A Link Layer Solution to Location Identification of VoIP Callers

by

Saeideh Ashtarifar

B.Sc., Isfahan University of Technology, 1997

A thesis submitted to the Faculty of Graduate Studies and Research

in partial fulfillment of the requirements for the degree of

Master of Applied Science in

Electrical and Computer Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering

Department of Systems and Computer Engineering

Carleton University

Ottawa, Ontario, Canada

August, 2010

Your file Votre référence
ISBN: 978-0-494-71510-9
Our file Notre référence
ISBN: 978-0-494-71510-9

Abstract

This thesis presents the details of design and analysis of a new solution to the location determination problem of VoIP users. This problem has such a great importance in the emergency cases that without a solution for it, supporting the emergency calls in IP telephony is impossible. We propose an efficient and accurate mechanism, based on a link layer protocol, named Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). In our solution, the first level LLDP-MED capable switches, provide location information based on the LLDP databases. Since providing location information in our solution is performed by the switches, it prevents presenting fake information by malicious users. We also study and evaluate the performance of an exiting solution to this problem which uses Location Information Server (LIS). Then we compare this solution with our proposed mechanism in different aspects, with emergency case considerations. Our simulation results prove that the delay of our proposed technique is much lower than the delay of the solution based on LIS.

Acknowledgments

First and foremost I would like express my deep gratitude and sincere thanks to my supervisor, Professor Ashraf Matrawy, for his immense guidance, support, and encouragement during the course of my thesis. Thanks to him I learned the skills necessary to conduct research in a professional manner. This work would not have been possible without his continuous direction and feedback.

I would also like to thank my family, although they were not here, their encouragement, support, and many sacrifices have allowed me to reach this stage in my life. I cherish them and I am always grateful to them.

Finally I would like to extend my thanks to all of my friends, specially Arash Shokrani, Kaveh Shahbaz, Yasin Miar, Shabnam Mizani, Mahoor Ahmadi, Behzad Azari, Mohammadreza Yazdani, Kimia Ansari, Abes Dabir and M.Singh Paul, who have provided me with invaluable assistance, support, and inspiration throughout the course of my studies at Carleton.

To my parents

Contents

List of Tables

List of Figures

List of Acronyms

CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IOS	Internetwork Operating System
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
LIS	Location Information Server
LLDP	Link Layer Discovery Protocol
LLDP-MED	Link Layer Discovery Protocol for Media Endpopint Devices
LoST	Location to Service Translation
LUMP	Location-to-URL Mapping Protocol

MAC	Media Access Control
NAT	Network Address Translation
NENA	National Emergency Number Association
NG-E-911	Next Generation Enhanced 911
NS-2	Network Simulator 2
PSAP	Public Safety Answering Point
RFC	Request for Comments
SIP	Seccion Inititation Protocol
TCP	Transmission Control Protocol
TLV	Type Length Value
TTL	Time To Live
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
VSP	VoIP Service Provider

Chapter 1

Introduction

The demand for Voice-over-IP(VoIP) telephony has been increasing in the past few years due to its cost effectiveness and enhanced features. Nowadays, more and more residential and enterprise customers are migrating from traditional landline phone services to VoIP telephony. In order to maintain a high level of customer satisfaction, VoIP service providers should deliver at least the same services as in traditional telephone networks. Supporting emergency calls (such as dialing 911 in North America or 112 in Europe) is one of the essential services in traditional telephone networks. Since in many emergency situations user may not be able to talk and give his/her address to the emergency call taker, it should be a mechanism in the network that determine the physical address of the caller automatically.

In land-line telephone networks, the phone number is used as a key to locate the callers. Based on the caller's location, the emergency call is routed to the most ap-

propriate Public Safety Answering Point (PSAP). However, the existing mechanism to support emergency calls used by the Public Switch Telephone Networks(PSTN) are not appropriate to handle emergency calls in IP-based voice networks. The reason is that the location of the users in IP telephony is not fixed and the phone number(or any other keys) can not be simply used to locate the users.

Therefore, the most of the VoIP service providers such as Skype or YAHOO! do not support calling emergency numbers.

Recently, determining the location of the Internet users has been the focus of several research efforts in which different solutions and mechanisms are proposed. However, none of them can be used as an general solution for location determination of VoIP users in all situations.

In 2004, Cisco developed *Cisco Discovery Protocol* (CDP) which can be used for discovering the location of an endpoint network device [1]. Using this protocol, the location of the VoIP user can be determined when an emergency call is made. The main drawback of using this protocol is that it is Cisco-specific and can only be used in a network where all devices are developed by Cisco. Since CDP was Cisco-specific, a generic solution called *Link Layer Discovery Protocol-Media Endpoint Discovery* (LLDP-MED) was introduced in 2005 which supports location identification of endpoints in the network. This protocol can be potentially used to devise a mechanism for locating the VoIP users.

In [2], another solution is proposed for location determination of users in the VoIP

networks by employing a series of *Location Information Servers* (LIS). However the time to locate the VoIP users in this method is unbounded and hence can not be used in case of emergency calls, which the call setup time must be less than 2 seconds [3]. Further, maintaining an up-to-date database in the corresponding servers is a big challenge in this method.

1.1 Motivation

Determining the user's location in the network is not only for the emergency cases and many non-emergency applications may use it. For instance, commercial services with a limited service region , localized content (such as local news and weather), and compliance with local law. However, identifying the location of the users, in the emergency cases, has a great importance. Given that without the location information, handling emergency calls is almost impossible. We should mention that supporting emergency calls is going to be mandatory for all telephony service providers not only from the technical but also from the legal points of view [4], [3]. Based on NENA technical information document for NG E9-1-1 (Next Generation Enhanced 9-1-1), call setup time (dialing of last digit on emergency number to ring at the PSAP), under expected peak load must be less than 2 seconds. These requirements were based on some life-critical cases [5] ,[6] on them the customers could not reach PSAP by dialing 911 and died. Although recently, the subject of supporting emergency calls for VoIP users has gained much interest due to the increasing number of VoIP users, still there

is no absolute solution suitable for all situations. Most of the location determination approaches suffer from shortcomings and other issues that make them inapplicable for the emergency cases. These drawbacks such as high latency, poor accuracy, incomplete coverage of the users, and etc., are discussed in more detail in Chapter 2. Our proposed solution addresses many shortcomings of determining caller's location in the SIP- based VoIP networks. The goal of this solution is to provide required users' information for the SIP proxy servers. Based on this information, the proxy servers can route the emergency calls to the appropriate destination.

One of the clear advantages of our proposed method is that the user can not put fake location information as opposed to other cases where the user (i.e. its client) is supplying the location information. Some of the VoIP service providers who support E-911, relay on the information that users provide once they register. How ever there is no guaranty that this information be correct and up-to-date. This solution has also a very significant benefit for the nomadic user because once a user disconnects from a port and connect to another port (at a different location) and starts to send packets, its packets will be stamped with the location information related to the port that the user is now connected to. Therefore with an updated database for the switch we can be sure that every packet will have the correct information stamped to its data link header. This should increase the chances reach at the destination with the up-to-date location information.

For clarification, for the rest of this thesis when we refer to the user we are assuming

that the VoIP client software does this process not something manually by the user.

1.2 Research Objectives and Thesis Contribution

The main objective of this research is to find an appropriate framework based on a link layer protocol in order to determine the actual physical location of Internet hosts with enough accuracy to handle emergency calls, in IP networks. Our approach is to devise a method by using the LLDP-MED protocol in the data link layer. In this method, all emergency requests are stamped with the location information by the first level LLDP-enabled switches. The switches perform this function based on their local databases. Hence, when the emergency requests reach at the SIP proxy servers, they contain the physical location of the emergency caller.

In order to evaluate our method, we have considered an existing application layer solution for this problem and compare it with our own proposed solution from different aspects.

Based on these objectives, the following contributions have been made:

1. A complete survey was performed on all existing techniques for location determination of the VoIP users. All techniques were categorized based on their approach in locating users. Furthermore, different measures were introduced to compare and evaluate all techniques. Based on this research, the following conference paper has been published:

- S. Ashtarifar and A. Matrawy, "Determining Host Location on the Internet: The Case of VoIP Emergency Calls", Proc. of the International Workshop on Next Generation Public Safety Communication Networks and Technologies (NGenSafe'09), in conjunction with IEEE ICC2009), Dresden, Germany, June 2009

2. A new method for locating VoIP users was proposed based on LLDP-MED protocol in SIP-based networks. Unlike the existing solutions, our proposed method can accurately locate the users in a timely manner which makes it an excellent choice for handling the emergency calls in VoIP applications.

3. An NS-2 model was developed to compare our proposed method with an existing technique to locate VoIP users. Based on the results obtained from this part of research the following journal paper has been published:

   - S. Ashtarifar and A. Matrawy, "A Link Layer Solution to Location Identification of Emergency VoIP Callers", International Journal of Computer Networks and Communications, Vol. 2, No. 5, 2010.

1.3 Thesis Outline

The rest of this thesis is organized as follows:

Chapter 2 surveys existing techniques for location determination of the VoIP users. These techniques are categorized based on their approach in locating users. Moreover,

advantages and shortcomings of each method are reviewed.

In Chapter 3, the research problem is stated.

In Chapter 4, one of the existing application layer solution, named LIS is explained in details.

In Chapter 5, our solution is proposed based on a data link layer protocol, named LLDP-MED. Some advantages of our proposed method are also discussed.

Chapter 6 deals with different simulation scenarios for wireless and wired topologies and provides simulation results. Finally, some concluding remarks are drawn in Chapter 7, and possible directions for future research are provided.

Chapter 2

Background on Location Determination Technologies

The ability to determine the geographical location of Internet user can enable a variety of location-aware applications such us commercial advertises or emergency cases. However, even putting mobility of Internet users aside, finding the geographical location of Internet users is a difficult problem that has been the subject of several researches [7], [8], [9], [10], [11], [12], [13]. Decentralized management of the Internet has lead to no database of host's location [14]. In this chapter we provide an overview of a number of approaches proposed in the area of determining the geographical location of Internet hosts. We first categorize them into two main groups which are introduced in Sections 2.2 and 2.1. Then, in section 2.3 we introduce some other techniques, out of these two categories. Finally, in Section 2.4 we discuss proses and

cones of each category in the case of emergency calls.

2.1 Database Approaches

In these types of methods information is registered in a database. Although database approaches are more accurate then other methods, they have one common fundamental drawback: the information must be entered and updated manually. Some of these techniques are as follow:

2.1.1 Geo Track

This method [15] uses some probe machines to determine the network path from the probe to the target hosts, based on a traceroute mechanism. After determining the path, the location will be inferred from the DNS names of router interfaces and the location of the last router is assumed to be estimate of the target host's location. The accuracy of this method depends mainly on how accurate the DNS records are. The traceroute result will also affect the location deduced from this method and this can not be guaranteed to reflect the actual location of the target host.

2.1.2 Geo Cluster

With this technique [15], IP addresses which correspond to the co-located hosts are grouped together. IP-to-location mapping information is then used to infer geograph-

ical location of the cluster. The address prefixes contained in BGP routing tables are then used to infer the location of the cluster. Given a target IP address, at first the geographic cluster to which it belongs is determined, and then an estimation of its location will be calculated to be that of the geographic cluster. Thus, the physical location of the cluster is considered as an estimation for the user's location. The accuracy of this method also depends mainly on accurate mapping information being available.

2.1.3 Who Is Lookup

Generally, the whois service provides a mechanism for finding contact and registration information for Internet resource, such as: telephone numbers and mailing addresses. Based on this information, the physical location of hosts can be determined. There are three methods for using the whois service [16]:

- Obtaining some information about registered IP addresses by look-up in a public whois database
- Obtaining details about Autonomous Systems (AS) from a public whois database
- Obtaining information about registrants in a DNS database from a public whois database

The main concern with this method is that all of the hosts may not be located at, or near, the addresses of the registered organizations. Additionally, whois database

data is provided manually, so incorrect or false data may be submitted. Further more, data must been updated periodically in order to be reliable.

2.1.4 MAC Address Mapping

The location of ethernet jacks and desktop machines are usually stored in a mapping database by system administrators. The location of target host can be determined simply by sending a query with MAC address retrieved from the receiving packet [17].

Like other database techniques, the accuracy of this method depends on how up-t-date the database is. In addition, a proper relationship must exist between the domains, because each administrator has only information about the devices in the network which is responsible for them.

2.1.5 DHCP lookup

Dynamic Host Configuration Protocol (DHCP) servers have additional configuration options that allow them to store more information for each client than just the IP address. This information can include: the subnet mask, the domain name, the router IP address, static routes and physical location information. The SIP proxy server can also obtain the location information of a User Agent (UA) by querying DHCP server [18]. The DHCP database must be updated with this additional information.

2.1.6 LIS: Location Information Server

This model tries to provide a user's geographical information (civic address or latitude/longitude) based on Internet accessible network information. LIS is a network entity which provides and stores location information that can be retrieved by a UA or an outbound SIP proxy in VoIP communications. There is a LIS associated with each access network, so when a device joins a particular access network, it discovers and uses an associated LIS that is responsible with that network. Thus, the process has two steps [2]:

a. Discovering the associated LIS

b. Requesting location information from the associated LIS

Then this information can be used or conveyed for handling emergency calls, for example by using a SIP event notification architecture.

Before a device can query a LIS, it should find the LIS. The process of finding a LIS is not easy for nomadic users, like emergency callers, and is the subject of an Internet draft [19].

After a device attaches to a network and finds the LIS which can serve it, it needs a protocol for querying the LIS. The HTTP Enabled Location Delivery (HELD) can be used[20]. Another issue with this model is how a LIS determines the location of devices that it is serving and how correct and trustable the information is. We have more discussion for this technique in Chapter 4.

2.1.7 CDP: Cisco Discovery protocol

Cisco Discovery Protocol (CDP) is a layer two protocol [21], used for discovering devices on a network. All CDP enabled Cisco devices, periodically send messages (containing the switch name and port ID of the sender) to a well-known multicast address. In each administrative domain a database is used which contains mapping information between switch/port ID information and its physical location. Hence, the location of each user can be inferred easily from this database. In addition, the covered area by a switch/port is small enough to have high accuracy of the emergency caller's location. If the caller's location, or the switch/port information changes, a new query is sent to the database and the location will be updated [1].

This method introduces less overhead on the network compared with other methods such as DHCP lookup, but it requires network administrators to manage a central up-to-date database that contains mapping between switch/port and the physical location. The overhead depends on how frequently switches are replaced or moved. This protocol is proprietary to Cisco devices.

2.1.8 LLDP-MED: Link Layer Discovery Protocol for Media Endpoint Devices

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is a generic solution that supports location identification of end points. LLDP-MED is an ex-

tension for IEEE 802.1AB (LLDP) standard [22] to support multiple vendors. This protocol, similar to CDP , can be used to deliver location information directly from the layer 2 network infrastructure. Usually in enterprise LANs, there is a database to store switch/port to building location mapping information which can be used to determine the location of users. The issue with this protocol is that like CDP, a central database must be maintained. In addition, this protocol can not be used for large-scale systems such as IEEE 802.16 (WiMAX) and IEEE 802.22, which typically have larger cells than those of IEEE 802.11 [22]. We have proposed our solution based on this protocol and will have more discussion on this protocol in Chapter 5.

2.1.9 User-Supplied Location Information

Some of the VoIP service providers require users to manually enter their location information at the time of registration or when changing their locations.

Users may enter incorrect or false information and sometimes they don't remember to update their location information. Moreover emergency calls may occur at an accident location other then the location of registration (such as at a workplace, or while in transit) and a user may not be able to provide this location information on their recorded information.

2.2 Measurement Approaches

These methods are commonly based on the relationship between network delay and geographic distance; however in these delay-based methods, several factors can affect delay: such as link failure, network congestion, etc. For these reasons these methods can not provide a good estimate of the caller's location. In these methods some nodes at known locations are considered to be "Landmarks" with the ability to respond to pings. Another issue with this class of techniques is that they are usually time consuming, so they individually are not appropriate for real time applications such as VoIP, and especially handling Emergency Calls. Further more, the nodes which are considered to be Landmarks, or probes should have some abilities like sending ICMP messages or responding to ping. Some of these techniques are as follow:

2.2.1 Geo Ping

GeoPing [15] is based on the relationship between network delay and geographic distance for estimating the location of a target host. In fact, this method locates a host by mapping it to the most representative landmark and using the location of landmark as an estimate for the location of the target. The assumption that is used in this technique is that two hosts with the same distance to a landmark, will measure similar delay.

The procedure of location determination in this method is as follow: A delay map should be constructed in which each entry contains the coordinates of a host at a

known location (the "Landmark"), and a delay vector containing the measured delay to the host from probes at known locations. To determine the location of the user, at first a delay vector is built and then a search is started through the delay map to find a delay vector which best matches it. Geo ping considers the location corresponding to the best match as an estimate for the location of the target host.

However, there is a poor correlation between network delay and geographic distance. Many other factors can effect delay such as congestion, bandwidth or cost of link.

2.2.2 CBG: Constraint-Based Geolocation

This approach [23] uses a triangulation technique by combining measured delay from multiple Landmarks. Using this method, each Landmark measures delay from itself to all other Landmarks instead of mapping targets to the location of a landmark. As a result, instead of returning one point (like Geo ping), CBG defines a position and confidence region which lies between Landmarks. With the confidence region, CBG provides a better estimate than pure delay approaches. In fact, the target is assumed to be within a circle, centered at the landmark whose radius is the estimated distance. Then the distance estimate from all landmarks are combined by intersecting all the circles, that make a feasible region. The target is assumed to lie in this region. The target is considered as the center of this region and size of the region is taken as an estimate confidence.

Like other delay-based techniques, this method provides a more accurate estimate for target host if Landmarks are ubiquitous. This is due to the fact that the estimation error is strongly correlated with the distance between the target host and Landmarks. Therefore the more Landmarks the lower the estimation error.

2.2.3 TBG: Topology-Based Geolocation

Both previous methods, Geo Ping and CBG only provide an accurate estimate in a small area with small RTT(Round-trip delay time) and ubiquitous Landmarks. To overcome this shortage, network topology and routes can be taken into account. A new method with this feature is TBG [14] which captures path-specific latency inflation. Using some attribute of delay-based methods and combining them with network topology information, TBG produces a finer granularity. In fact, routers in the path will be geolocated and and then can serve as "Passive Landmarks", so the average error for estimating location of hosts is reduced. The estimation of TBG is still accurate even though the target hosts are not close to Landmarks, or when there is path inflation in the network. Furthermore, TBG can produce an accurate estimate for the location of target hosts even outside the convex polygon formed by the Landmarks.

Although this method has finer granularity, a lot of probes are needed to generate the network topology, and that imposes an addition load on the network. In addition, handling emergency calls is a real time application and can't wait until a network's

topology is determined and delay is calculated before finding caller's location. Thus it is better that TBG be considered as a validation method.

2.3 Other Approaches

2.3.1 IP Clip

IP Calling Identification Presentation (IP Clip) [24] is a mechanism that adds Location Information (LI) of the user as IP option (as a part of IP header) with standard size and structure, at the IP level. In fact, IP Clip uses 40 bytes of extra information in the IP header for carrying the location information of the source hosts. This information can be provided either by the user or by the network. By using IP option, IP Clip is a standard-compliant solution to convey up to 40 bytes of extra information. Network devices can either process this IP option or ignore it. One of the advantages of using this method is that the user is not required to constantly update his LI so the overhead of the network will be reduced [25]. In addition, IP Clip options can be added only to selected IP packets, for example, every SIP packet, which is the most common-used protocol in VoIP services. Using this method, the geographical location of the user is determined based on the geographical location of nearby Access Node (AN), the user's access port number of the user, and an access node ID. IP Clip assumes that only users which are physically near to an AN can connect to it. Verification and validation of the user's LI are done by the ANs; thus accurate

and trustworthy information with good geographical accuracy, at least when accuracy of the AN is available. To trust the validation done by an AN, the information about geographical location of the AN and its ports should be available, valid and updated. In addition, to guarantee correct operation of IP Clip, some constraints should be taken into account; first, the network elements and end hosts which use IP Clip options must have an IP stack with IP Clip-capability and second, in all ANs, the presence of the IP Clip is mandatory [24].

2.3.2 IPv6

As the Internet is in a slow transition to IPv6 [RFC2460], location-awareness may be improved due to the adoption of IPv6. In IPv6, the IP address space is extended from 32 bit to 128 bit and a part of that can be reserved for LI. Addresses in IPv6 can be either statically assigned, distributed by DHCP, or assigned by an auto-configuration[RFC2462] method. By auto-configuration, hosts can generate their own IP address based on a combination of two logical parts: a 64-bit name for the subnetwork (Locator) or Subnet Prefix and a 64-bit name for the host (Identifier) or Interface ID which can be related to MAC address of the host, so it is globally unique. Because of this globally unique structure, it can be used for making a relationship with identification codes like location information.

On the other hand, IPv6 has another capability which reflects any changes in geographical location or movement of network device by updating the IP address [26].

Whenever the correspond subnetwork of a node is changed, first of all, it will update its Locator, recorded in DNS. Thus, a new session will be directly established to its current location. After that, the node will send an ICMP messages for updating Locator, to all of the correspondent nodes [27]. These updates can be used in end system caching which map a PSAP to each user after any location changes and before establishing an emergency call.

One of the features of IPv6 is Duplicate Address Detection (DAD). When a node first comes up on a network link this feature guarantees the uniqueness of the IP address of the node. However, this feature will increase the delay significantly when the location of a node changes in the network.

2.3.3 Outdoor Techniques

2.3.3.1 Getting Information from a GPS Receiver

Global Positioning System(GPS) [28] can provide a good estimate for the location of those users who are fitted with a GPS receiver. However, this method may face some challenges. First, the hardware should be bundled which is an obvious deployment challenge. Second, in some areas such as urban canyons or indoor environments, GPS does not work.

2.3.3.2 Triangulation Calculation

The other possible solution for the wireless users, is triangulation calculation. A wireless user location can be pinpointed by multiple access points and stored in a location server. Then the user can ask about its location from the location server by using SIP event notification [29].

2.3.3.3 Other Outdoor Systems

There are some other techniques which can be used for location determination such as Place Lab [8], Cricket [30] and RADAR [31] locate mobile hosts using 802.11 and GSM beacons. Although these systems potentially can produce a good estimate of host's location, their coverage is limited by the coverage of cell powers. For more coverage, dense deployment of nodes with 802.11 or GSM hardware at known location is required.

2.4 Considerations for Emergency Cases

2.4.1 Databased Approaches

The main problem of most of the existing solutions is keeping information updated requires centralized maintenance at specific times.

The main issue with this class of techniques is that the location information must be manually entered and updated (manually maintained database). In addition, they

often prone to incomplete coverage, outdated information and faulty or false data entry. Furthermore, some of these approaches like Geo Cluster and Geo Track, need special hardware, such as probes.

Another issue for DNS name -based methods in this group is that if DNS names be unavailable or incorrect, the location estimate can not be driven. In the methods which are based on IP addresses, one may face two problems; first, the actual IP address of the user is not always available; for example at the presence of NAT, proxy or VPN the actual IP address will be obscured, or in the case of remote control, the IP address attached to the network is that of a remote machine. Second, even if the actual IP address of a user is available, there is no guarantee that real information of that IP address, such as geographic address, will be available and correct.

However, the layer-2 mechanisms like LLDP-MED or CDP don't have such problems, because they don't use the IP address as the identifier for finding the location of devices. The other issue with these protocols is that every node which is some how involved with an emergency call must implement this protocol.

2.4.2 Measurement Approaches

Measurement techniques generally are time consuming and in the case of Emergency calls, finding the location of the user in a few seconds is vital. So measurement approaches can be used as a validation tool to confirm the location of the user after any change in his/her location and before establishing an emergency call. In addition,

most of measurement methods, need some probes in the network. In some of them like Geo Ping, the density of probing Landmarks is low and it's faster and cheaper than other measurement techniques but may not be accurate. Although CBG provides a better estimate than Geo Ping for the caller's location, it doesn't have enough accuracy. All of the delay-based techniques typically make a poor estimate for the location for most of the targets, with worst case error of 1000km or more [14] that is not accurate at all for the emergency purposes. Compared to Geo Ping, CBG does multiple measurements, so it imposes more overhead on the network and takes much more time to determine the location of the user. The worst cases usually happens for those targets that are far from landmarks. Further more, for the pure delay techniques like Geo ping or CBG, error estimate is related to the distance to the closest So these approaches have to use a lot of carefully chosen Landmark to have a reasonable level of accuracy.The worst case occurs when a user is far from Landmark. Methods like TBG which consider a combination of topology and delay provide a better estimate. The issue is that at first the topology of the network should be generated by an algorithm such as[32] , [33] and [34]. Then, the location of passive Landmarks, which provide the better accuracy, should be validated, so this technique could be costly in terms of delay when considered for a time-critical application.

However, there is a trade off between the time it takes to determine the actual location of Internet user and the accuracy. TBG can be used as a second tool for validation LI of users before an emergency occurs, because it has a rich set of topology

constraints which can be used to verify locations.

2.4.3 IPv6

Using IPv6, the location information of a user may be directly determined by IP address and no additional protocols or measurement tools are needed. The main issue with this protocol is that it is not widely used yet. Furthermore, since user's location information is inferred from the IP address, when the actual IP address of the user is not available, actual location information may not be provided. For instance, Network Address Translations (NATs), firewalls or Virtual Private Networks (VPNs), are generally problematic, because a virtual IP address is assigned to the user. Hence, the real physical location of the caller can not be determined.

2.4.4 Outdoor techniques

Generally, these group of methods are more appropriate for the outdoor users. Hence, they can not be considered as a trustful solution in emergency cases. For instance, in the situations that the emergency caller is inside the building or out of coverage area of a GPS signals. In addition, using these technique requires special hardware, that may not be available for all Internet users.

Figure 2.1 represents a summery of evaluation of some individual approaches in the emergency cases.

	Availability	*Freshness*	*Timeconsuming*	*Accuracy*	*ProxyorNAT*	*RemotLogin*	*NetworkOverhead*
Geo track	o	o	•	o	o	o	o
Geo Cluster	o	o	o	o	o	o	×
Whois look-up	o	o	•	o	×	×	o
MAC Address	o	o	•	•	o	o	o
DHCP	o	o	•	o	o	o	o
LIS	×	o	o	o	•	•	o
CDP	o	•	•	•	•	•	•
LLDP-MED	o	•	•	•	•	•	•
Geo Ping	o	•	×	×	•	•	o
CBG	o	•	×	o	•	•	×
TBG	o	•	×	o	•	•	×
Manually Entered	•	×	•	•	•	•	•
IPv6	×	•	•	•	×	×	×
IPclip	o	o	•	o	•	•	o

Figure 2.1: Evaluation of Some Individual Approaches: "o" denotes a partial limitation, "•" denotes providing a good estimate, "×" denotes a shortage

Chapter 3

Problem Statement

3.1 Emergency Call Handling in VoIP Networks

With a massive shift from the Public Switch Telephone Network (PSTN) to Internet telephony using Voice-over-IP (VoIP), users expect to have at least the same level of service when it comes to making emergency calls. One of the important services is handling emergency calls (e.g. dialing 911 in North America or 112 in Europe). Still, many VoIP service providers do not support this service such as Skype that explicitly refuse handling emergency calls and several other providers as well. However, emergency call handling is one of the mandatory features of every telephony services in future [4]. In section 3.2, the legal requirements on emergency call handling in VoIP networks in the North America and Europe is described, followed by some technical requirements.

In traditional land-line telephones, the telephone number is a key for identifying geographical location of caller, but in VoIP an IP address, for every user is often assigned dynamically, which is not related to a specific location, so the IP address can not be used just like telephone numbers in PSTN. In addition, Internet users can move from one point of wired access to another, while using the same device. For example users can move their VoIP phone or DSL modem to another house or city , so their IP address can be changed. This means that the issue of location determination exists even for fixed-point Internet access such as wired DSL broadband connections. Thus, handling emergency calls in IP telephony systems can not be based on the same mechanisms as the PSTN and a need exists to provide a generic mechanism. Since VoIP users or any other IP-based mobile devices can have access to the Internet anywhere Internet connectivity is available, this mechanism should be independent of the VSP or ISP architecture. Furthermore, with the presence of Network Address Translation (NAT) or Virtual Private Networks (VPN), a virtual IP address will be assigned to the users, so in these cases the IP geolocation[1] techniques are not able to determine actual location of users. Therefore, handling an emergency call in VoIP networks can be divided into four steps [17]:

a. Identifying a call as an emergency

b. Determining the caller's location in an appropriate time

[1]"IP geolocation is the problem of determining the physical location of an Internet user based on IP address" [16], [35].

c. Finding the closest Public Safety Answering Point (PSAP)

d. Providing and representing required information to call taker at the PSAP

The second step, determining the caller's location is the subject of this thesis.

Most VoIP service providers use Session Initiation Protocol (SIP) [RFC3261], for setting up and terminating calls. SIP uses Multipurpose Internet Mail Extensions (MIME) [RFC2045] to format its content. In the SIP-based VoIP networks, SIP User Agents (UAs) usually communicate through a series of SIP severs, using SIP methods such as: INVITE, REGISTER , or BYE. Generally, for each UA, an outbound proxy server is configured which forwards SIP messages on behalf of users [17]. Totally, the procedure of an emergency call in a SIP-based network is as follow:

The caller or the UA that is a soft or hard phone, initiates the emergency call by sending a REGISTER message to the proxy server. This message can include physical address of the user, obtained from any source, for instance as illustrated in figure 3.1, both UAs and outbound SIP proxies can acquire location information directly from a Global Positioning System (GPS) receiver, from data manually entered by the user or by using any other methods described in Chapter 2. The SIP proxy server should routes the call to the most appropriate PSAP based on the caller's location. Each PSAP is dedicated to a specific geographical area, responsible for emergency cases of the users located on that area.Once the proxy server gets the message, it can encode this information to a presence- based GEOPRIV location object format [36] and add the encoded document into the body of SIP message in MIME format,for routing

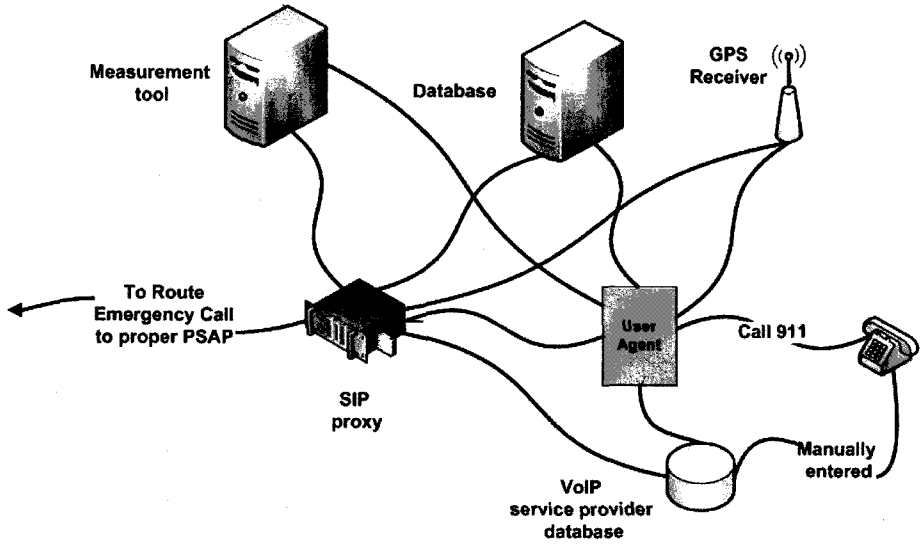

Figure 3.1: Request for location information by UA or SIP Proxy

calls to the proper PSAP. This information can be geographical coordinates, like latitude and longitude values, or civic addresses like: country, city, street names, street numbers and etc. On the other hand, VoIP users are usually nomadic and wherever that they can have access to the Internet, they maybe need to make emergency calls. The mobile users often do not know when they have left the coverage region of on PSAP and entered that of another. In order to route the emergency calls to the correct PSAP, the location information for these users should be always updated and their up-to-date physical address should be always available.

3.2 Requirements

3.2.1 North America

The phone number 911 is used nation wide for any kind of emergency in North America. Dialing 911, emergency caller is connected to the most appropriate PSAP(Public Safety Answering Point). This PSAP dispatches the emergency call to the closest fire station, police station, and medical station.

In 2005, the *First Report and Order and Notice of Proposed Rulemaking* [3], was published by the Federal Communication Commission (FCC), responsible for national and international communication in United State. In this document, some requirements for Enhanced 911 for VoIP service providers are defined. Some of these requirements are as follow:

- The emergency call has to be routed to the most appropriate PSAP based on the caller's location
- The call must provide the caller's number and location
- The location of the caller must be obtained by the VoIP service providers (VSPs) before service initiation
- Performance bounds in terms of delay for call establishment.

However, these requirements are not applied to Internet telephony yet [37].

3.2.2 European Union

European Union Regulatory Framework for Electric Communication [38], which is adopted by European Parliament and the Council of the European Union, contains some guide lines on the requirements for handling emergency calls. Currently, in 17 European countries there are some legal requirements on VoIP service providers for access to the emergency services. Some of these established legal requirements are as follow [39]:

- The emergency call has to be routed to an appropriate emergency response center
- A call back possibility for the emergency response team has to be provided
- A possibility to identify the caller has to be provided
- The location information of the caller has to be provided

Furthermore, in United State and Europe, there are some additional requirements on the latency in an emergency call in the PSTN [40] and GSM [41]. The maximum latency for the user to reach the proper PSAP must not be longer than 10seconds and the estimation of the caller's location must not be longer than 7seconds. [4]. Based on NENA technical information document for NG E9-1-1 (Next Generation Enhanced 9-1-1), call setup time (dialing of last digit on emergency number to ring at the PSAP), under expected peak load must be less than 2 seconds.

3.2.3 Technical Requirements

Totally, law requirements on emergency call handling over VoIP networks is still in progress. However, they are similar to the requirements in the North America. Based on the legal requirements, some technical requirements ca be obtained as follow: [4]

- Provision of caller's number for in order to identification and call back
- Fast provision of caller's location
- Routing the emergency call to the emergency which is responsible for the caller's location
- Highest delay priority for the emergency calls
- Provision of stable connection even under network congestion

In this thesis, we will focus on the first and second requirements: First, Providing location information for the emergency callers in VoIP networks. Second, providing this information with a minimum delay.

Chapter 4

Overview of Location Informtion Server(LIS) Method

4.1 Introduction

As we mentioned in the previous Chapter, in order to support emergency calls in the VoIP networks, the location of the callers must be clear prior to making emergency calls. One of the best proposed methods, which can be used as a general approach, is using Location Information Server (LIS) [42]. In this model, a network entity named LIS [2] is responsible to store location information of network entities. For instance, this information can be a mapping database between a key in the network, such as IP address, and physical location information of network entities. The architecture assumes that this server can be found and utilized at each point of access without

dependency on any remote or dissociated service provider.

Before a device can utilize the LIS to get location information, it should know the address of the LIS. In order to do that, once an VoIP end device attaches to the network, first, it requests it's IP address and obtains it form the local area network DHCP server. Then, based on the obtained IP address, the endpoint device performs a reverse lookup to discover the address of authoritative LIS for that network. Each application service provider (ASP) must have an authoritative LIS assigned to it. Therefor, discovery of the correct LIS in the local access network is the first step for the users that wish to acquire location information from the network. Procedure for LIS discovery is subject of an Internet draft [19]. There are different ways for users to get the address of LIS which contains their location information. For instance, one simple method is hard coding LIS information in devices. However this method is not suitable for nomadic users where the address of a LIS may not be accessible for another part of the network that the user has joint.

After LIS discovery, the next step is sending location query from the users to the discovered LIS. Making location request can be done in two modes: location-by-value and location-by- reference. The former asks about actual value of geographical address which is civic address (province, city, street name, street number, zip code). The second provides a URI which refers to a particular service. To send queries from the users to the LIS and get responses from the LIS to the users, a protocol named HTTP Enabled Location Delivery (HELD) is used [20]. This protocol basically

defines three types of messages: location-request, location- response, and error. The location is requested by users by value or reference and the result is provided by LIS in location-response message. If the location of the user can not be found in LIS database, en Error message is sent to the users. The last issue is how a LIS is going to determine the location of end devices [43]. However, this technique has some issues related to the emergency services which we will discuss in the next Chapter.

4.2 Architecture and Description

Figure 4.1 represents how the VoIP users can obtain their location information from the LIS and send the required information to the proxy server. The following steps are taken by each user in this mechanism:

- Step 1: The VoIP endpoint device gets IP address from the local DHCP server
- Step 2: The VoIP endpoint device discovers the LIS and sends a location query to it, the LIS responses to the user with the location information
- Step 3: The VoIP endpoint device puts the location information in the SIP REGISTER message and sends it to the SIP proxy server

After this steps, the proxy server is aware of the location of the caller. To handle the emergency calls, the proxy server routes the call to the most appropriate PSAP that has determined based on the user's location by a mapping protocol such as LoST [44].

Another protocol which can be used for routing emergency calls based on the caller's location, is LUMP(Location-to-URL Mapping Protocol) which maps a location to one or more URLs [45].

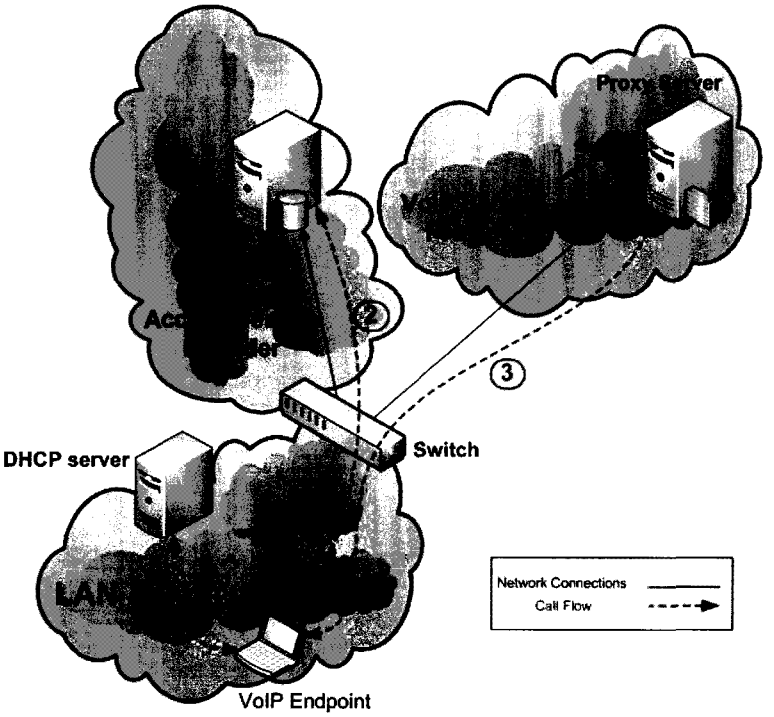

Figure 4.1: Basic LIS Architecture

Figure 4.2 represents the sequence diagram for making phone calls in the LIS model:

- **t1:** The user joints the network, gets the IP address of the local DHCP server, discovers the LIS and sends a query to the LIS and asks for the location information

- **t2:** The LIS receives the query from the user, starts lookup based on IP address of the user
- **t3:** The LIS has found an location object mapped to the IP address of the user and replies the user with its location object
- **t4:** The user receives location information from the LIS, puts this information into the REGISTER message and sends it to the Proxy server
- **t5:** The proxy server gets user's request with the location information in the SIP message
- **t6:** Based on the users location information in the REGISTER message, the proxy server determines the appropriate PSAP and forwards the call to it
- **t7:** The PSAP gets the emergency call with location information

Since there was no simulation results or other types of measurements in the literature for this method, we also have to implement the LIS method in the network simulator NS-2 to compare with our proposed solution. Then we have measured the delay imposed by this model in the network. The latency which we have measured is the time elapsed between the call initiation and the time that the proxy server gets the user's messages with the location information ($t5 - t1$ in Figure 4.2).

We have repeated the simulation with different topologies and different number of users. The results of the simulations is compared with our proposed model , and

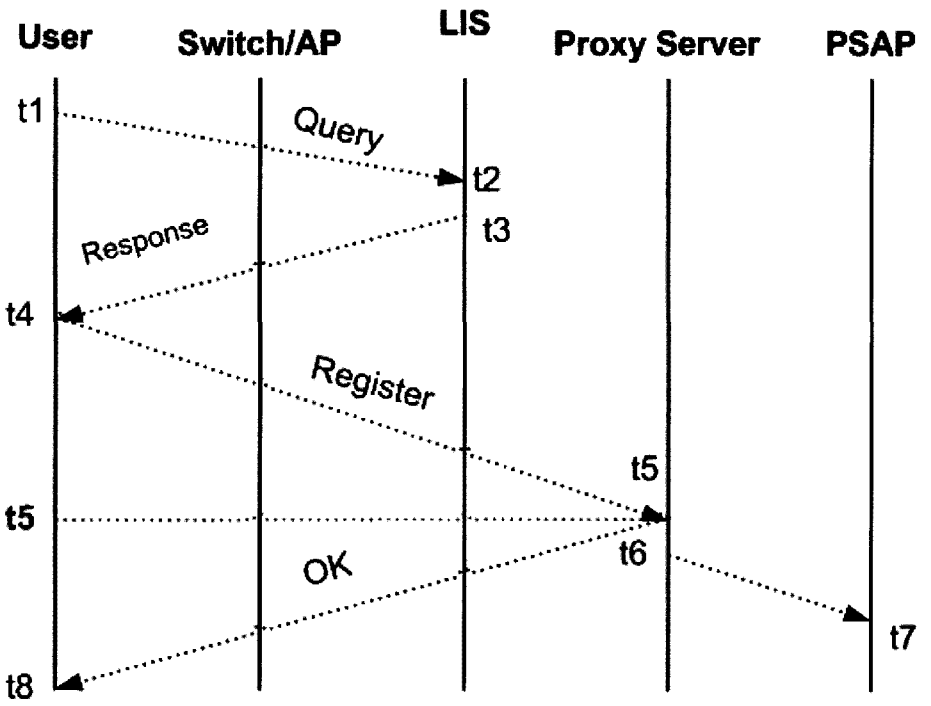

Figure 4.2: Call Sequence Diagram for the LIS Model

has been presented in Chapter 6.

Chapter 5

A Data Link Layer Proposal for Location Determination in VoIP

5.1 Overview of LLDP-MED

As we described in section 2, there are several methods to determine the physical location of a caller in VoIP networks. One of these techniques introduced in [1] is using Cisco Discovery Protocol (CDP). Using this protocol, all of the switches send messages contain the switch name and the port number periodically to the end users. Then every user can send a query to a database, located in the administrative domain, and ask about its physical location. This database contains a mapping between the switch/port number and the location object, that is refreshed on a periodic basis. Because every port of a switch leads to a jack in a specific room, the accuracy of this

method is room level which is enough for the emergency cases.

Since CDP is Cisco-specific, a general solution called Link Layer Discovery Protocol-Media Endpoint Discovery(LLDP-MED) is introduced. In fact, Link Layer Discovery Protocol (LLDP) or IEEE 802.1AB is a multi vendor standard which can be used for IP telephony in Enterprise networks.

LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP for the location discovery of end devices [22]. This standard allows some devices like switches to advertise information in LLDPDU frame to the endpoints. The information distributed via LLDP can be stored by the recipients in a standard management information base (MIB) which can be accessed by a network management system (NMS) [22]. This protocol can be used to support some advanced features for Voice Over IP (VoIP) endpoint devices such as handling emergency calls. Figure 5.1 illustrates how LLDP-MED works. The following steps are taken by users using this protocol:

- Step 1: The switch advertises switch/port number to the endpoint device
- Step 2: The endpoint device sends a query to the local LLDP database, existing in its administratively domain, and asks about the location, based on received switch/port number
- Step 3: The endpoint devices obtains its physical location from the LLDP database, existing in each administratively domain. This database is maintained and updated periodically by domain administrative.

- Step 4: The endpoint device uses the obtained information in location based applications

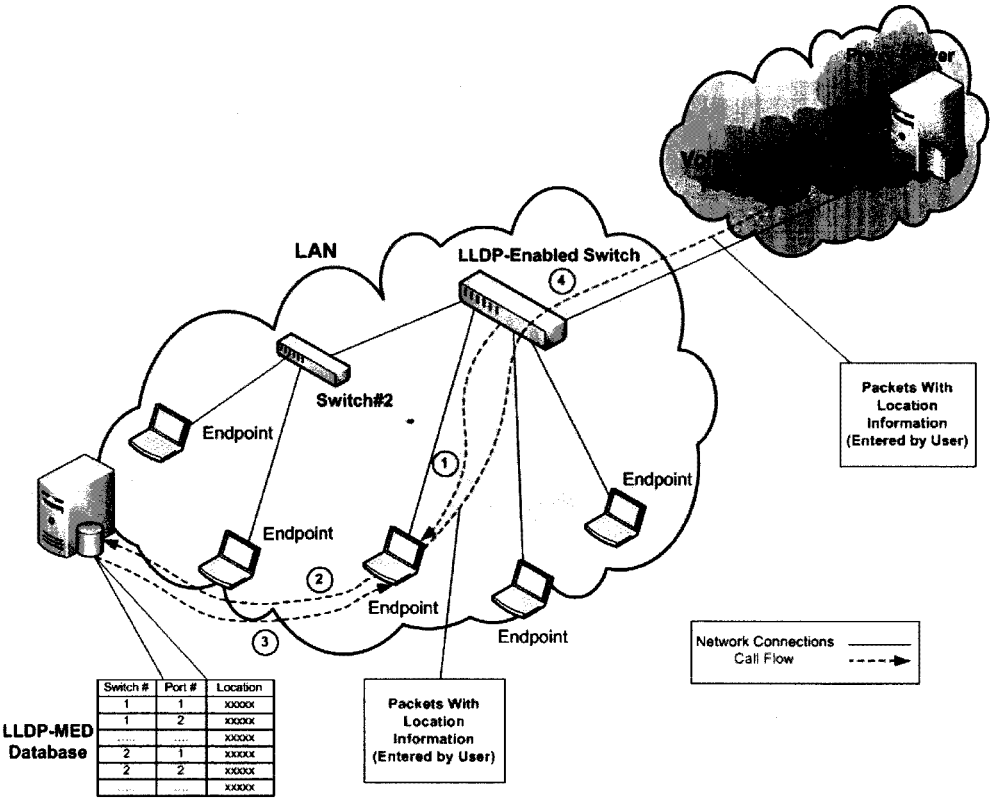

Figure 5.1: Basic LLDP-MED Architecture

This standard is not specific to any VoIP architecture or system management architecture. Basically, the LLDP-enabled switches advertise the location information to the end point devices periodically.

However, our proposed method is based on another potential of the LLDP -enabled devices. This ability is inserting information to the mac layer of the passing packets. In facts, once a packet goes through an LLDP-enabled switch, it will be stamped by

the location information. The switches can do it for all of the incoming packets or can check the LLDP-MED TLV types and just do it for special type of traffics such as VoIP packets. In the following section we have more explanation of different fields of LLDP-MED.

5.2 LLDP-MED Header Fields

Figure 5.2 shows the main format of LLDP-MED frame.

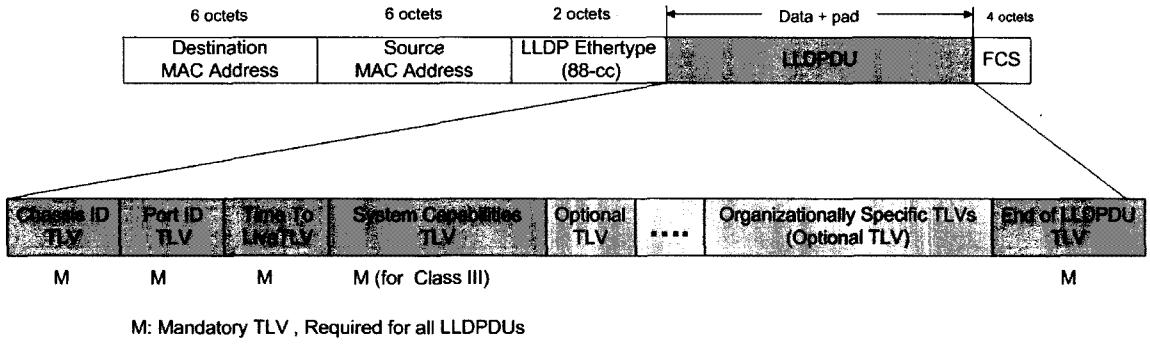

Figure 5.2: LLDP PDU Format

Some of these TLVs (Type Length Values) are mandatory: Chassis ID, Port ID, TTL, System Capabilities and End of LLDPDU. Each LLDPDU shall contain one, and only one of each mandatory TLVs. These fields value remain constant while the connection remains operational. Each mandatory TLV, has two main parts: header and information. The first part contains TLV type and the length of the information string and the second part contains the actual information. Figure 5.3 illustrates one of these TLVs which can be used for chassis or port ID.

The first mandatory TLV is chassis ID that identifies the chassis station. Based on

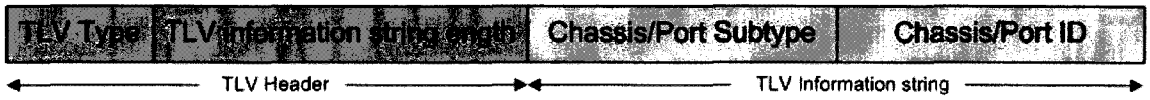

Figure 5.3: Chassis/Port ID LVs

the chassis subtype, different types of information can be used as chassis ID; These types can be MAC address, network address, or a locally assigned name. The second mandatory TLV is port ID that identifies the port component associated LLDP agent. Similar to chassis ID TLV, based on port subtype, different types of information such as MAC address, network address, agent circuit ID, or a locally assigned name can be used as port ID information. In the next TLV, TTL, the information string part has one field, an integer value in the range $0 < t < 65536$ seconds and must be set to the computed value at the the time the LLDPDU is constructed. In the system capabilities TLV, which is mandatory only for class III of endpoint devices (e.g. IP telephone, Soft-phone, etc.)[22], the information string contains two parts: the first one indicates the type of capabilities that a system may have and the second one indicates that these capabilities are enabled or not. The last mandatory TLV indicates the end of LLDPDU which is a two octets fields with all zero bites. In addition to the mandatory TLVs, some optional TLVs can be added to the LLDP PDU such as: Port description TLV, System name TLV, System description TLV, System capabilities TLV, and Management address TLV. These optional parts provide various details

about the connected device. Furthermore, some organizationally-specific TLV also can be defined, either by the professional organizations or the individual vendors. This category of TLVs is provided to allow different organizations to define TLVs that carry additional information for the network entities and can be set to use in special purposes. The basic format for organizationally specific TLV is shown in Figure 5.4.

Some of these specific TLVs are as bellow:

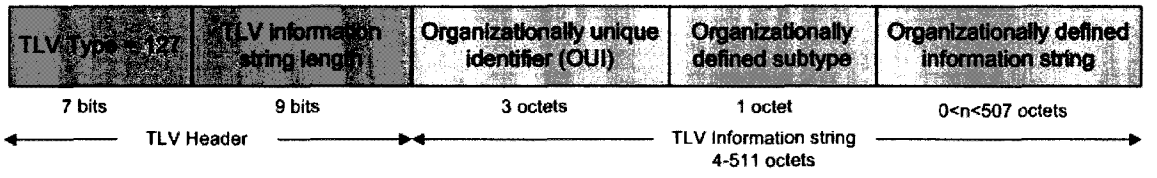

Figure 5.4: Basic Format for Organizationally Specific TLVs.

a. **LLDP-MED capabilities:** which indicates that network device supports this protocol or not.

b. **Network Policy:** which indicates the type of the application that the network device is using such as: voice, softphone voice, and etc.

c. **End Point Location Identification Discovery:** which indicates location data format and location information of the end device.

For the last one, "Location Identification TLV", there are three forms of identifier information that may be delivered by this standard:

I. Coordinate-based data format contains: Latitude, Longitude and Altitude, as defined by IETF RFC 3825 [46]

II. Civic address data format, as defined by IETF (refer to Annex B of [22]) contains: supported language, country code, province, city, street name, street number, zip code

III. Emergency call services ELIN (Equipment Line Item Number), as described for example by NENA TID 07-501 [47].

All of these formats are harmonized and supported by NENA (National Emergency Number Association) [47], TIA-TSB-146 Emergency Call Services [48] or other similar standards. The format of this TLV (Location ID) is shown in Figure 5.5.

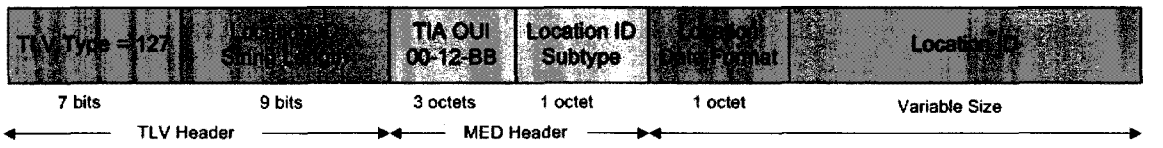

Figure 5.5: Location Identification TLV Format

We have used this TLV to provide location information of VoIP users. In our proposed solution, the switch fills the location identification TLV based on a mapping database which maps chassis/port number to a location object. The switch can do it for all of the incoming packets or just do it for some special application such as VoIP traffics, by checking the net policy TLV. In the next section, we provide more details

about the function of the switches on these TLVs in the network .

Another capability of this protocol is to provide topology change notification, when a new remote device is connected to a local port of an LLDP-MED-enable network device or when a remote device is removed from a local port. This ability allows move tracking on the endpoint devices in the network. However, based on the standard [22], it is not recommended that critical applications such as handling emergency calls be based on upon topology change notifications only.

For IEEE 802.11 wireless access points, LLDP-MED database provide sufficient location resolution. Then the location of the access point will be supplied as the location of each clients of that access point. However, this may not be true for the clients in the larger cells than those of IEEE 802.11 such as IEEE 802.16 (WiMAX) and IEEE 802.22

5.3 System Architecture of Proposed Solution

In our proposed model, we have assumed that all of the switches and the endpoint devices are supporting this protocol. In fact, we have considered LLDP-MED as the data link layer protocol in the network. The VoIP users use SIP protocol in order to make phone calls, including the emergency ones. The protocols that are used in transport and network layer are out of the scope of this research.

For clarification, for the rest of this thesis when we refer to the user we are assuming that the VoIP client software does this process not something manually by the user.

Figure 5.6 illustrated the architecture of our proposed solution. The main goal is providing the location information of each VoIP user for the related SIP proxy server. Based on the figure 5.6, we can summarized our solution into three steps:

1. The VoIP user initiates the call by sending a REGISTER message to the SIP proxy server. This message contains some information in the data link layer including LLDP headers, such as: the application type, the type of the device, and etc.

2. The first node in the network that receives this packet, is the first level switch or the access point, located at the LAN that the user is connected to it. In each administrative domain, there is a local database that binds a location object to every Chassis/Port ID in that network. Receiving each packet, the switch does a lookup in this database to find associated location object. This search is performed by the switch/access point based on its chassis ID and the ID of the port that it has received the packet.

3. The switch fills the location Information TLV in the data link layer of SIP REGISTER message and then forwards it to the SIP proxy server. Now the proxy server gets a message, with the information about the location of the sender in the data link layer.

We have implemented this model in the network simulator NS-2. In order to do this, we have added the LLDP-MED headers to the existing MAC headers in NS-2.

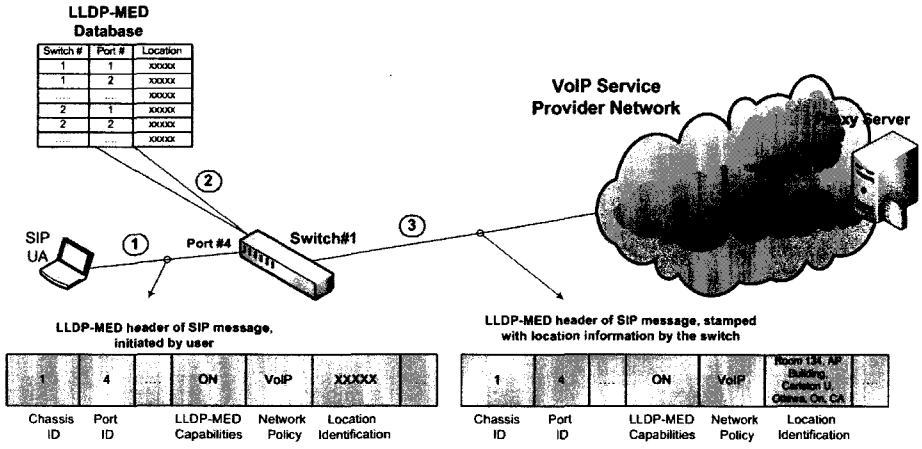

Figure 5.6: Proposed Solution Architecture

Then we have created a new agent as the switch/access point. This new agent receives the packets from the SIP users, fills the location information fields by searching in LLDP database, which we have created for that domain, and finally forwards the packet to the proxy server. Since we have generated only VoIP traffic in the network, the switch does it for all of the packets. in the next Chapter, we provide more NS-2 implementation details.

Figure 5.7 represents the sequence diagram for making phone calls in our proposed solution:

- **t1:** The user joints the network, initiates a call, and sends a REGISTER message to the proxy server via switch/AP

- **t2:** The switch/AP receives the message from the user, starts look up based on the switch/port number that the user is connected to it

- **t3:** The switch/AP has found a location object mapped to the port number, fills the location information field in LLDP-MED header and forwards the message to the proxy server
- **t4:** The proxy server gets users request with the location information in the MAC header
- **t5:** Based on the users location information in the REGISTER message, the proxy server determines the appropriate PSAP and forward the call to it
- **t6:** PSAP gets the EC with Location Information

Then we have measured the delay imposed by this model in the network. The latency which we have measured is the time elapsed between the call initiation and the time that the proxy server gets the user's messages with the location information in the MAC header ($t4 - t1$ in Figure 5.7).

We have repeated the simulations for different topologies and different number of users. The results of the simulations is compared with the other method, LIS, and has been presented in Chapter 6.

Now the proxy server by looking at the mac headers of the incoming packet is aware of the location of the emergency caller that is the main goal of this research. Then, by using a mapping protocol like LoST [44], the proxy server is able to route the emergency call to the most appropriate PSAP. Another protocol which can be used for routing emergency calls based on the caller's location, is LUMP(Location-to-URL

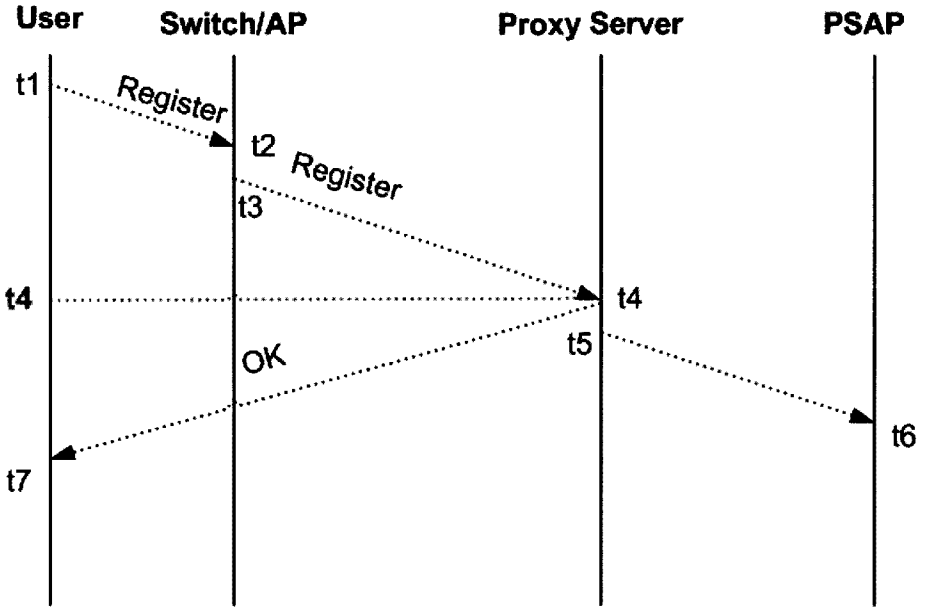

Figure 5.7: Call Sequence Diagram for the Proposed Solution

Mapping Protocol) which maps a location to one or more URLs [45].

5.4 Comparing The Proposed Solution with LIS

5.4.1 Security Issues

In the LIS solution, at first, the user should discover the related LIS and then send a request message to it and ask about its location. Then the LIS replies the user with the location information. Finally the user puts this information in the SIP INVITE message to make the emergency call. However, from the security point of view, this method may face some concerns. First, the procedure of LIS discovery raises security

issues. Some mechanisms should be considered in the access network to prevent man-in-the-middle adversaries from malicious nodes that present themselves as an LIS [49]. Second , the users, no matter that they have gotten information from the LIS or not, could put false information in the INVITE message and make fake emergency calls. This causes the PSAP and call takers to be busy and not be able to serve real emergency callers. The other possibility is that one user can make several fake emergency calls with different location information that can cause the same problem in the network.

The existing approaches by LLDP-MED is similar to LIS and finally it is the user that send location information to the proxy server [1]. Our LLDP-based solution relies on switches to insert the location information. Therefore users are not able to put fake information. On the other hand, users are directly connected to the switch, so the issues regarding discover the correct database is automatically removed. In addition, the switch can prevent making several emergency calls in a short interval from one port in the case that a malicious user tries to rub an application and make several fake emergency call at the same time to keep the PSAP and call takers busy.

5.4.2 More Accuracy and Suitable for Nomadic Users

LIS is a database that keeps information for mapping location objects and another identification object for the users, such as IP address or MAC address. Internet users may move their device from one point of wired access to another, so some

characteristics like MAC address of the device can't be used. When a user leaves a network and enters a new one, it takes a new IP address in the range of new network which may not exist in the LIS database. Then the users should discover the LIS and ask location from it. However, in LLDP case, since the location information is tied to port number, once a user connects a port in a new network, location of that port is automatically considered as its location and no additional messages are needed. Although some protocols such as LLDP can be used for topology changes notifications, based on the standard (ANSI/TIA-1057 TIA [22]), for the critical applications such as handling emergency calls, only this information is not reliable.

5.4.3 Coverage of all Users

The database in the LIS is based on the IP address. A lot of users in the network do not have a fixed IP address. Any time they connect to the network, they will get a new IP address from DHCP server. So there is no guarantee that the LIS database contains information for all possible IP addresses. The LLDP databases map switch/port number to location with higher accuracy since they are smaller and locally maintained. Since users will be connected through a specific switch/port at a given time, users are much more likely to have their location correctly identified in the LLDP case than the LIS case.

5.4.4 Determining the user's location at the time of making an Emergency call

For the cases that a user tries to make an emergency call at time that it joins a new network, several messages should be exchanged to find the LIS and then ask it for location. However, for LLDP, no additional messages are needed and the switch is able to insert information in the emergency call packets.

5.4.5 Dependency on IP Address

Since the LIS database is based on IP addresses, some problems may happen in the location discovery procedure, such as presence of NAT, proxy or VPN that obscured the actual IP address of the users or remote control cases that IP address of remote machine is attached.

Chapter 6

Simulation Results and Analysis

In this section, we evaluate the performance of the proposed solution through simulation results. Moreover, we compare the performance of our method with that of LIS. For this purpose, we have considered the latency and network congestion as the measures in this evaluation. The network congestion is defined at the proxy level and defined as the number of simultaneous calls that are dropped at the first level LLDP-MED switches/access point(s) rather that being forwarded to the SIP proxy server. The simulation model is implemented in NS-2 [50]. We are generally assuming that emergency callers use SIP for setting up and terminating the calls.

All of the simulation results are based on our implementations for LIS and our proposed solution. In both methods, we have not considered the processing time (the time that it takes to LIS or LLDP-MED agent to find the location object in the database). Furthermore, in LIS case, we have assumed that there is only one LIS for

all users in the network. Hence, the time that it takes to the users to find the related LIS in not considered in our simulations.

6.1 Simulation Setup

Unless otherwise specified, we assume that the links between the access points, routers and servers are 10-Mbps full duplex links with 10ms propagation delay. The NS-2 queuing model for each link is DropTail.

For the wireless scenarios, we have considered the NS-2 default wireless parameters. The default value for the wireless datarate is 2 Mbps. The datarate is proportionally increased with the number of users.

In all wired scenarios, wired users are connected through 2-Mbs full duplex links, where the propagation delay of each link is 2ms. and the NS-2 queuing model for each link is DropTail. The Size of the SIP packets carrying the location information of the VoIP users is assumed to be 300 bytes. The table bellow presents a summery of our simulation settings:

Table 6.1: Simulation Setups

	Bandwidth	**Propagation Delay**	**Queue Model**
Wired User Links	2 Mbps	2 msec	DropTail
Backbone Links	10 Mbps	10 msec	DropTail

6.2 NS-2 Modifications

In this section, we explain the main modifications that we have made in NS-2 codebase in order to implement our proposed solution as well as the LIS method. In Appendix A, we provide the list of all modified and created source files, and their descriptions. For the SIP protocol , we have used a SIP module developed by Rui Prior for NS 2.27 [51] and modified it to implement two methods. Although we have used SIP protocol to in order to making calls in our simulations, our proposed method does not depend on any upper layer protocols and any protocol rather than SIP can be used.
The most important modification that have been done are as follow:

6.2.1 LLDP-MED Modifications

- **LLDP-MED Switch:** *Agents* in NS-2 are used as traffic endpoints or at various protocol layers. They are responsible for sending and receiving the packets. One of the most important part of our implementations in NS-2 was defining the new agents. In order to deploy our proposed solution, we created a *SIP Switch Agent* for using in the wireline topologies. We have considered this agent as a first level LLDP enabled switch and defined two main functions for it. The first function is responsible for receiving the packets from the SIP user agents. Using this function, the packets are processed and the LLDP-MED fields of them is filled with the related location information, obtained from a database. After filling location information fields, another function in this agent forwards the

packet to their original destination.

- **Access Point :** Fixed and mobile nodes have different definitions in NS-2. If we want to have a combination of both groups, we need a gateway between the wireless and wired nodes. In NS-2, an agent, named *dsdv* is responsible to perform as a gateway. We have used this agent and modified it to become an LLDP-MED enabled access points. Doing the necessary modifications, this agent got access to the mac header of packets. Once it receives the packets from the wireless user agents, it adds location information to the location identification fields of packets and finally forwards them to their final destination.

- **LLDP-MED Headers:** We made the necessary modifications to the MAC headers of the packets in order to add *LLDP-MED* headers to it. The fields that we added contained four TLVs: Chassis ID, Port ID, System Capabilities, and Location Identification. Each TLV had several fields such as: type, length, information string, and etc. In our implementation we added all of the mandatory TLVs for the LLDP-MED. However, the only field that was filled with the real information was the location ID part.

6.2.2 LIS Modifications

- **LIS:** Another agent we implemented was a new SIP agent, *LIS*. This agent was modeled after the existing SIP Proxy Agent in NS-2 SIP module. In order to add this agent to the SIP module and also adding required message for this agent to communicate with the other SIP elements, we have added and modified several codebases in SIP module of NS-2.

  The LIS agent was responsible to receive the QUERY messages from the users, process their QUERYs and obtain the location identification of each user, and finally reply them with their location information. This information was sent by the users to the SIP proxy agent.

  In addition we had to modify SIP User Agent to communicate with the LIS agent. For this purpose, we added a new variable to the SIP setting which indicated the responsible LIS of each user agent. In our implementations, LIS discovery was done manually. I fact by define a user, its related LIS is defined as well. Furthermore, by adding some functions to the SIP user agent, it was able to process query response from the LIS, obtain its location information, add it to the REGISTER message and send it to the SIP proxy server.

- **QUERY and RESPONSE:** Based on the SIP module in NS-2, different SIP agents used various types of messages to communicate. In order to make communication between the user agents and the LIS agent, we created a pair of

messages, named *QUERY* and *QUERY RESPONSE*. The users send their location query with *QUERY* to the *LIS* agent and *LIS* agent replies them with *QUERY RESPONSE*, including location information.

We should mention that these type of messages are only added to implement the LIS method and they are not a part of SIP protocol.

6.3 Simulation Results and Discussions for Wireless Users

In the following, we compare the performance of our proposed solution with that of the LIS in a number of scenarios for wireless users. In each scenario, we measure the latency and network congestion in both methods.

It should be mentioned that we have assumed that there is only one LIS for all of the users in the network, hence the time that it takes to the user to discover the LIS, is not considered in our simulations.

6.3.1 Simultaneous Calls Using Single Access Point

In this scenario, all users are connected to the network through a single access point. We also consider a worst case scenario in which all users send their requests for the emergency calls simultaneously. This scenario can represent a real world case such as a natural disaster or fire in a large building where a large number of users try to

make emergency calls at the same time.

Figures 6.1 and 6.2 illustrate the network topology in this scenario for LLDP-MED and LIS, respectively.

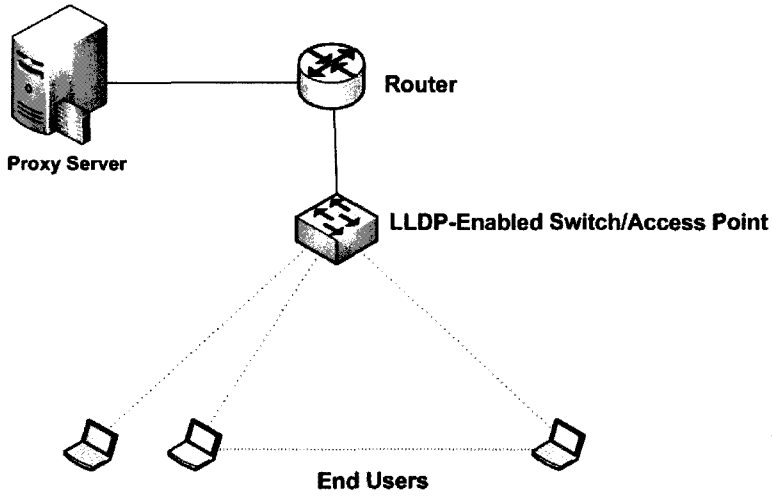

Figure 6.1: LLDP-MED topology Using Single Access Point

•Delay

The measured delay in this scenario is the time elapsed between emergency call initiation and the time that the proxy server gets the user's messages with the location information. (The delay in Figures 5.7 and 4.2 is equal to $t4 - t1$ and $t5 - t1$, respectively.)

Figure 6.3 shows the average delay in LLDP-MED and LIS for different number of wireless users in this scenario. The error bars depicted in the figure illustrate the 95% confidence interval. one can note that the average delay for the LLDP-MED is lower than the average delay for LIS. The reason is that based on the LIS method, each user making an emergency call has to first send a location query to the LIS and wait

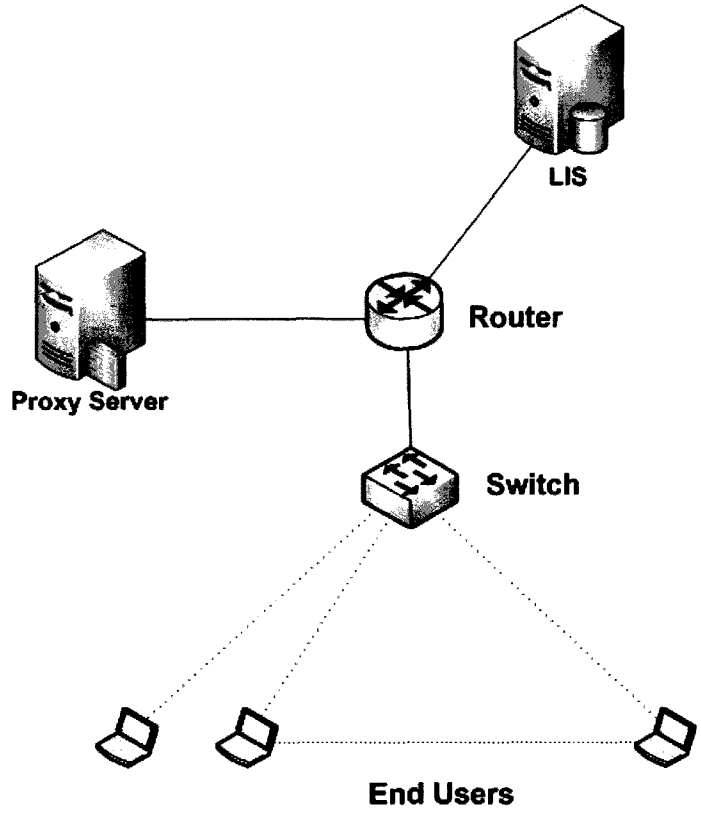

Figure 6.2: LIS topology Using Single Access Point

for the server reply. once the user receives the location information from the LIS, it can send REGISTER message to the proxy server. This means that the user can not make an emergency call before receiving location information from the LIS. However, in LLDP-MED the access point inserts the location information in the REGISTER message sent by the user. In other words, the user does not have to wait for the location information to make the emergency call in LLDP-MED method. Therefore, users experience much less delay with LLDPMED compared to LIS and there is no overlap for the confidence intervals.

It can also be seen that the average delay increases with the number of users for

both LLDP-MED and LIS. The reason is that as the number of users increases, the access point receives more requests and, hence, the queuing delay experienced by the packets raises.

Furthermore, it can be noted in figure 6.3 that for both LLDP-MED and LIS, the average delay parasitically increases when the number of users becomes more than 17. The reason is that the access point can service a limited number of simultaneously requests. As the number of users increases, some requests are dropped at the access point. Those users whose requests are dropped at the access point, do not receive any "OK" message from the proxy server. In this case, the users resend their request after a timeout (0.5 sec in our simulation). Therefore, the average delay for those users increases.

•Network Congestion

The number of dropped requests versus different number of users for LLDP-MED and LIS are presented in Figures 6.4 and 6.5, respectively. As the number of users increases, more users have to resend their requests due to dropped requests at the access point in both methods. For example in Figure 6.4, when 90 users try to make emergency calls simultaneously, the access point drops 71 requests.

In this case, those users with dropped requests resend their request after a time out (0.5 sec in our simulations). In the second round, some requests are dropped again and have to be resent after another timeout (1.5 sec in our simulations). This process repeats until all requests can get through the access point.

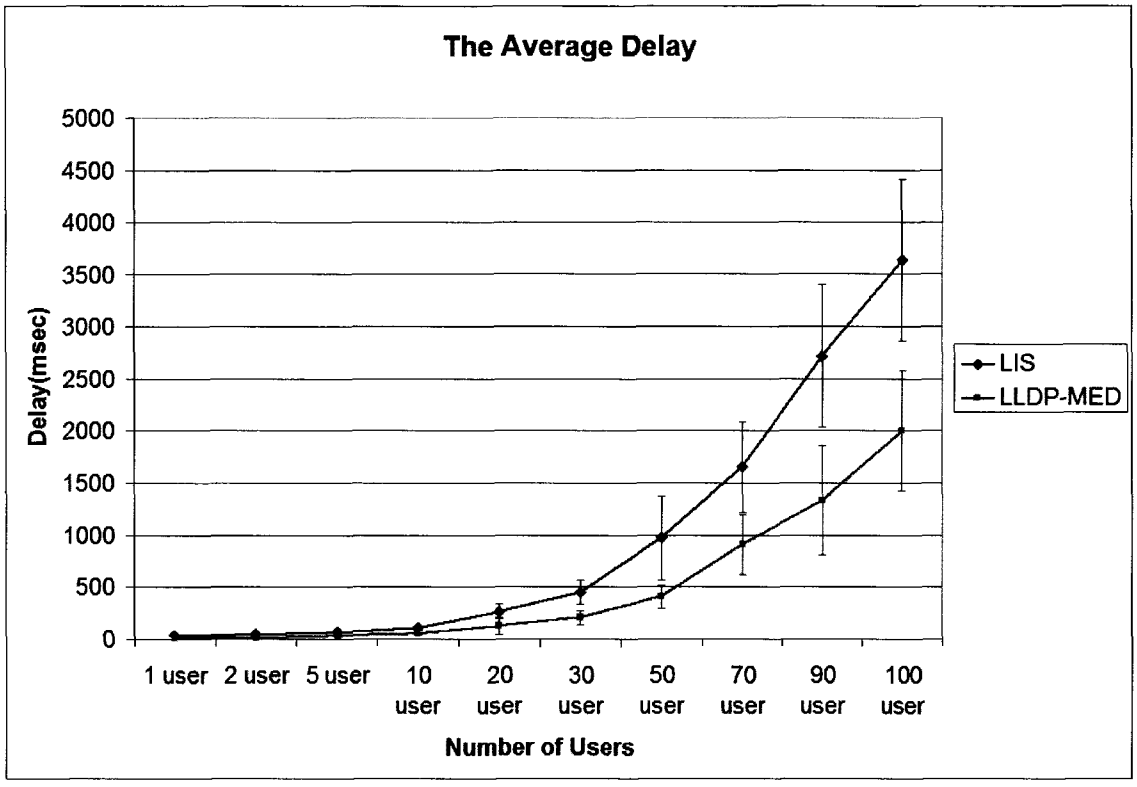

Figure 6.3: The Average Delay Versus the Number of Users, Using Single Access Point

6.3.2 Simultaneous Calls using Multiple Access Points

In the second scenario, we consider a different topology with multiple access points depicted in Figures 6.6 and 6.7 for LLDP-MED and LIS perspectively.

This scenario is a less pressing scenario compared to the previous one. We assumed that the number of access points is proportional to the number of users (one access point per 10 users). In these new topologies, the position of the access points and the their connected users effected the performance of the network. The access points and their connected users must be placed far enough from each other to avoid interference.

In the previous scenario a single access point was able to handle up to 17 users

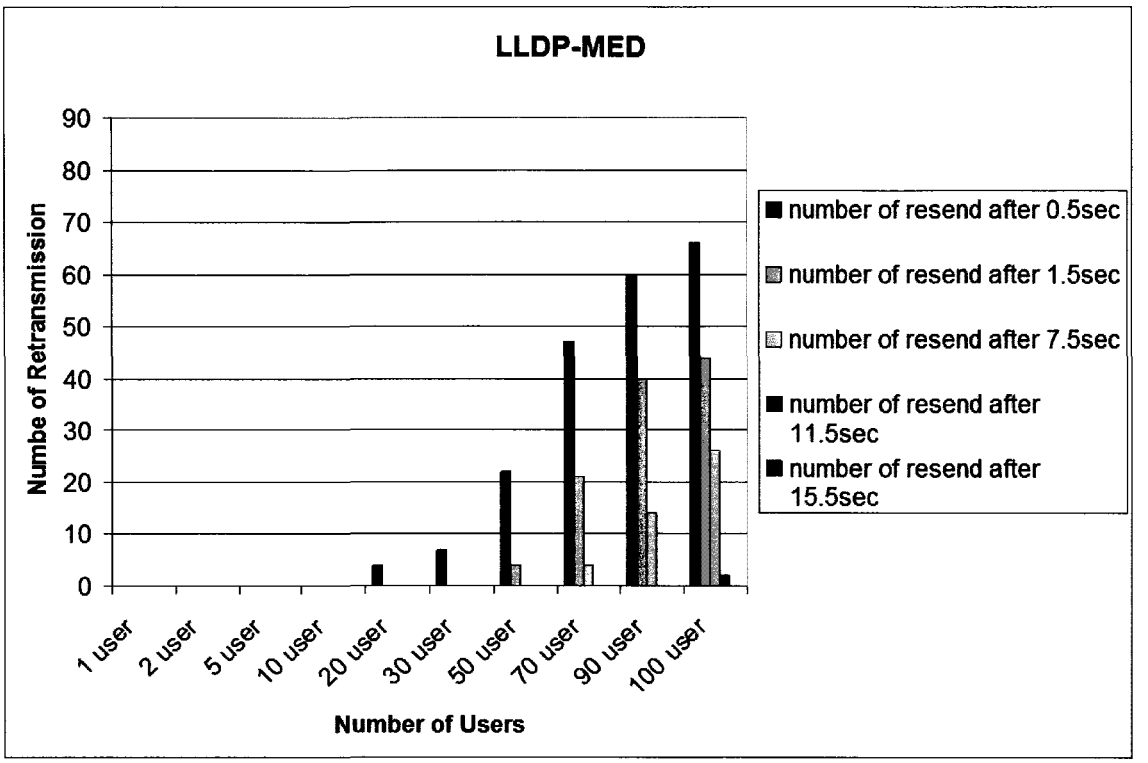

Figure 6.4: The Number of Retransmission Versus the Number of Users, in LLDP-MED Method

and we expected no packet drop and retransmission for this scenario, when there is an access point for every 10 users. However, still there was some packet drops for more than 50 users, happened at the access points.

•Delay

Similar to the previous scenario, the measured delay is the time elapsed between emergency call initiation and the time that the proxy server gets the user's messages with the location information. (The delay in Figures 5.7 and 4.2 is equal to $t4 - t1$ and $t5 - t1$, respectively.)

Figure 6.8 illustrates the measured delay for both LLDP-MED and LIS method in

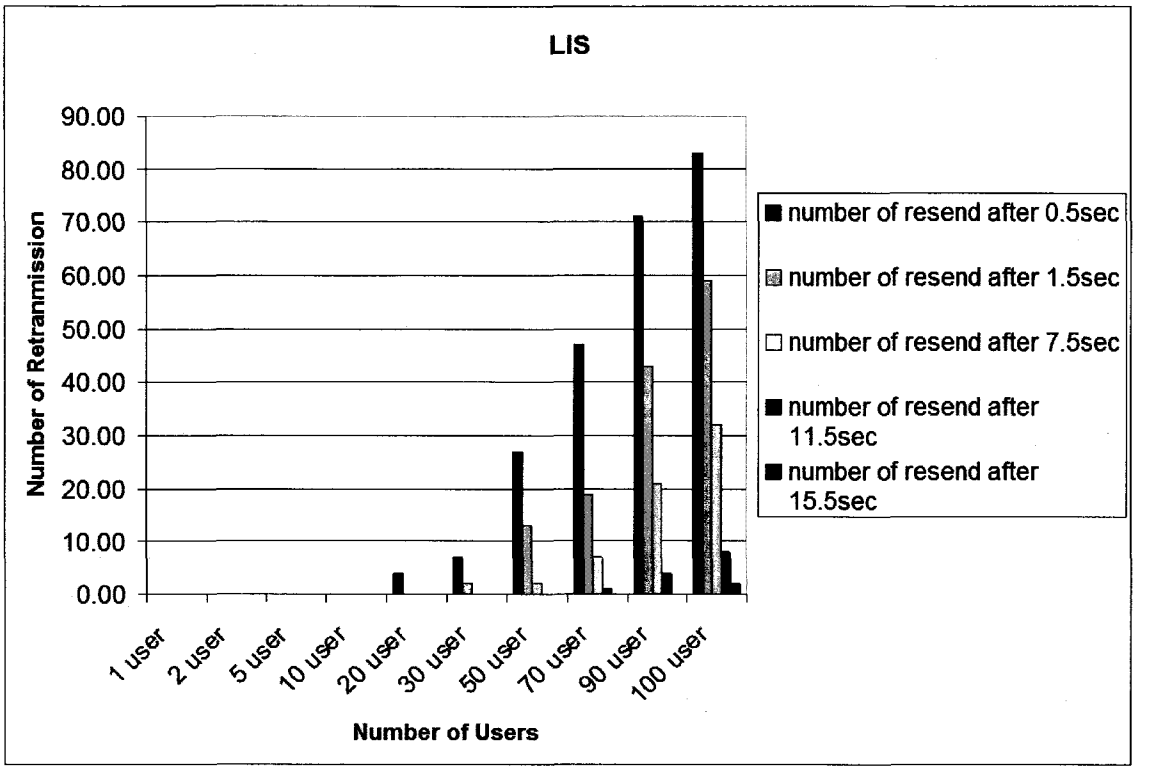

Figure 6.5: The Number of Retransmission Versus the Number of Users, in LIS Method

this scenario. The error bars depicted in this figure illustrate 95% confidence interval. It can be noted that the average delay for the LLDP-MED method in this scenario is much lower than the average delay for the LIS as well. The reason is very similar to the previous scenario; The time that takes to the users to obtain their location information from the LIS, befor sending REGISTER message to the proxy server causes more delay for the users in the LIS method.

However, the average delay in this scenario is significantly lower than the first scenario. The reason is that as the number of access points increases, there is more queues for the packets, hence, the queuing delay experienced by the packets decreases.

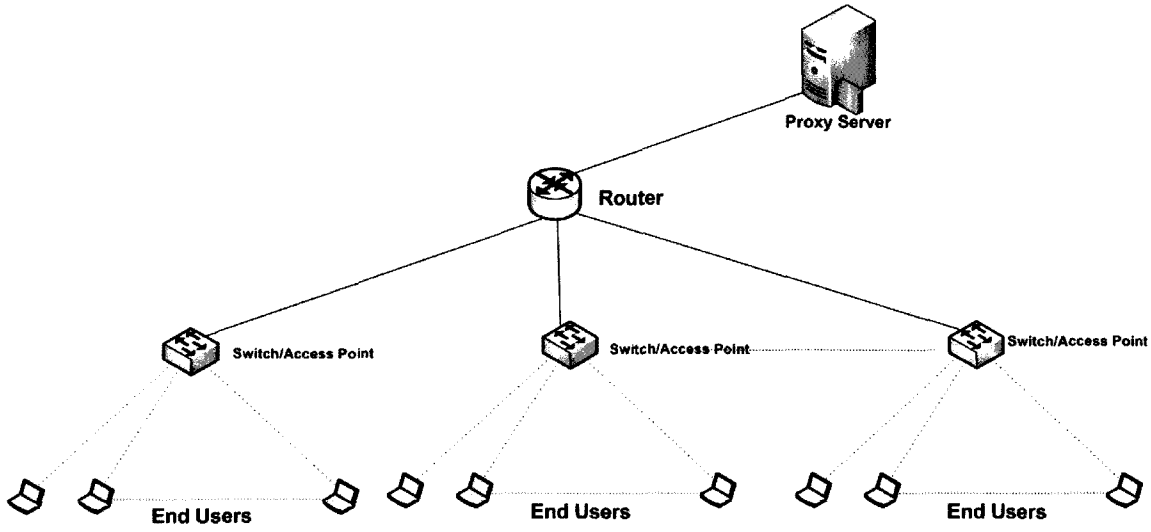

Figure 6.6: LLDP-MED Architecture Using Multiple Access Points

•Network Congestion

As it was mentioned before, for more than 50 users, even with using multiple access points, still some packet drops and retransmissions happen. Figure 6.9 illustrates the number of retransmission for LIS and LLDP-MED in this scenario. However, the number of dropped packets in this scenario, is significantly less than the previous one. Furthermore, all of the requests can get through the access point after the second attempt.

6.3.3 Non-Simultaneous Calls Using Single Access Point

In this part, we consider a different behavior of the emergency callers, making calls in the different portions of time. The topology of this scenario is the same as the first scenario. The only difference is that instead of simultaneous calls, the users initiate emergency calls at a random time. We generated this random time with a uniform

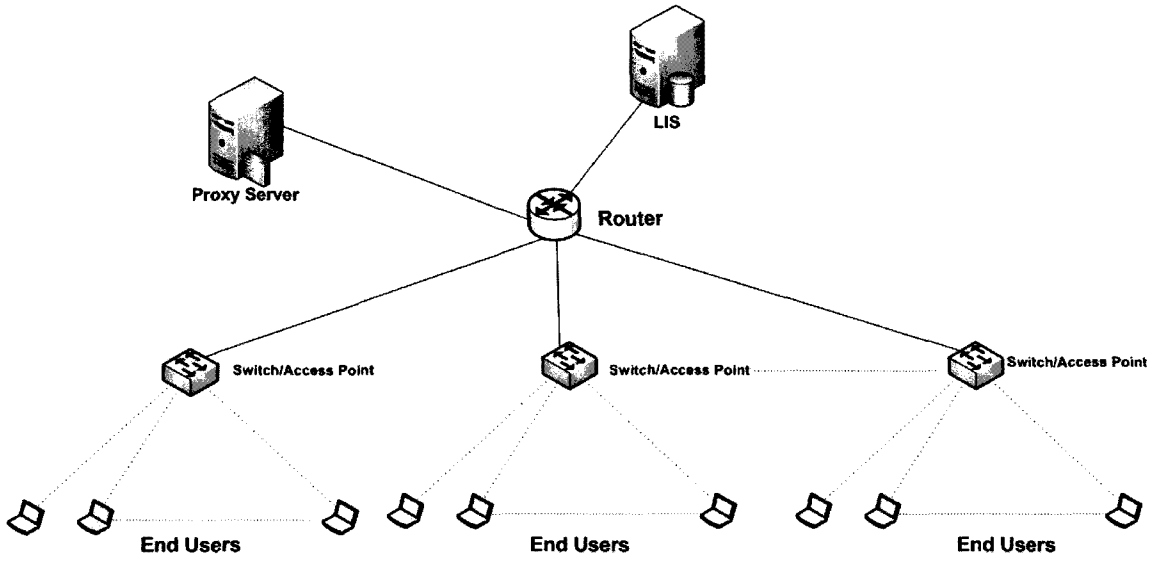

Figure 6.7: LIS Architecture Using Multiple Access Points

distribution in the interval [0,1].

•Delay

Figure 6.10 represents the average delay for LLDP-MED and LIS versus the number of users in this scenario. The error bars depicted in the figure illustrate the 95% confidence interval. The measured delay is similar to the previous scenarios as well. Although the average delay increases with the number of users for both methods, the maximum average delay is significantly less than the two previous scenarios. The reason is that the access point receives the requests at the different times. Therefore the queuing delay does not play an important role in this scenario. Furthermore, the difference between LLDP-MED and LIS is more remarkable.

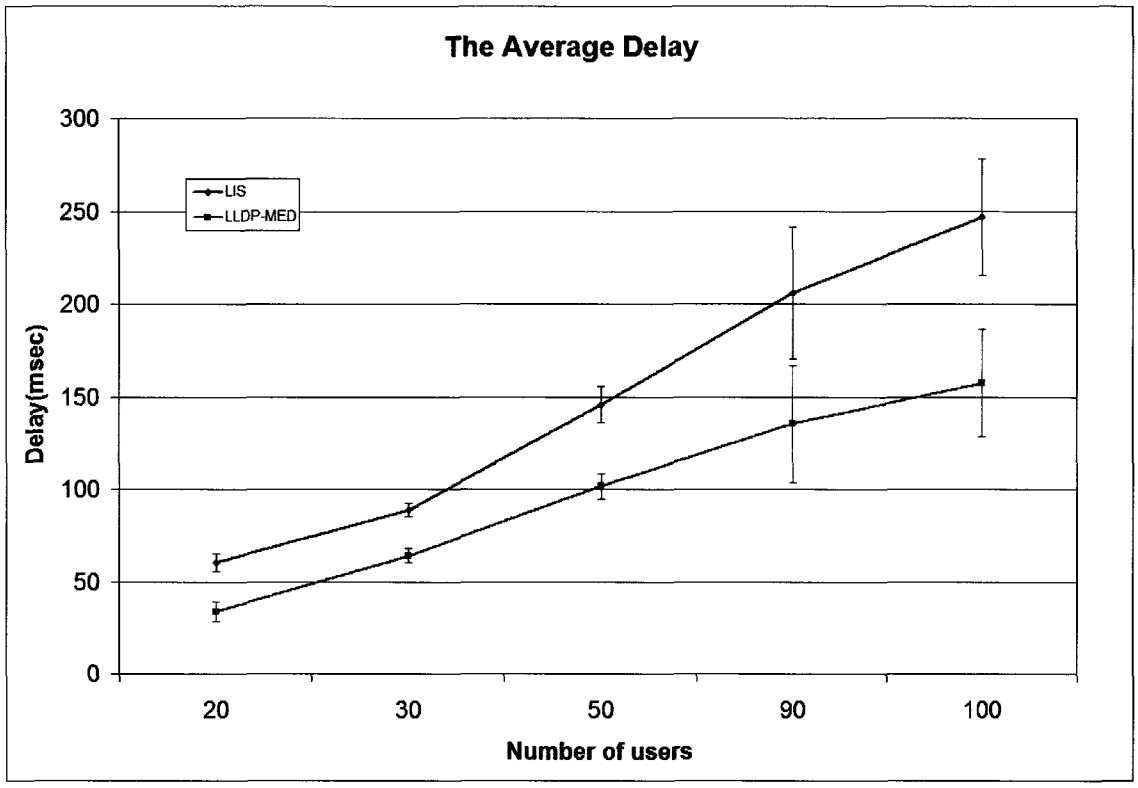

Figure 6.8: The Average Delay Versus the Number of Users, Using Multiple Access Point

•Network Congestion

In this scenario no dropped packet was experienced in LLDP-MED method. For the LIS one, there was only one dropped packet among 100 users. In fact, we can say that for non-simultaneous calls, the number of users is not a critical factor. In other word, the access point can service all of the non-simultaneous calls and pass them to the proxy server.

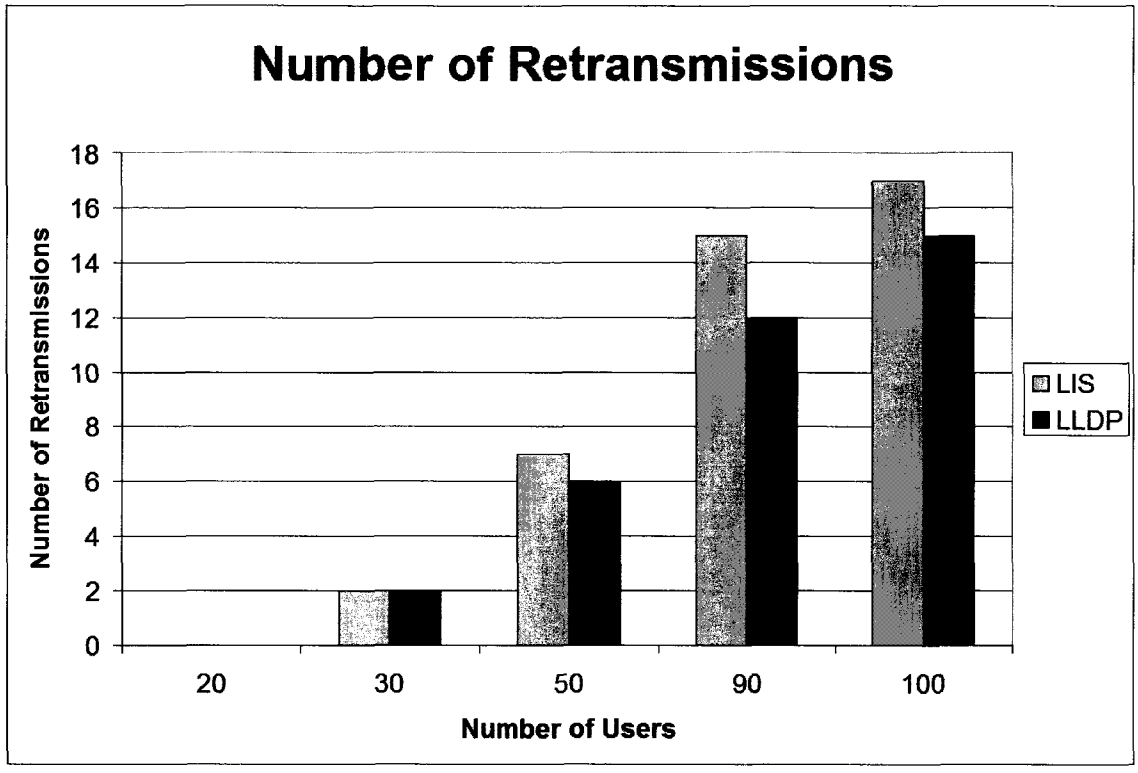

Figure 6.9: The Number of Retransmissions Versus the Number of Users Using Multiple Access Points

6.4 Simulation Results and Discussions for Wireline Users

In the following, we compare the performance of our proposed solution with that of the LIS in a number of scenarios for wireline users. In each scenario, we measure the latency in both methods.

It should be mentioned that we have assumed that there is only one LIS for all of the users in the network, hence, the time that it takes to the user to discover the LIS, is not considered in our simulations.

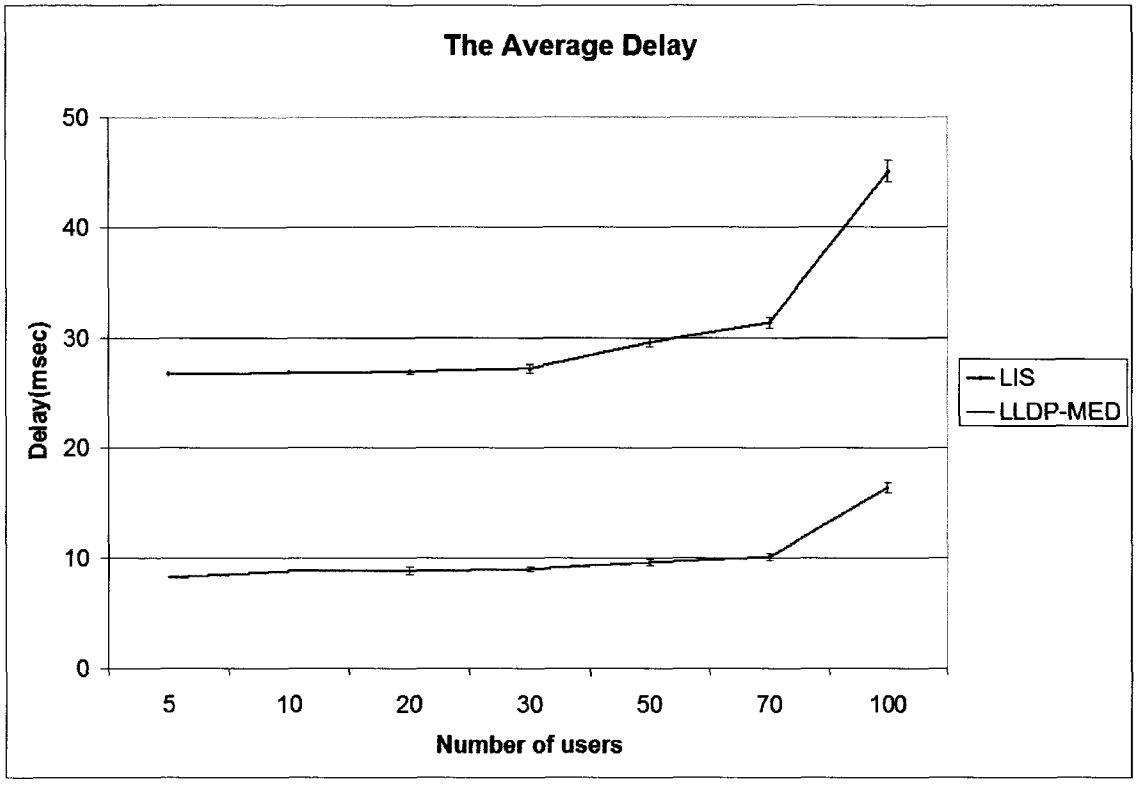

Figure 6.10: The Average Delay Versus the Number of Users Using Single Access Point, Random Start Time

6.4.1 Simultaneous Calls Using Single Switch

In this scenario, all users are connected to the network through a single switch. We also consider a worst case scenario in which all users send their requests for the emergency calls simultaneously. This scenario can represent a real world case such as a natural disaster or fire in a huge building where a large number of users try to make emergency calls at the same time.

Figures 6.1 and 6.2 illustrate the network topology in this scenario for LLDP-MED and LIS, respectively.

The measured delay in this scenario is the time elapsed between emergency call initiation and the time that the proxy server gets the user's messages with the location information. (The delay in Figures 5.7 and 4.2 is equal to $t4 - t1$ and $t5 - t1$, respectively.)

Figure 6.11 presents the calculated average delay in LLDP-MED and LIS versus the number of users in this scenario. All error bars illustrate 95% confidence intervals.

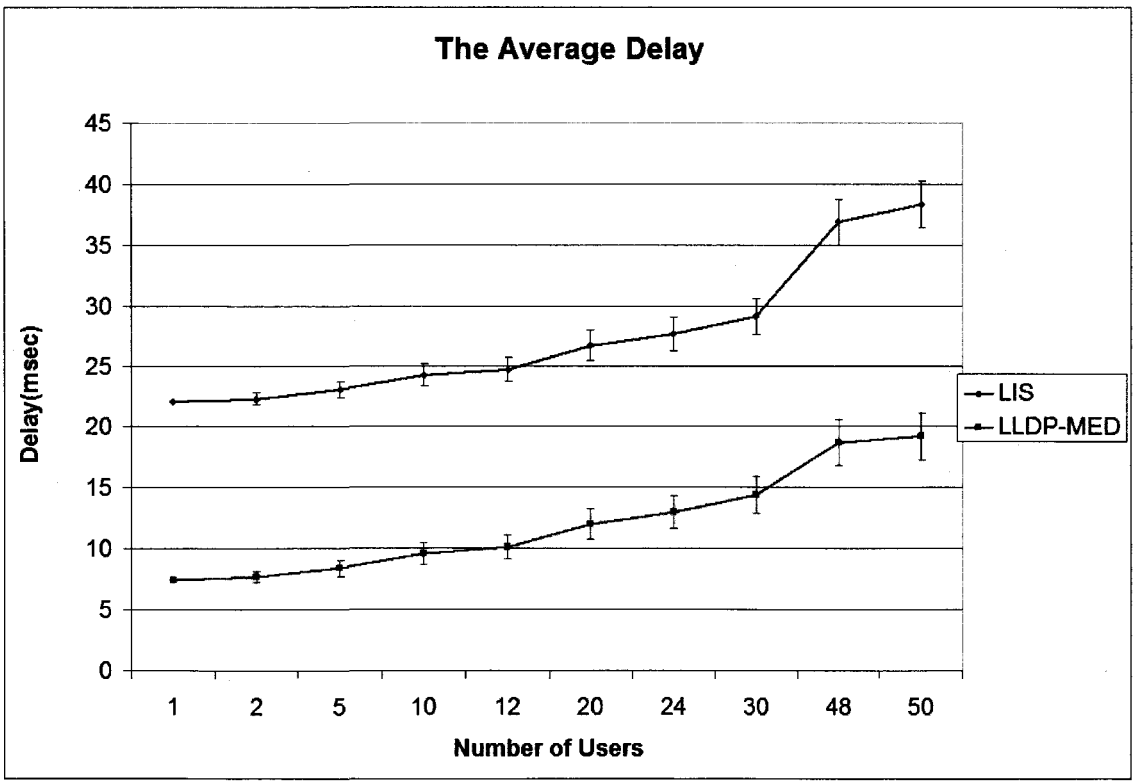

Figure 6.11: The Average Delay Versus the Number of Users Using Single Switch

From this figure, it can be noted that the average delay for the LLDP-MED is

lower than the average delay for LIS. Similar to the wireless scenario, the main reason is different mechanisms to provide the location information for each user at the proxy server. In LIS method, the users have to ask their location from the LIS and wait for its response. However, in LLDP-MED users do not have to wait for the location information to make the emergency call. Hence, the experienced delay by users in LLDP-MED is much less than the LIS.

Furthermore, one can note that the average delay increases with the number of users for both LLDP-MED and LIS. The reason is that as the number of users increases, the number of packets in the queue waiting to be served by the switch increases. However, for a large number of users, the difference between LLDP-MED delay and LIS is more remarkable and there is no overlap for the confidence intervals.

6.4.2 Simultaneous Calls Using Multiple Switches

In this scenario, we consider a different topology with multiple switches, similar the wireless scenarios with multiple access points, depicted in Figures 6.6 and 6.7 for LLDP-MED and LIS perspectively.

This scenario is a less pressing scenario compared to the previous one. We assumed that the number of switches is proportional to the number of users (one Switch per 24 users).

Similar to the previous scenario, the measured delay is the time elapsed between emergency call initiation and the time that the proxy server gets the user's messages

with the location information. (The delay in Figures 5.7 and 4.2 is equal to $t4 - t1$ and $t5 - t1$, respectively.)

Figure 6.12 illustrates the measured delay for both LLDP-MED and LIS method in this scenario. It can be noted that the average delay for the LLDP-MED method in this scenario is much lower than the average delay for the LIS as well. The reason is very similar to the previous scenario; The time that takes to the users to obtain their location information from the LIS, before sending REGISTER message to the proxy server causes more delay for the users in the LIS method.

On the other hand, from this figure it can be noted that in our proposed model based on LLDP-MED, the number of switches does not cause a significant difference in the average delay in these two scenarios (using single switch in the first scenario and multiple switches in the second one). However, with the LIS method, when the number of users increases the average delay in the scenario with multiple switches is significantly lower than the multiple switch scenario.

6.4.3 Non-Simultaneous Calls Using Single Switch

In this part, we consider a different behavior of the wireline users, making calls in the different portions of time. The topology of this scenario is the same as the first wireline scenario. The only difference is that instead of simultaneous calls, the users initiate emergency calls at a random time. We generated this random time with a uniform distribution in the interval [0,1].

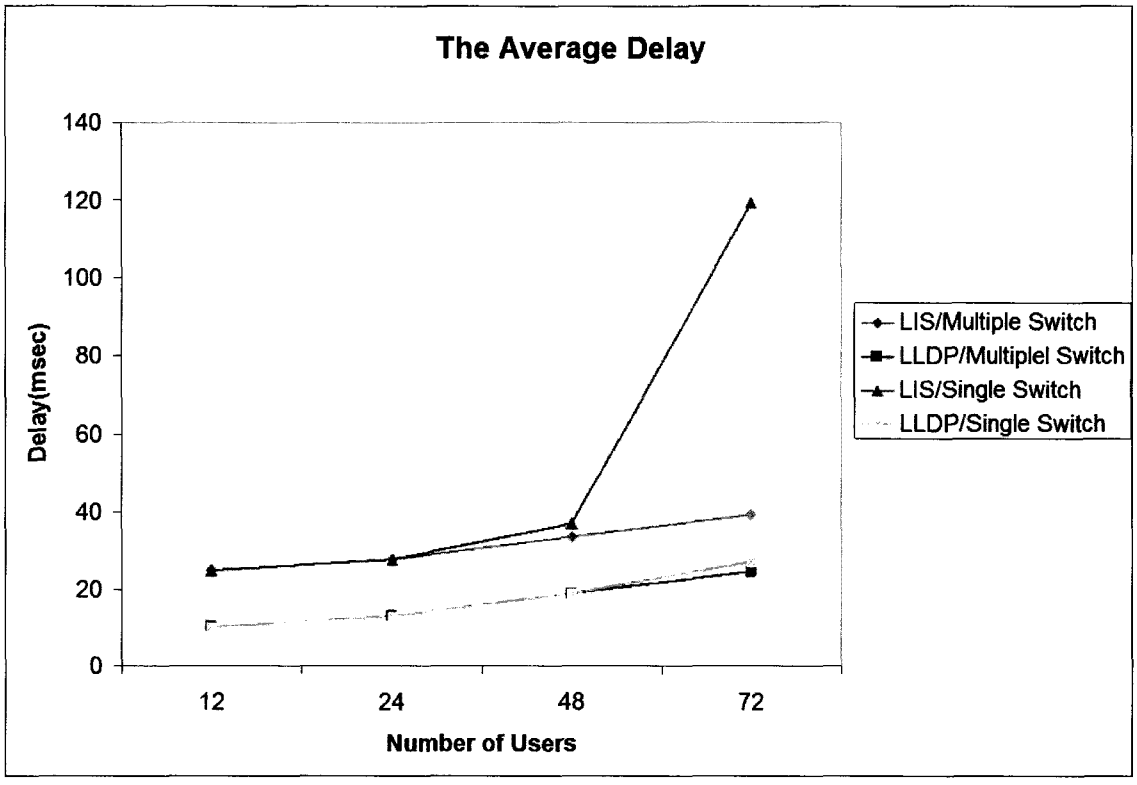

Figure 6.12: Compare The Average Delay Single and Multiple Switches Topologies in LLDP-MED and LIS methods

Figure 6.13 represents the average delay for LLDP-MED and LIS versus the number of users in this scenario. The measured delay is similar to the previous scenarios as well. As It can be noted from Figure 6.13, the number of users does not effect in this scenario. The reason is that the switch receives the requests at the different times. Therefore the queuing delay does not play an important role in this scenario. Similar to the previous scenarios, the measured average delay in LLDP-MED method is lower than the LIS one.

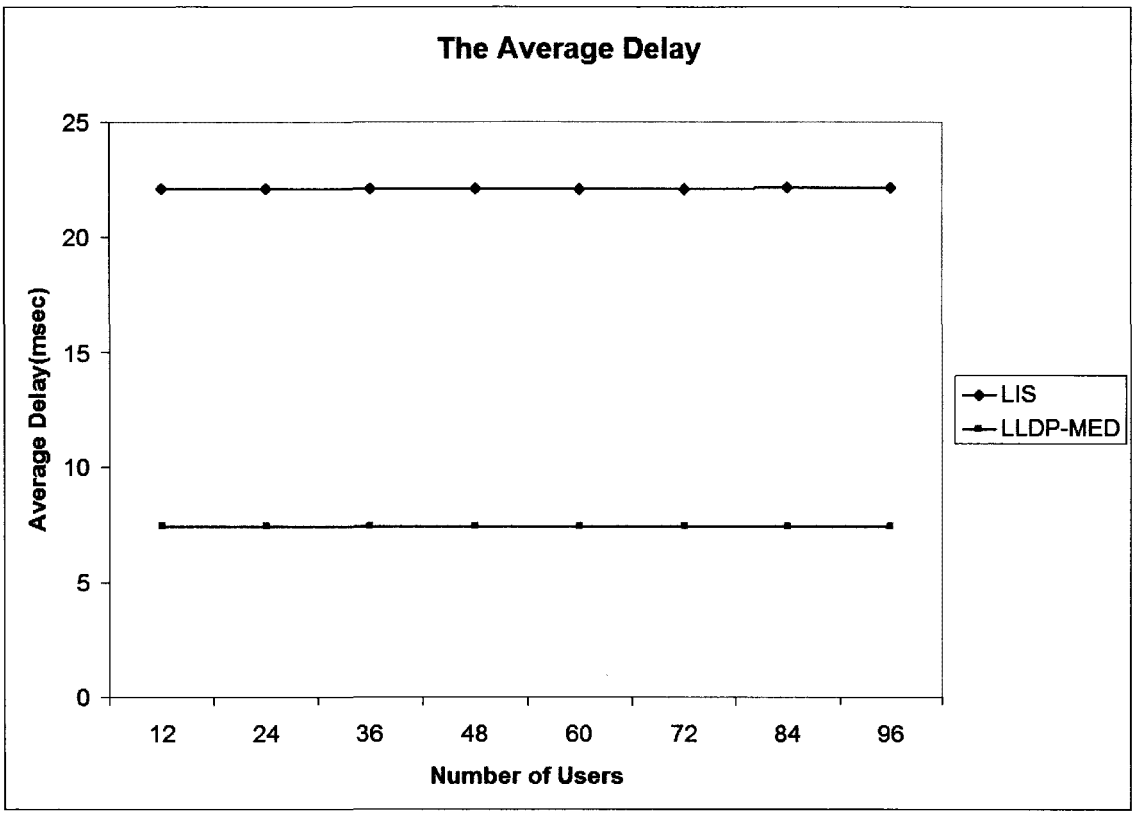

Figure 6.13: Compare The Average Delay for Non-simultaneous calls in LLDP-MED and LIS methods

6.5 Multiple LISs

In order to study the affect of the number of the LISs on the average delay on the network, we considered a different topology, depicted in Figure 6.14.

We repeated the simulations for some scenarios with two LIS in the network. Table 6.2 compares the average delay for 6 scenarios:

From this table it can be noted that for most cases, increasing the number of LISs in the network, does not decrease the average delay, comparing to the LLDP-

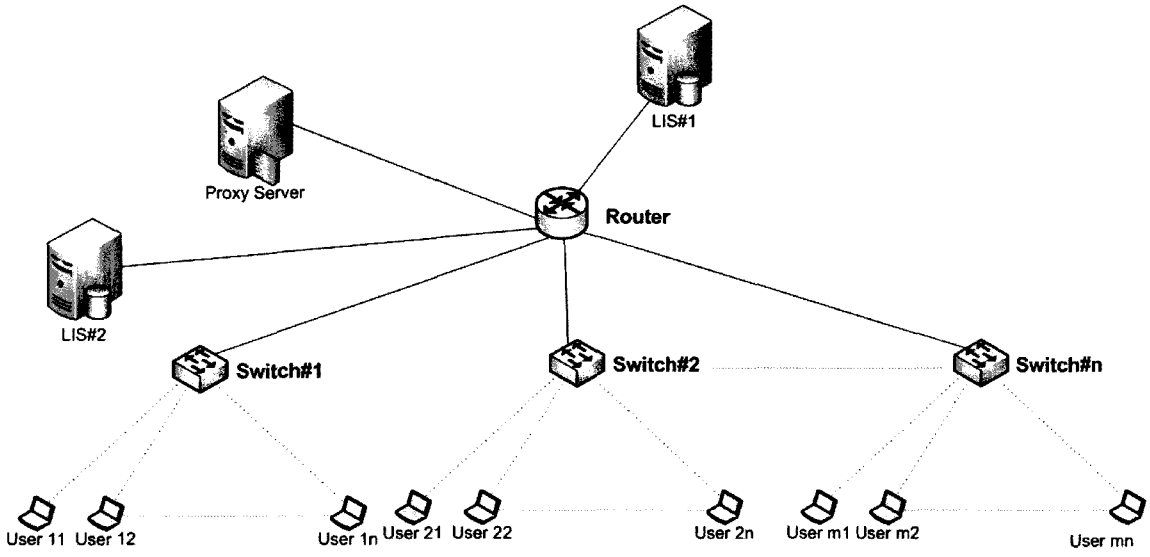

Figure 6.14: The Topology Using Multiple LISs

Table 6.2: Comparing The Average Delay in Topologies with Single and Multiple LISs

	48 users/1switch	**48users/2switches**	**96users/4switches**
1 LIS	36.88 msec	33.36 msec	161.257 msec
2 LISs	36.88 msec	33.36 msec	44.88 msec

MED method. In facts, increasing the number of the LISs in the network effects on the average delay in the network only for the scenarios that a large number of users initiate calls simultaneously. However, adding LISs to the networks imposed more maintenance and more expenses.

Chapter 7

Concluding Remarks

In this last chapter, an overview of the contributions of this thesis is presented. Then, recommendations for future researches are made.

7.1 Summery of Contributions

The main objective of this research was to propose an appropriate solution in order to determine the geographical location of VoIP users in the networks with enough accuracy, which has a great importance to support the emergency calls. More precisely this involved:

- Proposing an efficient and accurate link layer solution based on a protocol, named LLDP-MED.
- Choosing one of the existing solutions for this problem to compare with our

proposed method. For this purpose, an application layer method, using LIS was considered.

- Comparing these two solutions, in terms of imposed delay in the network, network congestion, security issues, accuracy, and etc.

In order to accomplish these objectives, the following contributions have been made as a result of this research:

- Performing a complete survey on all existing methods for location determination of Internet users. These techniques were categorized and compared and evaluate for the emergency cases.

- A new link layer solution to determine the geographical location of VoIP users, based on LLDP-MED protocol, has been proposed. This technique can accurately locate the users in a timely manner which makes it an excellent choice for handling the emergency calls in VoIP applications.

- To evaluate our proposed method, an existing application layer solution, using LIS has been studied in detail and compared in different aspects with our proposed technique.

- In order to compare the latency and network congestion of these two methods, two different NS-2 model were developed. Then a number of simulation experiments with various scenarios for both LIS and LLDP-MED were carried. We

used two separate groups of topologies, wireless and wireline users, in our tests. We tested the effect of varying the number of end users and varying the number of switches/access points, as well as using different start time for the calls in Chapter 6.

Our proposed technique is a general model and does not depend on any particular network architecture. Based on the discussions presented in Chapter 5, this method provides better security, accuracy and coverage. Since this method is independent of IP address, it is not involved with any IP Geolocations issues.

Based on our implementation, the simulation results show that the average delay that our proposed model impose to the network, is by far a much less. This model also causes less congestions in the networks, due to the less number of messages that is required to determine the user's location. Since the time of location determination of the VoIP users is very critical for the emergency case, we believed that this feature of our proposed solution, can make it a good candidate for emergency cases.

7.2 List of Limitations

7.2.1 Outdated Information

The first issue regarding proposed method is that the LLDP database, existing in each administratively domain should maintained and updated by the network administrator. However, this database does not need to be updated by changes in users'

location. Since every port of the switches lead to a jack in a specific room, only after any change on the switches connections, this database must be updated. Furthermore, in the cases that a new switch is added to the network or the ports are extended, this database must be updated.

7.2.2 Security Issues

Although our proposed method provides better security compare to other techniques such as LIS, some security issues may still remain. In the other methods that users supply the location information, they can put false information to make fake emergency calls. However, in our proposed method, it is harder for the attackers. The reason is that the only way that they can have access to the location information and change or overwrite it, is having access to the switches and LLDP databases. Compare to the other methods which attackers only need to have access to the user's equipment.

7.2.3 VPNs

At presence of VPNs, providing location information for the endpoint devices must be prior to the endpoint establishing a VPN back to the enterprise. In fact, to minimize the effects of VPNs , location configuration should be attempted before such tunnels are established [52].

7.3 Possible Directions for Future Research

In this thesis we presented results based on the simulation. For future works, several avenues could be followed. To that end, here are some directions in which more investigations could lead to intriguing results.

As we mentioned in Section 5.4, because users play different roles in sending location information to the destination in each of the LLDP-MED and LIS based solutions, the reaction of these methods to DoS (Denial- of- Service) attacks can be different. In LLDP, users can not put fake location information because the switch inserts this information, but in LIS users at first get information form the server, then they put it in a SIP message and send it to the proxy server, so the user can put anything for location information or make several fake calls with fake location information. We did not test the behavior of the network against DoS. We consider this to be a good topic for future work.

Appendix A

NS-2 Modification Summary

In table A.1 we list all the ns-2 files modified in order to implement our solution. We also provide a brief description of why each file was modified.

Filename	Location	Reason for Modification
sip-lis.cc	/sip	Newly added agent named Agent/SIPLis to the SIP module in NS-2. This agent plays the role of a Location Information Server (LIS) in our simulations. It receives the QUERY messages from the SIP User Agents, processes the queries and nd the location of each user from a simple database that we have created. Then this agents send a QUERY RESPONSE message to the users, contains their location information.
sip-lis.h	/sip	Newly added header file for sip-lis.cc

sip-sw11.cc	/sip	Newly Added agent named Agent/SIP-Switch to the SIP module. This agent acts as the first level LLDP-MED enabled switch in our simulations. It receives the *REGISTER* messages from the User Agents, destined to the Proxy Server. Then it inserts the location information in the LLDP-MED headers of the packets using the LLDP database that we have created. In order to do that, we have defined a *recv* function for this agent. Finally this agent forwards the packets with the location information in their mac header to the Proxy Server. This is done be define a *send* function for this agent.
si-sw11.h	/sip	Newly added header file for sip-sw.cc
sip.cc	/sip	Added on SIP method named *QUERY*. This method is used in implementation of LIS method. Using this method of SIP message, the User Agents can send location query to LIS, which has been set for them, and obtain their location information.
sip.h	/sip	Added some new fields and variables to the SIP module in order to implement both methods discussed in this research: LLDP-MED and LIS, as follow: Defined *Region* as a new variable for the SIP packets. Added *LIS* as a new concept to the SIP definitions. Added *QUE RY* as a new SIP method. Added *SIPLis* as a new SIP agent.
sip-message.cc	/sip	Added a new field named *region* to the *SIPURI*. This field indicates that the User Agent as the initiator of the call, has located in which region. Every LIS is responsible to provide the location information for the users of one region. This filed has been added to the SIPHeaders. Setting this field for the users, they know that they are located in which region and they should send their location query to which LIS.

sip-message.h	/sip	Added additional variable to SIPURI as region, and added this variable to SIPHeader fields.
sip-proxy.cc	/sip	Added a new function to the SIP-Proxy server, to read the location information of each user. This location information can be located in the LLDP-MED fields of mac header of packets (in our proposed model), or in the SIP headers in LIS method.
sip-ua.cc	/sip	Added a considerable amount of code to the source code of this agent. The most important functions which are added to this agent are *askli* and *ProcessQueryResponse*. Using *askli*, the User Agents send their location query to the LIS. This function is called by a tcl command, named *"qury"*. By *ProcessQueryResponse*, the User Agents read the location information obtained from LIS and add this information to their *REGISTER* message. After that, they send *REISTER* to the Proxy server, including their location information. In addition, some TCL object and commands are added to this file which can be used in the TCL codes. The first TCL command is *"query"*. Calling this command by user in TCL files, a *QUERY* message will be sent to the LIS. Another added TCL command is *"set-lis"*. Using this TCL command, the LIS which is responsible for each user is set.
sip-ua.h	/sip	Added two functions to the header file: One to send the location query to the LIS *askli* and another to process the response from the LIS and put the location information in the REGISTER message and send it to the Proxy server, *ProcessQueryResponse*

mac.h	/mac	Added a considerable amount of code in order to add LLDP-MED headers to the *mac* headers of packets. These fields contain 4 TLVs to indicate: Chassis ID, Port ID, System Capabilities, and Location Identification. Each TLV contains several fields such as: type, length, information string, and etc. Most of these newly added fields remain blank. We only use location ID fields. In the implementation of our proposed method, this field is filled by the LLDP-MED switch or the access point. At the proxy server, the proxy can get location information of each user by access to this field.
dsdv.cc	/dsdv	This existing NS-2 agent, acts as a gateway between wireless and wired parts of a network. Therefore, we decided to use it as access point in LLDP-MED implementation, by ding need modifications. In order to do that, we provided the access to the mac header of the packets, including LLDP-MED fields. Then we modified the forward function of this agent to add location information to the *location ID* part of mac header for each packets. This agent performs this based on the LLDP-MED database that we have created. Finally it forwards the packets with the location information to the final destination which is the proxy server in all scenarios.
lldpsink.cc	/app	Newly added sink agent for the wired scenarios.This agent can be used for any type of the traffic (not only SIP). It can read the mac headers of incoming packets. This would include the location information. The source of the packet in recorded in this agent as well. In the wired scenarios, this agent is used as the proxy server.
lldpsink.h	/app	Newly added header fille for lldpsink.cc

usersink.cc	/app	Newly added sink agent to get the location information from the LIS. Similar to lldpsink, this agent can be used for any type of traffic. It can read the location information obtained from LIS and send them to the proxy server. In the wired scenarios, this agent is used as the user agent.
usersink.h	/app	Newly added header file for usersink.h
ns-default.tcl	/tcl/lib	Modifications needed to support newly added agents. These had to do with the default values some of the variables in a new instance of our agent would be initialized with upon creation.
ns-sip.tcl	/tcl/lib	Modifications needed to support newly added SIP methods, agents and commands. These had to do with the default values some of the variables in a new instance of our agent would be initialized with upon creation. For the LIS implementations, some notifications are added as well to show that either the users have been able to communicate withe the LIS successfully or not.
Makefile	/	Include new agent files for compilation

Table A.1: List of all ns-2 files modified to implement our proposed design based on LLDP-MED protocol and the other method, LIS

Bibliography

[1] J. Kim, W. Song, and H. Schulzrinne, "An enhanced VoIP emergency services prototype," *Information Systems for Crisis Response and Management (ISCRAM)*, 2006.

[2] M. Dawson, "The Internet location services model," *Computer Communications*, vol. 31, no. 6, pp. 1104–1113, 2008.

[3] . Federal Communication Commission, ""FCC o5-116: First Report nd Order And Notice Of Proposed Rulemaking"," 2005. http://hraunfoss.fcc.gov/edocs-public/attachmatch/FCC-05-116A1.pdf.

[4] K. Graffi, A. Kovacevic, K. Wulffert, and R. Steinmetz, "ECHoP2P: Emergency call handling over peer-to-peer overlays," in *Proceedings of the 13th International Conference on Parallel and Distributed Systems-Volume 02*, pp. 1–10, IEEE Computer Society, 2007.

[5] . Attorney General of Texas, "Texas Attorney General Abbott Takes Legal Actio To Protect Internet Phone Customers," 2005, new Release.

http://www.oag.state.tx.us/oagnews.

[6] . Attorney General of Texas, "Attorney DCP Sue Broadband Phone Company For Misreperesentiong Its 9-1-1 Emergency Capabilities," 2005, press Release. http://www.oag.state.tx.us/oagnews.

[7] D. Clark, C. Partridge, R. Braden, B. Davie, S. Floyd, V. Jacobson, D. Katabi, G. Minshall, K. Ramakrishnan, T. Roscoe, *et al.*, "Making the world (of communications) a different place," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 3, p. 96, 2005.

[8] A. LaMarca, Y. Chawathe, S. Consolvo, J. Hightower, I. Smith, J. Scott, T. Sohn, J. Howard, J. Hughes, F. Potter, *et al.*, "Place lab: Device positioning using radio beacons in the wild," *Pervasive Computing*, pp. 116–133, 2005.

[9] L. Stringer, F. Dudek, and C. Bauer, "Location Information Discovery for IP Telephony," *Novel Algorithms and Techniques In Telecommunications, Automation and Industrial Electronics*, pp. 341–345, 2008.

[10] W. Song, J. Kim, H. Schulzrinne, P. Boni, and M. Armstrong, "Using IM and SMS for emergency text communications," in *Proceedings of the 3rd International Conference on Principles, Systems and Applications of IP Telecommunications*, pp. 1–7, ACM, 2009.

[11] H. Schulzrinne and K. Arabshian, "Providing emergency services in Internet telephony," *IEEE Internet Computing*, vol. 6, no. 3, pp. 39–47, 2002.

[12] X. Wu and H. Schulzrinne, "sipc, a multi-function SIP user agent," *Management of Multimedia Networks and Services*, pp. 269–281, 2004.

[13] X. Wu and H. Schulzrinne, "Location-based services in Internet telephony," in *2005 Second IEEE Consumer Communications and Networking Conference, 2005. CCNC*, pp. 331–336, 2005.

[14] E. Katz-Bassett, J. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, "Towards IP geolocation using delay and topology measurements," in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pp. 71–84, ACM New York, NY, USA, 2006.

[15] V. Padamanabban and L. Subramanian, "Determining the geographic location of Internet hosts," *ACM SIGMETRICS Performance Evaluation Review*, vol. 29, no. 1, pp. 324–325, 2001.

[16] J. Muir and P. Oorschot, "Internet geolocation: Evasion and counterevasion," *ACM Computing Surveys (CSUR)*, vol. 42, no. 1, pp. 1–23, 2009.

[17] M. Mintz-Habib, A. Rawat, and H. Schulzrinne, "A VoIP emergency services architecture and prototype," pp. 523–528, Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on, 2005.

[18] H. Schulzrinne, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," *draft-ietf-geopriv-dhcp-civil-09 (work in progress), January*, 2006.

[19] M. Thomson and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," *draft-thomson-geopriv-lis-discovery-03 (work in progress), March*, 2010.

[20] M. Barnes, J. Winterbottom, M. Thomson, and B. Stark, "HTTP Enabled Location Delivery (HELD)," *draft-ietf-geopriv-http-location-delivery-01 (work in progress), July*, 2007.

[21] "Cisco(2004)ConfigurationCiscoDiscoveryProtocol,[online]." Available:http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun c//fcfpr3/fcf015.htm.

[22] "Link Layer Discovety Protocol for Media Endpoint Devices (LLDP-MED)," 2006. ANSI/TIA-1057 TIA, TR41.4.

[23] B. Gueye, A. Ziviani, M. Crovella, and S. Fdida, "Constraint-based geolocation of internet hosts," *IEEE/ACM Transactions on Networking (TON)*, vol. 14, no. 6, pp. 1219–1232, 2006.

[24] S. Kubisch, H. Widiger, P. Danielis, J. Schulz, D. Timmermann, D. Duchow, and T. Bahls, "Trust-by-Wire in packet-switched networks: Calling line identification

presentation for IP," in *Innovations in NGN: Future Network and Services, 2008. K-INGN 2008. First ITU-T Kaleidoscope Academic Conference*, pp. 375–382, 2008.

[25] P. Danielis, S. Kubisch, H. Widiger, J. Schulz, D. Timmermann, T. Bahls, and D. Duchow, "IPclipAn Innovative Mechanism to Reestablish Trust-by-Wire in Packet-switched IP Networks," 2008.

[26] Ø. Thorvaldsen, "Geographical Location of Internet Hosts using a Multi-Agent System," Master's thesis, Norwegian University of Science and Technology, Faculty of Information Technology, Mathematics and Electrical Engineering, Department of Telematics, Nov. 2006.

[27] R. Atkinson, S. Bhatti, and S. Hailes, "A proposal for unifying mobility with multi-homing, NAT, & security," in *Proceedings of the 5th ACM international workshop on Mobility management and wireless access*, pp. 74–83, ACM New York, NY, USA, 2007.

[28] P. Enge and P. Misra, "Special issue on global positioning system," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 3–15, 1999.

[29] A. Roach *et al.*, "SIP-specific event notification," *RFC 3265, June 2002.*

[30] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 32–43, ACM, 2000.

[31] P. Bahl and V. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *IEEE infocom*, vol. 2, pp. 775–784, Citeseer, 2000.

[32] J. Farkas, V. de Oliveira, M. Salvador, and G. dos Santos, "Automatic discovery of physical topology in ethernet networks," in *Advanced Information Networking and Applications*, vol. 3, pp. 848–854, 2008.

[33] Y. Breitbart, M. Garofalakis, B. Jai, C. Martin, R. Rastogi, and A. Silberschatz, "Topology discovery in heterogeneous IP networks: the NetInventory system," *IEEE/ACM Transactions on Networking (TON)*, vol. 12, no. 3, pp. 401–414, 2004.

[34] E. Mota-Garcia and R. Hasimoto-Beltran, "A fast scheme for simple geographic Internet mapping," in *Sixth Mexican International Conference on Computer Science, 2005. ENC 2005*, pp. 230–234, 2005.

[35] Y. Shavitt and N. Zilberman, "A Study of Geolocation Databases," *Arxiv preprint arXiv:1005.5674*, 2010.

[36] J. Peterson, "A presence-based GEOPRIV location object format," 2004.

[37] R. Frieden, "Why The FCCs Proposed Openness Principles Cannot and Should Not Apply to Internet Application and Content Providers," *Rob Frieden*, p. 20, 2010.

[38] . The European Parliment and the Council of the Europran Union, "Directive 2002/22/EC: Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive)," *Official Journal of the European Communities*, vol. L 108, pp. 33–50, 7 Mar.2002.

[39] . European Regulators Group, "ERG Common Statement for VoIP regulatory Approaches, (ERG(05)12)," Feb.2005. Tech. Rep.

[40] . National Emergency Number Association (NENA) VoIP-Packet Technical Committee, "Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)," Dec.2005. Tech. Rep.

[41] . Co-ordination Group on Access to Location Information by Emergency Services CGALIES, "Report on Implementation Issues Related to Access to Location Information by Emergency Services(E112) in the European Union," Feb.2002. Final report.

[42] J. Polk and A. Newton, "ecrit B. Rosen Internet-Draft NeuStar Intended status: Standards Track H. Schulzrinne Expires: August 28, 2008 Columbia U.," *Framework*, 2008.

[43] M. Dawson, J. Winterbottom, and M. Thomson, *IP location.* McGraw-Hill Osborne Media, 2007.

[44] H. Schulzrinne, H. Tschofenig, A. Newton, and T. Hardie, "LoST: A Protocol for Mapping Geographic Locations to Public Safety Answering Points," in *Performance, Computing, and Communications Conference, 2007. IPCCC 2007. IEEE Internationa*, pp. 606–611, 2007.

[45] H. Schulzrinne, "Location-to-URL mapping protocol (LUMP)," *draft-schulzrinne-ecrit-lump-01 (work in progress)*, 2005.

[46] J. Polk, J. Schnizlein, and M. Linsner, "RFC 3825: Dynamic host configuration protocol option for coordinate-based location configuration information," 2004.

[47] . NENA TID 07-501, ""Network Interfaces for E9-1-1 and Emerging Technologies"," September 2002.

[48] TIA-TSB-146, ""IP Tlephony Support for Emergency Calling Service"," Mar 2003.

[49] H. Tschofenig and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements," *Internet Engineering Task Force (IETF),Request for Comments: 5687, March*, 2007. ISSN: 2070-1721.

[50] S. McCanne, S. Floyd, and K. Fall, "ns2 (network simulator 2)," *last accessed: February*, vol. 23, 2010.

[51] R. Prior, "A SIP module for NS 2.27, developed by Rui Prior," 2004. Available at: http://www.dcc.fc.up.pt/ rprior/ns/.

[52] B. Rosen and J. Polk, "ecrit B. Rosen Internet-Draft NeuStar Intended status: Standards Track J. Polk Expires: July 31, 2009 Cisco Systems January 27, 2009,"