

154621

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

**IP ÜZERİNDEN SES İLETİMİ
VE
ASKERİ AMAÇLI KULLANIMI**

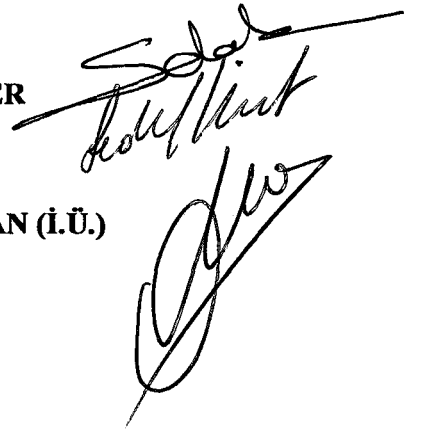
**YÜKSEK LİSANS TEZİ
Müh. Ozan BÜK
(514011045)**

**Tezin Enstitüye Verildiği Tarih : 26 Nisan 2004
Tezin Savunulduğu Tarih : 28 Mayıs 2004**

Tez Danışmanı : Yrd. Doç.Dr. Selçuk PAKER

Diğer Jüri Üyeleri Doç.Dr. Sedef KENT

Prof. Dr. Osman Nuri UÇAN (İ.Ü.)



MAYIS 2004

ÖNSÖZ

Sayın hocam Yrd. Doç. Dr. Selçuk PAKER'e ve aileme teşekkür ederim. Tüm çalışmalarında desteğini esirgemeyen Yük. Müh. Gökhan AKIN'a ve ağabeyim Onur BÜK'e teşekkür ederim.

Nisan 2004

Ozan BÜK



İÇİNDEKİLER

ÖNSÖZ.....	ii
İÇİNDEKİLER.....	iii
KISALTMALAR.....	v
TABLO LİSTESİ.....	vi
ŞEKİL LİSTESİ	vii
ÖZET	viii
SUMMARY	ix
1. GİRİŞ	1
2. VoIP SİSTEMİ.....	3
2.1. VoIP Oturum Başlatma Protokolleri	3
2.1.1. H323. Protokolü	3
2.1.1.1 H.323 Bileşenleri.....	3
2.1.1.2 H.323 Protokol Yapısı.....	6
2.1.1.3 H.323 Çağrı Kurulumu.....	7
2.1.2. SIP - Oturum Başlatma Protokolü.....	8
2.1.2.1. SIP Bileşenleri.....	9
2.1.2.2. SIP Mesaj Tipleri.....	11
2.1.2.3. SIP Adreslemesi.....	13
2.1.2.4. SIP Mesaj Yapısı.....	13
2.1.2.5. SIP Mesaj Kurulumu Örnekleri	14
2.1.3. H.323 ve SIP Karşılaştırması	18
2.2. SES Sıkıştırma Algoritmaları	24
2.3. RTP, cRTP, RTCP	25
2.3.1. RTP	25
2.3.2. RTP Başlık Sıkıştırması (cRTP)	27
2.3.3. RTCP	27
2.4. ENUM	28
2.4.1. E.164 nedir?	28
2.4.2. ENUM'un sağladığı faydalar	29
2.4.3. ENUM sisteminin yapısı.....	29
2.4.4. E.164.arpa etki alanının yönetimi.....	30
2.5. QOS (Servis Kalitesi) için kullanılan yöntemler	32
2.5.1. Veri Bağı Katmanı Servis Kalitesi (Data Link Layer QOS).....	32
2.5.2. Servis Tipi (Type of Service).....	33
2.5.3. RSVP	33

2.5.4.	DiffServ: (Farklılaştırılmış Servisler).....	33
2.5.5.	MPLS (Çoklu Protokol Etiket Anahtarlama).....	34
2.6.	VoIP’de Güvenlik	34
2.6.1.	SIP Güvenlik Mekanizmaları.....	35
2.7.	Askeri Sistemlerde VoIP kullanmanın yararları	36
2.7.1.	Askeri sistemlerde VoIP tasarımında ele alınması gereken kriterler ..	37
2.8.	VoIP Avantajları ve Kullanım Alanları.....	38
3.	SONUÇ VE TARTIŞMALAR.....	40
	KAYNAKLAR.....	42
	EKLER.....	43
	ÖZGEÇMİŞ.....	44



KISALTMALAR

ATM	: Asenkron Aktarım Modu
cRTP	: Sıkıştırılmış Gerçek Zamanlı İletim Protokolü
DNS	: Domain İsim Sistemi
IEEE	: Elektrik ve Elektronik Mühendisleri Enstitüsü
IETF	: İnternet Mühendisliği İş Gücü
IP	: İnternet Protokolü
ISDN	: Tümüleşik Hizmetler Sayısal Ağı
ISP	: İnternet Servis Sağlayıcı
ITU	: Uluslar Arası Telekomünikasyon Birliği
LAN	: Yerel Alan Ağları
MCU	: Çok Noktalı Denetim Birimi
MEGACO	: Ortam Geçiti Denetim Protokolü
MPLS	: Çoklu Protokol Etiket Anahtarlama
PABX	: Özel Telefon Santraller
PSTN	: Kamu Anahtarlama Telefon Şebekeleri
QoS	: Servis Kalitesi
RSVP	: Kaynak Ayırma Protokolü
RTCP	: Gerçek Zaman Denetim Protokolü
RTP	: Gerçek Zamanlı İletim Protokolü
SCTP	: Akış Denetimi Kontrol Protokolü
SDP	: Oturum Tanımlama Protokolü
SIP	: Oturum Başlatma Protokolü
TCP	: İletim Kontrol Protokolü
TDM	: Zaman Bölmeli Çoğullama
TLS	: İletim Katmanı Güvenliği
TOS	: Servis Tipi
UDP	: Kullanıcı Datagram Porotokolü
VoIP	: IP Üzerinden Ses İletimi
VPIM	: İnternet E-posta Trafığı İçin Ses Protokolü
WAN	: Geniş Alan Ağları

TABLO LİSTESİ

Sayfa No

Tablo 2.1 H.323 Protokolleri4

Tablo 2.2. SIP Talep Mesaj Tipleri 11

Tablo 2.3. SIP Cevap Mesaj Kodları ve Açıklamaları 12

Tablo 2.4. H.323 ve SIP özellik karşılaştırması.....23

Tablo 2.5. Ses Kodlama yöntemlerinin karşılaştırılması.....25

Tablo 2.6. VoIP protokol kümesi ve TCP/IP dayanak modeli.....26

Tablo 2.7. RTP Başlığı26

Tablo 2.8. VoIP güvenlik tehditleri ve tavsiye edilen çözüm metotları35



ŞEKİL LİSTESİ

	<u>Sayfa No</u>
Şekil 2.1. H.323 Bileşenleri	4
Şekil 2.2. H.323 protokol yapısı.....	6
Şekil 2.3. H.323 çağrı kurulumu	8
Şekil 2.4. SIP Oturum Kurulumu ve Çağrı Sonlandırılması.....	14
Şekil 2.5. Yönlendirme Sunucusu Kullanılarak Çağrı Yönlendirilmesi.....	15
Şekil 2.6. Proxy Sunucusu Senaryosu	16
Şekil 2.7 H.323 Çağrı Kurulumu.....	20
Şekil 2.8 SIP Çağrı Kurulumu	21
Şekil 2.9. H.323’de Hızlı Başlangıç Yapısı	22
Şekil 2.10. VoIP Servisleri arasında geçişin sağlanması	24
Şekil 2.11. RTP başlık sıkıştırması (cRTP)	27
Şekil 2.12. Ethernet’te QoS özelliğinin sağlanması	32
Şekil 2.13. IP önceliklendirmesi ve DiffServ paket sınıflandırma yapıları	34

IP ÜZERİNDEN SES İLETİMİ VE ASKERİ AMAÇLI KULLANIMI

ÖZET

1876 yılında Alexander Graham Bell'in icadıyla başlayan analog telefon şebekeleri günümüze kadar varlığını sürdürmüştür. Günümüzde sayısal teknolojilerin gelişmesi, ses iletiminin daha verimli olan sayısal şebekelere kaymasına neden olmuştur. Sesin IP üzerinden iletilmesi ile beraber daha düşük maliyetlerle, daha yüksek kapasitelere ulaşılmaktadır.

IP üzerinden ses oturumlarının kurulabilmesi için birçok protokol geliştirilmiştir. ITU tarafından geliştirilen H.323 ve IETF tarafından geliştirilen SIP protokolleri en yaygın kullanılan protokollerdir. Tez kapsamında, ses oturumlarının kurulması için kullanılan H.323 ve SIP protokollerinin bileşenleri incelenmiş, avantaj ve dezavantajları karşılaştırılmalı olarak sunulmuştur.

VoIP'de kullanılan adresler ile PSTN adresleri arasında uyum problemi bulunmaktadır. Mevcut PSTN altyapısında kullanılan E.164 numaraları ile VoIP entegrasyonunun sağlanması amacıyla ENUM protokolü geliştirilmiştir. On iki haneli uluslararası telefon numaralarının DNS temelli bir mimari kullanarak DNS adresine dönüştürülmesini sağlayan ENUM protokolü tez kapsamında incelenmiştir.

VoIP'in askeri amaçlı kullanılması birçok yenilik ve teknolojik kolaylık getirmektedir. Askeri birimler görevleri gereği çok geniş alanlara yayılabilmektedir. Bu sistemlerde VoIP kullanılması sınırlı bant genişliği kaynaklarına sahip RF ve uydu hatları üzerinden düşük maliyetler ve yüksek kapasiteler ile ses iletimine olanak tanımaktadır. Ses, görüntü ve veri iletiminde tümleşik servislerin tek bir altyapı üzerinden sağlanabildiği IP ortamı askeri sistemler için uygun bir altyapı oluşturmaktadır.

VoIP sistemi her geçen gün daha da yaygınlaşmakta ve gelecekte varolan telefon altyapısının yerini alacak gibi gözükmektedir.

VOICE OVER IP AND ITS USAGE IN MILITARY NETWORKS

SUMMARY

From 1876, the day Alexander Graham Bell invented the telephone; analog-based circuit-switched networks have been used up to date. Voice communication changes its direction from circuit-switched networks to packet-switched networks with the improvements in digital technologies. Voice over IP provides high capacity, low cost voice communication with enhanced flexibility.

In the last decade many protocols have been developed to establish voice sessions within TCP/IP. H.323 and SIP are the most commonly used session establishment protocols which are created by ITU and IETF respectively. In this study basic components of these protocols are defined and differences between these protocols are mentioned.

In order to provide the integration between PSTN and VoIP, the basics of ENUM protocol is presented. ENUM protocol is developed for the integration of VoIP addresses with the E.164 telephone numbers used in PSTN infrastructure. In ENUM twelve-digit international telephone numbers are transformed into DNS addresses using DNS based architecture. The required steps are listed to provide a global ENUM service.

VoIP usage in military-based networks provides many technological advances. Military systems are distributed in wide areas. Because of the limited bandwidth capacity of RF and satellite links, sending voice in multiple voice data with lower costs is an important concern in military systems. Converged voice, video and data services provided in a single IP infrastructure is a suitable way of implementing communication networks.

VoIP usage is becoming widespread and seems as it will be used instead of the existing circuit switched telephone infrastructure in the near future.

1. GİRİŞ

IP üzerinden ses iletimi, günümüz devre anahtarlamalı telefon santralleri yerine sesin IP paketlerine dönüştürülerek tamamen IP temelli şebekeler üzerinden iletilmesidir. 100 yılı aşkın bir süredir ses iletişimi Kamu Anahtarlamalı Telefon Şebekeleri (PSTN) üzerinden yapılmaktadır. Bu sistem devre anahtarlamalı ağlar (circuit-switched networks) üzerinden veya zaman bölmeli çoğullama teknikleri (TDM) kullanılarak ses iletimini gerçekleştirmektedir. PSTN üzerinden sesin taşınması için arayan tarafın bağlı olduğu santralden başlayarak, aradaki santraller ve diğer uçtaki santrale kadar bir devre kurulması gerekmektedir. Bu santraller arası sinyalleşme temel olarak çağrı kurma, çağrı yönetimi ve sonlandırma işlemlerinden oluşmaktadır. Fakat son yıllarda paket anahtarlamalı ağlar üzerinden sesin iletimi kişi ve kuruluşların ilgisini çekmeye başlamıştır. Bunun en önemli sebeplerinden bir tanesi ip üzerinden ses iletiminin daha ucuza ve daha az bant genişliği kullanılarak yapılabiliyor ve ip üzerinden pek çok veri servisi ile gerçek zamanlı ses iletim servislerinin birleştirilebiliyor olmasıdır.

VoIP yani IP tabanlı paket anahtarlamalı devreler üzerinden ses iletiminin gerçekleştirilmesi fikri ilk kez Şubat 1995 tarihinde VocalTec adlı bir şirketin gerçekleştirdiği yazılım sayesinde ortaya çıkmıştır. Geliştirilen yazılım ile 866/33 Mhz ve daha yüksek işlemci gücüne sahip her makine ses kartı, hoparlör ve mikrofona sahip olduğu takdirde bu yazılıma ve gerekli donanıma sahip diğer PC'ler ile çevirmeli bağlantı (dial-up) üzerinden IP şebekesine bağlanıp sesli görüşme yapabilmektedir. Yazılım, istenen ses trafiğini belli sıkıştırma algoritmaları ile sıkıştırıp IP paket verilerine dönüştürmekte ve iletişim kurmak istenen makineler ile sesli iletişim yapılabilmesini sağlamaktadır. Daha sonra IP üzerinden ses iletimi hızla gelişmeye başlamış, 1996 yılında VocalTec ile Dialogic firmasının PSTN ile Internet altyapısının entegrasyonunu sağlayan ilk ağ geçidini (gateway) üretmesiyle IP üzerinden ses iletimi büyük ivme kazanmıştır. [1]

IP üzerinden sesin iletilebilmesi için bir çağrı oturumunun kurulması yönetilmesi ve sonlandırılması gerekmektedir. Bunun için çeşitli protokoller geliştirilmiştir. İki yada daha fazla cihaz veya telefonun IP üzerinden ses iletimi yapabilmesi için en yaygın kullanılan protokoller H.323 ve SIP protokolleridir. H.323 çeşitli eklentilerle günümüze kadar gelmiş, SIP ise son yıllarda geliştirilmiş ve gelecek vadeden bir protokol konumundadır. İki protokol de yaygın kullanım alanına sahiptir.

IP üzerinden ses iletimi ve askeri amaçlı kullanımı konulu çalışmamda H.323 ve SIP protokollerinin yapısı incelenmiş, bu iki protokol arasındaki farklar detaylı olarak anlatılmıştır. Ses sıkıştırma algoritmaları, ses iletimi için kullanılan protokoller, güvenlik ve servis kalitesinin sağlanması için kullanılan mekanizmalar ele alınmıştır. Ayrıca IP üzerinden ses iletimi yapılırken PSTN şebekelerinde kullanılan (E.164) telefon numaralarının Internet'te kullanımını öngören ve yeni gelişmekte olan ENUM yapısı incelenmiştir. Son olarak VoIP'in askeri amaçlı kullanımı ve getirdiği faydalar ele alınmıştır.

2. VoIP SİSTEMİ

VoIP ile ses iletiminin gerçekleştirilebilmesi için birtakım protokoller kullanılır. İki uç arasında yada çoklu oturumlarda oturumun başlatılması için SIP, H.323 benzeri protokoller kullanılmaktadır. Bu protokoller oturumu başlatır, yönetir ve yeri geldiğinde sonlandırır. İki uç birim arasındaki adresleme DNS sorgusu ile belirlenir ve uçbirimler IP üzerinden iletişim kurarlar. PSTN şebekelerinde kullanılan (E.164) telefon numaralarının Internet ortamına aktarımı için ENUM benzeri protokoller önerilmiştir. Oturumun kurulması ile birlikte sıkıştırılmış ses paketleri RTP paketlerine dönüştürülerek gerçek zamanlı olarak iletilmektedir. RTP paketleri UDP paketleri kullanılarak paket anahtarlama IP ağları üzerinden gönderilir.

2.1. VoIP Oturum Başlatma Protokolleri

2.1.1. H323. Protokolü

H.323 paket anahtarlama ağlar üzerinden (LAN, WAN ve Internet) çoklu ortam iletişimi için geliştirilmiş uluslararası bir standarttır. İlk defa 1996'da ITU tarafından tanımlanmış ve daha sonraları protokol üzerinde güncellemeler yapılmıştır. Protokolün mevcut son sürümü (H.323 v5) 2003 yılında standartlaşmıştır.

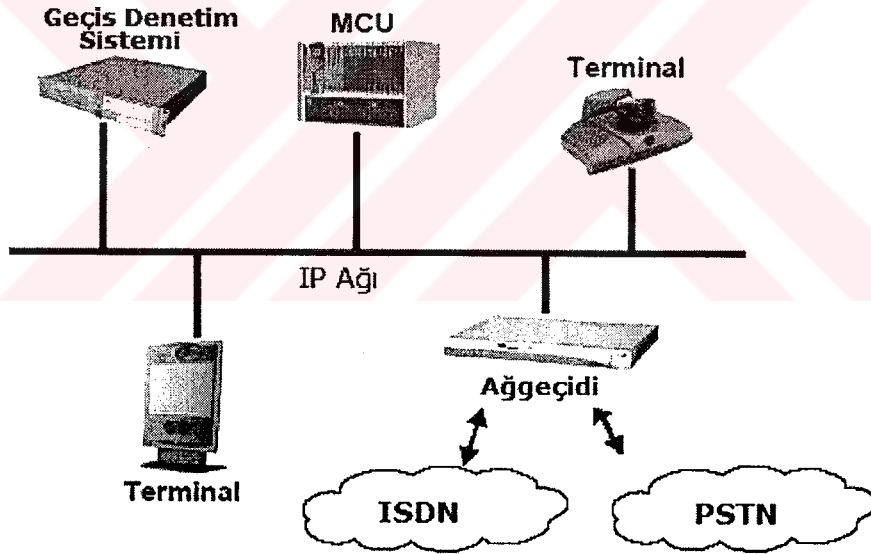
H.323 paket anahtarlama ağlar üzerinden gerçek zamanlı ses, görüntü ve veri haberleşmesini tanımlayan bir şemsiye standart olup birçok standardı kapsamaktadır. H.323, H.225.0-RAS, Q.931, H.245 RTP/RTCP, (G.711, G.723.1, G.728 vb) ses sıkıştırma algoritmaları ve (H.261,H.263) görüntü sıkıştırma algoritmalarını içermektedir. H.323 temelde bir paket anahtarlama çoklu ortam sisteminde çağrı sinyalleşmesi, çağrı kontrolü ve ortam akış protokollerinin işleyişini tanımlamaktadır. H.323 protokollerinin açıklamaları Tablo 2.1'de verilmiştir.

Tablo 2.1 H.323 Protokolleri

Ses Kodeği	Mikrofondan gelen ses sinyallerini ağda taşınacak şekilde kodlar. Yine terminalden gelen ses kodlarını ses sinyallerine çevirir. (G.711, G.723.1, G.728, G.729 vb.)
Video Kodeği	Kameradan gelen görüntü sinyallerini ağda taşınacak şekilde kodlar, yine ağdan gelen görüntü kodlarını görüntü sinyallerine çevirir. (H.261,H263)
H.225.0.RAS	Uç nokta ile geçiş denetim sistemi arasında kullanılır İstemci/Sunucu protokolüdür. Erişim izinlerini belirler.
Arama Sinyalleşmesi (Q931)	Denetim sinyalleşmesi için bir bağlantı oluşturma protokolüdür.
H. 245 Denetim Sinyalleşmesi	Denetim mesajlarının alınıp verilmesinde kullanılır
RTP (Gerçek Zamanlı İletim Protokolü)	Gerçek zaman desteği gerektiren uygulamalarda uçtan uca veri iletimini sağlar.
RTCP (Gerçek Zaman Denetim Protokolü)	Ses ve görüntü senkronizasyonu sağlar

2.1.1.1. H.323 Bileşenleri:

H.323 protokolünün tanımladığı dört tip H.323 bileşeni Şekil 2.1 de görülmektedir.



Şekil 2.1. H.323 Bileşenleri

Terminal:

Terminaller uç noktalarda diğer bir H.323 terminali, ağgeçidi veya MCU ile gerçek zamanlı, iki yönlü ses, görüntü ve veri haberleşmesinde bulunacak uçbirimlerdir. Terminaller arasındaki iletişim sadece ses iletimi olabileceği gibi, ses ve veri, ses ve

görüntü, ses, veri ve görüntü biçiminde de olabilir. Terminal PC üzerinde yazılımsal olarak çalışan bir uygulama yada donanımsal bir telefon olabilir.

Ağgeçidi (Gateway):

Bir H.323 uçbirimi ile PSTN, ISDN yada SIP gibi farklı protokol kümelerini kullanan uçbirimler ile gerçek zamanlı iki yönlü haberleşme kurulabilmesi için aradaki geçişi sağlayan H.323 uçbirimleridir. Örnek olarak ağgeçitleri bir H.323 terminali ile bir analog telefon kullanıcısının haberleşebilmesi için paket anahtarlama bir ağ ile devre anahtarlama ağ arasında geçişi sağlar. Geçitler genelde IP ağları ile PSTN şebekesini birbirine bağlamak için kullanılır.

Çok Noktalı Denetim Birimi (MCU): (Multi-Point Control Unit)

İkiden fazla terminalin yada ağgeçidinin bir çoklu-ortam konferansına katılmasını sağlayan H.323 bileşenidir. MCU iki kısımdan oluşur. Bulunması zorunlu olan MC (Multipoint Controller) ve bulunması zorunlu olmayan MP (Multipoint processor) kısımları. MC konferansa katılacak kullanıcıların konferans kaynaklarını denetler ve aynı iletişim seviyesinde bulunmalarını sağlar. Çok kullanıcı oturumları arasında çağrı sinyalleşmesi ve konferans kontrolünü gerçekleştirir. MP ise MC'nin kontrol ettiği konferansta ortam akışının işlenmesi ve anahtarlama işlemleri sağlar. İstendiğinde farklı ses kodlama tekniklerini kullanan kullanıcılar arasında gerekli dönüşümü sağlar.

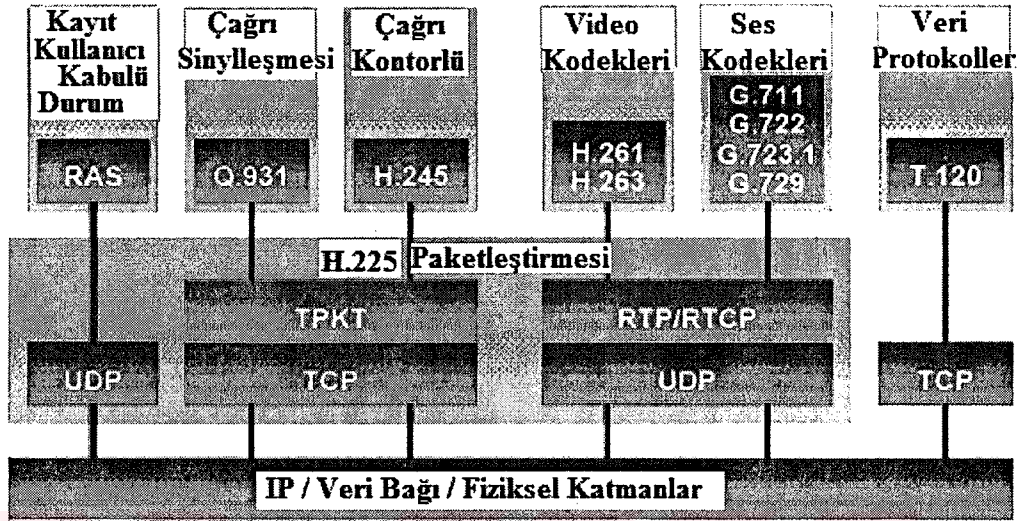
Geçiş Denetim Sistemi (Gatekeeper):

Geçiş Denetim Sistemleri terminal, ağgeçidi ve MCU'ların kaydını yapmak, gelen çağrıları kabul etmek ve statüsünü belirlemekle sorumlu ağ modülleridir. Uçbirimler kendilerini geçiş denetim sistemlerine kaydederler. Tek bir Geçiş Denetim Sistemi tarafından yönetilen uçbirimler, ağgeçitleri ve MCU'ların bulunduğu yapı alan (zone) olarak adlandırılır. Alan fiziksel network topolojisinden bağımsız birçok cihazı kapsayabilir.

Geçiş denetim sistemleri gelen kayıt mesajlarından faydalanarak adres dönüşümünü gerçekleştirir. Gerekliğinde kimlik denetimi ile kullanıcıların oturum başlatma yetkileri olup olmadığını kontrol eder. Bant genişliği yönetimi ile oturumun kurulması için yeterli bant genişliği olup olmadığını kontrol eder.

2.1.1.2. H.323 Protokol Yapısı

H.323'ün protokol yapısı Şekil 2.2'de gösterilmektedir. Çağrının kurulması, yönetilmesi, ve sonlandırılmasında birçok protokol görev almakta ve çeşitli işlevleri yerine getirmektedir. Aşağıda bu protokollerin görevleri ayrıntılı olarak anlatılmıştır.



Şekil 2.2. H.323 protokol yapısı

Terminaller uç noktalarda gerçek zamanlı ve iki yönlü haberleşme sağlayan yerel ağ sistemleridir. Bir H.323 terminali H.245, Q.931, RAS ve RTP protokollerini desteklemelidir.

RAS, terminallerin geçiş denetim sistemleri (gatekeeper) ile haberleşmesi için gereklidir. RAS mesajları ile geçiş denetim sistemleri yer tespiti, terminallerin geçiş denetim sistemine kayıt yaptırması, isim çözümlemesi (H.323 isimlerinden -> IP adreslerinin elde edilmesi), kullanıcının kabul edilmesi, bant genişliği kontrolü ve durum bilgilerinin gönderilmesi için kullanılır. RAS, geçiş denetim sisteminin yerini tespit etmek için 1718 no'lu UDP portunu, kontrol bilgileri için ise 1719 no'lu UDP portunu kullanır.

H.323'de çağrı kurulması ve sinyalleşme için ISDN-D kanalında da kullanılan Q.931 protokolü kullanılır. Noktadan noktaya tüm kontrol işlemleri H.245 protokolü tarafından sağlanmaktadır. H.245 yeteneklerin değiş tokuşu, ortam ve veri akışının yönetimi için kullanılır. TPKT, TCP akışı içerisine (mesaj tipi ve uzunluk gibi) protokole özel birtakım alanların eklenmesini sağlar. Q.931 1720 no'lu TCP portunu, H.245 ise dinamik olarak atanan 1024'ün üzerinde rasgele bir port değerini alabilir.

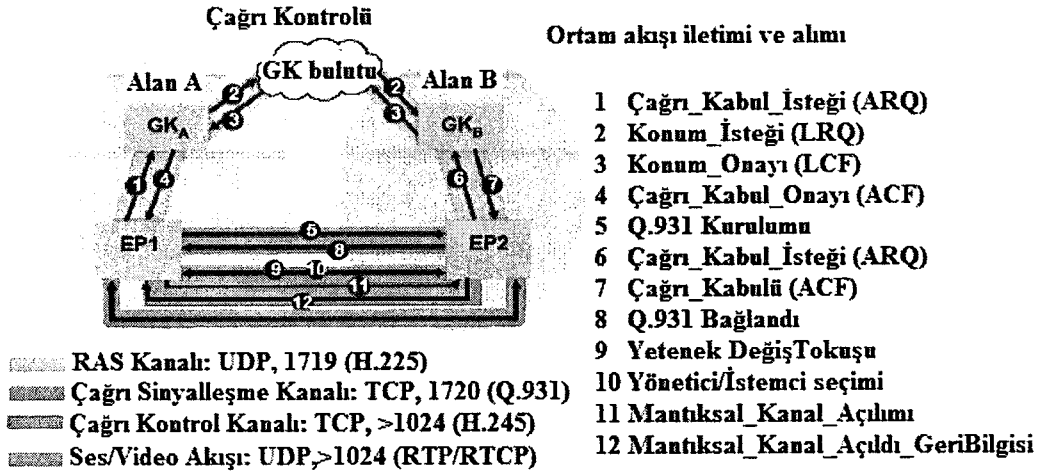
Ses ve video kodekleri sesin ve görüntünün IP ağlarında taşınmasını sağlamaktadır. Ses sıkıştırma algoritmaları ilerleyen kısımlarda anlatılmıştır. RTP gerçek ortamı (ses, görüntü ve veri) RTCP ise durum ve kontrol bilgilerini taşımaktadır. Sinyalleşme güvenli bir protokol olan TCP üzerinden yapılmaktadır. Bu protokoller ilerleyen kısımlarda detaylandırılmıştır.

T.120 veri konferansı yapmak için kullanılmaktadır. Karakter tabanlı sohbet etme, dosya transferi, uygulama paylaşımı, beyaz tahta ve görüntü paylaşımı için kullanılmaktadır. T.120 1503 no'lu TCP portunu kullanmaktadır. [2]

2.1.1.3. H.323 Çağrı Kurulumu

Bir çağrının kurulması 3 fazda gerçekleşir. İlk aşama geçiş denetim sistemi ile haberleşme aşamasıdır. Geçiş denetim sistemi çağrıyı kabul eder yada reddeder. Gerekli adres dönüşümlerini gerçekleştirir. İkinci aşamada terminaller arasında çağrı sinyalleşmesi gerçekleşir. Çağrı kurulumu, uyarılar ve bağlantı kurulumu bu aşamada tanımlanmıştır. Üçüncü aşama ise uygulama seviyesindeki sinyalleşme ile çağrı kontrolünün yapılmasını sağlamaktadır. Terminallerin yeteneklerinin değiş tokuş edilmesi, ortam akışının başlatılması ve kapatılması bu katmanın görevidir. [2]

Şekil 2.3'de iki H.323 terminali arasında oturumun kurulması aşamasında gerçekleşen mesajlaşma gösterilmiştir. Terminallerden biri bir çağrı başlattığı zaman geçiş denetim sistemi'nden Çağrı Kabul İsteği (ARQ) mesajı ile onay ister. Gatekeeper çağrıya onay vermeden önce hedef kullanıcının konum bilgisine ulaşmak için Konum Mesajı gönderir. Geçiş denetim sistemi Çağrı Kabulü (ARF) mesajı ile onay verir yada Çağrı Red (ARJ) cevabı ile mesajı reddeder. Çağrı isteği kabul edildiyse çağrıyı başlatan terminal çağırmak istediği adrese Q.931 Kurulum mesajı gönderir. Kurulum mesajını alan hedef terminal bağlı olduğu Gatekeeper'dan ARQ mesajı ile onay ister. Gatekeeper onay verdiği takdirde Q.931 işaret akışı H.245 uzlaşma mesajları ile tamamlanır. Uzlaşma mesajlarında yetenek değiş tokuşu, yönetici istemci seçimi, mantıksal kanal açılımı gibi bilgiler ile oturum parametreleri belirlenir. Son aşamada ses, video ve veri paket akışı gerçekleşir.



Şekil 2.3. H.323 çağrı kurulumu

2.1.2. SIP - Oturum Başlatma Protokolü

Oturum Başlatma Protokolü bir veya daha fazla katılımcı ile IP üzerinden çoklu ortam oturumlarını kurmak, yönetmek ve sonlandırmak için kullanılan bir uygulama katmanı işaretleşme protokolüdür. SIP ile Internet telefonu, multimedya (ses, görüntü ve data) iletimi, multimedya konferansları gibi oturumlar yönetilebilir. SIP esnek bir protokoldür. İstendiğinde devam eden çoklu gönderim bir konferansa yeni kullanıcılar eklenebilir (yada çıkartılabilir). Transparan olarak isim eşlemesi (name mapping) ve yönlendirme servislerini destekler. SIP, IETF içerisindeki SIP çalışma grubu tarafından geliştirilmiştir. Protokol ilk defa 1999 yılında IETF RFC 2543 isminde yayınlanmış, daha sonra geliştirilerek birtakım değişikliklerle RFC 3261 olarak yeniden yayınlanmıştır. [3]

SIP’de multimedya bağlantılarını kurmak ve sonlandırmak için 5 adet yüzey tanımlanmıştır.

- **Kullanıcı Konumu:** İletişim kurulması istenen uç noktanın yerinin belirlenmesi için kullanılır.
- **Kullanıcı Uygunluğu:** Çağrılan tarafın haberleşmeye katılma isteğinin belirlenmesi için kullanılır.
- **Kullanıcı Yetenekleri:** Ortam parametrelerinin belirlenmesi için kullanılır.
- **Oturumu Kurulumu:** “çalma işlemi”, çağrı gönderen taraf ve aranan tarafın oturum parametrelerinin nasıl kurulacağını tanımlar.

- **Oturum Yönetimi:** Oturumda veri transferleri, oturumun sonlandırılması, oturum parametrelerinin değiştirilmesi, ve çağırma servislerini tanımlar. [3]

SIP tam anlamıyla tümleşik bir haberleşme sistemi değildir. SIP'in ses, görüntü ve multimedya servislerini verebilmesi için birtakım başka protokollerle işbirliği içerisinde çalışması gerekmektedir. Bu protokoller arasında gerçek zamanlı veri iletimi için RTP protokolü , akan ortamın (ses,görüntü vs.) iletim kontrolü için RTCP, PSTN şebekesine bağlantıda kullanılan ağgeçitlerinin kontrolü için MEGACO, çoklu ortam oturumlarını tanımlamak için SDP protokolleri sayılabilir. Buna rağmen temel fonksiyonları ve kullanımı açısından SIP bu protokollere bağımlı değildir.

SIP kullanıcılara birtakım güvenlik servisleri sağlar . Bunlar arasında DoS (Denial of Service) saldırıları önlenmesi, kullanıcı doğrulanması (hem kullanıcılar arası, hem de kullanıcı ile proxy arası), içerik koruması, şifreleme sayılabilir. SIP IPv4'ün yanı sıra IPv6 ile beraber çalışabilen bir protokoldür. [3]

SIP, SMTP ve HTTP gibi metin bazlı bir protokoldür ve UTF-8 karakter setini kullanır. Ufak tefek farklılıklar dışında SIP'in mesaj ve başlık alanının biçimi HTTP/1.1 ile aynıdır.

SIP ağı dört mantıksal bileşenden oluşur. Her bir SIP bileşeninin özel bir fonksiyonu vardır. Bir fiziksel cihaz bu mantıksal bileşenlerden biri yada birkaçının görevini üstlenebilir. Örneğin Proxy sunucusu olarak çalışan bir sunucu aynı zamanda Yönlendirme sunucusu yada kayıt sunucusu görevini de üstlenebilir. [4]

2.1.2.1. SIP Bileşenleri:

SIP protokolünün tanımladığı dört tip SIP mantıksal bileşeni aşağıda tanımlanmıştır:

Kullanıcı Arabirimi: (User Agent-UA):

Uç noktadaki SIP bileşenleridir. Kullanıcı arabiriminin görevi çağrıyı başlatmak ve oturum tamamlandığında çağrıyı sonlandırmaktır. RFC 2543'de UA uç noktalarda çalışan bir uygulama olarak tanımlanmaktadır. Kullanıcı Arabirimi İstemci ve sunucu olarak iki alt bileşenden oluşmaktadır. Bir UA her iki durumda da bulunabilir.

İstemci Kullanıcı Birimi (User Agent Client - UAC): İstemci Kullanıcı Birimi SIP oturumunu çağrı gönderme isteği ile başlatır.

Sunucu Kullanıcı Birimi (User Agent Server - UAS): Sunucu Kullanıcı Birimi çağrının gönderildiği hedef kullanıcıyı tanımlar. UAS'ın görevi gelen çağrıyı cevaplamaktır.

Kullanıcı Arabirimi olarak çalışabilen cihazlara yazılımsal ve donanımsal tabanlı IP telefonlar, ağ geçitleri, otomatik cevap verme servisleri örnek verilebilir.

Proxy Sunucusu (Proxy Server):

SIP sunucusu kullanıcı arabiriminden gelen SIP oturum taleplerini alır ve oturum talebini hedef kullanıcı arabirimi yada hedef kullanıcının bulunduğu taraftaki başka bir sunucuya gönderir. Proxy Sunucusu hem kullanıcı arabirimi adına oturum talebinde bulunabilen, hem de bu taleplere gelen cevapları kullanıcı arabirimine gönderme fonksiyonunu üstlenen bir ara bileşendir. Proxy sunucusu hem istemci hem de sunucu rolünü üstlenmektedir. Bu sunucunun başka bir özelliği ise SIP protokolünü kullanmayan kullanıcılarla oturumun kurulabilmesini sağlamaktır. Bu sayede bir SIP kullanıcısı proxy sunucusu vasıtasıyla H.323 protokolünü destekleyen bir kullanıcı ile konuşabilir.

Yönlendirme Sunucusu (Redirect Server):

Kullanıcı Arabirimi'nden gelen SIP taleplerini alır, hedef kullanıcı ile bağlantı kurulabilmesi için çağrı gönderen kullanıcıya hedef kullanıcının adresini gönderir. Kullanıcı adına hedef kullanıcıya doğru herhangi bir oturum talebinde bulunmaz.

Kayıt Sunucusu (Registrar):

Kayıt sunucusu kullanıcılarının konum bilgilerini girmelerini sağlayan sunucudur. İstek gönderen kullanıcıların konum bilgilerini veritabanında günceller. [4]

SIP sunucuları SIP uçbirimlerinin mesaj gönderebilmesi, konum bilgisi kaydı yaptırabilmesi, ağlar arası iletişim kurabilmesi ve ağlar arası bağlantı kurabilmesi için gerekli ağ elemanlarıdır. SIP sunucularının desteklediği özellikler sayesinde istenilen yönlendirme ve güvenlik politikaları yüklenebilir, kullanıcıların kimlik doğrulamaları sağlanabilir. SIP sunucuları genelde çok sayıda bağlantıyı destekleyen, düşük gecikmeli, yüksek gerçek zaman performansı gösteren, ölçeklenebilir sunucular olmalıdır. [5]

2.1.2.2. SIP Mesaj Tipleri

SIP haberleşmesinde iki tip SIP mesajı tanımlanmıştır. Bu mesajlar kullanıcının sunucuya gönderdiği talep mesajları (Request) ve sunucunun kullanıcıya gönderdiği cevap mesajlarıdır (Responses).

Talep Mesajları:

SIP haberleşmesi altı tip talep mesajından oluşmaktadır. Talep yöntemleri Tablo 2.2’de verilmiştir.

Tablo 2.2. SIP Talep Mesaj Tipleri

Yöntem	Tanım
INVITE	Çağrıyı başlatmak için kullanılan mesaj tipidir
ACK	Çağrı başlatma talebinin sonucunu bildirir
OPTIONS	Kullanıcı Arabirim yetenlerinin ve sunucu yeteneklerinin sorgulanması için kullanılır.
BYE	Oturuma devam eden kullanıcıların çağrıyı sonlandırma için kullandıkları mesaj tipidir.
CANCEL	Devam eden çağrı talebinin iptal edilmesi için kullanılır.
REGISTER	Kullanıcıların konum bilgilerinin kayıt sunucusuna bildirilmesinde kullanılır.

Cevap Mesajları:

SIP cevap mesajları talep mesajlarına cevap olarak gönderilen mesaj tipleridir. Mesajlar HTTP cevap kodlarına benzer sayısal kodlar içerir. Bu mesaj tipleri geçici mesajlar ve sonuç mesajları olarak iki kısımda incelenebilir. Geçici mesajlar talep mesajının sonuçlanması sürecine kadar gönderilen bilgilendirme mesajlarıdır. Sonuç mesajları ise çağrı isteğinin sonucunu bildirir.

Tablo 2.3. SIP Cevap Mesaj Kodları ve Açıklamaları

Cevap Sınıfı	Durum Kodu	Açıklaması
Bilgilendirme	100	Deneniyor
	180	Çalıyor
	181	Çağrı Yönlendirildi
	182	Kuyruğa alındı
Başarı	200	Tamam
	300	Çoklu Seçim
	301	Sürekli olarak taşındı
	302	Geçici olarak taşındı
	3xx	
İstemci-Hatası	400	Hatalı talep
	401	Yetkisiz
	402	Ücretlendirme gerekli
	403	Yasak
	404	Bulunamadı
	405	Yöntem kabul edilmedi
	4xx	
Sunucu Hatası	500	Dahili sunucu hatası
	502	Hatalı ağgeçidi
	5xx	
Global Başarısızlık	600	Meşgul
	603	Ret
	604	Mevcut değil
	606	Kabul edilemez

2.1.2.3. SIP Adreslemesi

SIP Adresleri e-posta adreslerine benzer bir yapıda kullanıcı@etki_alanı yapısındadır. Kullanıcı kısmında kullanıcı adı yada telefon numarası bulunabilir. Etki_alanı kısmında etki alanı yada ağ adresi bulunabilir. E-posta adresleri ile aynı formatta olması bir kişinin SIP adresinin bulunmasını kolaylaştırmaktadır. Örnek SIP Adresleri:

- deneme@itu.edu.tr
- 902122853030@160.75.1.1

2.1.2.4. SIP Mesaj Yapısı

SIP karakter tabanlı bir protokoldür ve UTF-8 karakter setini kullanır. SIP mesajları istemciden sunucuya giden bir talep mesajı formatında ya da sunucudan istemciye giden cevap mesajı yapısındadır. Bütün SIP mesajları bir başlangıç satırı, bir veya daha fazla başlık alanı ve isteğe bağlı mesaj gövdesinden oluşur. [3]

Başlangıç Satırı

Başlangıç satırı SIP mesajının başlık kısmını tanımlar. Bu alan mesaj türüne göre farklılaşmaktadır.

- Talep Mesajları için bu alanda talep mesajı türü (invite, ack, bye vs.), çağrılan kişinin SIP adresi ve SIP protokol sürümü belirlenir. SIP adresi proxy sunucusu tarafından değiştirilebilmektedir.
- Cevap Mesajları için bu alanda cevap mesajının durum kodu (200, 300 vs.) ve durum kodunun metinsel ifadesi bulunur.

Başlık Kısmı:

SIP başlık alanları mesaj niteliklerini barındırarak mesajın anlamını tanımlar. Birkaç ufak tefek fark dışında SIP mesajları ve başlık kısmının biçimi HTTP ile aynıdır. Hatta bazı kısımlar HTTP'den ödünç alınmıştır.

Mesaj Gövdesi:

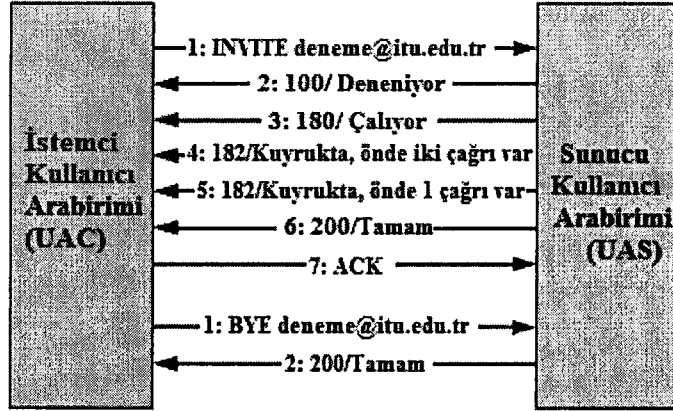
Mesaj gövdesi kurulacak oturumun detaylandırılmasını sağlamak için kullanılır. Örnek olarak kurulacak çoklu ortam oturumunda kullanılan ses kodekleri, örnekleme oranları gibi parametreler bu kısımda tanımlanmıştır. Bu alanda ayrıca oturum ile ilgili ikili yada metin formatında veri bilgileri taşınır. Bu kısım hem talep mesajlarında hem de cevap mesajlarında bulunabilir. SIP'de gövde kısmında bulunan bilgiler ile başlangıç satırı ve başlık kısmında tanımlanan sinyalleşme bilgisi arasında herhangi bir ilişki bulunmamaktadır. Gövde türleri aşağıdaki yapılarda olabilir:

- SDP- Oturum Tanımlama Protokolü
- Çok amaçlı Internet Posta Uzantıları (MIME)
- IETF tarafından ileride geliştirilmesi planlanan diğer protokoller.

2.1.2.5. SIP Mesaj Kurulumu Örnekleri

SIP bileşenlerinin oturum kurma aşamaları aşağıdaki örneklerde incelenmiştir.

Örnek 1:



Şekil 2.4. SIP Oturum Kurulumu ve Çağrı Sonlandırılması

Şekil 2.4’de iki SIP uçbirimi arasında SIP oturumu kurlumu ve sonlandırılması aşamaları incelenmiştir.

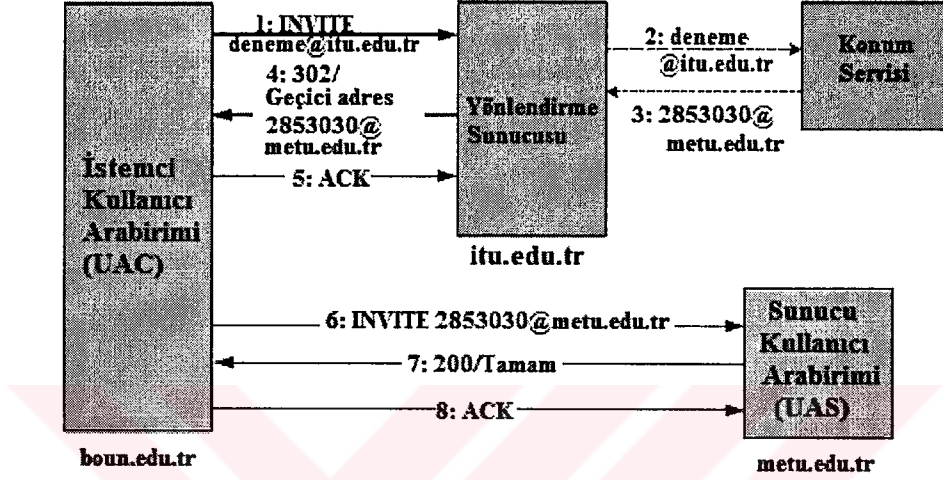
Oturum kurulumu ve sonlandırılması:

- 1) İstemci Kullanıcı Arabirimi deneme@itu.edu.tr SIP adresini yazarak INVITE mesajı ile çağrı talebinde bulunur. Bu mesajın içerisinde UAC’in yeteneklerini tanımlayan SDP paketi bulunmaktadır.
- 2) UAS çağrı talebini alır ve hemen “100” cevap kodlu ”deneniyor” mesajını gönderir.
- 3) UAS uçbirimi çaldırırken aynı anda UAC’ı bilgilendirme amaçlı “180” cevap kodlu “çalışıyor” mesajını gönderir
- 4) UAS “182” cevap kodlu mesaj ile çağrının mevcut iki çağrının arkasında kuyrukta olduğunu bildirir.
- 5) UAS “182” cevap kodlu mesaj ile çağrının mevcut bir çağrının arkasında kuyrukta olduğunu bildirir.
- 6) UAS çağrıyı cevaplar ve UAC’a “200” cevap kodlu çağrının cevaplandığını bildiren “tamam” mesajı gönderilir. Bu mesajda UAS’in yeteneklerini tanımlayan SDP paketi de bulunmaktadır.

- 7) UAC ACK cevap kodlu mesaj ile cevabın alındığı bilgisini iletir. Bu mesaj ile birlikte ortam akışı başlamış olur.
- 8) UAC çağrıyı sonlandırmak istediğinde UAS'a 'BYE' talebini gönderir.
- 9) UAS bu talebi "200" cevap kodlu mesaj ile onaylar ve çağrı sonlandırılır.

Örnek 2:

Şekil 2.5'de basit bir çağrı yönlendirme senaryosu ele alınmıştır.



Şekil 2.5. Yönlendirme Sunucusu Kullanılarak Çağrı Yönlendirilmesi

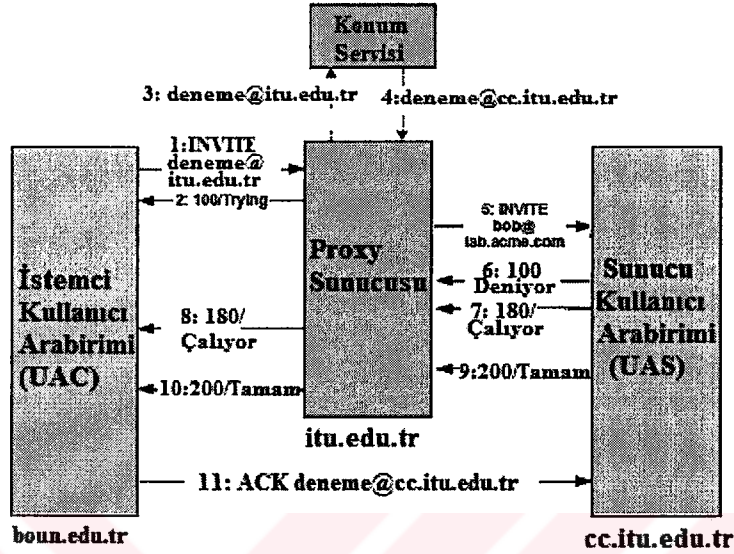
Çağrı Akışı:

- 1) İstemci Kullanıcı Arabirimi deneme@itu.edu.tr SIP adresini yazarak INVITE mesajı ile çağrı talebinde bulunur.
- 2) Yönlendirme sunucusu hedef SIP adresini çözümleyemiyorsa adres çözümleme işlemi için Konum Servisi sunucusuna istekte bulunur.
- 3) Konum servisi UAS'ın o anki konumunu 2853030@metu.edu.tr olarak döndürür.
- 4) Yönlendirme sunucusu yeni konum bilgisini UAC'ye "302" cevap kodlu "geçici taşıma" cevabı ile iletir.
- 5) UAC yönlendirme sunucusuna ACK mesajı yollayarak cevabı onaylar.
- 6) UAC 2853030@metu.edu.tr SIP adresini yazarak yeni bir INVITE mesajı ile çağrı talebinde bulunur.
- 7) UAS çağrıya cevap verir ve bu mesaj "200" cevap kodu ile UAC'a bildirilir.

8) UAC ACK mesajı ile çağrı kurulumunu onaylar.

Örnek 3:

Şekil 2.6'da istemcilerin proxy üzerinden oturum kurmaları ile ilgili bir senaryo incelenmiştir.



Şekil 2.6. Proxy Sunucusu Senaryosu

Çağrı Akışı:

- 1) İstemci Kullanıcı Arabirimi deneme@itu.edu.tr SIP adresini yazarak INVITE mesajı ile çağrı talebinde bulunur.
- 2) Proxy Sunucusu “100” cevap kodlu “deneniyor” mesajını gönderir.
- 3) Yönlendirme sunucusu hedef SIP adresini çözümleyemiyorsa adres çözümleme işlemi için Konum Servisi sunucusuna istekte bulunur.
- 4) Konum servisi UAS’ın o anki konumunu deneme@cc.itu.edu.tr olarak döndürür.
- 5) Proxy Sunucusu UAC adına UAS’ın yeni SIP adresini deneme@cc.itu.edu.tr yazarak INVITE mesajı ile çağrı talebinde bulunur.
- 6) UAS “100” cevap kodlu “deneniyor” mesajını gönderir.
- 7) UAS uçbirimi çaldirırken aynı anda UAC’ı bilgilendirme amaçlı “180” cevap kodlu “çalıyor” mesajını gönderir
- 8) Proxy Sunucusu “180” cevap kodlu mesajı UAC’a iletir.

9) UAS çağrıya cevap verir ve bu mesaj “200” cevap kodunu UAC’a bildirilir. Artık proxy sunucusu devreden çıkarılmış olur.

10) UAC ACK mesajı ile çağrı kurulumunu onaylar.

2.1.2.6. SDP (Oturum Tanımlama Protokolü)

SDP çoklu ortam oturum duyurularını tanımlamak, çoklu ortam oturumlarına davet etme işlemlerini tanımlamak için kullanılan bir protokoldür. SDP paketleri aşağıdaki bilgileri içerir.

Oturum Bilgisi:

- Oturum ismi ve amacı
- Oturumun aktif olduğu zaman dilimi
- Oturum tarafından kullanılmak üzere gerekli bant genişliği ile ilgili bilgi (eklenebilir özellik)
- Oturum ile ilgili sorumlu kişinin kontak bilgileri. (eklenebilir özellik)

Ortam Bilgisi:

- Ortamın tipi (ses, görüntü vs.)
- İletim protokolü, RTP/UDP/IP ve H.320
- Ortamın biçimi (H.261 görüntüsü, MPEG görüntüsü vs)
- Çoklu gönderim Adresi ve iletim katmanı port numarası.
- Uzak ucun adresi ve iletim katmanı port numarası.[4]

SIP iki veya daha fazla katılımcının çoklu ortam uygulamaları için geliştirilmiş IETF temelli bir sinyalleşme protokolüdür. SIP ilave özellikler ve servisler sağlamak için genişleme yetenekleri olan esnek bir protokoldür. IETF tarafından belli özellikleri ve işlevselliği gerçekleştirmek üzere tasarlanan SIP katmanlı ve fonksiyonel bir mimariye sahiptir.

SIP, H.323’e göre daha basit bir yapıya sahiptir ve çağrı kurma süresi daha hızlıdır. Modüler yapısı ve farklı protokoller ile işbirliği içerisinde çalışabilmesi , HTTP benzeri yapısı SIP’i cazip kılmaktadır. Sunucular çağrı durumunu takip etmek zorunda değildir. [7]

HTTP’nin aksine SIP oturumları UDP yada diğer güvenli olmayan iletim katmanı protokollerini kullanabilir. Bu tip datagramların her biri bir talep yada cevap bilgisi taşır.

SIP oturumları TCP,UDP ve SCTP gibi birden fazla iletim katmanı protokolü üzerinden taşınabilir. Ayrıca TCP üzerinden TLS’de desteklenmektedir. Bunun için karşılıklı sunucuların hangi iletim protokolü kullanacakları konusunda uzlaşmaya varmaları gerekmektedir. [8]

2.1.3. H.323 ve SIP Karşılaştırması

H.323 ve SIP VoIP pazarında birbirleri ile yarışan iki protokol konumundadır. H.323 çok daha önce geliştirilen bir protokol olmanın avantajı ile pazarda lider durumda olup halen yaygın olarak birçok ağda kullanılmaktadır. Diğer taraftan SIP’deki gelişmeler yakın gelecekte SIP’in , H.323’ün yerini alacağını işaret etmektedir.

H.323 bir örtü tanımlamasıdır, tek başına bir protokol değildir. Yeni bir servis yaratmak için diğer protokollerin nasıl kullanılacağını bildirmektedir. H.323 1990’ın ortalarında ITU (International Telecommunications Union) tarafından geliştirilmiştir. Yapısında H.225 RAS sinyalleşmesi, Q.931 çağrı sinyalleşmesi (call signaling, H.245 kontrol sinyalleşmesi RTP gerçek zaman protokolü, ses ve görüntü sayısallaştırılması ve sıkıştırılması işlemlerini yerine getiren birçok standart barındırmaktadır.

H.323 yerel alan ağlarında çoklu ortam konferanslarının kurulabilmesi için tasarlanmıştır. Orijinal yapısında bazı konferansların önceden anons edilmesi ve bu konferansa katılmak isteyen kullanıcıların konferansa kayıt yaptırması düşünülmüştür. Bu konferanslar interaktif olabileceği gibi sadece katılımcıların görebileceği, dinleyebileceği genel yayın paketleri de olabilir.

Daha sonra protokol daha fazla arama seçeneklerini ve aynı yerel alan ağı’nda (LAN) bulunmayan kullanıcıları da kapsayacak şekilde genişletilmiştir. Bu, protokolün ve altında yatan uygulamaların daha da karışmasına sebep olmuştur. H.323 kodlama ve veri alanı için geniş bir hafızaya ihtiyaç duyan çok geniş bir protokol kümesidir. Mesajlaşma biçimi olarak Abstract Syntax Notation’ı kullanmaktadır (ASN.1). ASN.1 ITU tarafından yaygın olarak kullanılmakla beraber, kullanıcıların bu protokolü doğrudan okuması ve anlaması zordur. ASN.1’in anlamlı olabilmesi için ASN.1 mesajlarını çözen daha kolay ağ testi ve hata ayıklama (debugging) özelliklerini destekleyen ve insanın anlayabileceği yapıya çeviren özel yazılımlara ihtiyaç duyulmaktadır.

H.323 temelli ağların kurulabilmesi için ITU tarafından değişik kategorilerde bileşenler tanımlanmıştır. Şekil 2.1’de gözüken bu bileşenler H.323 terminalleri, Ağgeçitleri (Gateway), Geçiş Denetim Sistemleri, ve Çok Noktalı Denetim Birim’lerinden (MCU)

oluşmaktadır. H.323 terminalleri son kullanıcılar olup bu cihazlar arasında telefon cihazları, görüntü sistemleri, ses sistemleri gibi birçok çeşit ürün bulunabilir. Ağgeçitleri (gateway) diğer networklere (PSTN, ISDN, ATM ve diğer VoIP networkler etc) erişimi sağlamaktadır. Geçiş Denetim Sistemleri kimin kiminle konuşup, konuşamayacağını düzenleyen cihazlardır. Bir terminal başka bir kullanıcı ile haberleşmeye başlamadan önce gatekeeper'dan izin almalıdır. MCU'lar köprü vazifesi ile bir konferansta birçok kullanıcının konferansa katılımını yönetir.

H.323'ün karmaşıklığı basit bir çağrı kurulumunda bile çok sayıda mesajın gönderilmesine neden olur. Ağ farklı gatekeeper'lar tarafından yönetilen segmanlara ayrılabilir. Bir çağrı kurulumunda birden çok gatekeeper işin içine girdiğinden mesajlaşma çok daha karmaşık bir hal almaktadır.

H.323'e alternatif olarak Internet Engineering Task Force (IETF) çağrı kurulumu ve VoIP uygulamalarının yönetimine destek sağlayacak çok daha basit ama daha güçlü bir protokol oluşturmak üzere çalışmalara başlamıştır. Oluşturulan çalışma grubu IETF tarafından 1999'da RFC 2543'de yayınlanan SIP protokolünü geliştirmiştir.

IETF ve ITU protokol özelliklerini geliştirirken çok farklı yaklaşımlarda bulunmuşlardır. ITU'nun protokolü geliştirirkenki yaklaşımı herhangi birinin ihtiyaç duyacağı bütün servisleri ele alıp bunlara çözüm bulacak şekilde tanımlamalarda bulunması şeklinde olmuştur. Uzun bir süreç sonunda geliştirilen standartlar çok genişlemiş ve fazla detay içermiştir. Çok nadir kullanılması olası birçok VoIP uygulaması için anlaşılması güç elemanlar yerleştirilmiş ve detaylı tanımlamalar yapılmıştır. Diğer taraftan IETF "bir problem, bir çözüm" prensibi ile tam ters bir yaklaşımı ortaya atmış ve VoIP uygulamaları için çok daha az mesajlaşma adımı kullanarak kendini göstermiştir. SIP RFC'sinde VoIP dışındaki diğer uygulamalar için detaylı bir tanımlama yapılmamıştır. Sonuç olarak RFC tanımı dışında kalan birçok eklenti elemanı geliştirilmiştir. SIP, H.323'e göre esnek yapısıyla çok daha hızlı geliştirilmiş ve çok daha az kod içeren bir protokol ortaya çıkmıştır.

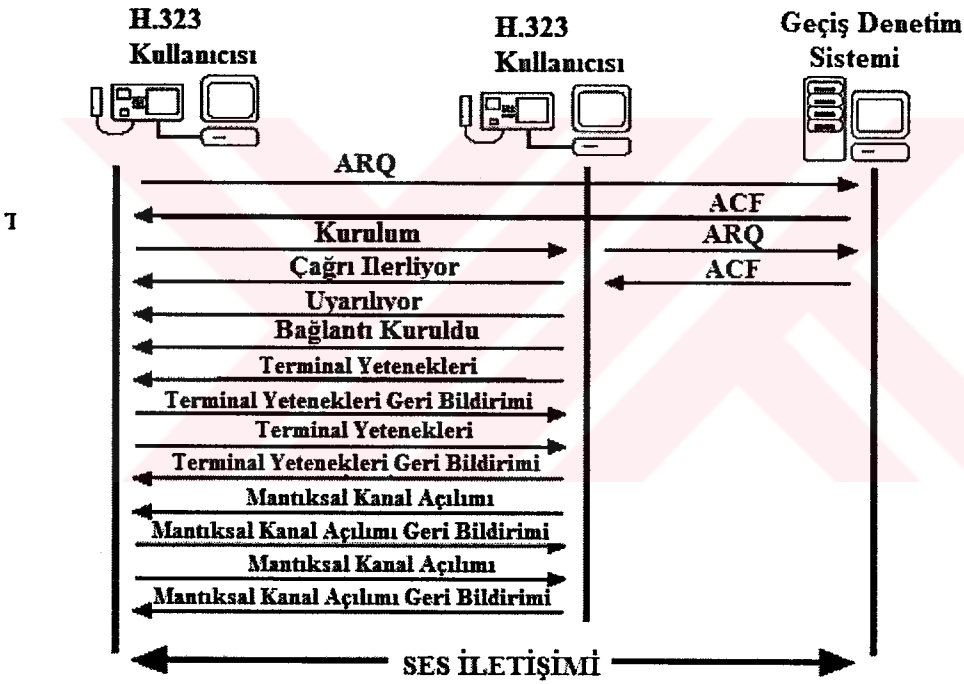
Aşağıda SIP ve H.323 protokolleri birtakım kriterlere göre karşılaştırılmıştır.

2.1.3.1. Karmaşıklık

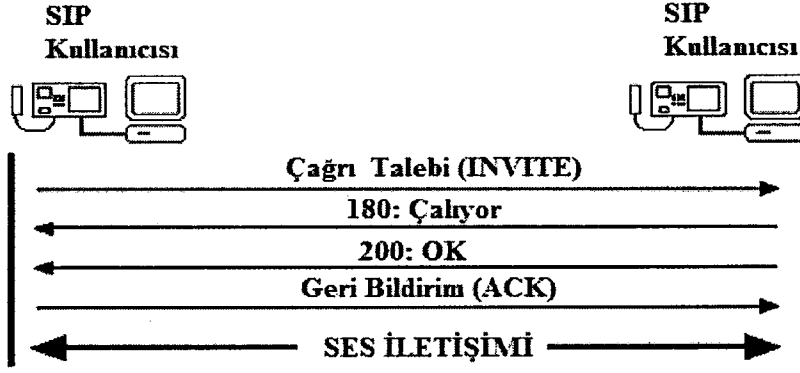
Yukarıda da belirtildiği gibi H.323 çok karmaşık bir protokol grubudur. H.323 ile ilgili yapılan en büyük eleştiri bu protokolün network üzerinde gereksiz yere bir sürü mesaj

göndermesi yönündedir. H.323 geniş bir sistem için ölçeklenebilir bir yapı sunmamaktadır. Çok yoğun oturumların kurulduğu bir sistemde çok sayıda mesajın gidip gelmesi sistem performansını olumsuz yönde etkilemektedir. Bu da ses kalitesinin düşmesine sebep olmaktadır.

Şekil 2.7’de çağrı kurulacak kişinin adresi bilindiği durumda çağrı kurulması aşamasında gerekli olan mesajlaşma gösterilmektedir. Mesajların detayına girmeden baktığımızda bir çağrı kurulması için 16 adet mesajın LAN üzerinde değiş tokuş edilmesi gerekmektedir. Bu sayı, terminallerin farklı geçiş denetim sistemleri tarafından yönetilen networklerde olması durumunda belirgin bir biçimde artmaktadır. Şekil 2.8 ise aynı çağrı kurulumu için SIP kullanıldığında gerekli olan mesajlaşma yapısını göstermektedir. Bu yapıda çağrının kurulabilmesi için sadece 4 adet mesaj yeterlidir.



Şekil 2.7 H.323 Çağrı Kurulumu

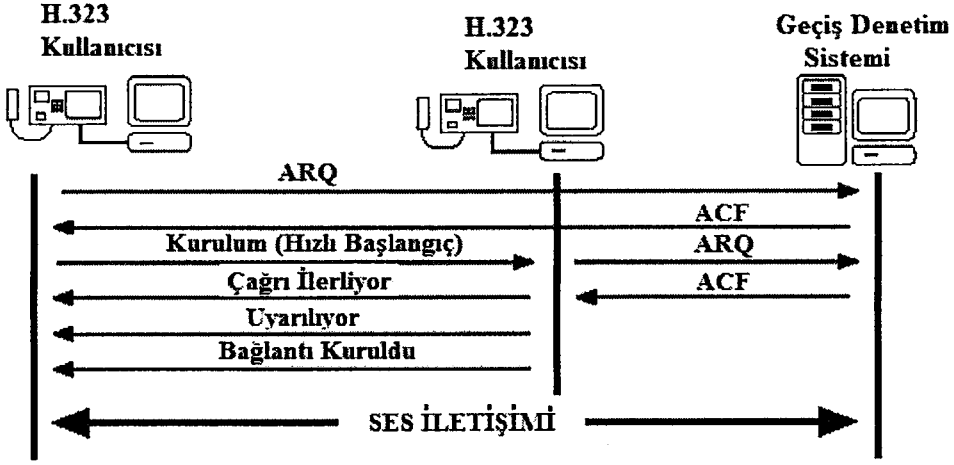


Şekil 2.8 SIP Çağrı Kurulumu

Bu farkın açık bir sonucu olarak SIP kullanıldığında H.323'e göre gerekli olan kullanıcı uygulaması çok daha basit olmaktadır. H.323'de terminaller konfigürasyon bilgisini karşılıklı olarak gönderdikleri mesajlarla oluşturmaktadır. Bu sayede karşılıklı uçlar kullanılacak parametreler konusunda anlaşmaktadır.. SIP'de ise bu mesajlaşma farklı mesajlara ihtiyaç duymadan sadece Talep ve Cevap (200:OK) mesajları ile tamamlanmaktadır. İki protokolde de ses paketlerinin ilerlemesi için uçlar arasında mantıksal bağlar kurulmaktadır. SIP'de bütün bu bilgiler aynı talep ve cevap mesajının içerisinde yer almaktadır.

SIP mesajları H.323'e göre daha fazla yer kaplamaktadır. Ama birçok küçük çerçeve göndermektense birkaç büyük çerçeve göndermek her zaman daha performanslı bir yöntemdir.

H.323'ün bu zayıflığının önüne geçmek, basit çağrıların daha hızlı kurmak için bir takım yöntemler geliştirilmiştir. Bu yöntemlerden bir tanesi "Hızlı Başlangıç" olarak adlandırılmaktadır. Şekil 2.9'da da görüldüğü üzere "Hızlı Başlangıç" yapısında iki tarafın da mesajlarında detaylı bilgi göndermesi ve haberleşme için daha önceden belirlenmiş portların kullanılması ile gönderilecek mesaj sayısı azaltılmıştır. Ama bu da aynı anda birçok noktaya çağrı yapılmasını sınırlamaktadır. Çünkü bu durumda terminalin birçok noktaya "Hızlı Başlangıç" ile çağrı kurabilmesi için diğer terminallerin adreslerini bilmesi ve bu uçlarla ilgili gerekli konfigürasyon bilgisini barındırması gerekmektedir. Diğer taraftan bütün terminaller "Hızlı Başlangıç" özelliğini desteklememektedir. Bu da protokolün faydalarını sınırlamaktadır. "Hızlı Başlangıç" daha çok kullanıcıların birbirini tanıdığı ofis ortamları gibi kapalı sistemler için geliştirilmiştir.



Şekil 2.9. H.323’de Hızlı Başlangıç Yapısı

Hızlı Başlangıç sistemi ile ilgili diğer bir problem de faturalandırılabilir durum tespitinin yapılamamasıdır. Bu sistemin çağrının gerçekten kurulup kurulmadığını tespit edemeyeceği ve ücretli çağrıları desteklemeyeceği belirtilmektedir. SIP’de cevap mesajlarında iletilen 200:OK mesajı kaynağın karşı uçtaki çağrıyı kabul ettiğini belirtir. H.323 Hızlı Başlangıç’ta ise eğer CONNECT mesajı kaybolursa çağrı kurulmuş olsa bile karşı ucun bağlantı kurulduğunu anlamaması ve çağrının bir süreliğine faturalandırılmaması söz konusu olabilir.

2.1.3.2 Boyut ve Performans

SIP daha basit bir protokol olduğundan H.323 kurulumuna göre daha az kod gerektirir. Bu sayede gerekli kod satırı sayısının yanı sıra hem protokol kümesi için hem de kullanıcı uygulaması için daha düşük dinamik belleğe ihtiyaç duyar. Çağrı kurulması için işlemcinin daha az sayıda mesajı ele alması SIP’in H.323’e göre daha hızlı bir protokol olmasını sağlar. Bunun anlamı SIP’in saniyede ele alabileceği çağrı sayısı H.323’e göre daha fazladır ve SIP aynı sayıda çağrıyı ele almak için daha düşük kapasiteli işlemciye ihtiyaç duymaktadır. Sonuç olarak SIP’in sistem kurulum maliyeti daha düşüktür.

2.1.3.3 Özellik Karşılaştırması

Mesaj biçimi olarak ASN.1 kullanılması her protokol değişikliğinde H.323 hata ayıklama (debugging) araçlarında güncellemelere ihtiyaç duyulmaktadır. SIP mesajları metin tabanlı olduğu için hata ayıklamada güncelleme ihtiyacı duymazlar. SIP araçları SIP’e yeni özellikler eklendikçe eskimezler.

İki protokolde gelişmelere açıktır. Ama SIP çok daha fazla genişleyebilir ve yapılan eklentiler kolaylıkla yüklenebilir. İki protokolde de kullanıcılar kendi eklentilerini ekleyebilirler ama H.323’de bu eklentiler ASN.1 formatında olmalıdır. SIP’da ise eklentiler geliştirilmesi çok daha kolay olan metin mesajları biçiminde eklenebilir.

H.323 elemanlarının hepsi durum (state) bilgisini tutmak zorundadır. SIP’da ise sadece UA’nin bunu yapması zorunludur. Bazı durumlarda proxy sunucusu da durum bilgilerini tutabilir. Bu H.323’lere ek yük getirmekle beraber H.323 kodunun karmaşıklığını arttırmaktadır.

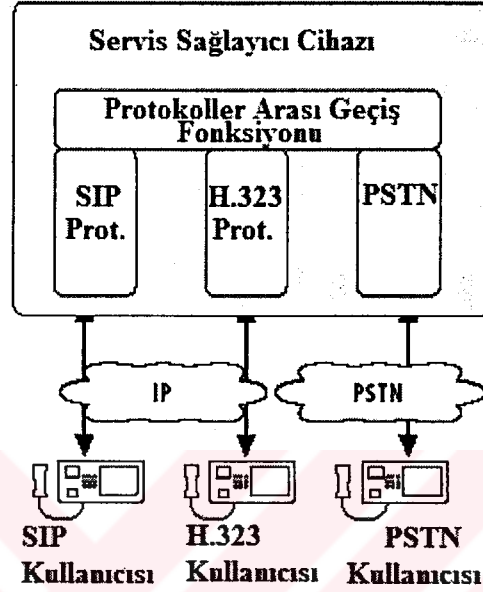
İki protokol de güçlü telefon özelliklerini destekler. Bir protokolün diğeri üzerinde belirgin bir avantajı yoktur. Tablo 2.4’de H.323 ve SIP protokolleri karşılaştırılmıştır.

Tablo 2.4. H.323 ve SIP özellik karşılaştırması

Ölçüt	H.323	SIP
Karmaşıklık	Çok Karmaşık	Basit
Mesaj Kümesi	Birçok Mesaj İletimi	Az Sayıda Mesaj İletimi
Hata Ayıklama	Protokol genişlediğinde araçlarda değiştirilmeli	Basit Araçlar Sürekli Kullanılabilir.
Genişleyebilme	Genişleyebilir	Çok Genişleyebilir
Durum bilgilerini tutmak zorunda olan elemanlar	Terminaller, Geçiş Denetim Sistemleri, MCU, Ağgeçitleri	UA ve bazı Proxy Sunucular
İşlemci Kullanımı	İşlemciye fazla yük bindirir	İşlemciye az yük bindirir
Telefon Özellikleri	Güçlü	Güçlü
Kullanıcı Uygulamaları	Karmaşık	Basit
Kod Büyüklüğü	Uzun	Kısa
Dinamik Hafıza Kullanımı	Geniş	Orta

Diğer taraftan H.323 çok yaygın bir kullanım alanına sahiptir. Kullanıcılar VoIP ürünleri üretirken geçmiş cihazlar ve servisler ile uyumlu bir yapı kurmak istemektedir. SIP ürünlerine H.323 özelliklerini de eklemek SIP temelli ürün maliyeti yanında çok büyük yatırım maliyetlerini de beraber getirmektedir. (H.323 lisanslaması, kullanıcı uygulamalarının geliştirilmesi, test edilmesi vs.) SIP ve H.323’ün uyumlu hale getirilmesi

uzun mühendislik çalışmalarına gereksinim duyar. SIP daha iyi bir protokol olsa da H.323 ağlarla konuşabilmek için H.323 gereklidir. Aslında şu an piyasada bulunan çoğu H.323 ürün aynı zamanda SIP'i de desteklemektedir ve SIP/H.323 entegrasyonu sağlanmıştır. Yani bir protokolü kullanan bir network diğer protokolün ürünleri ile iletişim kurabilmektedir. [9]



Şekil 2.10. VoIP Servisleri arasında geçişin sağlanması

2.2. SES Sıkıştırma Algoritmaları

Ses iletiminde en önemli noktalardan biri sesin ip ağları üzerinden iletilirken hangi algoritma ile kodlanacağıdır. Bu amaçla çeşitli sıkıştırma algoritmaları geliştirilmiştir. Sesi sıkıştırma ve çözülme işini yapan yazılımsal yada donanımsal araçlara kodek (coder-decoder) denir. Sesin sayısal olarak iletilmesi için ilk olarak G.711 PCM algoritması kullanılmıştır. Halen PSTN şebekelerinde ve Türk Telekom'da kullanılan bu algoritma sesi sıkıştırmadan 64kbps hızında iletmektedir. Sesin sayısal ağlarda sıkıştırılması için ise ilk olarak G.726 ADPCM ve G.728LD-CELP algoritmaları kullanılmıştır. Bu algoritmalar ile ses 32 kbps ve 16 kbps olarak kodlanmış. Bit oranındaki sıkıştırmaya paralel olarak sesin kalitesinde de bir miktar azalma olmuştur. İnsan sesinin sıkıştırılmasına yönelik algoritmalar ve DSP teknolojisindeki gelişmeler kalitede çok fazla bozulma olmadan sesin çok daha küçük boyutlarda sıkıştırılmasına olanak tanımaktadır. Örnek olarak G.723.1

MP-MLQ algoritması G.711 PCM algoritmasına göre sesi 10 kata kadar daha fazla sıkıştırabilmektedir.

Her kodek belli bir ses kalitesi sunar. İletilen sesin kalitesi dinleyen kişiye göre sübjektif olarak farklılık göstermektedir. ITU değişik ses sıkıştırma algoritmalarını karşılaştırmak ve (International Telecommunication Union) konuşma kalitesini ölçmek için bir yöntem geliştirmiştir. Bu yöntemle değişik algoritmalar kullanılarak iletilen ses konuşmaları 8-10 saniye arasında kaydedilmektedir. Dinleyiciler özel odalarda dinledikleri bu konuşmalara algıladıkları ses kalitesine göre 1 ile 5 arasında bir değer vermektedirler. Daha sonra bu değerlerin ortalamaları alınarak ses kalitesi değeri hesaplanmaktadır. MOS değeri hesaplanırken normal telefon konuşması (MOS değeri 4.1) referans olarak alınmaktadır.

Tablo 2.5. Ses Kodlama yöntemlerinin karşılaştırılması

Sıkıştırma Yöntemi	Bit Hızı (kbps)	MOS Değeri	Sıkıştırma Gecikmesi (ms)
G.711 PCM	64	4.1	0.75
G.726 ADPCM	32	3.85	1
G.728 LD-CELP	16	3.61	3-5
G.729 CS-ACELP	8	3.92	10
G.729a CS-ACELP	8	3.7	10
G.723.1 MP-MLQ	6.3	3.9	30
G.723.1 ACELP	5.3	3.65	30

Her ne kadar data altyapısı maliyetlerini düşürmek için ses paketlerinin düşük bit oranlarında sıkıştırılması uygun bir çözüm gibi gözükse de ses taşınması planlanan bir ağ tasarımında seçilecek kodek tipi iyi tasarlanmalıdır. Çoklu kodlama standartları sesin daha düşük oranlarda sıkıştırmakla beraber sinyal distorsiyonuna sebep olmaktadır. G.729 ses kodlama standardı ile ses üç kez kodlandığında MOS değeri 3.92'den 2.68'e düşmektedir. Diğer taraftan düşük bit oranlı kodlamalarda sıkıştırma gecikmesi artmaktadır. [1]

2.3. RTP, cRTP, RTCP

2.3.1. RTP

RTP gerçek zamanlı ses ve görüntü verilerinin uçtan uca taşınmasını sağlayan iletim protokolüdür. İlk olarak çok katılımcılı çoklu ortam konferanslarındaki ihtiyaçları karşılamak için ortaya atılmıştır. Veri paketlerinin gerçek zamanlı iletimini garanti eden bir protokol değildir. Gerçek zamanlı iletim RSVP gibi kaynak ayırımı yapan protokoller

tarafında gerçekleştirilir. RTP veri iletimini gözlemlemek için yardımcı bir protokol olan RTCP'den faydalanır. RTP ve RTCP UDP servisi kullanılarak iletilir. RTP gerçek zamanlı içerik taşınmasında fonksiyonellik sağlayan bir protokoldür. Veri akışının senkronizasyonunu kontrol eder. RTP paket kayıplarını telafi etmek üzere bir yapıya sahip değildir. Kayıp paketlerin tekrar iletilmesi için H.261 RTP başlığı kullanılabilir. Kayıp paketlerin telafisi için diğer bir yöntem de düşük bit oranı ile beraber aynı ses paketlerinin yedekleme amaçlı birden çok kez iletilmesidir. [10]

Tablo 2.6. VoIP protokol kümesi ve TCP/IP dayanak modeli

TCP/IP Dayanak Modeli VoIP Protokol Kümesi

Uygulama Katmanı (Application Layer)	Ses Uygulamaları Ses Kodlayıcıları G.711; G.723.1; G.726; G.727; G.728; G729A
İletim Katmanı (Transport Layer)	Gerçek Zaman Protokolü (RTP) Kullanıcı Datagram Protokolü (UDP)
İnternet Katmanı (Internet Layer)	İnternet Protokolü (IP)
Ağ Erişim Katmanı (Network Access Layer)	IEEE 802.3
Fiziksel Katman (Physical Layer)	IEEE 802.3

RTP başlığı verinin zamanlama ve senkronizasyonunu sağlamak için birtakım başlık alanları kullanır. Bu başlık alanları ve açıklamaları aşağıda belirtilmiştir:

Tablo 2.7. RTP Başlığı

Yük Tipi	Sıra Numarası	Zaman Etiketi Alanı	Senkronizasyon Kaynak Belirteci Alanı	Çeşitli Alanlar
-------------	------------------	------------------------	---	--------------------

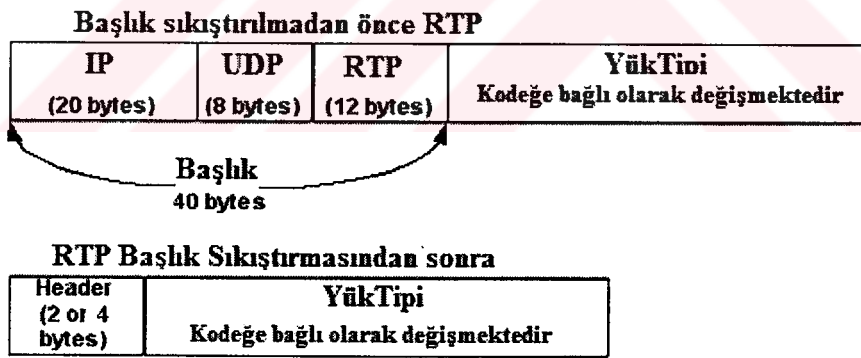
- **Yük Tipi** (Payload Type): 7 bitlik bir alandır. Hangi tip kodlama kullanılacağını belirtir. Örnek olarak PCM, MPEG2, görüntü gibi kodlama türlerini içerir.
- **Sıra Numarası** (Sequence Number): 16 bitlik bir alandır. Paket kayıplarını tespit etmek için kullanılır. Ayrıca paketin akıştaki yerini belirtir.
- **Zaman Etiketi Alanı** (Timestamp): 32 byte'lık bir alandır. Paketteki ilk ses/görüntü byte'nın örnekleme anını belirtir. Ağda oluşan gecikme süresi farkını (jitter) yok etmek için kullanılır.

- **Senkronizasyon Kaynak Belirteci (Synchronization Source identifier (SSRC)):**
32 bitlik bir alandır. Kaynak tarafından rasgele atanan bir değerdir. Akışın kaynağını belirten bir “id” içerir.

2.3.2. RTP Başlık Sıkıştırması (cRTP)

Bütün ses paketleri iki bileşenden oluşmaktadır: Ses paketleri ve IP/UDP/RTP başlıkları. Ses örnekleri DSP tarafından sıkıştırılmakta ve bu örnekler kullanılan kodek türüne göre boyut olarak değişse de IP/UDP/TCP başlıkları sabit olarak 40 byte uzunluğundadır. Bu başlık alanı varsayılan 20 byte uzunluğunda bir G.729 çağrısı ile karşılaştırıldığında belirgin bir yük getirmektedir. Noktadan noktaya iletişimlerde cRTP (compressed RTP) kullanılarak 40 byte’lık bu alan 2 yada 4 byte’a kadar sıkıştırılabilir. Bu sıkıştırma belirgin derecede bant genişliği kazancı sağlamaktadır. Varsayılan bir G.729 çağrısı RTP ile iletildiğinde 24 Kb harcarken cRTP kullanıldığında 12 Kb ile iletilebilmektedir.

cRTP VoIP çağrılarını noktadan noktaya sıkıştırdığı için IP bağlantısında iki uçta da cRTP konfigüre edilmelidir. cRTP konfigürasyonu ile paket boyutları belirgin bir şekilde azalmaktadır. Fakat cRTP kurulumu için ağ üzerindeki tüm yönlendiricilerin başlık sıkıştırma yeteneğine sahip olması ve sıkıştırılmış başlığı anlayabilmesi gerekir. [10]



Şekil 2.11. RTP başlık sıkıştırması (cRTP)

2.3.3. RTCP

RTCP veri iletimi kalitesi konusunda geribildirim sağlamak için kullanılır. Periyodik olarak kontrol paketlerinin iletilmesine dayanan bir protokoldür. Gönderici ve alıcı raporları tüm katılımcılara periyodik olarak iletilir. Bu raporlar paket sayısı, paket kayıp oranları, paket iletim gecikmeleri, ve gecikme süresi farkını içerir. RTCP ağına mevcut

durumu hakkında önemli bilgiler sağlar. Bazı uygulamalar bu bilgileri iletim oranları ve yığılmayı azaltmak için kullanmaktadır. [10]

2.4. ENUM

ENUM Internet'ten PSTN kaynaklarına ve Internet'ten Internet kaynaklarına E.164 numaraları ile ulaşmak için kullanılan bir sitemdir. ENUM ağ elemanlarının sadece PSTN'de kullanılan telefon numaralarını kullanarak Internet servislerine bağlanabilmeleri ve aynı zamanda sadece 12 tuşa sahip telefon numaralarının nasıl Internet servislerinden yararlanabileceği sorularına cevap bulmak için geliştirilmiş bir sistemdir. ENUM temel olarak PSTN ve IP ağlarının entegrasyonunu sağlamak üzere çıkmış bir modeldir. Aslında ENUM Kamu Anahtarlama Telefon Şebekeleri'nde (PSTN) kullanılan telefon numaralarını Internet fonksiyonelliği katacak şekilde eşleştirilmesidir.

ENUM'un birçok anlamı vardır. Tam teşekküllü bir telefon numarasının DNS temelli bir mimari kullanarak DNS adresine dönüştürülmesi olarak tanımlanabilir. Aynı zamanda IETF içerisinde, Internet'teki DNS kaynaklarını telefon numaralarına eşleştirilmesiyle ilgili oluşturulan bir çalışma grubunun ismidir. Son olarak E.164 adreslerinin tutulması için DNS adreslerinin kullanılması ve E.164 adresleri üzerinden servis verilmesini sağlayan sistemi öneren ve onaylanan bir protokol olan RFC 2916 'nın başlığı anlamını taşımaktadır.

ENUM'un telefon sistemini değiştirmek gibi bir amacı yoktur. ENUM telefon numaralarını tüketmez. Zaten varolan telefon numaralarını kullanır.

2.4.1. E.164 nedir?

E.164 "International Telecommunication Union" (ITU) tarafından yönetilen uluslararası telefon numaralama planıdır. Bu planda telefon numaralarının biçimi, yapısı ve telefon numaralarının yönetsel hiyerarşisi tanımlanmıştır. ITU özerk uluslara ülke kodları atamıştır. Bu numaraların yönetimi her ülkenin telekomünikasyon düzenleme acenteleri tarafından yönetilmektedir. Tam anlamıyla bir E.164 telefon numarası sırasıyla ülke kodu, bölge yada şehir kodu ve telefon numarasında oluşmaktadır. Örnek olarak bir E.164 numarasında +90 212 285 39 30, (90) Türkiye kodunu, (212) İstanbul Avrupa bölgesini, (285 39 30)'da telefon numarasının sahip olduğu kişiyi işaret etmektedir.

E.164 numaraları ulusal olarak takip edilebilir bir yapıya sahip olduğundan ENUM için uygun numaralardır. Daha da ötesi bu numaralar genellikle sabit numaralardır.

2.4.2. ENUM'un sağladığı faydalar

ENUM Internet-temelli bir sistem olup hedef kullanıcının sadece telefon numarası bilindiğinde yada sadece telefon tuşlarına sahip bir cihazla iletişim kurmak istendiğinde uzak kullanıcıya Internet üzerinden ulaşılabilmesi için kullanılan bir protokoldür. ENUM kullanıcıların Internet temelli servisleri kullanarak Internet-anlamalı telefonlardan ağgeçitleri (gateway) sayesinde geleneksel telefonları aramayı sağlamak amacıyla geliştirilmiştir. İstenilen kişiyi aramak için telefon numarası bilgisi yeterlidir.

ENUM kullanıcılara gelen çağrı karşılama istekleri için seçenekler sunar, bu da iletişime daha fazla kullanıcı kontrolü sağlar. Örnek olarak bir kullanıcı günün belli saatlerinde çağrıyı sesli maillere yönlendirebilir, yada çağrı yönlendirmesi için başka bir hedef gösterebilir.

ENUM kişisel ikamet eden telefon müşterileri, şirketlerde çalışan kullanıcılar, hükümet kuruluşları, askeri birimler ve diğer kullanıcılar tarafından kullanılabilir. Internet'e bağlı iki telefon arasında bir konuşma yapıldığında aynı PSTN'de olduğu gibi sadece bir telefon numarası çevrilerek haberleşme sağlanabilir. Ses paketleri uçtan uca IP ağları üzerinden veya belli bir noktaya kadar IP üzerinden ilerleyip daha önceden tanımlanmış bir ağgeçidi üzerinden PSTN'e geçiş yapılabilir. Aradaki bağlantı SIP yada H.323 uyumlu uçbirimleri bağlamak için kullanılabilir.

ENUM'un uygulamaları iki alanda toplanmıştır. Biri IP üzerinden ses iletimi (VoIP) diğeri ise Internet E-posta Trafığı İçin Ses Protokolü (VPIM). VPIM yapısı IP ağları üzerinden sesli posta sistemini kullanarak mesaj değiş tokuşu yapılmasını sağlamaktır. ENUM, VoIP ve VPIM sistemlerinin dışında Internet üzerinden faks ve anlık mesajlaşma (Instant Messaging) gibi uygulamaları da geliştirmektedir. [11]

2.4.3. ENUM sisteminin yapısı

ENUM sistemine herhangi bir telefon numarası girildiğinde bu adres aşağıdaki aşamalardan geçerek bir Internet adresine dönüştürülür.

- 1) Telefon numarası (ülke kodu ve şehir kodu da eklenerek) öncelikle bir E.164 numarasına dönüştürülür. Örnek olarak 212 285 39 30 çevrildiğinde bu adres +90-212-285-39-30 adresine çevrilir.
- 2) Rakamlar dışında bütün karakterler çıkartılır. Örnek: 902122853930
- 3) Rakamların sırası yer değiştirilir. Örnek: 039358221209
- 4) Her rakamın arasına birer nokta yerleştirilir. Örnek: 0.3.9.3.5.8.2.2.1.2.0.9

5) Numaranın sonuna “e.164.arpa” etki alanı eklenir. Örnek:
0.3.9.3.5.8.2.2.1.2.0.9.e164.arpa

ENUM daha sonra bu etki alanı için bir DNS sorgusu başlatır. Yetkilendirilmiş bir isim sunucusu bulunduktan sonra ENUM ilgili NAPTR Kaynak kaydını alır ve kullanıcının kayıt olduğu servise göre gerekli haberleşmenin kurulmasını sağlar. [12]

Bu uygulamada numaraların ters çevrilmesinin nedeni DNS sorgulamasında ilk önce en üst seviyeli etki alanı olan arpa’yı tarayacak, daha sonra ikinci seviyeli etki alanı e164 ve sırasıyla ülke kodu, şehir kodu ve telefon numarası sorgulayarak ilgili kaydı kolaylıkla bulacaktır.

ENUM da kullanılacak DNS etki alanı olarak E.164.arpa önerilmiştir. Aslında .arpa etki alanı Internet altyapısı amacıyla atanmıştır. IANA tarafından yönetilmektedir. ENUM telefon numaralarını ENUM destekli uygulamalar (telefon, SIP sunucular, sesli mesajlaşma servisleri) tarafından kullanılmak üzere DNS temelli kaynak dizinlerine çevirir.

ENUM telefon numarası ile ilişkilendirilmiş kaynakların keşfini sağlar. Ama gerekli kaynağın yeri belirlendikten sonra uygulama katmanında çağrının yönlendirilmesi, işaretleşme ve iletişim yöntemleri konusunda herhangi bir işlevi gerçekleştirmez. Sadece telefon şirketleri çağrıları yönlendirirken ENUM servislerini kullanabilirler.

2.4.4. E.164.arpa etki alanının yönetimi

E.164.arpa etki alanını organize ederken ITU tarafından tanımlanmış her ülke koduna karşılık DNS de yetki verme işlemi gerçekleştirilmelidir. Kök e.164.arpa etki alanında aşağıdaki örnekleri verilen NS listelenmesi yapılmalıdır.

- (1) ülke kodunu temsil eden US, Kanada ve diğer Karayıp Ülkeleri için .1.e164.arpa kaydına karşı düşen NS (name server) listelemesi
- (44) ülke kodunu temsil eden İngiltere için 4.4.e164.arpa kaydına karşı düşen NS (name server) listelemesi
- (90) ülke kodunu temsil eden İngiltere için 9.0.e164.arpa kaydına karşı düşen NS (name server) listelemesi

DNS kayıtlarında telefon numarası ile ilintili olarak hangi kaynakların, hangi servis ve uygulamaların kullanıldığı ile ilgili SRV ve NAPTR kayıtları tutulur. Bu servisler aboneler tarafından belirlenir.

ENUM sisteminin entegrasyonu birtakım arařtırmaları da beraberinde getirmektedir. Yanlıř çağrı yapan bir kullanıcı e164.arpa etki alanında ekstra sorgulara sebep olacak ve bir miktar yük getirecek. ENUM servislerini anons ederken yanlıř, eksik çağrıların kök yapısı tarafından bastırılması gerekmektedir. Telefon uygulamaları için performans ve yük analizi kritik olmakta, cevap süreleri, istek yükü gibi konular dikkatlice ele alınmalıdır.

Eđer DNS tarafından çözülemeyen bir numara ile karřılařılırsa istek gönderen cihaz yada yazılıma aynı web sunucusunda olduđu gibi 404-Bulunamadı mesajı gönderilir. Herhangi bir SIP telefonu böyle bir hata ile karřılařtıđında çağrıyı ađgeçidine (gateway) üzerinden PSTN řebekesine yönlendirmekte böylece geleneksel yöntemler ile çağrı kurulması sağlanmaktadır. Benzer řekilde bir SIP telefonunda 155 gibi e.164 adresleri dıřında bir adres sorgulandıđında SIP bađlantısı kurulamayacađında çağrı PSTN'e yönlendirilir.

ENUM protokolden bađımsız çalıřır. Herhangi bir numaranın hangi uygulamaya cevap vereceđini bilmez sadece o numarayla ilgili kaynak bilgisini verir. Bu yüzden H.323 yada SIP ile uyumlu çalıřabilir. Örnek olarak SIP ile bir noktadan birçok noktaya çağrı yapılırken adres çözümlemesi için ENUM kullanılabilir.

ENUM servisi için kullanıcılar dolaylı yoldan bir ücret ödeyecektir. Çünkü ENUM DNS temelli bir servistir ve birilerinin etki alanı kayıtlarını yapması gerekmektedir. Servis sağlayıcılar yada operatörler tarafından bir servis bedeli alınacaktır. Her telefon ENUM tarafından çözülemeyecektir. Servis sağlayıcılar kullanıcılar adına bütün telefonlar için bu servisi açabileceđi gibi sadece servis talebinde bulunan kullanıcılar da ENUM servisi verilebilir.

ENUM hayatı kolaylařtıran bir servis olarak öngörölse de hala bir takım eksiklikleri vardır. E164.arpa etki alanının uygulamaya konmadan önce bir takım testlerden geçmesi gerekmektedir. Amerika, Japonya, Avusturya gibi ülkeler bu sistemi kendi ülkelerine nasıl entegre edebilecekleri ile ilgili yoğun çalıřmalar yapmaktadırlar. Sistemin Internet ortamına entegre edilmesi için yapılması gerekenler:

- Küresel ENUM servisinin tanımlanması
- IANA ENUM'a katılmak istenen ulusal TN/NS'lere nasıl bir yol izlemek istedikleri ile ilgili danıřmalı.
- TN/NS yöneticilerinin bu servisi nasıl uygulayacakları planlanmalıdır.
- ENUM kaynaklarının nasıl uygulanacađı ile ilgili bir kullanıcı politikası tanımlanmalıdır.

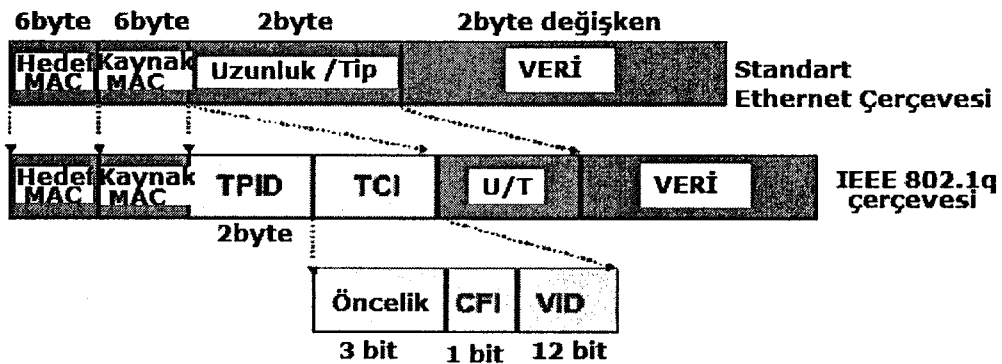
Ulusal Telefon numarası sunucuları için birçok organizasyon sırada beklemektedir. Hatta deneysel amaçlı bu işi ücretsiz yapacak şirketler de bulunmaktadır. [13]

2.5. QOS (Servis Kalitesi) için kullanılan yöntemler

İnsan kulağı ses sinyallerindeki küçük değişikliklere karşı bile çok hassastır. Bu durumda Servis Kalitesi önem kazanmaktadır. IP ağlarında ses paketlerinin yanında birçok veri paketi de ilerlemektedir. Ses paketleri ile beraber büyük bir veri paketi de iletilmek istendiğinde ses paketinin veri paketi iletilene dek beklemesi gerekebilir. Bu gecikmenin artmasına sebep olmaktadır. Servis kalitesinin sağlanması için garanti edilmiş bant genişliği (reserved bandwith) , belli limiti aşmayan gecikme değerleri (guranteed maximum delay), sınırlı gecikme süresi farkı (jitter), sıfır paket kaybı gibi birtakım istekler sağlanmalıdır. Bu amaçla çeşitli QOS mekanizmaları geliştirilmiştir. IP üzerinden ses taşımada servis kalitesinin sağlanması için kullanılan yöntemler aşağıda belirtilmiştir:

2.5.1. Veri Bağı Katmanı Servis Kalitesi (Data Link Layer QOS)

ATM teknolojisi veri bağı katmanında servis kalitesi ilgili parametreleri barındırmaktadır. Ethernet'te ise veri bağı katmanında servis kalitesi ile ilgili bir tanımlama yapılmamıştır. Ethernet en yaygın kullanılan LAN teknolojisidir. Ethernet'te servis kalitesinin sağlanması için IEEE 802.1q VLAN başlığının kullanılması gerekmektedir. VLAN başlığında her çerçeve için sekiz seviyeli önceliklendirme seçeneği sunulmaktadır. Bu önceliklendirme değerleri iletişim yapan uçlar arasında yol boyunca kontrol edilerek ses paketlerindeki gecikme minimize edilmektedir. Ama Ethernet'ten Frame Relay gibi bir WAN teknolojisine geçiş söz konusu olduğunda veri-bağı katmanında önceliklendirme yapılması mümkün olmamaktadır.



Şekil 2.12. Ethernet'te QoS özelliğinin sağlanması

2.5.2. Servis Tipi (Type of Service)

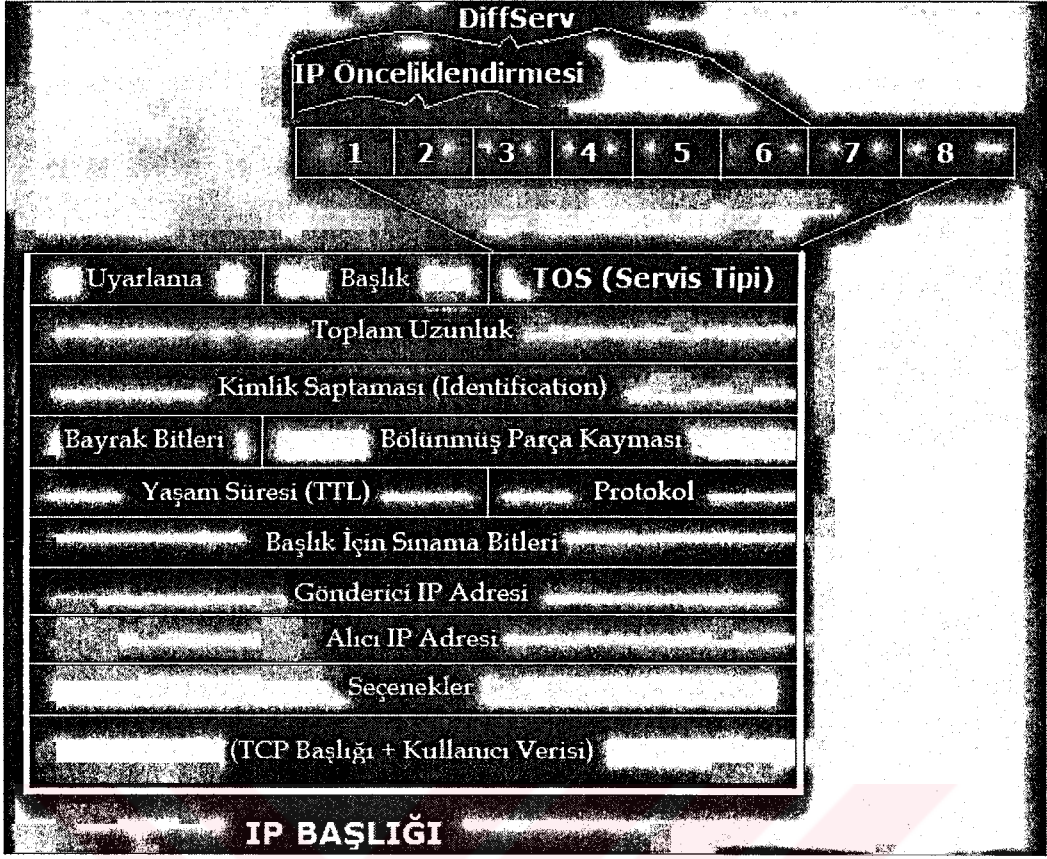
Her bir IPv4 başlığında 8 bitlik bir TOS alanı bulunur. Bu alanın 3 biti önceliklendirme için ayrılmıştır. Geriye kalan 4 bit ise servis tipini belirtmektedir. TOS kısmını kullanarak servis kalitesi sağlamak için iki özelliğe ihtiyaç duyulmaktadır. Öncelikli olarak yönlendiricilerin TOS kısmını fark edebilir özellikte olması gerekmektedir. Bu alandaki bit değerlerine bakarak farklı servis sınıfları oluşturup buna önceliklendirme yapabilmelidir. İkincil olarak TOS alanının doldurulması gereklidir. TOS değerleri uçbirim tarafından doldurulabileceği gibi trafik tipine göre bir yönlendirici tarafından da atanabilir.

2.5.3. RSVP

RSVP ses oturumu başlatıldığı zaman oturumun kurulması için gerekli kaynakların rezerve edilmesini sağlar. Eğer uygun kaynaklar sağlanamıyorsa (örnek: bant genişliği yetersiz kalıyorsa) bağlantı isteği reddedilir. Bu yaklaşım çok güçlü bir servis kalitesi sağlamaktadır ama ölçeklenebilir bir servis değildir. Bunun sebebi bu kaynakların iletişim kurmak isteyen uçlar arasındaki bütün yönlendiricilerde rezerve edilmesi gerekmektedir. Şirket içi uygulamalarda uygun bir yöntem olsa da yoğun IP iletişiminin kullanıldığı Internet ortamı için uygun bir çözüm değildir.

2.5.4. DiffServ: (Farklılaştırılmış Servisler)

Farklılaştırılmış Servisler ağ trafiğini sınıflandırarak kontrol etmek ve ses trafiği gibi bazı trafik türlerinin öncelikli olarak iletilmesi için kullanılır. DiffServ TOS baytında bulunan 6 bitlik alanı önceliklendirme için kullanır. DiffServ ile iletilen bir paket birbirinden farklı 64 olası iletim sınıfından biri ile gönderilebilir. DiffServ RSVP'den daha basit bir yapıya sahiptir ve uygulamaların ihtiyaçlarına göre paketler sınıflara ayrılabilir. Internet temelli uygulamalarda servis kalitesi sağlaması açısından kullanışlı bir yöntemdir.



Şekil 2.13. IP önceliklendirmesi ve DiffServ paket sınıflandırma yapıları

2.5.5. MPLS (Çoklu Protokol Etiket Anahtarlama)

MPLS ağında IP datagram başlığı çok daha kısa olan 13 baytlık bir etiketle değiştirilir ve bu alan servis sınıfını tanımlamak için kullanılır. Bu sayede aradaki yönlendiriciler trafiği doğru bir şekilde önceliklendirebilir. MPLS ile servis kalitesi sağlamak üzere ses trafiği gibi önceliklendirilmesi istenen trafik akışı farklı rotalar üzerinden yapılabilir. MPLS pahalı bir yatırım gerektiğinden Türkiye’de sadece birkaç ISP (Internet Servis Sağlayıcı) tarafından desteklenmektedir. [14]

2.6. VoIP’de Güvenlik

VoIP’de güvenlik ses paketlerinin güvenliği ve IP güvenliği adı altında iki kısımda incelenebilir. Ses paketlerinin güvenliği uygulamaya yönelik güvenlik problemleri IP güvenliği ise ağ yada iletim katmanı protokolünün güvenliğinin sağlanması olarak ele alınmaktadır.

Internet ortamı birçok tehdidin gelebileceği açık bir ortamdır. Bu saldırıların birçoğu takip edilemez. Internet ortamında tam anlamıyla bir güvenlik hiçbir zaman mümkün olamaz.

VoIP uygulamaları ağ güvenliği tehditlerine ve saldırılarına karşı açık kapılar barındırmaktadır. IP üzerinden ses iletiminin olduğu SIP temelli ağlarda iki tür tehditten söz edilebilir. Dış kaynaklı ve iç kaynaklı tehditler. Dış kaynaklı tehditler SIP temelli oturuma eşlik etmeyen yani dışarıdan bir kullanıcının oluşturduğu saldırılardır. Dış kaynaklı saldırılar ses ve sinyalleşme paketleri güvenli olmayan üçüncü bir ağ üzerinden (Internet ortamı) geçerken oluşabilir. İç kaynaklı tehditler ise genelde oturuma eşlik eden kullanıcılar üzerinden başlatılır. Bu tip saldırılar daha tehlikelidir.

SIP oturumunda herhangi bir kullanıcı iç kaynaklı bir saldırı başlattığında güven ilişkisi atlatılmış olur. Genelde bir kurum içerisindeki uçbirimler ateş duvarları tarafından dış tehditlere karşı korunsa da iç kaynaklı tehditlere karşı çok büyük bir koruma sağlanamamaktadır.

VoIP güvenlik tehditleri ve tavsiye edilen çözüm metotları aşağıda belirtilmiştir:

Tablo 2.8. VoIP güvenlik tehditleri ve tavsiye edilen çözüm metotları

Tehdit:	Çözüm:
Denial-of-Service (DoS) saldırıları: SIP proxy sunucusuna yada ağgeçidi cihazlarının ağ servislerini vermesini engellemek için paket bombardımanına tutulmasıdır.	Cihazlar bu tip saldırıları önleyecek şekilde konfigüre edilmelidir.
Gizlice Dinleme: Yetkisi olmayan kullanıcıların geçen RTP ortam akışının önünü kesmesi ve mesajları çözmesi.	Gönderilen verinin SRTP (güvenli RTP) gibi yöntemler ile şifrelenmesi.
Paket taklit edilmesi (packet spoofing): Veri gönderen yetkili bir kullanıcının yerine geçmek.	Çağrıya katılan kullanıcıların adres (IP adresi gibi) bilgilerini kaynak doğrulaması için birbirine göndermesi.
Ses paketlerinin tekrar gönderilmesi: Gerçek mesajın yeniden gönderilmesi bu sayede hedef kullanıcının mesajı yeniden işlemesi.	Gönderilen mesajın şifrelenmesi ve her mesaja uygulama katmanında bir sıra numarası atanması.
Mesaj İçeriği: Alınan mesaj ile gönderilen mesajın içeriğinin aynı olduğunun kontrol edilmesi.	HTTP Digest gibi yöntemlerle mesajın gerçekliğinin doğrulanması.

2.6.1. SIP Güvenlik Mekanizmaları

SIP’de güvenliğin sağlanması için uçtan uca başlık kısımlarının ve mesaj gövdesinin sıkıştırılması, kimlik doğrulama yöntemleri, iletim ve ağ katmanı güvenliğinin sağlanması gerekmektedir. Kullanılan yöntemler aşağıdaki gibidir:

Kimlik Doğrulama:

Bir çağrı başlatıldığında bir saldırgan kimliğini gizleyerek sanki SIP kullanıcı-arabirimi sunucusu gibi davranıp gönderilen çağrıya cevap verebilir. Kimlik doğrulama hedef kullanıcının gerçekten o kişi olduğu hakkında bilgi vermektedir.

Kimlik doğrulama kullanıcı arabirimi ile proxy arasında gerçekleşebilir. Proxy sunucusu talep mesajını işlemeyen önce kullanıcının kimlik doğrulaması yapmasını ister. Aynı şekilde SIP kullanıcısı SIP sunucusunun kimliğini doğrulamasını isteyebilir. SIP kimlik doğrulama için birtakım başlık alanları barındırır.

Yetki Verme (Authorization):

Kimlik Doğrulama işlemi başarılı olduktan sonra kullanıcının istenen servisi verme yetkisi olup olmadığı kontrol edilmelidir. Kimlik doğrulaması yapıldıktan sonra bile belli kullanıcıların bazı servislere ulaşma yetkisi bulunmayabilir.

IPSec:

IPSec özel sanal ağlarda kullanılan bir protokoldür. IPSec iletim katmanı güvenliği sağlayan popüler bir ağ güvenlik mekanizmasıdır. SIP sinyalleşme trafiğini şifreler, bu sayede mesaj güvenilirliği sağlanmış ve ses paketlerinin içeriği korunmuş olur. Güvenilir olmayan ağlara bağlanırken aradaki trafiğin şifrelendiği güvenli tüneller kurulur. [15]

2.7. Askeri Sistemlerde VoIP kullanmanın yararları

Günümüz iletişim sistemleri savaş alanında artan bilgi servisi ihtiyaçlarını karşılayamamaktadır. Elektronik mesajlaşma, ses,görüntü ve veri haberleşmesi gibi servisler savaş alanı iletişiminde birtakım değişiklikler yapılması ihtiyacını doğurmuştur. TCP/IP aslen Amerikan Savunma Bakanlığı tarafından her türlü savaş ortamında ve de her türlü iletişim ortamı üzerinde çalışabilecek esnek, ölçeklenebilir bir teknoloji geliştirme çalışmaları sonucunda ortaya çıkmıştır. İlk aşamada IP sadece veri iletimi için düşünülse de ses kodlama tekniklerinin gelişmesi ve bant genişliği kapasitelerinin artması ile ses iletişimi için uygun bir platform oluşturmuştur.

Sesin sayısal olarak işlenmesi analog işlenmesine göre bir takım üstünlükler taşır. Sayısal işleme, sesin iletimi ve saklanması önemli bir boyutta bellek alanı ve bant genişliği tasarrufu sağlar. IP üzerinden sayısal olarak iletilen ses güvenli bir şekilde iletebilir ve kriptolanabilir. Burada önemli noktalardan bir tanesi gönderilen ses verisinin uç noktaya ulaşana kadar güvenliğinin sağlanmasıdır. VPN güvenlik konusundaki ihtiyaçlara cevap

vermektedir.

Ses sinyallerinin yüksek frekans(HF) kanallarından, dar bantlı, yüksek güvenilirlikli ve gizli bir şekilde iletimini sağlayabilmek için sesin düşük hızlarda kodlanması gerekmektedir. WAN haberleşmesinde ses iletişimlerinin sayısal olarak gönderilmesi özellikle sınırlı kaynaklar sunan radyo telefonlar ve Uydu trunk hatları üzerinde bant genişliği ihtiyaçlarını azaltır. Tez kapsamında değişik ses kodlama algoritmaları incelenmiştir.

Ses haberleşmesi, günümüzde ve gelecekte sadece sivilde değil, stratejik ve taktik askeri uygulamalarda da haberleşmenin ana dalı olarak mevcudiyetini koruyacaktır. Sinyal işleme tümleşik devre teknolojisindeki hızlı gelişmeler ve telsiz, seyyar ve taşınabilir ses haberleşmesi için gittikçe artan talep sonucunda çok daha yaygın bir kullanım alanına sahip olacaktır.

Askeri sistemlerde VoIP çözümleri sadece savaş alanında kullanılan sistemler olarak düşünülmemelidir. Askeriye ülke genelinde birçok noktada konuşlanmış ve noktalar arasında kiralık hatlar ile birbirine bağlı İntraneti olan gelişmiş bir iletişim ağına sahiptir. Bu hatlar sadece kiralık hatlar ile birbirine bağlanmakta ve Internet erişimine kapalı olduğundan dış saldırılara karşı korunaklı bir yapı söz konusudur. Aslında birbirinden uzak birçok şubenin birbirine bağlanması için VoIP en uygun çözümü sağlamaktadır. Daha az sayıda ekipman gerektirmesi, minimum PSTN kiralık hatta ihtiyaç duyması ve sonuçta da maliyetlerin azaltılması VoIP kullanılmasında önemli bir faktördür. Ses, görüntü ve verinin birleştirilmesi ve tümleşik bir ağ oluşturması merkezi yönetim kolaylığı sağlamaktadır. Aynı zamanda PSTN santralleri ve IP gibi farklı teknolojilerin güvenliğinin ayrı ayrı sağlanması yerine tek bir ağın güvenliğinin sağlanması, bakımı ve yönetimi çok daha kolaydır.

2.7.1. Askeri sistemlerde VoIP tasarımında ele alınması gereken kriterler

Her ne kadar VoIP eski tip PSTN ağlarına karşı birçok üstün özelliğe sahip olsa da özellikle askeri amaçlı iletişimde hesaba katılması gereken bazı önemli faktörler vardır. Bu faktörler aşağıda incelenmiştir.

Gecikme:

ITU-T standartları ses iletiminde tek yönlü gecikme için 150ms sınırı koymaktadır. Bunun üzerindeki gecikmeler ses iletişimde kesintiler oluşturmaktadır. Diğer taraftan askeri sistemlerde önemli bir yere sahip uydu iletimi 250ms'ler civarında gecikmelere neden

olmaktadır. Bu da kaliteli bir ses iletişimi için belirlenen değerin üstünde bir gecikmedir. Askeri sistemlerde gecikme kritik haberleşme ihtiyaçlarında problemler teşkil etmektedir. Bunun için hızlı anahtarlama ve yönlendirme yapabilen, gecikmeyi minimize eden cihazlar kullanılmalıdır.

Gecikme süresi farkı (jitter):

Paketlerin hedefe ulaşma zamanlarındaki varyasyonlar iletişimin bozulmasına sebep olabilir. Bu noktada dinamik tamponlar kullanılarak gecikme süresi farkının yarattığı etkiler minimize edilmelidir.

Bant genişliği Sınırları:

Askeri sistemlerde özellikle WAN'da bant genişliği çok sınırlıdır. Bunun için ses kalitesi yüksek ve minimum bant genişliği tüketen sıkıştırma algoritmaları kullanılmalıdır. Ayrıca paket başlıklarının sıkıştırılması gibi yöntemler ile bant genişliği daha efektif kullanılabilir.

Paket Kayıpları:

Askeri ağlar ticari ağlara nazaran bit hata oranı açısından daha hassastır. Bit hata oran 1000 bitte 1 bit olan sistemler kritik uygulamalarda iletişim kopukluklarına sebep olmaktadır. Kayıpları minimize etmek için gelişmiş servis kalitesi çözümleri sağlanmalıdır.

Yüksek Uygunluk ve Güvenilirlik:

Askeri sistemlerde PSTN/PABX şebekelerindeki gibi uygunluk ve güvenilirlik sağlanmalıdır. Sistemlerin ayakta durma sürelerinin yüksek olması ve paketlerin güvenli bir şekilde karlı tarafa ulaşması beklenmektedir. [16]

2.8. VoIP Avantajları ve Kullanım Alanları

PSTN sistemlerine göre VoIP kullanmanın sayısız avantajı vardır. Öncelikle PSTN yeni özelliklere adapte olma konusunda yeterince çevik değildir. Sadece santral üreticisi mevcut cihaz için yeni özellikler ekleyebilir. VoIP de ise diğer üreticiler de yeni uygulamalar geliştirebilirler ve mevcut sistemlere bunu entegre edebilirler.

VoIP'de ses, görüntü ve veri tek bir altyapıda altında birleştirilmektedir. Bu sayede iki farklı kablolamaya, iki farklı ekipmana (PABX, Anahtar, yönlendirici) ihtiyaç duyulmamaktadır. Ses, görüntü ve verinin tümleşik olarak iletimi için mevcut LAN/WAN altyapısı yeterli olmaktadır. Bu sayede tek bir teknik servis departmanı ile iletişim

sağlanmaktadır. Diğer taraftan VoIP kurulumunun getireceği birçok maliyet kazanımları bulunmaktadır. VoIP kullanıcıları çağrı başına fatura ödemek yerine sadece aradaki hat ve kullanılan bantgenişliği için ücret ödemektedirler. [16]

Şirketler uluslar arası ve şehirler arası görüşme maliyetlerini azaltmak için VoIP çözümlerine gitmektedir. Özellikle uluslararası görüşmelerde ses maliyetleri ciddi miktarlarda azalmaktadır. Bu yüzden uluslararası görüşmelerde VoIP en çok tercih edilen haberleşme yöntemlerinden biridir. 2010 yılında uluslararası bütün ses iletişimin VoIP üzerinden sağlanacağı düşünülmektedir.



3. SONUÇ VE TARTIŞMALAR

Analog telefon şebekeleri 100 yılı aşkın bir süredir varlığını sürdürmektedir. Dijital teknolojinin gelişmesiyle beraber telefon şebekelerinin değişmesi kaçınılmaz hale gelmiştir. Başlangıçta sadece veri taşıma amaçlı tasarlanmış olan TCP/IP protokolünün ses taşıma amaçlı kullanılmasıyla beraber de VoIP doğmuştur. Günümüzde bant genişliklerinin yükselmesi ve ses sıkıştırma algortimalarının gelişmesi VoIP için uygun bir zemin yaratmıştır.

IP'de ses oturumun başlatılması için birçok protokol geliştirilmiştir. İlk çoklu ortam iletişimi için geliştirilmiş protokol H.323'dür. H.323'ün açık bir standart olması, ses, veri ve görüntünün tümleşik olarak iletilmesi yaygın olarak kullanılmasını sağlamıştır. H.323 çok sayıda servise hizmet amaçlı geliştirilmiş bir protokol olduğundan dolayı hantal bir yapıya sahiptir. Basit bir çağrı kurulmunda bile çok sayıda mesajın gönderilmesi gerekmektedir. Üzerinde çok sayıda uygulama geliştirilmiş olan H.323'ün karmaşık yapısı, fazla hafıza kullanımına ve cpu yükünün artmasına neden olmaktadır.

Diğer bir oturumu başlatma protokolü olan SIP (Session Initiation Protocol), 1999 yılında IETF tarafından geliştirilmiştir. Basit yapısı, daha az kod gerektirmesi uçbirimlerde düşük hafıza ve cpu kaynağı tüketmesine neden olur. Az sayıda bileşenden oluşması, diğer protokoller ile uyumlu bir şekilde çalışabilmesi gelişmeye uygun bir platform sağlamaktadır. H.323'e nazaran oturum kurlumu için az sayıda mesajlaşmaya ihtiyaç duyar. SIP üstün özellikleri sayesinde geleceğin VoIP protokolü olma yolunda ilerlemektedir.

VoIP'nin önündeki engellerden birisi uluslararası bir adresleme mekanizmasının oluşturulmamış olmasıdır. PSTN şebekesi ile VoIP entegrasyonu sağlanmalıdır. PSTN'de kullanılan e.164 standardındaki telefon numaralarının VoIP'te kullanılması için ENUM protokolü önerilmiştir. ENUM ile çevrilen bir PSTN numarası düşük maliyetli IP altyapısı üzerinden hedef kullanıcıya ulaşabilecektir. Bu standardın gelişmesiyle beraber bütün PSTN altyapısı IP-bazlı bir networke geçiş yapılabilir. Ancak ENUM'un tam anlamıyla kullanılabilmesi için tüm ülkelerin bu sisteme nasıl entegre olacağıyla ilgili ortak bir çalışma içerisine girmesi gerekmektedir.

Askeri amaçlı sistemlerde VoIP kullanılması çok geniş alanlara yayılabilecek kısıtlı bant genişliklerine sahip RF ve uydu hatları üzerinden askeri birimlerin çok daha az maliyetli ve daha yüksek kapasitede iletişim yapabilmesine olanak tanımaktadır.

IP üzerinden ses iletimi endüstrisinin uzun dönemdeki amacı telefon konuşmalarının Internet üzerinden PSTN şebekeleri kadar kolay ve yüksek kalitede yapılmasını sağlamaktır.



KAYNAKLAR

- [1] **Güçlü, S.**, 2003. VoIP (Voice over IP), *Windows & .NET Magazine*, 2, 56-67.
- [2] **International Telecommunication Union**, ENUM Protocol
<http://www.itu.int/osg/spu/enum/#faq>
- [3] **Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler**, 2002. "SIP:Session Initiation Protocol", RFC 3261
- [4] **Radvision Ltd.**, 2001 SIP: Protocol Overview,
<http://www1.radvision.com/NR/rdonlyres/0F6C2E81-72B3-4C42-B33C-DDBC9115AC3D/234/SIPProtocolOverview.pdf>
- [5] **Radvision Ltd.**, 2002. Understanding SIP Servers.
[http://www.sipcenter.com/sip.nsf/html/WEBB5YMUHL/\\$FILE/RADVISION_Understanding_SIP_Servers.pdf](http://www.sipcenter.com/sip.nsf/html/WEBB5YMUHL/$FILE/RADVISION_Understanding_SIP_Servers.pdf)
- [6] **Schulzrinne, H.**, 2000 "The Session Initiation Protocol (SIP)" New York.
- [7] **Davidson, J. and Peters, J.**, 2000. Voice over IP Fundamentals, Indianapolis, USA
- [8] **Rosenberg, J. and H. Schulzrinne**, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.
- [9] **Wind River** White Paper SIP vs. H.323 "A Business Analysis"
- [10] **Keagy, S.**, 2000 Integrating Voice and Data Network. Cisco Press Indianapolis.
- [11] **International Telecommunication Union**, ENUM Protocol <http://www.itu.int/osg/spu/enum/#faq>
- [12] **Faltstrom, P.**, "E.164 number and DNS", RFC – 2916, 2000.
- [13] **ENUM Protocol**, <http://www.enum.org>
- [14] **Carden, P.**, 2000 Building Voice over IP
http://www.networkcomputing.com/netdesign/1109voip5.html?ls=NCJS_1107bt
- [15] **Cisco Systems**, White Paper: Security in SIP-Based Networks.
- [16] **Tadiran Co.**, White Paper: Meeting The Challenge of VoIP in Military Networks
<http://www.tadirancom.co.il/technologies/battlespace.asp> #Figure1
- [17] **Schlatter C.**, 2003 Basic Architecture of H.323

EKLER

EK-A: Tezin dökümanlarına ait dosyalar (CD'ye kaydedilmiştir)



ÖZGEÇMİŞ

OZAN BÜK

1978 yılında İstanbul'da doğdu. İlkokulu Kuva-i Milliye İlkokulu, Ortaokul ve Liseyi ise Bilgi Lisesi'nde tamamladı. 2001 yılında İstanbul Teknik Üniversitesi'nden, Elektronik ve Haberleşme Mühendisi ünvanı aldı. 2001'de Fen Bilimleri Enstitüsü, Savunma Teknolojileri Anabilim dalında Yüksek Lisans eğitime başlamıştır.2002'den beri İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığında araştırma görevlisi olarak çalışmaktadır.

