP', <http://www.cs.columbia.edu/~hgs/rtp/faq.html#transport> (May 31, 2004)

[13] RFC 3550 'RTP: A Transport Protocol for Real-Time Applications', July 2003. <ftp://ftp.rfc-editor.org/in-notes/rfc3550.txt> (May 31, 2004)

[14] <http://www.freesoft.org/CIE/Topics/127.htm> (May 31, 2004)

[15] Johan Bilien, 'Key Agreement for Secure Voice over IP', Master of Science Thesis at IMIT/KTH, December 2003. <ftp://ftp.it.kth.se/Reports/DEGREE-PROJECT-REPORTS/031215-Johan-Bilien-report-final-with-cover.pdf > (May 31, 2004)

[16] RFC 3711 'The Secure Real-time Transport Protocol (SRTP)', March 2004.

<http://www.networksorcery.com/enp/rfc/rfc3711.txt> (June 2, 2004)

[17] RFC 2406 'IP Encapsulating Security Payload (ESP), November 1998. <http://www.ietf.org/rfc/rfc2406.txt> (June 1, 2004)

[18] 'Security in SIP-Based Networks', White paper from Cisco. <http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml> (June 2, 2004)

[19] Israel M. Abad Caballero, 'Secure Mobile Voice over IP', Master of Science Thesis at IMIT/KTH, June 2003. <ftp://ftp.it.kth.se/Reports/DEGREE-PROJECT-REPORTS/030626-Israel_Abad_Caballero-final-report.pdf> (June 1, 2004)

[20} <http://www.stockholmopen.net/> (May 25, 2004)

[21] <http://www.ethereal.com> (May 10, 2004)

[22] <http://www.netstumbler.org/> (May 12, 2004)

[23] <http://www.wildpackets.com/products/airopeek_nx> (May 12, 2004)

[24] <http://www.ethereal.com/lists/ethereal-users/200311/msg00003.html> (May 23, 2004)

[25] VoWIP Quick Start: Getting up to Speed on VoIP on 802.11 Wireless LANs <http://www.devx.com/wireless/Article/11423> (May 23, 2004)

[26] SpectraLink Voice Priority White Paper, Quality of service for voice traffic on wireless LANs <http://www.spectralink.com/products/pdfs/SVP_white_paper.pdf> (May 23, 2004)

[27] Video CODEC for Audiovisual Servies at p x 64 kbits, ITU-T Recommendation H.261, March , 1993

Appendix A – Acronyms and Abbreviations

AP	Access Point
CDMA	Code-Division Multiple Access
CPU	Central Processing Unit
CSRC	Contributing Source identifiers count
DNS	Domain Name System
DoS	Denial of Service
DSP	Digital Signal Processor
ESP	Encapsulated Security Payload
GPRS	General Packet Radio Service
HTTP	Hyper Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
LS	Location Service
MIKEY	Multimedia Internet KEYing
PBX	Private Branch eXchange
PC	Personal Computer
PDA	Personal Digital Assitant
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RTP	Real Time Protocol
SCCP	Skinny Client Control Protocol
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRST	Survivalbe Remote Site Telephony
SRTP	Secure Real Time Protocol
SSRC	Synchronization Source Indentifier
SVP	SpectraLink Voice Priority Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UAC	User Agent Client

UAS	User Agent Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol
VoWLAN	Voice over Wireless Local Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

Appendix B – RTP

The testing was based on RTP (Real-Time Protocol) information. The basic RTP understanding needed in the testing is as follows [12, 13]. RTP is a transport protocol that runs on end systems and provides demultiplexing.

RTP header:

Field	Bits	Description	Data observed in testing
Version	2	Version of RTP.	RFC 1889 Version (2), obsoleted by RFC 3550.
Padding	1	If set, the packet contains one or more additional padding octets at the end.	False
Extension	1	If set, one header extension follows the fixed header.	False
Contributing source identifiers count (CSRC count)	4	Number of CSRC identifiers that follow the fixed header.	0
Marker	1	Indicate the beginning of a talkspurt.	
Payload type	7	Format of the RTP payload.	ITU-T G.711[8] PCMU (0)
Sequence number	16	Incremented by one for each RTP packet transmitted. Detect losses	
Timestamp[9]	32	Reflect the sampling instant of the first octet. Incremented by the time covered by a packet. Place the incoming audio and video packets in the correct timing order	
Synchronization source identifier (SSRC)	32	Identify the synchronization source.	

Table 1: RTP Header

RTP Control Protocol (RTCP) provides a mechanism to check the quality of the data distribution and provide other control information. It can be used to calculate delay, jitter, etc. RTCP is not implemented in MiniSIP, so we are not going to discuss this further. This brought us some difficulties when we were trying to calculate delay in our testing.
How to compute jitter:

[8] G.711 is the international standard for encoding telephone audio on a 64 kbps channel. It is a pulse code modulation (PCM) scheme operating at an 8kHz sample rate, with 8 bits per sample [14].

[9] Timestamp: it is incremented by the packetization interval times the sampling rate. For example, for audio packets containing 20 ms of audio sampled at 8000 Hz, the timestamp for each block of audio increases by 160.

It is computed in timestamp units.

Appendix C – MiniSIP Crashed with upgraded Access Points

Johan Bilien wrote an email to Enrico Pelletta, the Network Administrator of IT-University describing the MiniSIP crashing problem. The reply from Enrico to this email is shown in the following section in italic text.

Johan Bilien wrote:

>Hi all,
>Khurram and Ming-Shuang, who are doing some tests with our VoIP stuff,
>have experienced something strange on their access point (there are
>sitting in the exjobbers' space at TSLab): they were receiving a lot of
>packets which seemed to be corrupted (the UDP checksum seems wrong).
>
It sounds strange...

>This was not happening yesterday, nor on the wired network or on another
>access point. Could it be that the new access point has the integrity
>control disabled, or something like that?
The 802.11 standard provides a reliable data link on the radio channel. Thus, transmission errors are managed by the link with packet retransmissions when CRC errors are detected on the 802.11 frame. Radio interferences and/or radio transmission failure cannot produce the delivery of corrupted packets on the radio link. Instead, user experience a drop of performance due to massive frame retransmissions on the radio link. So, I exclude that the problem came from the radio link unless a general failure of the AP (i.e. the AP is broken).

I have a different hypotheses. Yesterday we rebuilt the WLAN network backbone. We put in place new switches and we connected with 100Mbps Full-Duplex links using 100Mbps TX/FX converters (RJ45/Fiber). After setting up the system, I got some troubles with duplex mismatches between the different converters in use. I think that I solved the problems around 15:00/15:30. At which time did you get the problem? Yesterday evening the central network switches was not reporting any kind of warning about large numbers of transmission errors (this happened when the converters were not properly working). Please, let me know if you still have troubles, however I'm going to verify the status of the backbone again.
Best,
Enrico.
>Thanks,

Appendix D – Figures and Tables Index

Table of Figures

Table of Tables