T.C.

FIRAT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AĞ ÜZERİNDEN SES İLETİMİ ESNASINDA HARİCEN OLUŞABİLECEK İSTEM DIŞI TRAFİĞİN DENETİMİ

Aytuğ BOYACI

Tez Yöneticisi:
Yrd. Doç. Dr. Fikret ATA

YÜKSEK LİSANS TEZİ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

ELAZIĞ, 2007

T.C.

FIRAT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

AĞ ÜZERİNDEN SES İLETİMİ ESNASINDA HARİCEN OLUŞABİLECEK İSTEM DIŞI TRAFİĞİN DENETİMİ

Aytuğ BOYACI

Yüksek Lisans Tezi

Elektrik-Elektronik Mühendisliği Anabilim Dalı

Bu tez, ... tarihinde aşağıda belirtilen jüri tarafından oybirliği /oyçokluğu ile başarılı / başarısız olarak değerlendirilmiştir.

Danışman:

Üye:

Üye:

Bu tezin kabulü, Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ...../...../..... tarih ve ..... sayılı kararıyla onaylanmıştır.

TEŞEKKÜR

Bu tez çalışmam boyunca, ilgi ve yardımlarını esirgemeyen, çalışmalarımın oluşturulmasını ve tamamlanmasını sağlayan danışmanım Sayın Yrd. Doç. Dr. Fikret ATA' ya ayrıca çalışmam boyunca beni destekleyen Sayın Yrd. Doç. Dr. Hasan H. BALIK'a, aileme ve tüm arkadaşlarıma sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

ACF: Admission Confirm (Giriş Onay Cevabı)

ACL: Access List (Erişim Kontrol Listesi)

ACK: Acknowledge (Onay Mesajı)

ARP: Adress Resolution Protocol (Adres Çözümleme Protokolü)

ARQ: Admission Request (Giriş Kabul İsteği)

ATM: Asynchronous Transfer Mode (Asenkron Transfer Modu)

CERT: Computer Emergency Response Team (Bilgisayar Acil Cevap Takımı)

CODEC: Coding Decoding (Kodlama – Çözme)

DHCP: Dynamic Host Configuration Protocol (Dinamik Kullanıcı Konfigürasyon Protokolü)

DNS: Domain Name Server (Alan Adı Sunucusu)

DoS: Denial Of Service (Servis Yoksaması)

DSP: Digital Signal Processing (Sayısal Sinyal İşleme)

GK: Gatekeeper (Şebeke Kapı Sorumlusu)

GSM: Global System For Mobile Communication (Global Mobil Haberleşme Sistemi)

GW: Gateway (Ağ Geçidi)

HTTP: Hyper Text Transfer Protocol (Hiper Metin Transferi Protokolü)

IETF: Internet Engineering Task Force (İnternet Mühendisliği Görev Birliği)

IGMP: Internet Group Management Protocol (İnternet Grup Yönetim Protokolü)

IP: Internet Protocol (İnternet Protokolü)

IPSec: Internet Protocol Security (İnternet Protokol Güvenliği)

ISDN: Integrated Services Digital Network (Tümleşik Hizmetler Sayısal Şebekesi)

ITU-T: Telecommunication Standardization Sector (Uluslararası Telekominikasyon Birliği)

LAN: Local Area Network (Yerek Alan Ağı)

LZ: Lempel Ziv Compression Algorithm (Lempel Zıv Sıkıştırma Algoritması)

MOS: Mean Opinion Score (Ortalama Yargı Değeri)

NAT: Network Address Translation (Ağ Adres Dönüştürmesi)

ORDB: Open Relay Database (Anahtarlamaya Açık E-posta Sunucusu)

OSI: Open System Interconnection (Açık Sistem Arabağlantısı)

PPP: Point To Point Protocol (Noktadan Noktaya Protokolü)

PSTN: Public Switched Telephony Network (Kamu Bağlaşmalı Telefon Şebekesi)

QoS: Quality Of Service (Servis Kalitesi)

RTP: Real Time Transport Protocol (Gerçek Zaman Taşıma Protokolü)

RSVP: Resource Reservation Protocol (Kaynak Ayırma Protokolü)

RTCP: Real Time Control Protocol (Gerçek Zaman Kontrol Protokolü)

SAP: Session Announcement Protocol (Oturum Duyuru Protokolü)

SDP: Session Description Protocol (Oturum Açıklama Protokolü)

SIP: Session Initiation Protocol (Oturum Başlatma Protokolü)

SMTP: Simple Mail Transfer Protocol (Basit E-posta İletim Protokolü)

SPIT: Spam over Internet Telephony (İnternet Telefonu Üzerinde Spam)

SSL: Secure Socket Layer (Soket Düzeyi Güvenlik)

TCP: Transmission Control Protocol (İletim Kontrol Protokolü)

TLS: Transport Layer Security (İletim Katman Güvenliği)

UA: User Agent (Kullanıcı Ajanı)

UAC: User Agent Client (İstemci Kullanıcı Ajanı)

UAS: User Agent Server (Sunucu Kullanıcı Ajanı)

UDP: User Datagram Protocol (Kullanıcı Datagram Protokolü)

URL: Uniform Resource Locator (Standart Kaynak Bulucu)

VoIP: Voice Over Internet Protocol (IP Üzerinden Sesin Aktarılması)

VPN: Virtual Private Network (Sanal Özel Ağ)

WAN: Wide Area Network (Geniş Alan Şebekesi)

WWW: World Wide Web (Dünyayı Saran Ağ)

ÖZET

Yüksek Lisans Tezi

AĞ ÜZERİNDE SES İLETİMİ ESNASINDA HARİCEN OLUŞABİLECEK İSTEM DIŞI TRAFİĞİN DENETİMİ

Aytuğ BOYACI

Fırat Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik-Elektronik Mühendisliği Anabilim Dalı

2007, Sayfa: 106

Telekomünikasyon alanındaki hızlı gelişim ile, geleneksel ses iletişimin yerini dinamik, etkileşimli, katma değeri olan servislere bırakmaktadır. GSM haberleşmesinin altyapısında bile radikal değişikliklerin olduğu görülmektedir. Gerek ISDN, PSTN gerekse GSM alt yapısında kullanılan sinyalleşme sistemi yerini IP altyapısına bırakacağı görülmektedir. IP altyapısını kullanmakta olan VoIP iletişimide bu gelişime paralel olarak hızlı bir şekilde gelişmektedir. Gelişim sürecinde olan VoIP iletişimi avantajlarının yanında birçok güvenlik sorununu da getirmektedir. Bunun yanı sıra VoIP iletişiminin IP altyapısını kullanmasının da getirdiği güvenlik sorunları olduğu görülmektedir. Bu güvenlik sorunları kullanıcıları ve ağ trafiğini tehdit etmektedir. Sunulan çalışmada VoIP iletişiminin güvenli bir şekilde yapılabilmesi ve ağ üzerinde oluşabilecek istem dışı trafiğin önlenmesi üzerine odaklanılmıştır.

Sunulan çalışmada internet üzerinden ses iletiminde minimum bant genişliği ile, kaliteli bir ses sinyalinin güvenli ve hızlı bir şekilde alıcıya aktarılması ile ilgili incelenen konuların uygulamaları yapılmıştır.

Anahtar Kelimler: İnternet Üzerinden Ses İletimi, Servis Kalitesi, IP Telefonu, İstenmeyen Ses-Postalarının Önlenmesi,

ABSTRACT

Master Thesis

CONTROLLING OF UNWANTED TRAFFIC EFFECTING VOICE TRANSPORTATION QUALITY OVER NETWORK

Aytuğ BOYACI

Firat University
Graduate School of Natural and Applied Sciences
Department of Electric-Electronic Engineering

2007, Page: 106

With increasing developments on telecommunications conventional communications system left their places to dynamic, interactive and valued services. It is visible even on GSM system. It is evident that ISDN, PSNS and GSM system will be on IP based system. Voip communication is rapidly developing with increasing problems. One of the main problems is security. The security problem threatened users as well as Networks. This study focus on controlling of unwanted traffic effecting voice transportation quality over network

As a result, new approach which offers more security as wells as quality while consuming less bandwidth.

Keywords: Voice over IP, Spam over Internet Telephony, IP Telephony Quality of Services

1 GİRİŞ

Teknolojinin gelişimi incelendiğinde, özellikle son yüzyıl içerisinde sanayi devrimini takip eden zaman diliminde, tarih boyunca görülmemiş baş döndürücü bir gelişmenin yaşandığı kabul edilen bir gerçektir. Bu gelişmenin bu denli hızlı olmasının sebepleri irdelendiğinde en göze çarpan unsurlardan birinin birbirinden kopuk insan toplulukları arasında mesafeleri ortadan kaldıran haberleşme teknolojilerinin olduğu görülmektedir.

Çağlar boyunca birbirinden kopuk yaşayan insan toplulukları haberleşme ortamlarının gelişmesiyle fiziksel olarak olmasa bile düşünsel olarak bir araya gelme olanağı bulmuşlar ve sonuçta ortaya çıkan etkileşim, başta düşünce, medeniyet ve değişik teknoloji alanlarında alışverişe imkan sağlamış, doğal haliyle on yıllar belki yüzyıllarca çözüm bulunamayacak sıkıntılar aşılmış, bilim ve teknolojide gelişmeler hızlanmıştır.

Elbette haberleşme ortamlarının sağladığı bu hızlı teknolojik gelişme, yine haberleşme alanındaki teknolojilerin çeşit ve güçlerini artırmaktadır. Şu an en hızlı teknolojik gelişmelerin yaşandığı alanlardan biri de haberleşme teknolojileridir. İnternet teknolojisinin gelişimi ile birlikte haberleşme alanında yeni yönelimler olmuştur. İnsanlar klasik haberleşme yöntemlerinin yanında iki kişinin iletişimi yerine çoklu iletişimlerin sağlanabildiği, gerçek zamanlı ve ayrık zamanlı iletişim sistemleri ile tanışmıştır.

İnternet coğrafik ve ulusal sınırlardan bağımsız olarak bireylerin ve kurumların dünya çapında bir noktadan başka bir noktaya bağlanabilmesine imkan sağlayan bir ağ ortamı olarak adlandırılmaktadır. 1969 yılında ARPANET olarak adlandırılan bir araştırma projesinin başlatılması ile internet teknolojisi tahmin edilemeyecek kadar hızlı bir şekilde ilerleme sağlamıştır. Öyle ki bu ilerleme 1997 yılına kadar her yıl kendini ikiye katlamıştır. Akademik, idari ve finans kuruluşları bu küresel ağ ortamından bir çok yarar sağlamıştır. Buna ek olarak IP protokolünün kullanımı ile içerik tabanlı sistemlerin çok hızlı bir şekilde yayılması mümkün olmuştur. İçerik tabanlı haberleşme sistemlerinin internet teknolojisinin gelişmesine paralel olarak bu kadar hızlı gelişmesi internet üzerindeki haberleşmenin güvenliği hakkında endişelere yol açmaya başlamıştır. Kişisel gizlilik konusundaki endişeler kişisel bilgilerin otomatik olarak veritabanlarına toplanması ile artmıştır. Buna ek olarak kötü niyetli kullanıcıların virüs, solucan (worm) gibi yazılımlarla ve paket izleme programları ile kişisel bilgilere ulaşmaya çalışması internet güvenliğini tehdit etmeye başlamıştır [1].

İnternet teknolojisinin hızlı yayılım göstermesi internet üzerindeki güvenlik önlemlerinin arttırılması gerekliliğini ortaya çıkartmıştır. CERT tarafından yapılan bir araştırmaya göre 1988 yılında ağ saldırılarının miktarı yüzler ile ifade edilir iken 1995 yılında

bu sayı 2500'e çıkmıştır. Günümüzde ise ağ üzerinde yapılan saldırıların sayısı tahmin bile edilememektedir [2]. Bu durum interet kullanımının ve kullanıcılarının artmasıyla kötü niyetli saldırıların artması arasında bir bağlantı olduğunu göstermektedir. Bu da internet teknolojisinin çok büyük faydalarının olmasına rağmen bir çok tehlikeleri de beraberinde getirdiğini kanıtlamaktadır.

İnternet ağı üzerinden yapılan haberleşme sürekli olarak çeşitlenmektedir. İnternetin ilk uygulamaları veri transferi, metin tabanlı içeriklerin yayımı, metin tabanlı e-posta haberleşmesi iken, günümüzde internet uygulamaları daha interaktif hale gelmiştir. İnternet üzerinden ses iletimi (VoIP) uygulaması buna en iyi örnek olarak gösterilebilir.

İnternet ağı üzerindeki güvenlik tehlikeleri yapılan uygulamaları da tehdit ettiği gibi uygulamaya yönelik ek tehlikeleri de ortaya çıkarmaktadır. İnternet üzerinden ses iletimi esnasında da internet ağ güvenliğinin yanı sıra VoIP üzerindeki güvenliğinde ayrıca irdelenmesi gerekmektedir.

1.1 Tez Konusunun Tanıtılması

İnternet ağı üzerindeki güvenlik tehlikelerinin ciddi boyutlara ulaşması ve her geçen gün yeni güvenlik tehlikelerinin ortaya çıkması internet haberleşmesinin önündeki en önemli tehdit olarak görülmektedir. İnternet ağ güvenliği üzerinde yapılan çalışmaların yanında internet ağı üzerindeki uygulamalara yönelik güvenlik çalışmalarının da yapılması gerekmektedir. İnternet ağı üzerinde uçtan uca güvenlik çözümleri oluşturulamadığı sürece tam anlamı ile güvenlikten söz etmek mümkün değildir.

Bu çalışmada internet üzerinden yapılan sesli görüşme veya sesli mesajlar esnasında oluşabilecek güvenlik tehlikeleri incelenmiş, güvenlik tehditlerine karşı oluşturulabilecek önlemler irdelenmiştir.

İnternet üzerinden yapılan sesli iletişim esnasında oluşabilecek güvenlik tehditleri kullanıcıya yönelik olabileceği gibi, internet ağı üzerinde aşırı trafik yaratarak sistemin zarar görmesine yönelikte olabilmektedir. Bu amaçla çalışmada kullanıcı güvenliği ve internet ağı üzerinden ses iletimi esnasında haricen oluşabilecek trafiğin de önlenmesine yönelik çalışmalar yapılarak sistem güvenliğinin bir bütün olarak alınması için gerekli olan önlemler araştırılmıştır.

1.2 Tezin Amacı ve Önemi

Son yıllarda internet bant genişliğinin yeterli seviyelere ulaşması ile birlikte internet üzerindeki uygulamaların metin tabanlı iletişim ortamdan sesli iletişim ortamına geçtiği görülmektedir. Bu geçiş ile birlikte klasik sesli iletişim yöntemlerine, internet üzerinden sesli iletişim (VoIP) uygulamasını iyi bir alternatif olarak ortaya çıkarmaktadır. VoIP iletişiminin, klasik yöntemlere göre bir çok avantajı olmasına rağmen, kişisel gizlilik, doğruluk ve bütünlük

gibi noktalarda dezavantajları da bulunmaktadır. Bu dezavantajları VoIP uygulama güvenliği sağlanabildiği takdirde ortadan kaldırmak mümkün olacaktır.

Bu tezin amacı, VoIP uygulamaları üzerindeki güvenlik tehlikelerini saptamak, güvenlik açıklarına karşı önlemler alarak internet ağı üzerindeki oluşan harici trafiğin önlenmesi, kişisel gizliliğin sağlanabilmesi, ses verisinin doğru ve bütün bir şekilde internet ağı üzerinden iletilmesini sağlamaktır. Çalışmada kullanıcı güvenliği ve internet ağı üzerinde trafiğe yönelik tespitler yapılarak, gerekli olan güvenlik modelleri oluşturulmuştur.

1.3 Tezin Yapısı

Tez 8 ana bölümden oluşmaktadır.

Birinci bölümde, tez konusunun tanıtımı, yapılarak tez çalışmasının konusu ve amacına yönelik bilgiler verilmiştir.

İkinci bölümde, internet üzerinden yapılan iletişim esnasında kullanılan protokoller ve yapılarına değinilmiştir. İnternet ağı iletişiminin anlaşılabilmesi için OSI referans modeli ve TCP/IP protokol kümesinin çalışması, katman yapıları incelenmiştir. Ayrıca internet üzerinden ses iletişimini sağlayan VoIP uygulamasının önünde önemli bir güvenlik tehlikesi olarak görülen istenmeyen sesli mesajların anlaşılabilmesi ve çözüm yöntemleri geliştirilebilmesi için metin tabanlı istenmeyen e-postaların yapısı, tespiti ve alınan önlemler incelenmiştir.

Üçüncü bölümde, internet protokolü üzerinden sesin aktarımının işleyişi, yapısı kullanılan protokoller anlatılmaktadır. Ses aktarımı sırasında oluşacak iç trafiğin, gecikmelerin ve VoIP servis kalitesinden de bahsedilen bu bölümde VoIP mimarisi üzerinde kullanılacak şebeke elemanları da ele alınmıştır.

Dördüncü bölümde, VoIP protokol yapıları incelenmektedir. Ses iletimi için oturumun başlatılması, görüşmenin kişisel gizlilik, doğruluk ve bütünlük unsurları dikkate alınarak gerçekleştirilebilmesi, iletişimin sonlandırılması için kullanılan protokoller bu bölümde anlatılmaktadır. VoIP uygulamalarında uçtan uca güvenliğin sağlanabilmesi için kullanılan protokollerin anlaşılması son derece önemlidir. Bu bağlamda tez konusu ile yakından ilgili olan bu bölümde protokollerin haberleşme yapıları incelenerek takip eden bölümlere temel oluşturması amaçlanmıştır.

Beşinci bölümde, VoIP uygulamasının karşı karşıya kaldığı güvenlik tehlikeleri anlatılmaktadır. İnternet ağı üzerindeki genel güvenlik tehlikelerinin yanında VoIP uygulamalarına özgü güvenlik açıkları ve tehlikelerine değinilerek çözümlerin bulunmasına kaynak teşkil edecek saptamalar yapılmıştır.

Altıncı bölümde, internet üzerinden ses iletiminde oluşabilecek güvenlik tehlikelerine, istenmeyen ağ trafiğinin önlenmesine yönelik çözümler sunulmaktadır. VoIP uygulama

güvenliğinin ve istenmeyen trafiğin önlenmesinin iletişimin başından sonuna kadar yapılması gereken çözümler bütünü olduğunun vurgulandığı bu bölümdeki tespitler bir sonraki bölümde uygulamaya konulmuştur.

Yedinci bölümde, VoIP iletişiminin kurulmasına yönelik çalışmalar yapılmıştır. Bu çalışmalarda veri güvenliği, bütünlüğü, kimlik tespiti, kişiye yönelik yetkilendirmeler, servis kalitesi gibi unsurlar göz önüne alınarak mümkün olabilecek en verimli iletişim ortamlarının sağlanması amaçlanmaktadır.

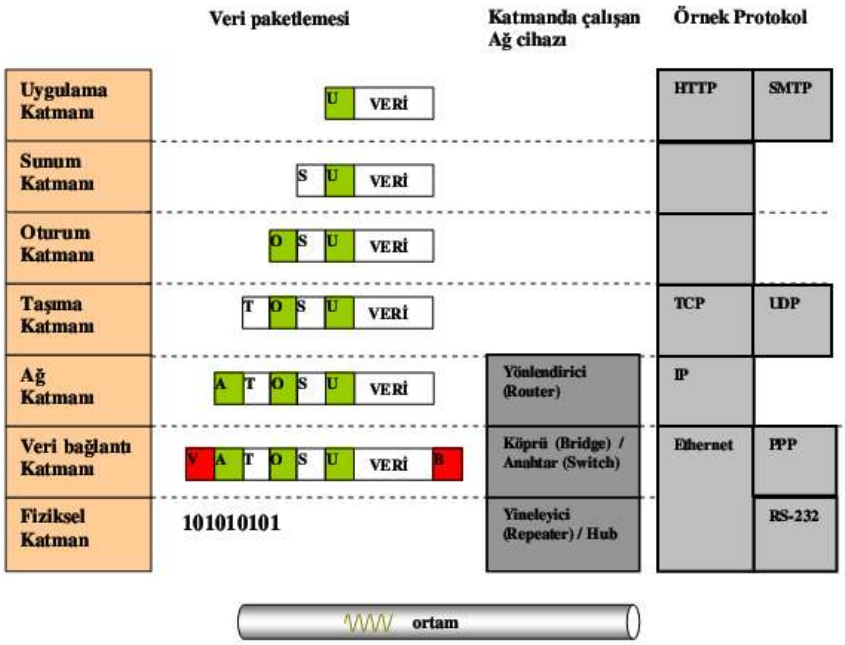
Sekizinci bölümde, çalışmanın sonuçları irdelenmektedir. Ayrıca bu konu ile ilgili olarak gelecekte yapılabilecek çalışmalar hakkında bilgiler verilmektedir.

2 GENEL BİLGİLER

Bu bölümde ağ üzerinden ses iletimi esnasında haricen oluşabilecek dış trafiğin önlenmesi konusundaki çalışmamın kolay anlaşılabilmesi için gerekli olan temel bilgiler verilecektir. Konuya temel teşkil etmesi açısından OSI referans modeli, TCP/IP protokol kümesi, mevcut haberleşme sistemlerindeki şebeke teknolojileri ve VoIP spamların önlenmesine temel teşkil edebilecek olan e-posta spamları hakkında bilgiler verilecektir.

2.1 OSI Referans Modeli

1984 yılında ISO (International Standards Organization) tarafından geliştirilen OSI referans modeli haberleşme ortamının fiziksel olarak oluşturulması, veri aktarımı için gerekli kodlamaların yapılması, paketlerin oluşturularak alıcı noktaya yönlendirilmesinin gerçekleştirilmesi, veri aktarımı sırasında kontrollerin yapılarak verinin sağlıklı bir şekilde alıcıya gönderilmesi için gerekli ortamın sağlanması, hataların farkedilerek düzeltilmesi, paketlerin birleştirilerek uygulama protokolü ile alıcıya sunulmasını amaçlar. Bu işlemlerin düzenli olarak gerçekleştirmesi için OSI referans modeli Şekil 2.1'de gösterildiği gibi 7 katmandan oluşmaktadır.



U: Uygulama Başlığı T: Taşıma Başlığı

S: Sunum Başlığı A: Aktarım Başlığı

O: Oturum Başlığı V: Veri Başlığı

Şekil 2.1 OSI referans modeli katmansal gösterimi

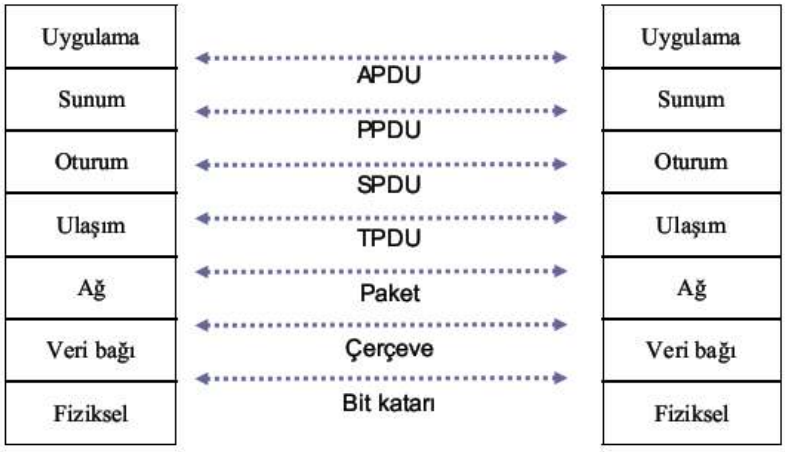
Haberleşmenin sağlıklı bir şekilde tamamlanması için her katmanın ayrı bir görevi vardır. Bu katmanlar sırasıyla uygulama katmanı, sunum katmanı, oturum katmanı, taşıma katmanı, ağ katmanı, veri bağlantı katmanı ve fiziksel katman olarak isimlendirilirler.

Bir uygulama, ağ üzerinden başka bilgisayarda çalışan uygulamaya veri göndermek istediğinde; göndermek istediği veriyi, uygulamaya en yakın katman olan uygulama katmanına iletir. Uygulama katmanı, alıcı uçtaki uygulama katmanına göndermek istediği bilgileri üstbilgi olarak veri paketine ekler, ve bir alt katmana geçirir. Veri, bu şekilde her katmanda bir üstbilgi eklenerek 2. katmana kadar ulaşır. 2. Katman olan veri bağlantı katmanına gelindiğinde, hem üst bilgi hem de kuyruk bilgi (trailer) eklenir. Oluşan bu en son pakete çerçeve denilir. En alt katman olan fiziksel katman hiçbir şey eklemeden çerçeveyi bit dizisi olarak ortam üzerinde üretir.

Veri, alıcı uç fiziksel katmanına ulaşınca OSI mimarisinde yukarı doğru ilerlemeye başlar. Veri bağlantı katmanı üst bilgi ve kuyruk bilgiyi kullandıktan sonra çıkarır ve kalan veriyi bir üst katmana geçirir. Bu şekilde her katman kendisiyle ilgili üst bilgiyi çıkararak kalan veriyi bir üst katmana geçirir. Bu şekilde, uygulama katmanı da kendisiyle ilgili bilgiyi çıkardıktan sonra, veri ilk halinde alıcı uçtaki uygulamaya ulaşmış olur.

2.1.1 OSI Katmanları

Yukarıda belirtildiği gibi OSI referans modeli 7 katmandan oluşmuştur. Alt katmanlara bit katarı, çerçeve, paket gibi isimler verilirken, üst katmanlarda ulaşım katmanı protokolü, veri birimi gibi katmana özel isimlendirme yapılmaktadır. Şekil 2.2'de OSI referans modelinde katmanlara göre taşınan verinin isimlendirilmesi gösterilmiştir.



Şekil 2.2 Katmanlara göre taşınan verinin isimlendirilmesi

Aşağıda OSI referans modelinin katmanları ve işlevleri anlatılmaktadır.

- **Uygulama Katmanı:** Kullanıcıların çalıştırdıkları uygulamalar ile uygulama programlarının ağa erişimi için ihtiyaç duyduğu bir çok protokol bu katmanda bulunmaktadır. Kullanıcıların etkileşimde bulunduğu uygulama programları bu katmanla iletişim kurmaktadır. HTTP, Telnet, FTP uygulama katmanı protokollerinden bir kaçıdır.
- **Sunum Katmanı:** Bu katmanda paketler bilgi haline dönüştürülmektedir. Bilgisayarlar arasında iletilen verinin değişimini standartlara uygun olarak yerine getirmek bu katmanın görevidir. Ayrıca, iletilen verinin sıkıştırılması / açılması, şifrelenmesi / çözülmesi, güvenlik ve kullanıcı doğrulamasının yapılması da bu katmanın görevleri arasında sayılmaktadır.
- **Oturum Katmanı:** Bu katman ağ ortamındaki farklı bilgisayarlar arasında oturumun açılması, yönetilmesi, sonlandırılması gibi işlemlerin yönetildiği katmandır. Oturum açma işleminde tek yönlü veya çift yönlü veri akışının kontrolü, iletim sırasının kontrolü de bu katman tarafından gerçekleştirilmektedir. Oturum katmanının diğer bir görevi bağlantının kopması gibi durumlarda, önceden belirlenmiş senkronizasyon noktaları sayesinde bağlantı yeniden kurulduğunda veri iletiminin kaldığı yerden devam etmesini sağlamaktır.
- **Taşıma (Ulaşım) Katmanı:** Bu katman verinin bir uçtan diğer uca doğru bir şekilde iletilmesini kontrol etmektedir. Başka bir deyişle katman gelen verinin doğruluğunu kontrol etmektedir. Verinin iletimi esnasında oluşabilecek hataları tespit ederek bu hataları düzeltmeye çalışmak taşıma katmanının görevidir. Veri paketlerinin doğru şekilde alıcıya teslim edilmediği tespit edilirse tampon bellekte (buffer) bulunan veri paketleri alıcıya tekrar gönderilir. Aynı zamanda taşıma katmanı, oturum katmanı tarafından ihtiyaç duyulan her taşıma bağlantısı için bir sanal ağ bağlantısı oluşturur. Eğer taşıma bağlantısı yüksek bir kapasiteye ihtiyaç duyarsa ulaşım katmanı, birçok ağ bağlantısı oluşturup kapasiteyi arttırmak için veriyi bu bağlantılara paylaştırır. Ayrıca, farklı ağ bağlantılarının oluşturulması, maliyeti arttırdığı durumlarda ulaşım katmanı çeşitli taşıma bağlantılarını bir ağ bağlantısı üzerinde birleştirerek maliyeti azaltabilir.
- **Ağ Katmanı:** Bu katmanda taşınan veri "paket" adını alır. Verinin kaynaktan hedefe ulaşması için takip edeceği yolun bulunması bu katmanın görevidir. Veri aktarımı sırasında bazı düğümler (yönlendiriciler) üzerinde tıkanıklıklar olabilir. Bunların sezilmesi ve gerekli önlemlerin alınması da ağ katmanının görevidir. Bunlar servis kalitesini (Quality of Service, QoS) arttırıcı görevler olarak da adlandırılmaktadır.

Heterojen altağların bulunduğu bir ortamda, altağlardan geçiş sırasında adresleme, paket boyu farklılığı gibi problemler bu katmanda çözülmektedir [3].

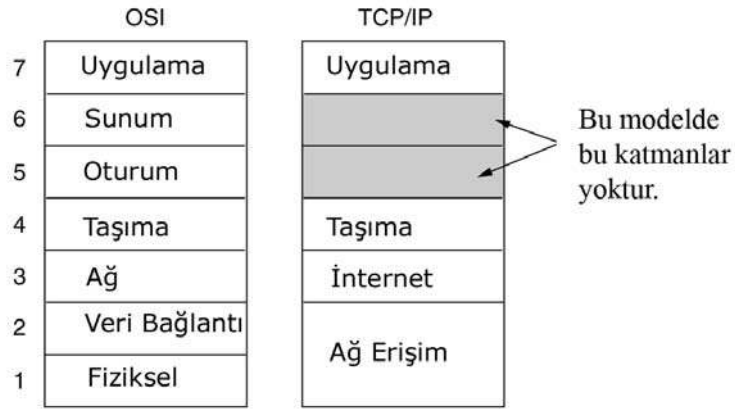
- **Veri Bağlantı Karmanı:** Ağ katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek "çerçeve (frame)" halinde fiziksel katmana iletme işinden sorumludur. Ayrıca iletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol etmek, çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlamak bu katmanın sorumluluğundadır.
- **Fiziksel Katman:** Verilerin fiziksel olarak iletilmesi ve alınmasından sorumlu olan katmandır. Bu katmanda tanımlanmış olan standartlar verinin içeriği ile ilgilenmezler. Daha çok işaretin şekli, fiziksel katmanda kullanılacak konnektör türü gibi elektriksel ve mekaniksel özellikler bu katmanda tanımlanmaktadır. Bit katarı seviyesinde ki bu katmanda veri kablolar üzerinden aktarılıyorsa elektriksel büyüklüklere, hava veya boşluk gibi bir ortam üzerinden aktarılıyorsa da yüksek frekanslı taşıyıcı dalgaya genlik, frekans veya faz değişimi şeklinde bindirilerek iletilmektedir.

2.2 TCP/IP Referans Modeli

Bir başka referans modeli TCP / IP referans modelidir. Kablolu veya kablosuz ağlarda kesintisiz bir iletişim kurmak amacı ile ARPANET tarafından geliştirilen TCP/IP modelinin diğer bir amacı ise iletim hatlarının kopması durumunda iletimin alternatif yolları kullanarak devam etmesini sağlamaktır. Şekil 2.3'te TCP/IP katmanları gösterilmektedir. Şekil 2.4'de ise TCP/IP referans modeli ile OSI referans modelinin bir karşılaştırılması sunulmaktadır.

Uygulama Katmanı
Taşıma Katmanı
İnternet Katmanı
Ağ Erişim Katmanı

Şekil 2.3 TCP/IP referans modeli



Şekil 2.4 OSI ve TCP/IP referans modellerinin karşılaştırılması

2.2.1 TCP/IP Katmanları

TCP/IP referans modelinde her katman değişik görevlere sahip olup altındaki ve üstündeki katmanlar ile gerekli bilgi alışverişini sağlamakla yükümlüdür. Aşağıda TCP/IP referans modelinin katmanları ve işlevleri anlatılmaktadır.

- **Uygulama Katmanı:** Bu katman TCP/IP referans modelinin en üst katmanıdır. Telnet, HTTP, FTP, SMTP gibi ağ üzerinde iletişim kurabilme yeteneğine sahip protokoller bu katmanı kullanmaktadır.
  - **Telnet:** Herhangi bir bilgisayara uzaktan bağlanmak için kullanılan bir protokoldür. Bu protokol ile DoS ekranından uzak bilgisayara bağlanılarak yönetim yapılabilmektedir.
  - **HTTP (Hyper Text Transfer Protocol):** İnternet üzerinde içerik tabanlı veri paylaşımı yapılabilmesi için geliştirilmiş bir protokoldür. Bu protokol sayesinde internet kullanıcıları verilerini paylaşabilmektedir.
  - **FTP (File Transfer Protocol): A**ğ ortamında dosya paylaşımı yapılabilmesi için geliştirilmiş bir protokoldür.
  - **SMTP (Simple Mail Transfer Protocol):** E-posta gönderim protokolüdür. E-postanın kim tarafından gönderildiğini ve kime gideceğini kontrol eden protokoldür.
- **Taşıma Katmanı:** TCP/IP referans modelinin 3. katmanıdır. Bu katman farklı bilgisayarlar üzerindeki uygulamaların birbirleri ile görüştürülmesinden sorumludur. Datagram adı verilen paketlerin içerisindeki kimlik bilgileri bu katmanda yerleştirilir ya da çözülür. Taşıma katmanı karşılıklı işlem bazında görüşme sağlar. TCP/IP protokol grubundan bağlantısız servis veren UDP ile bağlantı tabanlı servis veren TCP, bu katmanının iki protokolüdür.

- **TCP:** Verilerin alıcı bilgisayara ulaşmasını sağlayan protokoldür. Verinin bir uçtan diğer bir uca çeşitli hata algılama yöntemleri ile doğru bir şekilde iletilmesini sağlar.
- **UDP:** Gerçek zamanlı uygulamalarda tercih edilen UDP protokolü, TCP protokolünün yapmış olduğu hata denetimlerini yapmadığı için veri iletimini daha hızlı gerçekleştirmektedir.

- **İnternet Katmanı:** TCP/IP referans modelinin 2. katmanıdır. Bu katman aktarım katmanından gelen verilerin IP paketlerine dönüştürülerek yönlendirme işleminin yapılmasından sorumludur. IP (İnternet Protocol), ARP (Adress Resolution Protocol), IGMP (Internet Group Managment Protocol) ve ICMP (Internet Control Message Protocol) bu katmanda çalışan protokollerdir.
  - **IP (İnternet Protokolü):** Bir ağ ortamında bilgisayarların iletişim kurabilmesi için ağa dahil olan her bilgisayara bir adres verilmektedir. Bilgisayarların iletişimi için gerekli olan bu adresleme türüne IP adresi denilmektedir. TCP/IP protokolünde veriler IP paketleri halinde alıcı bilgisayara gönderilmektedir. Alıcı ve göndericinin bilgisayar arasında doğru bir bağlantı kurulabilmesi için IP adresleme sistemine ihtiyaç duyulmaktadır. Ayrıca gönderilecek olan veri IP paketlerine ayrılarak alıcıya gönderilir. Bu paketlere datagram da denilmektedir. IP protokolü gönderici bilgisayarda verinin paketlere ayrılması, alıcı tarafta ise bu paketlerin birleştirilerek verinin bir bütün hale getirilmesinden sorumludur.
  - **ARP (Adres Çözümleme Protokolü):** İnternet adreslerini fiziksel adrese dönüştürmek için kullanılır. Bir paketin bir bilgisayardan çıktıgında nereye gidecegini IP numarası değil gideceği bilgisayarın fiziksel adresi belirlemektedir. Işte bu adreste paketin gidecegi ip numarası kullanılarak elde edilmektedir. Bu işlemden sonra paket hedef ip adresine sahip bilgisayara gitmek için gerekli yönlendirmelerle yolculuğuna başlar. Bilgisayara takılı olan ethernet kartlarının bir ethernet adresi vardır. Bu adres IP adresinden farklıdır. Bir paket bilgisayardan çıktığı anda gidecegi adres diğer bir bilgisayarın ağ kartıdır ve bu ağ kartı ile IP numarası arasında bir bağ yoktur. Paket bu karta gidebilmesi için kartın fiziksel numarasını bilmek durumundadır. ARP adres çözümlemek istedigi zaman tüm ağa bir ARP istek mesaji gönderir ve bu IP adresini gören yada bu IP adresine giden yol üzerinde bulunan bilgisayar bu isteğe cevap verir ve kendi fiziksel adresini gönderir. ARP isteğinde bulunan bilgisayar bu adresi alarak verileri artık bu bilgisayara gönderir.
  - **IGMP (İnternet Grup Yönetim Protokolü):** IGMP iletilecek olan verinin birden çok bilgisayara gönderilmesi işleminden sorumlu olan protokoldür.

- **ICMP (Internet Control Message Protocol):** ICMP iki yada daha fazla bilgisayar arasındaki veri iletimi sırasında meydana gelebilecek hatalardan ve kontrol mesajlarından sorumludur. Bu nedenle ICMP ağ problemlerini tespit etmek için kullanılan en önemli protokoldür. ICMP ağ ortamında ki bir bilgisayarın canlı olup olmadığı, ağ geçitlerinin tıkanık olup olmadığı gibi noktaları kontrol etmektedir.

- **Ağ Erişim Katmanı:** TCP/IP referans modelinin en alt katmanıdır. Fiziksel iletişim ortamı üzerinden paketleri çerçeveleyeret (frame) alıcıya gönderen katmandır. OSI referans modelinde ki fiziksel katmanı ve veri bağlantı katmanlarının her ikisine birden karşılık gelmektedir. Verilerin elektriksel işaretler yolu ile alıcıya iletilmesini sağlamaktadır. ATM (Asenkron Transfer Modu), Ethernet gibi protokoller bu katmanı kullanmaktadır.
  - **ATM (Asenkron Transfer Modu):** Bir paket anahtarlama teknolojisi olan ATM, verileri byte büyüklüğünde hücrelere ayırma, bu hücreleri 53 hücrelik paketler haline getirme ve verinin paketler halinde iletilmesini sağlamaktadır. Yüksek veri işleme ve iletme hızlarına sahip olan ATM teknolojisi genel olarak donanım tabanlıdır. ATM teknolojisi genel olarak ISDN ağlarda kullanılan bir tekniktir.
  - **Ethernet:** Günümüzde yerel alan ağlarında veri iletimi için en çok kullanılan ağ teknolojisidir. Ethernet verilerin kabloya iletilmesini sağlayan bir teknolojidir. Bu teknolojide veriler 60 byte'tan oluşan ethetnet paketlerine ayrılır. Paket tam olarak, 6 byte uzunluğundaki bilginin yaratıldığı kaynak adresinden, 6 byte bilginin gönderileceği alıcı adresinden, 2 byte uzunluğundaki bilginin tipini belirten bilgiden ve 46 byte uzunluğundaki veri'den oluşmaktadır. Oluşturulan paketler ağ ortamının boş olup olmadığı kontrol edilerek uygun ortam oluştuğunda alıcı bilgisayara gönderilerek, tüm paketler alıcı bilgisayarda tekrar birleştirilir ve veri iletimi gerçekleşmiş olur.

2.3 İstenmeyen Elektronik Postalar

Tez konusunun anlaşılabilmesi için öncelikle ağ üzerindeki içerik tabanlı harici saldırıların (e-posta spamların) anlaşılması gerekmektedir.

2.3.1 Spam Tanımı

İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı bir şekilde gönderilmesi spam olarak adlandırılmaktadır [4]. Spam kullanıcıların e-posta haberleşmesini engelleyebilme potansiyeli olan ciddi bir problemdir. Son yıllarda yapılan çalışmalar e-posta spamların iletiminin toplam posta iletiminin %80-85'lere ulaştığını göstermektedir [5].

2.3.2 Spamın Karakteristiği

İstenmeyen elektronik postaların 4 önemli özelliği mevcuttur.

- Alıcılar tarafından talep edilmemiş olmaları
- Çok fazla alıcıya iletilmeleri
- Gelen mesajın kişisel özellikleri olmaması
- İstenmeyen e-postaların maliyetinin olmaması

Bir e-postanın spam olduğunu düşünmek için öncelikle o e-postanın istenmeyen bir ileti olması ve e-postanın çok fazla alıcıya gönderilmiş olması gerekmektedir. Bireysel içeriği olan ve gönderici bilgileri olan mesajların ilk etapta spam olarak düşünülmemesi gerekmektedir. Gelen e-postanın gönderici ile ilgili bilgileri barındırmaması yani kişisel özellikler taşımaması durumunda bu e-postanın istenmeyen bir mesaj olabliceğini gösterebilmektedir. Buna ek olarak kişisel bilgiler içermeyen bu tarz e-postalar bir bilgisayar tarafından otomatik olarak oluşturup gönderilmesi de mümkündür. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajin alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır. Ayrıca telefon, faks, posta gibi iletişim araçlarına göre maliyetsiz bir haberleşme sistemi olan e-posta haberleşmesi özellikle kalitesiz bir ürünü yüksek kazançlar ile satmak isteyenler için önemli bir iletişim yöntemidir. Bu yüzden gelen reklam içerikli e-postaların büyük bir bölümünün de spam olduğunu düşünmek mümkündür. Bu noktada ayırt edilmesi gereken doğru amaçlar için e-posta haberleşme sistemini kullanan kuruluşlardır. Bu karmaşık bağıntılar yüzünden istenmeyen e-postaların anlaşılması, tanımlanması ve önlenmesi önemli ve bir o kadar da zordur [5].

2.3.3 İçerik Tabanlı E-posta Spam Türleri

İnternet kullanıcıları üzerindeki etkileri incelendiğinde iki tip spam vardır. E-posta aracılığıyla gönderilen spam doğrudan gönderilen mesajlarla, bireysel kullanıcıları hedef almaktadır. E-posta spam listeleri genellikle gönderilerinin taranması, tartışma gruplarının üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur. E-posta yolu ile gönderilen spam türlerinden ticari içerikli olan UCE (Unsolicited Commercial E-mail- Talep Edilmemiş Ticari e-posta) adından da anlaşılacağı gibi istenmediği halde alıcıya gönderilen bir ürünü yada hizmeti tanıtıcı elektronik posta iletileridir. İçeriğinin mutlaka ticari olması gerekmeyen UBE (Unsolicited Bulk E-mail Talep Edilmemiş Kitlesel e-posta), aynı anda yüzbinlerce e-posta hesabına gönderilen e-posta iletileridir. Bu iletiler ticari içerikli olabileceği gibi politik bir görüşün propagandasını yapmak yada bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileri de olabilir. Spam hakkında önemli bir nokta, bir iletinin spam olarak nitelendirmek için kullanılacak ölçütün iletinin içeriği ile hiç alakalı olmamasıdır.

Herkesin üzerinde hemfikir olduğu, önemli bir toplumsal duyarlılığa sahip bir konu hakkında görüş bildirmek için kitlesel olarak gönderilen bir ileti de aslında spam olarak nitelendirilebilir [6].

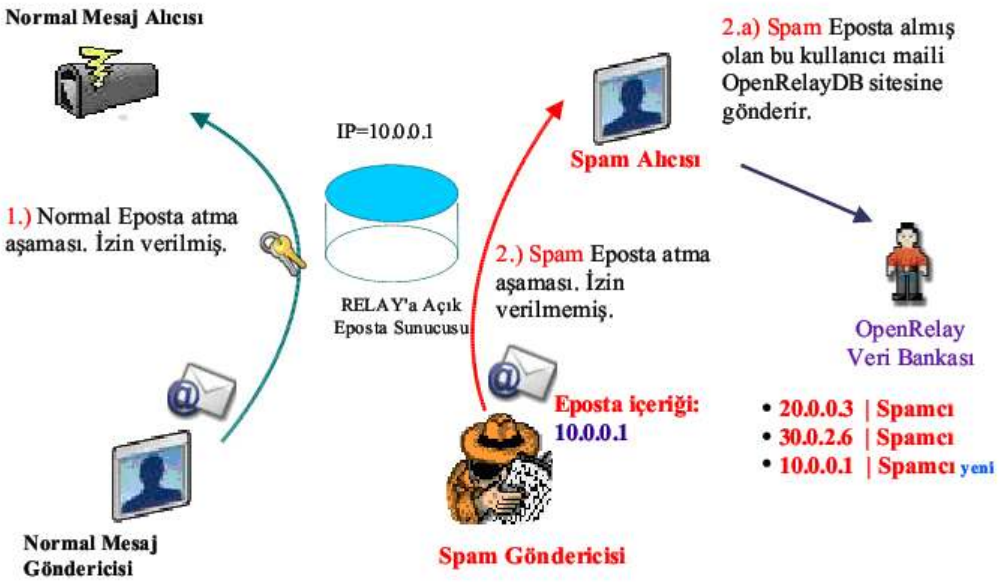
Sıkça rastlanılan e-posta spam tiplerinden biri ise MMF (Make Money Fast – Kolay Para Kazanın) iletileridir. Zincir iletiler yada piramit benzeri pazarlama yapıları ile ilgili gelen iletilerdir. Piramitin en üstündeki isme para gönderip listenin altına kendinizi eklediğinizde para kazanmaya başlayacağınıza ilişkin iletiler bu tip spam iletilerine örnek olarak verilebilir.

E-posta türündeki spamın rahatsız edici bir tipi ise, iletinin tartışma listelerine gönderilmesi durumudur. Bir çok tartışma listesinde, kimi işlemler sadece liste üyeleri tarafından gerçekleştirilebildiğinden, spam göndericileri, mümkün olduğu kadar çok listeye üye olmaya çalışarak, liste üyelerinin adreslerini temin ederler [6].

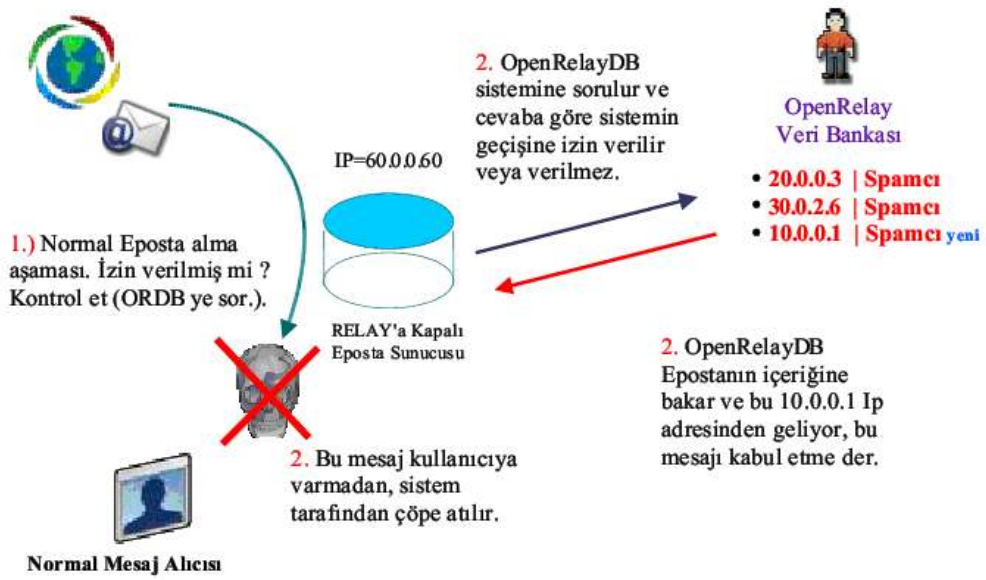
Diğer bir Spam tipi ise, iptaledilebilir (cancellable) Usenet mesajları aracılığı ile yapılan spamdır. 20 veya daha fazla haber öbeğine aynı anda gönderilen bir ileti spam kapsamında incelenir. Kullanıcılar açısından bu kadar çok sayıda haber öbeğine gönderilen bir iletinin genellikle öbeklerin çoğu, hatta hepsi açısından konu dışı kaldığı tesbit edilmiştir. Bu tür spam, sıklıkla haber öbeklerini okuyan ancak çok ender veya hiç gönderi yapmadıklarından email adresleri elde edilemeyen kullanıcı grubunu hedefler. Spamları haber öbeklerini reklemlar veya ilgisiz iletilerle doldurarak kullanıcı açısından faydasız ve kullanılması zor hale getirir [6].

2.3.4 İçerik Tabanlı Spam Gönderme Yöntemleri

Doğrudan veya dolaylı yollar ile toplanan e-posta adreslerine yakalanmadan spam mesajı göndermenin etkin olarak üç yöntemi bulunmaktadır. Birinci yöntem spam göndericisi SMTP sunucularını her hangi bir internet bağlantısı ile kullanarak gerçek olmayan IP adresi ve sunucu ismi ile e-postanın gönderilmesi şeklindedir. İkinci yöntem spam göndericisinin SMTP sunucularını bulup sistem yöneticilerinin haberi olmadan e-postaları göndermesi yöntemidir. Diğer bir yöntem ise virüs veya truva atı denilen yazılımlar aracılığı ile kullanıcıların kendi istekleri dışında ağ ortamındaki e-posta adreslerini tarayarak rasgele e-postalar atması ve internet trafiğini sıkıştırması durumudur. Şekil 2.5'te örnek bir spam gönderme yöntemi, şekil 2.6'da ise gönderilen bir spam içerikli e-postanın kullanıcı tarafından alınışı ile ilgili senaryolar gösterilmektedir.



Şekil 2.5 Spam göderme yöntemlerine örnek gösterim



Şekil 2.6 Kullanıcıları spam almasına örnek gösterim

2.3.5 E-Posta Spamları Önleme Yöntemleri

İstenmeyen e-postaların gönderilmesi için ilk adım e-postaların adreslerinin toplanması aşamasıdır. Bu e-posta adresi toplama işlemi genellikle yazılımlar aracılığı ile gerçekleşmektedir. Bu yazılımlar aracılığı ile web sayfalarından, haber gruplarından ve e-posta adresi listeleri taranarak adresler toplanmaktadır. Bu tarz yazılımlar genel olarak metin tabanlı çalışmaktadır. Bu yüzden e-posta adreslerini toplayan programlardan korunmanın en iyi

yöntemlerinden biri web sayfalarında bulunan e-posta adreslerinin resim tabanlı hale dönüştürülmesi işlemidir. Programlar haricinde e-posta toplama yöntemlerinden biride sözlüksel saldırı yöntemidir. Sözlükte bulunan anlamlı kelimeleri alan adı ile birleştirerek rasgele e-posta adresleri oluşturma ve bu adreslere e-posta gönderme de etkili bir yöntemdir.Bu yöntemde rasgele oluşturan e-posta adreslerine bir deneme postası gönderilir. Eğer ileti gönderme hatası alınmamış ise bu e-posta adresi geçerli bir e-posta adresidir. Geçerli olarak kabul edilen e-posta adresleri listeye eklenerek liste genişletilir.

Hazırlanan listede ki e-posta adresi yeterli bir sayıya ulaştığında bu listeler isteyenlere pazarlanmakta veya spam e-postalar bu listelere gönderilmektedir. Bu listeler özellikle ürünlerini pazarlamak isteyen firmalara cazip gelmektedir.

Spam e-postaları önlemenin birinci yolu e-posta listelerinin toplanmasının önüne geçilmesi olarak gösterilebilir. Ama bu spamları önlemek için yeterli bir çaba değildir. Bir çok yöntem ile spamlar önlenmeye çalışılsa bile spam üreticileri bu yöntemleri çeşitli yöntemler ile egale ederek spam yaymaya devam etmektedirler.

Spam e-postaların önlenmesi ile ilgili teknikler VoIP uygulamasında ki istenmeyen sesli mesajlar arasında benzerlikler açısından önem teşkil ettiği için bu algılama veya önleme tekniklerinin kısaca anlatılması gerekmektedir.

Kaynak Filtreleme Önlemleri:

Spam olarak kabul edilen e-postalardan korunmanın en klasik yöntemi kullanıcıların ve sistem yöneticilerinin kullandığı spam kara listeleridir. Bu listeye girmiş IP adresi veya sunucuların gönderdiği e-postalar istenmeyen e-posta yani spam olarak tanımlanmaktadır. Bu önleme sisteminde ki amaç kaynağın tespiti ve ona karşı önlem alınmasıdır. Kabul edilebilir bir yöntem olmasına rağmen spam üreticileri kara listelere girdiğinde yeni IP adresi veya sunucular ile kimliklerini değiştirerek tekrar spam e-postalar gönderme yolunu kolaylıkla bulabilmektedirler. Özellikle IPv6'ya geçildikten sonra IP sıkıntısı da olmayacağı için bu tür korunma yöntemi etkisini kaybedecektir. Kaynak filtrelemenin farklı yöntem ve teknikleri bulunmaktadır. Bunlar;

- **IP Bloklama:** İletişim ortamları teknolojinin gelişmesi ile birlikte yönlerini internet alt yapısına çevirmeye başlamaktadır. Klasik haberleşme sistemleri olan telefon, fax, posta ve televizyon gibi sistemler güncelliğini kaybetmektedir. İnternet teknolojisinin bu hızlı gelişimi ile birlikte ürünlerinin reklamını yapmak isteyen firmalar da maliyeti düşük olan bu teknolojiden faydalanma yoluna gitmektedirler. Reklam yapmanın en etkili yollarından biri ise e-posta yolu ile ilgili kitleye ulaşmaktadır. Bu e-postaların alıcı tarafından istenmeden alınması sebebi ile bu e-postaların önlenmesi gereği

duyulmaktadır. Uluslararası kabul görmüş spam üreticilerini tespit etme kuruluşları tarafından tespit edilen IP adresleri kara listelere alınmaktadır. Kara listeye alınan IP adreslerinden gönderilen e-postalar spam olarak kabul edilmektedir. Oluşturulan bu uluslararası listeler belli kuruluşlar tarafından sürekli güncellenmekte ve kara listeye alınan IP adresleri de sürekli incelenmektedir. Kara listede bulunan IP adresleri normal kullanıma geçtiği taktirde listeden çıkarılmaktadır. Böylece bu listelerin sürekli güncel kalması sağlanmaktadır. Ancak bu listeye giren spam üreticileri sürekli olarak internet servis sağlayıcılarını değiştirdikleri için IP adresinin bloklanması tam olarak çözüm sağlayamamaktadır.

- **ORDB:** Spam üreten kişi veya kuruluşlar IP adreslerinin karalisteye girmesi durumunda alternatif IP adresleri bulmaktadır. IP adreslerinin karalisteye girebilme ihtimaline karşın çoğu spam üreticisi e-posta sunucusu kiralamaktadır. IP adresi kara listeye girdiğinde ise başka bir e-posta sunucusu kiralayarak spam üretmeye devam etmektedir. Sunucu kiralamanın bir avantajıda kiraladığı sunucunun bant genişliğini kullanmaktır. Spam üreticileri için sunucu kiralamanın diğer bir avantajı ise genellikle bu tarz sunucuların güvenlik ayarları standart seviyede olduğu için e-posta listesindeki kullanıcılara spam yaymak daha kolay olmaktadır [7]. Bu tarz sunucularda ki veritabanlarına kaydedilen e-posta adreslerini kullanarak veya sunucunun güvenlik açıklarından yararlanarak sunucunun herkese e-posta atmasını sağlamak da spam üreticilerinin kullandığı bir yoldur. Bu güvenlik açıklarının önlenmesi için RBL (Gerçek zamanlı karaliste) adı verilen listeler uluslar arası belli kuruluşlarca oluşturulmaktadır. Kendi kaynaklarını kullanarak bu tarz güvensiz e-posta sunucularını tespit etmekte ve tespit edilen sunucuları gerçek zamanlı karalistelere almaktadırlar. Bu sunucular tarafından spam üretilmemiş olsa bile güvensiz bulunduklarından dolayı kara listelere alınmaktadırlar [8].
- **Bilinçli Güvenlik Ayarları:** İstenmeyen e-postaları önlemek için sunucu bilgisayar üzerinde bir çok güvenlik ayarı yapılmış olsabile bu ayarlar yeterli olamamaktadır. Web teknolojilerinden yararlanan spam üreticileri çoğunlukla web üzerindeki hazır formlara "Perl" dilinde yazdıkları yazılımlar ile müdahale ederek sunucu bilgisaya üzerinde bulunan veritabanı üzerindeki e-posta adreslerini ele geçirerek onlara spam e-posta gönderebilmektedirler [9]. Bu işlem gerçekleştirilirken yazılmış olan yazılım sayesinde spam üreticisinin kimlik bilgileri gizlenmekte olup sunucu bilgisayarın geçmişte yapılan işlemlerin tutulduğu log dosyalarından bile IP adresi gibi bilgilerde silinerek gizlilik sağlanmaktadır. Bu tarz e-posta saldırılarını önlemek için Vekil (proxy) sunucular kullmaktadır. Proxy sunucuların kullanım amacı spam üreticileri tarafından kullanılan

bu bağlantı yöntemini engellemektir. Ayrıca proxy sunucular üzerinde yapılan ayarlamalar ile port kontrolüde yapılarak daha güvenli bir iletişim ortamı sağlanabilmektedir [10].

- **İstemci güvenliğinin geliştirilmesi:** İstenmeyen e-postaların önlenebilmesi için sunucu bilgisayarların güvenliği kadar istemci bilgisayarların da güvenliği önemlidir. İstemci bilgisayarlar üzerinde bulunan adres listelerinin ele geçirilmesi veya istemci bilgisayarın ele geçirilerek başka bilgisayarlara saldırı yapması amacı ile spam üreticileri tarafından istemci bilgisayarlara kötü niyetli yazılımlar yüklenmeye çalışılır. Solucan (worm) yazılım ve truva atı adı verilen bu yazılımlar internet kullanıcısı olan bilgisayarlara yüklendiğinde o bilgisayar üzerinde ki e-posta servisleri kullanılabilmektedir. Bununla birlikte kullanıcının kendi e-posta listeleri de ele geçirilebilmektedir. Bu saldırıların önlenmesi amacı ile kullanıcıların mümkün olan en üst seviyede güvenlik önlemlerini alması gerekmektedir. Bilgisayarların güncel tutulması, antivirüs yazılımların kullanılması, güvenlik duvarlarının kurulması ve gereksiz servislerin kapatılması gibi tedbirler ve bilinçli kullanım ile bu tarz kötü yazılımların önüne geçmek mümkündür.

İçerik Tabanlı Önlemler:

İstenmeyen e-postaların engellenmesi için diğer bir yöntem kaynağın engellenmesi yerine gönderilen e-postanın içeriğinin kontrol edilmesi yöntemidir. Bu yöntemde gelen e-postanın içeriği kontrol edilerek gelen e-postanın gelenler listesine değil de yararsız e-postalar listesine alınması amaçlanmaktadır. Bu yöntem ile tespit edilen spamlar sunucudan istemciye ulaştığından dolayı internet bant genişliğinin kullanılmasının önüne geçilememektedir. İçerik tabanlı önleme yöntemlerinde içeriğin kontrol edilerek önleme ve içeriğin geldiği adresin kontrol edilerek önlem alınması şeklinde iki yöntem mevcuttur.

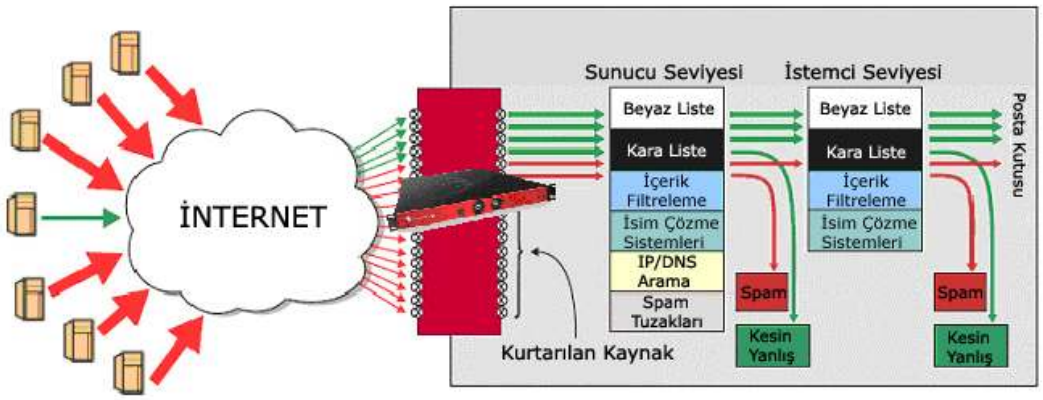
- **Metin ve HTML Filtreleme:** Bu yöntemde gelen mesajın içeriği incelenmektedir. Bu işlem sattı satır gelen içeriğin incelenmesi şeklinde olabileceği gibi önceden tanımlanmış olan spam kalıplarının metin içerisinde araştırlması şeklinde de olabilir. İncelenen mesajın içeriğinde spam sayılabilecek kelime gruplarının fazla olması o e-postanın spam olma oranını arttıracaktır [11]. Buna ek olarak gelen e-postalar spam içerikli olsa bile bu yöntem yeterli olamamaktadır. Çünkü gelen mesajın içeriği çoğunlukla düz metinler şeklinde değil de HTML tagları arasında yazılmış metinler halinde olduğundan dolayı gelen mesajın içeriği tam olarak tespit edilememektedir. Hatta gelen mesaj tamamen metin tabanlı olmak yerine resim tabanlı içeriğe sahipte olabilir. Böyle bir durumda içerik kontrolü yapılması doğru sonuç vermemektedir. Bu

nedenle içeriğin kontrol edilmesinin yanında gelen mesajın rasgele benzersiz bir imzası oluşturlur. Oluşturulan bu imza bir veritabanında saklanır. Veritabanında toplanan imzalar gelen diğer mesajların imzaları ile karşılaştırılır. Gelen mesajlar benzer imzaları barındırıyorsa bu mesajları diğer kullanıcıların alması engellenir. İçerik filtrelemenin diğer bir faydası ise spam üreticilerinin IP adreslerini ve kimlik bilgilerini sürekli değiştirerek istenmeyen e-postalarını göndermeye devam etmelerinin önüne geçmektir [12].

- **URL Kontrolü:** Metin tabanlı filtrelemenin resim veya html içerikli istenmeyen e-postaların tam olarak önüne geçememesi yüzünden geliştirilen istemci tarafında bir diğer güvenlik önlemi ise gelen e-postanın gönderici adresinin bir spam üretici adres olduğunun duyurulmasıdır. Spam üreten bir web sitesi tespit edildiğinde bu web sitesinin adresinin duyurulması, daha az spam önleme için kaynak ayrılması, filtreleme metodlarının engelleyemediği e-posta sunucularının tespit edilerek erişimlerinin engellenmesi gibi bir çok fayda sağlamaktadır [13].

Kimlik Tanıma ve Doğrulama ile İletim:

İstenmeyen mesajların önlenmesinde ki asıl sorun gelen iletinin gerçek kimliğinin tespit edilmesinin çok zor olmasıdır. Eğer gelen e-postanın tam olarak kim tarafından gönderildiği tespit edilebilirse bu tarz mesajların önüne geçmek mümkün olacaktır. Bu konu üzerinde çalışmalar devam etmesine rağmen henüz tam olarak doğru sonuçlar alınamamıştır. Bu yüzden kimlik tanıma işleminde normal e-postalar ile spam e-postaların karşılaştırılması yoluna gidilmiştir. Yapılan çalışmalar genellikle gelen e-postanın konu başlıklarının karşılaştırılması yönündedir. Alıcıya gelen e-postalar bir ticari faaliyet gösteren kuruluş tarafından gönderilen e-posta ise, içerik kontrolü yapılmadan sadece konu başlığının kontrol edilmesi ile e-postanın spam içerik taşıdığına karar verilebilir. Bu amaçla spam önleme filtreleri ticari faaliyet yürüten kuruluşlar tarafından reklam yapmak amacı ile gönderilen spam içerikli e-postaları büyük ölçüde tespit edebilmektedir [13]. İstenmeyen e-postaların önlenmesi ile ilgili örnek yapı Şekil 2.7'de gösterilmektedir.



Şekil 2.7 İstenmeyen e-postaların önlenmesi örnek gösterim [14]

Günümüzde internet bant genişliğinin büyük bir bölümünü istenmeyen e-postalar kullanmaktadır ve bu e-postaları tam olarak engellemek hala mümkün değildir. İstenmeyen e-postaların önlenmesi için araştırmalar yapılmakta ve bir çok yöntem geliştirilmeye devam etmektedir.

3 İNTERNET PROTOKOLÜ ÜZERİNDEN SESİN AKTARILMASI

3.1 VoIP'in Tanımı

VoIP, Voice over Internet Protokol (Internet üzerinden ses protokolü) açılımına karşılık gelmektedir. VoIP, ses paketlerini internet ağı üzerinden IP paketleri gibi taşınarak alıcıya iletilmesini sağlayan teknolojinin adıdır. Bir başka deyişle VoIP, telefon görüşmesi yapmak için PSTN şebekeleri kullanmak yerine internet ağını iletim ortamı olarak kullanan teknoloji olarak da adlandırılabilir.

Etkileşimli iletişim ortamı olarak günümüzde hala çok yaygın bir şekilde kullanılan PSTN (genel anahtarlamalı telefon ağı) şebekeler, internet teknolojisinin gelişmesi ve internet ağı üzerindeki kullanılabilen bant genişliklerinin yeterli miktarlara ulaşması ile birlikte yerini VoIP ağlara bırakması öngörülmektedir.

PSTN şebekeler, bir telefon görüşmesi için iki uç arasında devre bağlantısı sağlaması temeline göre çalışmaktadır. Bu haberleşme sisteminde bir telefon görüşmesi yapılabilmesi için arayan kullanıcının santralinden başlamak suretiyle aradaki tüm santraller ve aranan kullanıcı arasında bir devre kurulmaktadır. Şekil 3.1'de örnek bir PSTN şebeke yapısı görülmektedir. Bu yüzden iki kullanıcı arasındaki mesafenin uzak olması durumunda iletişim ortamının kurulması PSTN şebekelerde oldukça maliyetli olabilmektedir. Kullanıcı sayısının artması ile birlikte PSTN şebeke altyapısının sürekli olarak yenilenme gereksinimi ve gelişen teknolojiler ile birlikte kullanıcıların taleplerinin artması yüzünden iş gücü, ekipman ihtiyacı, yönetilebilir bir yapının oluşturulması gerekliliği ve ses ve veri trafiği için servis sağlayıcıların ayrı şebekeler kurması gerekliliğinden dolayı oluşan yüksek maliyetler yeni bir etkileşimli iletişim ortamına gereksinim duyulmuştur.

Şekil 3.1 PSTN şebeke örnek gösterim

İnternet teknolojisinin gelişmesine paralel olarak ses ve diğer verilerin bu ağ ortamı üzerinden iletilmesine olanak sağlamıştır. İnternet üzerindeki verinin sayısal bir veri olması, küçük paketler halinde alıcıya ulaştırılabilmesi gibi nedenlere paralel olarak VoIP haberleşme sistemi gelişmeye başlamıştır.

3.2 VoIP'in Avantaj ve Dezavantajları

İletişim yatırım maliyetlerini çok büyük oranda düşürmesi, bakım onarım giderlerini düşürmesi, hareketliliği arttırması ve dünyanın her yerinden erişebilirlik sağlaması, kurulum maliyetlerini düşürmesi, işletim maliyetleri düşürmesi [15], yüksek güvenirlilik, gelişme ve yeniliklere açık olması [16], var olan internet alt yapısı üzerine kurulabilmesi, ses ve veri hizmetlerinin bir arada verilebilmesi, paket bağlaşmalı birleşik şebeke hizmetlerinin devre bağlaşmalı ISDN'den çok daha verimli olarak sağlaması yeni bir teknoloji olarak sayılabilecek olan VoIP'in en önemli avantajları olarak sayılabilmektedir [17].

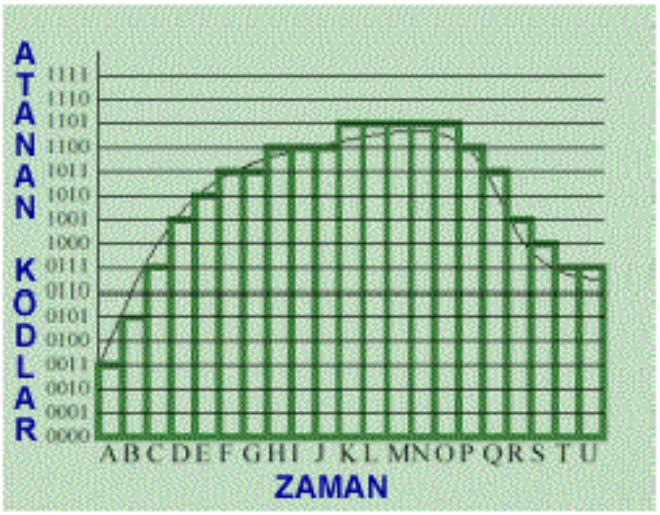
VoIP'nin bir çok avantajı olmasına rağmen karşılaşılabilecek bir çok sorunu da bünyesinde barındırmaktadır. Bu sorunlar, servis kalitesinin hep aynı seviyede tutulamaması, ses paketlere ayrılıp iletim ortamına yollandıktan sonra paket iletiminde yaşanacak hataların seste kesilmelere yol açması, ses kalitesini klasik PSTN sistemlerdeki seviyeye çekilmesi için gerekli olan bant genişliğinin sağlanmasındaki zorluklar, VoIP'in güvenliği hakkındaki soru işaretleri sayılabilmektedir. Özellikle IP üzerinden ses iletirken kullanılacak olan UDP portları sistemde büyük açıklar oluşmasına sebep olabilmektedir. Bu açıklar sayesinde kötü niyetli bilgisayar korsanlarının gerçekleştirecekleri DoS saldırıları ile sistemi aşırı yüklemeleri söz konusu olabilmektedir. Bunun sonucunda, VoIP için gerekli olan QoS değerleri şebekedeki aşırı yük yüzünden sağlanamayabilir [18]. Ayrıca, ses iletiminin IP tabanlı sistemler üzerinden gerçekleştirilmesinde verinin analog bilgiden dijital bilgiye dönüştürülmesi sonucunda ses verisinin kötü niyetli kişiler tarafından dinlenmesi de söz konusu olabilmektedir.

Bu sorunlara rağmen kaliteli ve güvenli bir VoIP oluşturulabilirse avantajları sayesinde vazgeçilemez bir sistem olması beklenmektedir.

3.3 VoIP Sisteminin Çalışması

Zaman içerisinde sürekli olan verinin yani analog verinin sayısallaştırılarak uzak noktalardaki alıcılara gönderilebilmesi, veri iletim teknolojilerinin en önemli atılımı olarak sayılabilir. IP üzerinden sesin iletiminde de bu prensip kullanılmaktadır. Öncelikle ses sinyali ADC'ler (analog sayısal dönüştürücü) sayesinde analog bilgiden sayısal bilgiye dönüştürülmektedir. Bunun için kullanılacak en basit donanım ses kartlarıdır. Analog bilginin sayısal bilgiye dönüştürülme işlemi PCM (darbe kod modülasyonu) ile yapılabilmektedir. Analog bilginin sayısal bilgiye dönüştürülmesi üç aşamadan oluşmaktadır. Birinci aşama örnekleme aşamasıdır ve analog veriden belirli aralıklarla örnekler alınması işlemidir. İkinci aşamada alınan darbe şeklindeki veri örneklerinin belirli değerlere yuvarlanması işlemidir. Bu aşamaya kuantalama da denmektedir. Üçüncü ve son aşamada daha önceden belirlenmiş genlik değerlerine ötelenmiş sayısal ses işaretinin her genlik seviyesi için ikili kodlama şeklinde

kodlanması işlemidir. Böylece PCM işaret elde edilmiş olur. VoIP sistemlerinde çoğu zaman 4 bitlik kod kelimeleri kullanılmaktadır [19]. Şekil 3.2'de bilginin öncelikle darbe genlik modulayonu kullanılarak sesin örneklenmesi işlemi ve örneklenmiş verinin, kuantalanması ve kodlanması işlemleri gösterilmektedir.



Şekil 3.2 Sesin örneklenmesi ve örneklenmiş ses işaretinin kuantalanması ve kodlanması işlemi

Elde edilen PCM sinyal ITU-T'nin G.764 ses sıkıştırma standartlarına uygun olarak paketlenerek ve alıcı bilgisayara iletilmektedir. Oluşturulan paketlerin minimum band genişliği ile alıcı bilgisayara gönderilmesi için ABD ve Japonya'da μ-Kuralı, Avrupa da ise A-kuralının kuantalama şemaları kullanılmaktadır. Tablo 3.1'de belirli giriş genlik değerlerine karşılık μ-kuralı ile kodlanan işaret için çıkış genlik değerleri ve bu değerler için gerekli olan kod çözücü genlik değerleri verilmiştir.

Tablo 3.1 μ-kuralı sıkıştırma – çözme tablosu [20]

GİRİŞ GENLİK ARALIĞI	BASAMAK BOYUTU	SEGMENT KODU	KUANT. KODU	KOD DEĞERİ	KOD ÇÖZÜCÜ GENLİĞİ
0-1	1		0000	0	0
1-3			0001	1	2
3-5	2	000	0010	2	4
....			....	....	....
29-31			1111	15	30
31-35			0000	16	33
....	4	001	....	....	....
91-95			1111	31	98
95-103			0000	32	99
....	8	010	....	....	....
215-223			1111	47	219
223-239			0000	48	231
....	16	010	....	....	....
463-479			1111	63	471
479-511			0000	64	495
....	32	100	....	....	....
959-991			1111	79	975
991-1055			0000	80	1023
....	64	101	....	....	....
1951-2015			1111	95	1983
2015-2143			0000	96	2079
....	128	110	....	....	....
3935-4063			1111	111	3999
4063-4319			0000	112	4191
....	256	111	....	....	....
7903			1111	127	8031

Ses Tablo 3.1 değerlerine göre sıkıştırılmaktadır. Bir sonraki aşama sıkıştırılarak hedef bilgisayara gönderilmiş olan verinin tekrar çözülmesi işlemidir. G.711 haricinde Huffmann sıkıştırması, G.723 ve G.729 gibi çeşitli sıkıştırma teknikleri de band genişliğinden kazanmak amacıyla kullanılmaktadır. Tablo 3.2'de ise belirli giriş genlik değerlerine karşılık μ-kuralı ile

kodlanan işaret için çıkış genlik değerleri ve bu değerler için gerekli olan kod çözücü genlik değerleri verilmektedir.

Tablo 3.2 A-kuralı sıkıştırma – çözme tablosu [20]

GİRİŞ GENLİK ARALIĞI	BASAMAK BOYUTU	SEGMENT KODU	KUANT. KODU	KOD DEĞERİ	KOD ÇÖZÜCÜ GENLİĞİ
0-2			0000	0	1
2-4		000	0001	1	3
....			....		....
30-32	2		1111	15	31
32-34			0000	16	33
....		001	....	....	....
62-64			1111	31	63
64-68			0000	32	66
....	4	010	....	....	....
124-128			1111	47	126
128-136			0000	32	66
....	8	011	....	....	....
248-256			1111	63	252
256-272			0000	64	264
....	16	100	....	....	....
496-512			1111	79	504
512-544			0000	80	528
....	32	101	....	....	....
992-1024			1111	95	1008
1024-1088			0000	96	1056
....	64	110	....	....	....
1088-2048			1111	111	2016
2048-2176			0000	112	2112
....	128	111	....	....	....
3968-4096			1111	127	4032

3.4 İnternet Üzerinden Ses İletiminde Kullanılan Sıkıştırma Algoritmaları

Ses iletilirken gürültü, kullanılacak band genişliği ve dış etkiler önem kazanmaktadır. Bu etkileri azaltmak için darbe genlik modulasyonu ve darbe kod modulasyonun haricinde çeşitli sıkıştırma teknikleri de kullanılmalıdır.

Sistem performansını arttırmak ve gerçek sese en yakın sesi elde edebilmek ve band genişliğini en verimli bir şekilde kullanabilmek için çeşitli sıkıştırma algoritmaları geliştirilmiştir. Bu bölümde bu teknikler irdelenmiştir.

3.4.1 Huffman Sıkıştırması

Huffman, bilgisayar biliminde veri sıkıştırması için kullanılan algoritmadır. David A. Huffman tarafından 1952 yılında geliştirilen Huffman algoritması, her sembol (veya karakter) için özel bir kod üretmektedir. Bu kodlar (ikilik sistemdeki 1 ve 0`lardan oluşan) bit haritası şeklinde oluşturulmaktadır. Algotirma veri içerisinde en az kullanılan karakter için en uzun, en çok kullanılan karakter için ise en kısa kodu üretir. Huffman, veri içerisindeki karakterlerin kullanım sıklığına (frekans) göre bir ağaç oluşturur. Bu ağaçlara göre bit haritaları oluşturulur. Oluşturulan bit haritaları karakterlerin veri içerisindeki konumlarına göre yerleştirilir. Ortaya çıkan bit haritası sıkıştırılmış veridir. Huffman algoritması az sayıda karakter çeşidine sahip ve büyük boyutlardaki verilerde çok kullanışlı olabilir. Fakat oluşturulan ağacın sıkıştırılmış veriye eklenmesi zorunludur. Bu da sıkıştırma verimini düşürür.

3.4.2 LZ Sıkıştırması Algoritmaları

Günümüzdebirden çok LZ algoritması kullanılmaktadır. LZ77 ve LZ78 bunlardan birkaçıdır. Açıklarsak;

LZ77 algoritmasında pencere olarak adlandırılan bellek alanı ve katar uyuşma yordamı kullanılır. Kodlanacak veriye ait karakterler bu pencere içine sokulur. Herhangi bir anda, kodlanacak veriye ait bir hecenin pencere içinde olup olmadığına bakılır. LZ algoritmasında pencere boyu büyüdükçe sıkıştırma başarımı artar, ancak çok fazla da büyür ise işaretçi için gerekli bit sayısı artacağından belirli bir boydan sonra arttırmanın yararı olmaz. Pencere boyunun büyümesi kodlama zamanını artırır. Çünkü uyuşma yordamı uyuşan heceyi aramak için daha fazla çevrim gerekir. Pencere içinde uyuşma gösteren hecenin etkin bir şekilde aranması ve pencere boyunun ne olacağı birçok çalışmaya kaynak olmuştur. Öyle ki, LZ77'nin türevleri olan algoritmaların hemen hemen hepsi, sıkıştırma başarımını azaltmadan hecenin etkin bir şekilde aranması ve pencere boyunun ne olacağının etkin bir şekilde gerçeklenmesi üzerinedir.

LZ78 algoritmasında sözlük olarak adlandırılan bellek alanı, sözcükleri heceleme ve katar uyuşma yordamları kullanılmaktadır. Verideki karakterler, kodlama işlemi anında, heceler ve

sözcükler şeklinde sözlükte saklanır ve onlara birer kod verilir. Herhangi bir anda, karakter düzeyinde gelen veri parçası sözlükte aranır. Eğer bulunursa (uyuşma gösteriyorsa) bir sonraki karakter o anki sözcüğe eklenerek yeni sözcük oluşturulur ve arama işlemine devam edilir. Bu işlem en uzun sözcüğü bulana kadar sürdürülür. Yeni oluşturulan sözcük sözlükte yoksa bir önceki sözcüğün kodu kullanılır ve yeni sözcük kendisine yeni kod eklenerek sözlüğe eklenir. LZ78'de sözlüğün kurulması için sözlük ağacı kullanılırsa zaman açısından çok verimli olmasına rağmmen bellek alanı ihtiyacı çok büyüktür.

3.5 İnternet Üzerinden Ses İletiminde Kullanılan Ses Kodlayıcı ve Kod Çözücüleri

VoIP işleyişi için gerekli olan verinin sıkıştırılması ve eş zamanlı olarak alıcı tarafa gönderilerek orada çözülmesi isteniyorsa normal sıkıştırma teknikleri verimli sonuç vermemektedir. Normal veri sıkıştırma tekniklerinin asıl amacı veriyi sıkıştırarak arşivlenmesini sağlamaktır. Bu yüzden ses verisinin sıkıştırılarak alıcıya eş zamanlı olarak gönderilmesini sağlayan sıkıştırma yapıları oluşturulmuştur. Bu yapılar Codec (coding/decoding-kodlama/çözme) olarak adlandırılırlar. Codeclerin görevi ses verisini sıkıştırmak ve gerektiğinde sıkıştırılan veriyi çözmektir.

3.5.1 G.711 Sıkıştırması

Örnekleme frekansı 8 KHz.'dir. Örnek başına 8 bit kullanılır. Toplam bit hızı gereksinimi 64 Kbit/sn dir. Standart PCM sıkıştırmasıdır. MOS (Mean Opinion Score – Ortalama Yargı Değeri) 4,3 tür.

3.5.2 G.723 Sıkıştırması

Genel olarak düşük bit hızlarında iletim için kullanılmaktadır. Kalite olarak G.711 den kötüdür. Ancak band genişliği gereksinimi G.711 in onda biri kadardır. Cebirsel CELP yada MP-PLQ algoritmaları kullanır. MOS (Mean Opinion Score) 4,1 dir.

3.5.3 G.726 Sıkıştırması

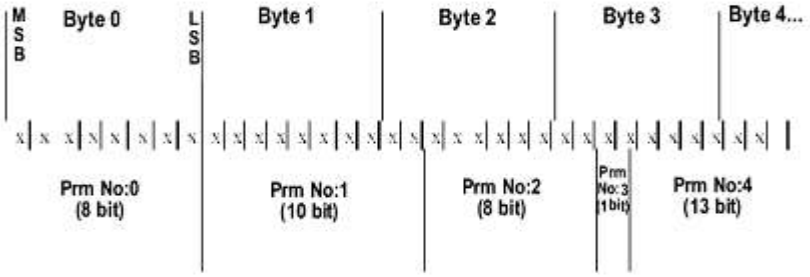
16, 24, 32 ve 40 kbit/sn bit hızlarında adaptif diferansiyel PCM kodlaması kullanır. MOS değeri 2 ila 4,3 arasında değişmektedir [21].

3.5.4 G.728 Sıkıştırması

Düşük gecikmeli CELP kullanır. Bit hızı 16 Kbit/sn, MOS 4,1 dir [22].

3.5.5 G.729 Sıkıştırması

Bit hızı 8 Kbit/sn 'dir. MOS değeri 4,1 dir. Kodlayıcı ses işaretlerini 10 ms'lik çerçeveler halinde kodlar. Ayrıca 5 ms lik aktarım gecikmesi oluşur. Şekil 3.3 ve Tablo 3.3'te G.729 Sıkıştırmasıda bit paketlenmesi ve bitlerin dizilimine örnek verilmiştir.



Şekil 3.3 G.729 bit dizilişi örnek gösterim

Tablo 3.3 G.729 bit paketlenmesi

Parametre	Açıklama	Kullanılan Bitler
Prm#0	Birinci kod kitabı	8 Bit
Prm#1	İkinci kod kitabı	10 Bit
Prm#2	Düzey peryodu	İlk alt çerçeve
		8 Bit
Prm#3	Denklik kontrolü ilk peryota	1 Bit
Prm#4	Kod kitabı birinci indeksi (Pozisyonlar)	13 Bit
Prm#5	Kod kitabı ikinci indeksi (İşaretler)	4 Bit
Prm#6	Düzey ve kontrol kazançları	7 Bit
Prm#7	Göreceli düzey peryodu	İkinci alt çerçeve
		5 Bit
Prm#8	Kod kitabı birinci indeksi (Pozisyonlar)	13 Bit
Prm#9	Kod kitabı ikinci indeksi (İşaretler)	4 Bit
Prm#10	Düzey ve kod kitabı kazançları	7 Bit

3.6 İnternet Üzerinden Ses İletiminde Ses Kalitesi (MOS)

Uzun yıllar süren araştırmalar sonucunda insanların sesleri algılayış biçimleri değerlendirilmiş ve bir notlandırma sistemi oluşturulmuştur. MOS (Ortalama yargı değeri) derecelendirmesi denen bu sistem ITU'nun P.800 tavsiyesinde bulunabilir. Kısaca MOS derecesi 5 ile 1 arasında değişirken, müşterilerin bu işten tatmin olma yüzdeleri de MOS sayısıyla orantılı olarak değişir. Tablo 3.4'de codecler için derecelendirme katsayıları ve paket gecikmesi gibi unsurlar bulunmaktadır.

Tablo 3.4 Codec özellikleri

Codec	Veri Hızı	Paket Süresi	Paket Gecikmesi	Jitter Tampon Süresi	MOS
G.711u	64 kbps	20 ms	1.5 ms	2 datagram (40 ms)	4.4
G.711o	64 kbps	20 ms	1.5 ms	2 datagram (40 ms)	4.4
G729	8 kbps	20 ms	15 ms	2 datagram (40 ms)	4.07
G.723.1 MPMLQ	6.3 kbps	30 ms	37.5 ms	2 datagram (60 ms)	3.87
G.723.1 ACELP	5.3 kbps	30 ms	37.5 ms	2 datagram (60 ms)	3.69

3.7 Sesin Paketlenmesi

Ses işleme uygulamalarında bu iş için özelleşmiş DSP (Sayısal İşaret İşleme) işlemcileri kullanılmaktadır. Bu işlemciler, sahip oldukları güçlü yongalar sayesinde birçok karmaşık işlemi rahatlıkla yapabilmektedirler. DSP'lerin yerine getirdikleri en önemli görev ise; analog telefon işaretlerini IP şebekesinin algılayabileceği sayısal formasyona dönüştürmek ve bunları telefon hatlarına vermektir. Bir DSP'de aranan başka bir özellik ise; insan tarafından oluşturulmuş sesleri rasgele dağılıma sahip olan gürültüden ayırmaktır [23].

Tablo 3.5'den çıkarılabilecek bir önemli sonuç, sessizlik bastırması yapıldığında gerekli olan band genişliği ihtiyacının yarı yarıya azalmasıdır. Bu durum, sistem kaynaklarının daha ekonomik olarak kullanılmasını sağlar. Ancak burada dikkat edilmesi gereken bir nokta vardır. O da; sessizlik bastırması olduğu takdirde konuşan tarafın dinleyen tarafın hala hatta olduğunu anlaması için arkaya yazılım yardımıyla biraz gürültü verilmesi gereklidir. Aksi takdirde iki taraf arasında çeşitli iletişim problemleri çıkacaktır. Tablo 3.5'den çıkan diğer bir sonuç ise G.729 ses codecinin en düşük paket büyüklüğüne sahip olmasıdır. Bu durum düşük hızlı şebekelerde gerçek zamanlı iletimi mümkün kılarken, codecin içindeki başlık/yük oranı yüksek olduğundan şebeke verimi biraz düşebilir. Son olarak, G.723 gibi yüksek sıkıştırma yapan codecler kullanılırken codec gecikmesinin de sistem performansını olumsuz etkileyeceği göz ardı edilmemelidir. Bu durumda band genişliğinden kazanılsa bile işlemci gücünden kaybedilmiş olacaktır [24].

Tablo 3.5 Band genişliği hesaplamaları [25]

Codec	Ses Band Genişliği (kbps)	MOS	Codec Gecikmesi	Paket Büyüklüğü (byte)	IP/UDP/RTP Başlığı (byte)	cRTP	L2 Başlığı (byte)	Toplam Band Genişliği	Sessizlik Bastırmalı BG.
Ethernet									
G.711	64	4.1	1.5	160	40		14	85.6	42.8
G.711	64	4.1	1.5	160		2	14	70.4	35.2
G.729	8	3.9	15	20	40		14	29.6	14.8
G.729	8	3.9	15	20		2	14	14.4	7.2
PPP									
G.711	64	4.1	1.5	160	40		6	82.4	41.2
G.711	64	4.1	1.5	160		2	6	67.2	33.6
G.729	8	3.9	15	20	40		6	26.4	13.2
G.729	8	3.9	15	20		2	6	11.2	5.6
G.723	6.3	3.9	37.5	30	40		6	16	8
G.723	6.3	3.9	37.5	30		2	6	8	4
Çerçeve Aktarma									
G.711	64	4.1	1.5	160	40		4	81.6	40.8
G.711	64	4.1	1.5	160		2	4	66.4	33.2
G.729	8	3.9	15	20	40		4	19.7	9.9
G.729	8	3.9	15	20		2	4	9.6	4.8
G.723	6.3	3.9	37.5	30	40		4	15.5	7.8
G.723	6.3	3.9	37.5	30		2	4	7.6	3.8
ATM									
G.711	64	4.1	1.5	160	40		5 hücre	106	53
G.711	64	4.1	1.5	160		2	4 hücre	4	42.4
G.729	8	3.9	15	20	40		2 hücre	2.3	14.1
G.729	8	3.9	15	20		2	1 hücre	14.1	7.1
G.723	6.3	3.9	37.5	30	40		4	22.3	11.1
G.723	6.3	3.9	37.5	30		2	4	11.1	5.6

3.8 Servis Kalitesi

Servis Kalitesi çok farklı yöntem ve teknolojileri kullanarak bir ağ üzerindeki trafik akışının istikrarlı bir şekilde düzenlenmesini sağlayan teknikler bütünüdür. Bir ağ sahip olduğu bant genişliğinin kullanımını aktif bir biçimde monitör eder ve herhangi bir zamanda kalabalık oluşup oluşmadığının izini tutar. Bilgisayar ağı aktif bir biçimde kullanım modellerini üretir ve bant genişliği istatistiklerini tutar. Bunun yanında hizmet sağlama, kullanım ve mevcut bant genişliğinin dağıtımına bağlı olarak hali hazırdaki kurallara uyulmasını zorlar.

Servis kalitesi bir aktarım sisteminin performans ölçüsüdür. Bu bakımdan aktarım sisteminin kalitesini ve ayakta kalma gücünü yansıtır. Hizmetin ayakta kalması ve istenen her

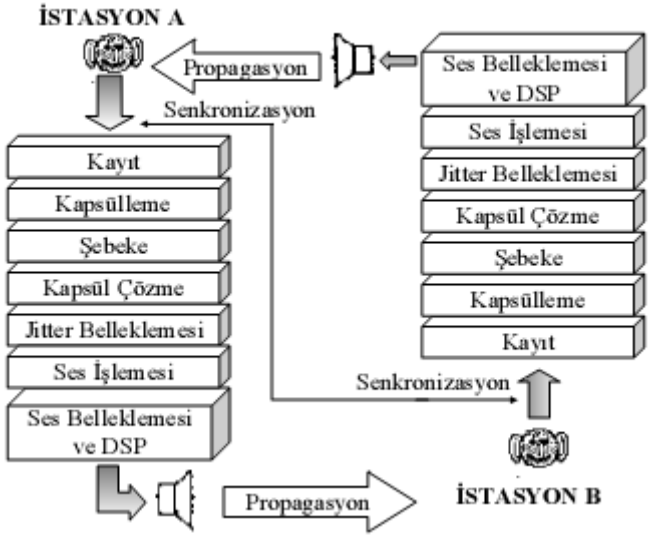
zamanda ona erişilebilmesi servis kalitesinin temel elemanıdır. Herhangi bir servis kalitesi gerçekleştirimi uygulamaya alınmadan önce yapılması gereken en yararlı iş altyapının daima ayakta kalacak şekilde düzenlenmesidir. Aktarım kalitesinin karar verilmesinde etkili üç faktör bulunur bunlar: kayıp, gecikme ve gecikme miktarıdır.

VoIP konusu göz önüne alındığında servis kalitesi (quality of service), önceden tanımlanmış uçtan uca hizmet gereksinimlerinin IP şebekesi gerçekleştirilebilme yeteneği olarak tanımlanabilir. Özel olarak, IP şebekesinde QoS sadece şebeke tarafından güvenilirlik gereksinimlerini sağlamak değildir. Belirli gecikme gereksinimlerinin de sağlaması lazımdır. Örneğin, IP QoS teknikleri, sistemin ihtiyaç duyduğu yeterli bant genişliğini sağlamalı ve belirli gecikme ve jitter değerlerinin gerçeklenmesini öngören ses ve görüntü aktarım uygulamalarında bu teknikler sistem önceliklerini de dikkate alacak şekilde gerekli manipulasyonlarda bulunmalıdır [17].

3.8.1 Servis Kalitesini Etkileyen Unsurlar

Performanslı bir iletişim için önemli bir kriter olan servis kalitesini etkileyen her etken, sistem performansını doğrudan etkileyecek, belirli bir QoS değerinin tutturulabilmesi için de sisteme ek maliyet getirecek yatırımlar yapmak gerekecektir. Bu yüzden servis kalitesini etkileyen unsurları iyi analiz edebilme çok önemlidir. Bu unsurlar;

- **Gecikme:** Ses paketinin kaynaktan yollanması ile alıcı tarafından alınması arasında geçen süre olarak tanımlanır [17,26]. Gecikme yankı ve konuşmaların üstüste binmesi gibi iki probleme neden olmaktadır.Yankı, uzak uçtan konuşan kişinin ses sinyallerinin yansıyarak yine kendisine dönmesine sebep olur. Yankı gidiş-dönüş gecikmesinin 50 milisaniyeden fazla olması durumunda önemli sorunlara yol açar. Eğer yankı önemli bir kalite problemi olarak algılanırsa paket ağları üzerinden ses taşıma sistemlerinin yankı kontrolü (echo control) ve bir anlamda yankı iptaline (echo cancellation) ihtiyacı vardır. Konuşmanın üstüste binmesi (ya da bir konuşmacının diğeri konuşurken araya girmesi), tek yönlü gecikmenin 250 milisaniyeden uzun olduğunda önemli hale gelir. Bu yüzden uçtan-uca gecikme paket ağların üzerinde en büyük tehdit ve gecikmeyi azaltmak için bir gereklilik durumuna gelir. Ses paketinin oluşturulup alıcıya gönderilmesine kadar geçen sürede bir çok gecikeme türü vardır. Şekil 3.4'te sistem üzerindeki gecikmeler gösterilmektedir.



Şekil 3.4 Sistemdeki tüm gecikmeler

- **Biriktirme Gecikmesi:** Bu gecikme ses kodlayıcısı tarafından ses örnekleri içeren çerçevelerin (frames) biriktirilmesinden kaynaklanır. Ses kodlayıcısının tipi ile direk bağlantılıdır [23].
- **Sıkıştırma Gecikmesi:** Sesin belirli bir codec ile kodlanması sırasında geçen süredir. Bu süre kodlama algoritmasının karışıklığına ve kodlama yapan işlemcinin işlem yapma hızına bağlıdır [23].
- **Süreç Gecikmesi:** Bu gecikme, normal kodlama süreci ve kodlanmış örneklerin pakete çevrilerek paket ağları üzerinden geçirilmesi sonucunda oluşmaktadır. Kodlama gecikmesi, kullanılan işlemci yürütme zamanı ve algoritmanın fonksiyonudur. Paket ağlarının bant genişliğinin fazla kullanılmaması için sık sık birden fazla ses-kodu çerçevesi bir pakette birleştirilir [23].
- **Ağ Gecikmesi:** Bu gecikme fiziksel ortamdan, ses verilerini geçirmek için kullanılan kurallardan ve alıcı tarafında paket stresini kaldırmak için kullanılan tamponlardan kaynaklanır. Ağ gecikmesi, ağdaki bağlantıların kapasitesinin ve ağ üzerinden geçirilen paketler üzerinde yapılan işlemlerin bir fonksiyonudur. Paket ağından geçen her paketin, paket-gecikme değişiminin ortadan kaldırılması için maruz kaldığı stres tamponları gecikme ekler. Bazı frame relay ve IP ağlarında paket-gecikmesi değişimi 70 ila 100 milisaniye civarına eriştiğinde bu gecikme tüm gecikmeler içinde önemli bir yer alır [23].
- **Bekleme Gecikmesi:** Tüm paket gecikmelerinin aynı yapılması amacıyla verilerin belirli bir süre belleklerde (buffer) tutulmasından kaynaklanan gecikmedir. Ayrıca bu gecikme sadece karasal transmisyonda görülmez. Bunun yanı sıra uydu

haberleşmesinde de uydunun Dünya ile olan konumunun devamlı değiştiği orta (MEO) ve kısa yörünge (LEO) uydularının veri aktarımı esnasında da görülür [23].

- **Kod Çözme Gecikmesi:** Belirli bir codec ile sıkıştırılmış sesin açılması (kod çözme) sırasında geçen süredir. Bu süre de kod çözücü işlemcinin hızına ve sıkıştırma algoritmasının karmaşıklığına bağlı olarak değişir.

- **Stress (Jitter):** Bir kaynaktan çıkan paketlerin her birinin farklı gecikme değerleriyle alıcıya ulaşması sonucu oluşur. Buna gecikme varyasyonu da denir. Gecikme problemi, stresin, paketlerin geçtiği ağ yüzünden ortaya çıkan değişken iç paket zamanlaması, kaldırılması gereksinimiyle birleşir. Stresi kaldırmak için paketlerin biriktirilmesi ve bu paketlerin yeteri kadar süre tutularak yavaş paketlerin de gelip dinleyiciye doğru sırada çalınması gerekir. Bu ek gecikmeye sebep olur. İki zıt amaç olan gecikmeyi en aza indirme ve stresi kaldırma üzerine ağdaki stresin kaldırılması için stres tampon boyutunun, zaman değişimi gereksinimine uydurulması için çeşitli yaklaşımlar ortaya çıkmıştır. Bu adaptasyon stres tamponunun boyutunu ve gecikmesini en aza indirmek için açık bir amaçtır ve aynı zamanda stres yüzünden oluşan tamponun akışının düşük kalmasını engeller. Stres tampon boyutunu adapte etmek için iki yaklaşım mevcuttur. Seçilecek olan yaklaşım paketlerin geçtiği ağa göre olmalıdır. Birinci yaklaşım, stres tamponundaki paket seviyesi değişimi belirli bir zaman periyodunda ölçülerek, tampon boyutu yükseltilerek hesaplanan strese uydurulmasıdır. Bu yaklaşım en iyi ATM ağları gibi istikrarlı bir stres oluşturan ağlarda çalışır. İkinci yaklaşımda geç gelen paket sayılarını belirledikten sonra bu paketlerin başarıyla işlenmiş paketlere oranı oluşturulur. Bu oran daha sonra stres tamponunu, daha önceden belirlenmiş, mazur görülebilecek geç gelen paket oranına uydurmak için kullanılır. Bu yaklaşım daha çok paket içgeliş değişkenliği yüksek olan IP ağlarında kullanılmaktadır.

- **Kayıp-Paket Telafisi:** Kullanılan paket ağı ile bağlantılı olarak paket kayıpları çok daha önemli bir sorun olabilmektedir. IP ağları servis garantisi veremedikleri için ATM ağlarından çok daha fazla oranda kayıp ses paketine sebep olmaktadır. Mevcut IP ağları bütün ses çerçevelerine veri çerçeveleriymiş gibi davranırlar. Bant genişliği yüklenmeleri ve tıkanıklık şartlarında ses çerçeveleri, veri çerçeveleriyle aynı oranda iptal edilirler. Fakat veri çerçeveleri zaman-duyarlı değildirler ve iptal edilen paketler yeniden transfer edilerek düzeltilebilirler. Kayıp ses paketleri ise bu şekilde düzeltilemez. Kayıp ses paketlerinin telafi edilebilmesi için çeşitli teknikler kullanılmaktadır.

  - Kayıp ses paketinin bulunması gereken yerde son paketi tekrarlayarak kayıp paket için iç değerlendirme yapar. Bu yaklaşım sürekli olmayan konuşmalar içindeki

boşlukları doldurmak için çok basit bir metoddur Sık olmayan kayıp çerçeve oranları için iyi sonuçlar vermektedir.

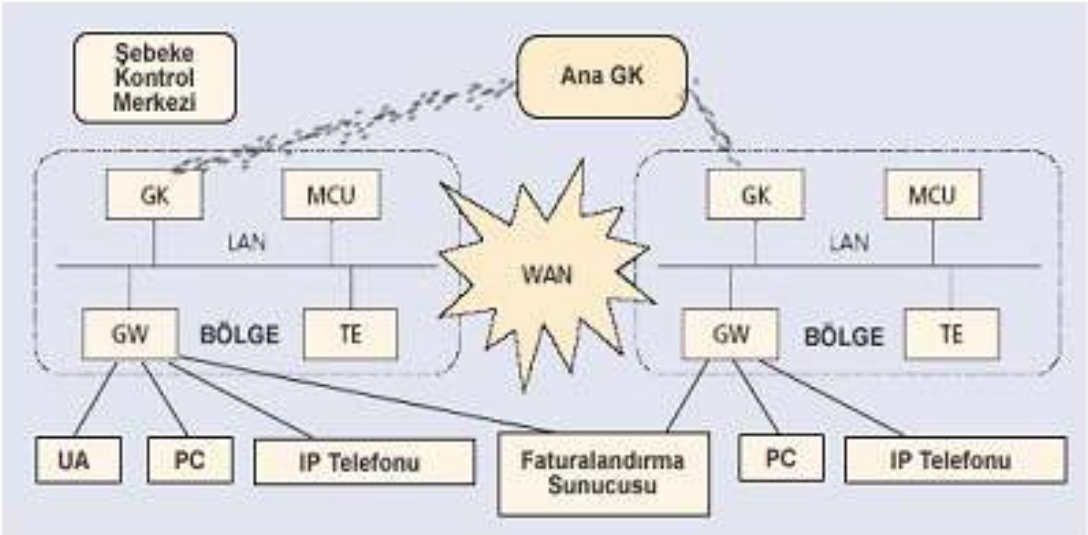
- Bant genişliği harcamasını arttırmak koşulu ile yedek bilgi yollanması; bu temel yaklaşım n'inci ses paketini (n+1)'inci ses paketi olarak da yollar. Bu metodun avantajı kayıp ses paketini tamamıyla düzeltmesidir. Ancak bu yaklaşım daha fazla bant genişliği kullanır ve daha fazla gecikme yaratır.
- Melez bir yaklaşımla daha az bant genişliğinde bir ses kodlayıcısı kullanılarak yine (n+1)'inci yedekleme paketini yollamak; bu fazladan kullanılan bant genişliğini azaltır ama gecikme problemine çözüm olmaz.

- **Yankı (Echo):** İletim hatlarındaki ek noktalarında veya hattın uygun empedans ile sonlandırılmaması nedeniyle oluşur. Empedans uyuşmazlığı olan noktalarda işaretlerin bir bölümü hatta yoluna devam ederken elektriksel işaretin diğer bir bölümü ise yansır. Benzer etki PSTN'deki iletim hatlarında kullanılan 2 tel – 4tel dönüşümü yapan hibrit trafolarda da ortaya çıkar [17,27]. Telefon ağındaki yankı, 4-telli devreler ve 2 telli devreleri birbirine çeviren melez devrelerdeki sinyal yansımalarından kaynaklanır. Bu yansımalar konuşan kullanıcının kendi sesini duymasına sebep olur. Yankı, geleneksel devre-anahtarlı telefon ağlarında bile bulunmaktadır. Fakat dolaşım süresi 50 milisaniyeden az olduğu için ve yankının her telefon cihazında çıkan çevre sesiyle maskelenmesinden ötürü bu gürültü kabul edilebilir boyuttadır. Yankı, paket üzerinden ses taşıma sistemlerinde dolaşım süresi hemen hemen her ağda 50 milisaniyeden fazla olduğu için problem yaratır. Bu nedenle her zaman yankı iptal etme teknikleri kullanılır. Yankı telefon ağından paket ağına doğru yaratılır. Yankı iptalleyicisi paket ağından gelen ve giden ses verisini karşılaştırır. Melez telefon ağından, paket ağına geçen yolda yankı sayısal bir filtreyle kaldırılır.
- **Gürültü:** Ses iletimi esnasında iltim hattının servis kalitesini etkileyen bir başka unsur da gürültüdür. Hatta bulunan gürültü arttıkça kanal kapasitesi düşecektir. Dolayısıyla iletim süresi artarak, servis kalitesi olumsuz etkilenecektir. Gürültünün azaltılması için DSL sistemlerinde ayırıcı (splitter) denen bir cihaz kullanılırken, radyo link sistemlerinde eliptik dalga kılavuzları, GSM gibi hücresel kablosuz mobil sistemlerde verici işaret gücünün arttırılması gibi yöntemler kullanılır. İkinci bir gürültü kaynağı ise; sesin kaydedildiği ortamın gürültüsü ya da arka fon gürültüsüdür. Bu gürültünün engellenmesi, hat gürültüsüne nispeten daha kolaydır. Mikrofon tarafından alınan ses işaretinin genliği, özel bir eşik sezici aracılığıyla belirli bir genlik değeriyle karşılaştırılır ve bu genliğin altında kalan değerler karşı tarafa iletilmezler, çünkü bu bileşenler çoğunlukla gürültüden kaynaklanan işaretlerdir. Buna ek olarak, verici tarafta

konuşma olmadığı zaman karşı tarafa sessizlik olduğunun anlatılması için özel bir işaret yollanır. Böylece kısıtlı band genişliği daha verimli kullanılmış olur ve hatta gereksiz veri paketleri yollanmaz.

3.9 VoIP Mimarisi

İnternet üzerinden sesli haberleşme yapabilmek için cihaza ihtiyaç vardır. VoIP haberleşmesi PSTN teknolojisinde olduğu gibi servis sağlayıcıdan gelen bir hat ve hattın ucuna bağlanan bir telefondan ibaret değildir. İnternet ağı üzerinden sesli haberleşme yapılabilmesi için, haberleşmenin yapısına bağlı olarak çeşitli cihazlar kullanılmaktadır. İnternet üzerinden yapılacak olan sesli haberleşme için standart kullanılması gerekli olan cihazlar ve amaca yönelik olarak isteğe bağlı kullanılacak cihazlar mevcuttur. Şekil 3.5'te VoIP şebekelerinin genel yapısı verilmiştir.



Şekil 3.5 VoIP şebekesinin genel yapısı örnek gösterim

VoIP şebekelerinde sıkça kullanılan cihazlar aşağıda verilmiştir.

3.9.1 Standart Şebeke Elemanları

İnternet üzerinden yapılacak olan sesli haberleşme de kullanılması gerekli olan şebeke elemanları bu kategoriye girmektedir.

- **Kullanıcı Birimi (User Agent - UA):** Kullanıcı birimi kullanıcı adına çalışan uç sistemdir. Bu birim iki parçadan oluşur, İstemci ve Sunucu. İstemci kısmı İstemci Kullanıcı Birimi (User Agent Client - UAC) diye bilinir. Sunucu kısmı ise Sunucu Kullanıcı Birimi (User Agent Server - UAS) şeklinde ifade edilir.

- **İşaretleme Ağ Geçidi (Signalling Gateway - SG):** İşaretleşme bilgisinin IP şebekesi ile CSN (Devre Bağlaşmalı Şebeke) arasında aktarılmasını sağlar. Bu tür GW'ler hem SS7 hem de SIP ve H.323 desteklerler.
- **Medya Ağ Geçidi (Media Gatewat - MG):** PSTN ile IP şebekeleri arasında aktarılan verinin hedef şebeke tarafından anlaşılabilir hale getirilmesi için gerekli değişiklikleri yapmaktan sorumludur [17,28].
- **Terminal:** Terminaller uç noktalarda gerçek zamanlı iki yönlü haberleşme sağlayan yerel ağ istemcileridirler. Şebekenin sonlanma noktalarıdır. H.323 protokolünde çift yönlü transfere izin veren ve hem GW'ler hem de MCU (Multi Point Control Unit)'larla haberleşme yeteneğine sahip olan cihazlardır. Bir terminal diğer bir terminali arama yeteneğine sahip olduğu gibi bu arama işlemi bir gatekeeper (GK) üzerinden de yapılabilir.
- **Çok Noktalı Kontrol Ünitesi (MCU):** MCU ağda ikiden fazla terminalin ya da gateway' in çoklu bir konferansa katılımlarını sağlamaya yarayan ekipmanlardır. Sonradan çoklu bir konferansa dönüşebilecek ikili görüşmeler de MCU' lar aracılığıyla sağlanabilir.
- **Geçit Sorumlusu (Gatekeeper - GK):** Şebeke üzerindeki adres çözümlemeleri, yetki denetimleri ve bant genişliği yönetimi geçit sorumlusu tarafından kontrol edilmektedir.

3.9.2 Seçime Bağlı Şebeke Elemanları

Kurulacak sistemin amacına yönelik olarak sistemde olması gereken cihazlardır. Genel olarak ticari faaliyet göstermek amacı ile bu haberleşme sistemini kuran kurum veya kuruluşların oluşturdukları sistemlerde bulunması gereken şebeke elemanları bu kategoriye girmektedir.

- **Faturalandırma Sunucusu:** VoIP haberleşme sistemini kullanan abonelerin kullandıkları hizmetin faturalandırılması amacı ile kullanılan sunucudur. Şebeke üzerindeki ağ geçitleri faturalandırma sunucusuna bağlıdır. Faturalandırma sunucusuna ağ geçiti üzerinden gelen bilgi doğrultusunda servis sağlayıcı kuruluşun, kullanım süresi veya aktarılan veri baz alınarak faturalandırma işlemini yapabilmektedir.
- **Şebeke Yönetim Merkezi:** Servis sağlayıcı kuruluşun tüm sistemi kontrol ettiği, herhangi bir problem esnasında problemin fark edilip, anında müdahale etmesi şebeke yönetim merkezi tarafından gerçekleştirilir. Bu işlem şebeke yönetim merkezinin belirli aralıklarla bağlı olduğu tüm cihazlara belirli veri paketleri gönderip onların çalışıp çalışmadıklarını belirlemesiyle olur. Şebeke elemanlarından herhangi birinde bir problem çıktığı takdirde şebeke yönetim merkezi önceden tanımlanmış olan program

kodlarını çalıştırarak sisteme müdehale eder veya sistem yöneticisine e-posta yollayabilir.

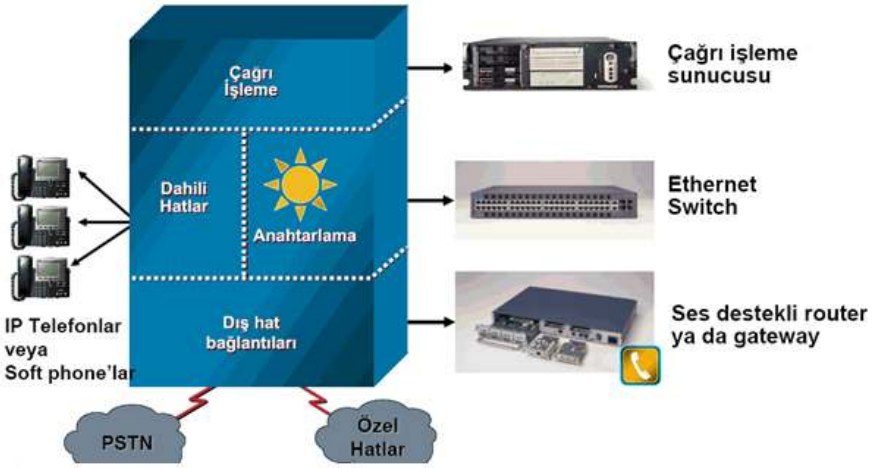
- **Servis Yönetim Merkezi:** Sesvis yönetim merkezinin görevi yetkilendirme, doğrulama ve hesapların kontrol edilmesi işlemleridir. Kullanıcıların sisteme kaydı, kullanıcı bilgilerininin kontrol edilmesi bu cihaz tarafından gerçekleştirilmektedir.
- **Vekil (Proxy) Sunucu:** Dış ağlardan gelen çağrı isteklerinin ağ içinde ki çağrının yapıldığı kullanıcıya aktarılmasını sağlayan sunucudur. Dış ağ ile iç ağ arasında bir köprü vazifesi görmektedir [17,23].
- **Şebeke Adres Çözücü (NAT) Sunucusu:** NAT sunucusu IP v.4'deki adres kısıntısının önüne geçilmek geliştirilmiş bir şebeke elemanıdır. Böylece çok sayıda IP adresine ihtiyacı olan büyük firmalar tek bir uluslararası sabit IP alarak bütün sistemlerini bu IP adresi üzerinden dış ağlara açabilmektedirler [17,25]. NAT sunucusunun bir önemli özelliği de, sesli görüşme yapılan şebekedeki IP adreslerini gizlemesi nedeniyle şebekenin daha dışarıdan gelebilecek saldırılara karşı daha güvenli hale getirilebilmesidir. Ayrıca tek IP üzerinden giden ve gelen trafiğin gözlenmesi ve o adresteki cihaza yapılabilecek saldırılara karşı çeşitli yöntemlerle (güvenlik duvarı ve saldırı tespit sistemi gibi) önlem alınabilmesi çok daha kolaydır [29].

3.9.3 IP Telefon Sistemleri

İnternet üzerinden sesli iletişim kurabilmek için gerekli olan cihazların en önemlisidir. IP telefon ses bilgisinin IP olarak paketlenerek oluşturulan verinin internet ağı üzerinden iletilmesini sağlayan cihazdır. Genel anlamda bakıldığında normal telefon ile IP telefon arasında büyük bir fark mevcut değildir. Fark sadece adresleme mantığının değişmesi, eski usul TDM adreslemeden IP adreslemeye geçişle sınırlıdır. Eski usul adresleme mantığında her bir haberleşme birimi için uçtan uca bir iletişim kanalı kurulması gerekmektedir. Her bilgi her noktada tanınır (ses, veri vb. gibi) ve ayrı işlemler görür. Bu kanal iletişim olsun veya olmasın farklı bir amaç için kullanılamamaktadır. Bu da iletişim altyapısının verimsiz olarak kullanılması sonucunu yaratmaktadır. Bu yapının yatırım maliyeti de oldukça yüksektir. IP üzerinden haberleşmede ise haberleşme kanalı aynı anda birden fazla iletişim için aynı anda kullanılmaktadır. Bilgilerin ayrıştırılması sadece son noktalarda yapılır. Ara noktalarda ses, e-posta, HTML gibi bilgilerin tamamı aynı işlevi görür. İletişim için uçtan uca bir kanal kurulması gerekmediği için kullanılmayan bir servis alanı diğer servislere tahsis edilebilir. Bu da iletişimde verimlilik anlamına gelmektedir. Şekil 3.6'da IP telefon sistemine bir örnek Şekil 3.7'de ise IP telefon mimarisi gösterilmektedir.

- **Avantajları:** IP telefon sistemleri bir veri ağı üzerinden çalışmaktadır. Bu nedenle her birime, her kullanıcıya iki adet (telefon ve internet için) yerine bir tek kablo (aynı kabloda hem veri hem de ses) gitmesi yeterli olacaktır. Farklı birimlerde farklı santraller kullanılmasına gerek kalmamaktadır. Tek noktadan yönetim, Hız ve verimlilik, ölçeklenebilirlik, güvenilirlik, hizmet sürekliliği, düşük iletişim maliyeti, dış kaynaklı hizmetlere daha az bağımlılık, esneklik, mevcut teknolojilerin entegrasyonu, mevcut yatırımı koruyarak genişleyebilme, çağrıları mekan bağımsız aynı numaradan kabul edebilme gibi bir çok avantaja sahiptir.

Şekil 3.6 Uçtan uca IP telefon uygulaması



Şekil 3.7 IP telefon mimarisi

4 VoIP PROTOKOLLERİ

IP ağı üzerinden sinyalleri taşıyan protokollere VoIP denir. VoIP, katman 3 protokolüdür ve katman 2 ’deki pek çok noktadan noktaya (point-to-point) ve link katman protokollerini (PPP, Frame Relay, ATM gibi) veri transferi için kullanır.

VoIP protokollerinin önemli olan protokllerinden birisi RTP (real-time transport protocol –gerçek zamanlı iletim protokolü)’dir. RTP, ses ve video verisini internet üzerinden taşımak için paket biçimi standartları tanımlamıştır. RTP bir çoklu yayın (multicast) protokolü olarak tasarlanmıştır. Ancak sonradan pek çok tekli yayın (unicast) olarakta uygulanmıştır.

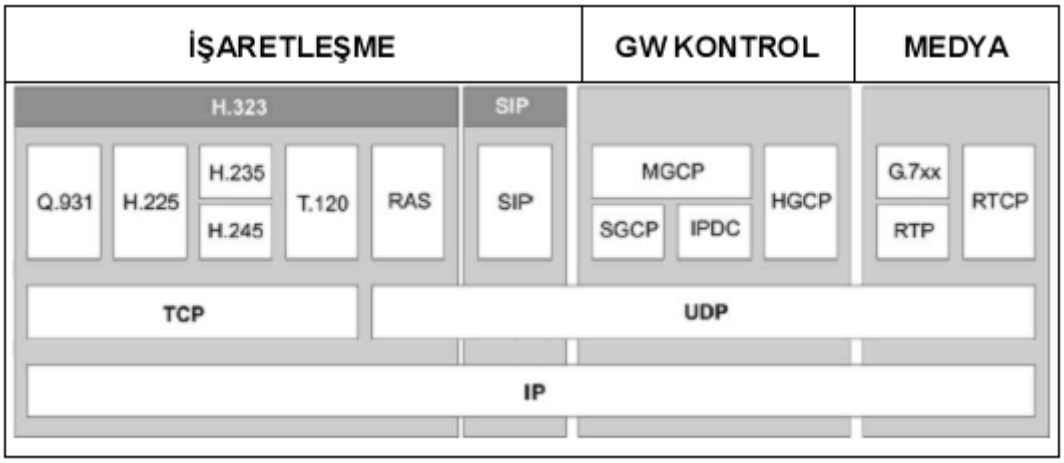
RTP dışında, SIP (Session Initiation Protocol – Oturum Başlatma Protokolü), H.323 gibi protokoller de mevcuttur. H.323 ve SIP ağ üzerinde dağıtık bir yapıda çalışır ve bir çağrı başlatılırken uç nokta ekipmanları dışında başka ağ elemanlarının desteğine ihtiyaç duymaz. SIP, IETF tarafından geliştirilen noktadan noktaya multimedya sinyalleşme protokolüdür. ASCII tabanlı HTTP benzeri bir yapıdadır. H.323, ITU-T 'ye ait H.320 standardının video konferans için geliştirilmiş şeklidir. Tablo 4.1’de VoIP protokolu ve fonksiyonlarının OSI referans modelinin hangi katmanlarında çalıştığı gösterilmektedir.

Tablo 4.1 VoIP protokolu ve fonksiyonları

OSI Katmanı	**VoIP Protokolu ve Fonksiyonları**
7. Uygulama	NetMeeting benzeri uygulamalar
6. Sunum	Codec’ler
5. Oturum	H.323/MGCP/SIP
4. Taşıma	RTP/TCP/UDP
3. Ağ	IP
2. Veri Bağlantı	Frame Relay, ATM, Ethernet, PPP, MLP vs...

İnternet üzerinden ses taşınırken iki önemli protokol grubu vardır. Bunlar işaretleşme ve veri aktarım protokolleri olarak adlandırılabilir. Tablo 4.2’de IP üzerinden sesli iletişim esnasında hangi protokol grubunun kullanıldığı gösterilmektedir.

Tablo 4.2 Çoklu ortam şebeke protokolleri [30]



4.1 İşaretleme Protokolleri

İşaretleme protokolleri oturumun başlatılması, yönetilmesi, sonlandırılması gibi işlevleri yerine getiren protokoller kümesidir. Bu grupta bulunan protokollerden biri veya birkaçı aynı sistem içerisinde kullanılabilir.

4.1.1 SAP ve SDP

SAP ve SDP protokolleri ağ üzerindeki kullanıcılara çoklu oturumlar ile ilgili duyuruları ve bilgileri sağmaktadırlar. Yani konferans görüşme olarakta bilinen iki kullanıcıdan daha çok kullanıcının iletişime dahil olması için gerekli olan yönetimsel işlevleri bu protokoller sağlamaktadır [31]. SAP, oturum bilgilerinin çoklu görüşme yapılabilmesi için tanımlanmasını sağlamakla görevlidir. Oturumun başlatılması aşamasında oturumu başlatan kullanıcı bu protokol sayesinde oturum bilgilerini bildirmektedir. SDP ise oturum bilgilerinin formatını belirlemektedir. Bu bilgiler arasında uç noktaların gerçek zamanlı veri transferi için hangi portları kullanmaları gerektiği, adres bilgileri, medyanın format bilgileri (H.261 Video, MPEG video vb.), oturumun aktif kalacağı süre, oturumu oluşturan medyanın türü (görüntü, ses vb.), taşıma protokolü bilgisi (RTP/UDP/IP, H.320 vb.), gibi birçok bilgi barındırılmaktadır. Ayrıca kaynakların bir oturuma katılmak için sınırlı olduğu durumlarda kanferans görülmede kullanılacak bant genişliği bilgisi, oturum yöneticisinin iletişim bilgileride SDP'nin sorumlu olduğu bilgilerdir [32,33].

SAP mesajları çoklu oturum için hazırlanan ortamdaki bildirim işlemleri için UDP paketlerini kullanmaktadır. SAP mesajlarının başlık ve metin olmak üzere iki bölümü vardır. Bildirim için başlık kısmı kullanılmaktadır. Metin bölümünde ise SDP oturum açıklaması bilgileri mevcuttur. Bir pakette bir adet oturum bildiri mesajına yer verilen paketlerin maksimum büyüklüğü 1 KB'dır.

4.1.2 SIP

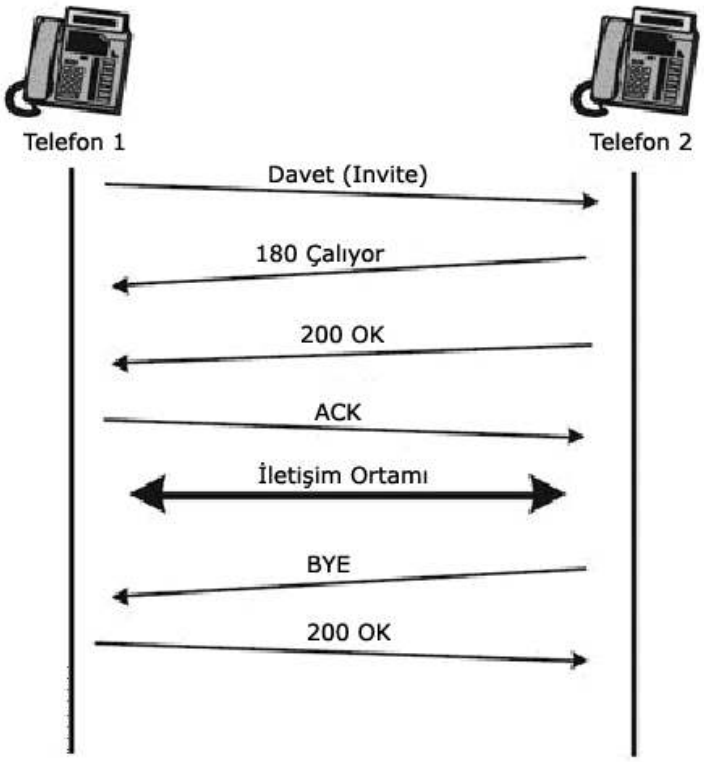
SIP, IETF'nin multimedya uygulamaları için geliştirilen bir protokol grubudur. MMUSIC H.323'ün aksine küçük bir çekirdek protokol ile başlayıp bu protokolü ihtiyaçlara göre geliştirmeyi amaçlamaktadır. Temel olarak HTTP protokolünü alan bu protokol, e-posta gibi diğer internet servisleri ile de benzerlik göstermektedir.

Bu protokole göre bir çağrı başlatıldığı zaman, gelen çağrı, çağrıyı başlatan tarafa servis veren bir sunucuya yönlendirilmektedir. Çağrının yönlendirildiği sunucu çağrıyı reddedebilir veya bir başka sunucuya yada terminale yönlendirebilir. Çağrı bu şekilde cevap verecek bir sunucu bulununcaya kadar ağda hiyerarşik olarak ilerletilir. SIP basit bir protokoldür ve basitliği nedeni ile karmaşık hizmetlerin verilmesi gerektiği durumlarda diğer protokollerden faydalanması gerekebilir.

SIP'in çağrı kontrol mesajlarının geçirilebileceği güvenilir bir kanal açmak için INVITE ve ACK mesajları bulunmaktadır. SIP bir alt seviye taşıyıcı protokol için minimum varsayımları yapar. Bu protokol güvenilirliğini kendisi sağlayıp TCP'nin güvenlik ile ilgili normlarını kullanmaya gerek duymaz. SIP kullanılacak codec uzlaşması (negotiation) için yani o oturumda hangi codec'in kullanılacağına karar vermek için Oturum Tanımlama Protokolünü (SDP) kullanmaktadır.

Bu protokolün getirdiği birçok avantaj bulunmaktadır. Öncelikle web tabanlı bir protokol olması sebebi ile basit, anlaşılabilen bir protokoldür. Bu suretle web tabanlı programlama dili olan html dilinde yazılmış kodlar SIP programlama içinde kullanılabilir. Bu yüzden web teknolojilerinin gelişim süreci ile paralel olarak genişleme imkanı vardır. SIP modüler bir yapıya sahiptir. Büyük bant genişlikleri ve trafik istenilen uygulamalar da kolaylıkla kullanılabilir. TCP ve UDP protokollerinin ikisi ilede kullanılabilmektedir.

Bir oturumun başlatılmasından sonlandırılmasına kadar SIP sinyalleşmesin de kullanılan bir çok SIP mesajı bulunmaktadır. Bu mesajları istek ve cevap mesajları olarak ikiye ayırmak mümkündür. Her iki mesaj grubu da bir başlık ve gövde alanından oluşmaktadır. Şekil 4.1'de örnek bir SIP haberleşmesi gösterilmektedir.

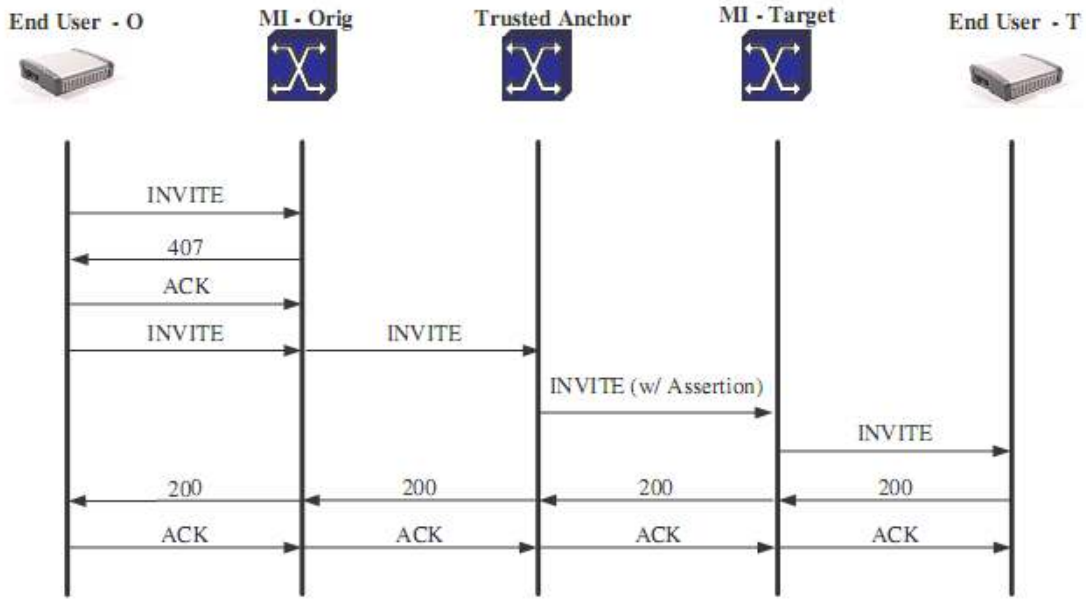


Şekil 4.1 SIP oturumu örnek gösterim

Şekil 4.1'de de gösterilen SIP mesajları aşağıdaki gibidir.

- **INVITE (Davet):** Oturumun başlayabilmesi için ilk adım diğer konuşmacı veya konuşmacıların oturuma davet edilmesi gerekmektedir. Invite mesajı sesli iletişim kurulacak olan kullanıcıların oturuma davet edilmesini sağlar. Bu mesajın gövdesinde konuşmaya davet edilen kullanıcının çağrı kimliği (Call-ID) bilgisi, aranan ve arayan kullanıcıların adresleri, çağrının konusu, çağrı önceliği, çağrı yönlendirme istekleri, kullanıcının konum bilgileri, cevabın niteliği ile ilgili bilgiler bulunmaktadır.
- **ACK (Onama):** Oturum için davet edilen kullanıcının görüşmeyi onayladığına dair mesajdır. Bu mesajın gönderilmesi iletişimin kurulabilmesi için onayın verildiği anlamına gelmektedir.
- **BYE (Çözülme):** Arayan veya aranan kişinin sunucuya görüşmenin sonlandırılması isteğini verdiği mesajdır. Kurulmuş olan bağlantının sonlandırılmasını sağlar.
- **CANCEL (İptal):** Çağrı kurma işleminin iptali için kullanılan mesajdır. Oturum başlatma işlemi devam ederken vazgeçilerek işlemin sonlandırılması olarakta ifade edilebilir.
- **OPTIONS (Seçenekler):** Arayan kullanıcının oturumu başlatmadan önce aranan cihaz veya sistemin özellikleri ile ilgili bilgileri istemesi için gerekli olan mesajdır. Bu mesaj en verimli bağlantının kurulması amacı ile kullanılmaktadır.

- **REGISTER (Kayıt):** Arayan kişinin adresinin kayıt edilmesi için kullanılan mesaj tipidir. Bu mesaj ile gövde içinde bulunan adres bilgiler kayıt edilmektedir.



Şekil 4.2 Karmaşık ağ yapılarında SIP mesajlaşması örnek gösterim

```
INVITE sip:marconi@radio.org SIP/2.0
Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b
Max-Forwards: 70
To: G. Marconi <sip:Marconi@radio.org>
From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341
Call-ID: 123456789@lab.high-voltage.org
CSeq: 1 INVITE
Subject: About That Power Outage...
Contact: <sip:n.tesla@lab.high-voltage.org>
Content-Type: application/sdp
Content-Length: 158

v=0
o=Tesla 2890844526 2890844526 IN IP4 lab.high-voltage.org
s=Phone Call
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Şekil 4.3 SIP mesajlaşması kodsal görünüm [34]

Şekil 4.2'de karmaşık bir ağ yapısında SIP mesajlaşması, Şekil 4.3'te ise SIP oturumunun başlatılması aşamasında ki mesajlaşmanın kodsal yapısı görülmektedir. SIP mesajlaşması istekte bulunma ve isteğe cevap mesajı şeklinde gerçekleşmektedir. İstek mesajına

karşılık olarak gönderilen SIP cevap mesajının ilk satırı statü satırı olarak adlandırılmaktadır. Bu satır üç haneli statü kodu ve metin öbeğinden oluşmaktadır. Cevap mesajları altı grupta toplanabilir [34].

1xx Geçici Cevaplar: İstek mesajının alıdığı ve işleme konulduğunu bildirmektedir. SIP geçici cevapları aşağıda verilmiştir.

- 100 = Deniyor
- 180 = Zil çaldırıyor
- 181 = Çağrı yönlendiriliyor
- 182 = Çağrı sıraya kondu

2xx Başarılı: Arama işleminin başarılı bir şekilde kabul edildiğini bildirmektedir.

- 200 = Tamam

3xx Yönlendirme: Arama isteğinin yerine getirilebilmesi için yeni işlemlerin yapılması gerektiği bildirilmektedir.

- 300 = Çoklu seçim
- 301 = Kalıcı olarak yer değiştirmiş
- 302 = Geçici olarak yer değiştirmiş
- 305 = Proxy sunucusu kullanılmalı

4xx Kullanıcı Tarafı Hata (İstek Başarısız): İsteğin yerine getirilemeyeceğini anlatan mesajdır.

- 400 = Hatalı istek
- 401 = Gerekli izin bulunamıyor
- 403 = Giriş yasaklı
- 404 = Bulunamadı
- 405 = Metoda izin verilmiyor
- 406 = Kabul edilemez
- 408 = İstek zaman aşımına uğradı
- 415 = Desteklenmeyen medya türü

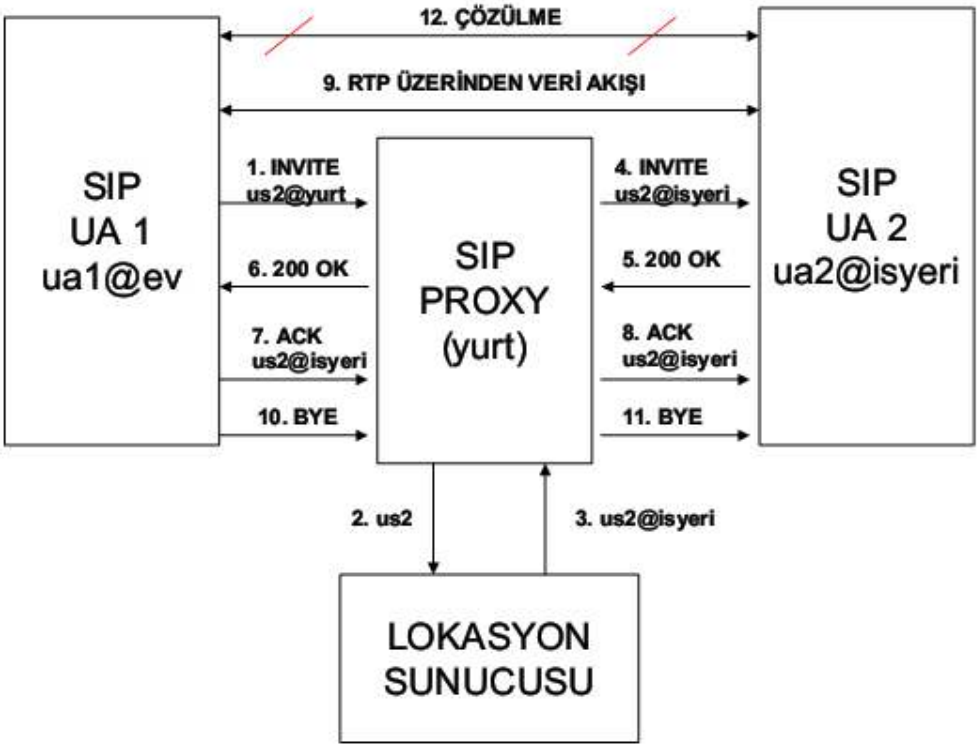
5xx Sunucu Taraflı Hata: Sunucunun, çağrı isteğini yerine getirememesi durumunda kullanılan mesajdır.

- 500 = İç sunucu hatası
- 501 = Uygulanamadı
- 503 = Servis dışı

6xx Genel Hata: Herhangi bir sunucu tarafından isteğin yerine getirilemediğini bildiren mesaj tipidir.

- 600 = Tüm sunucular meşgul
- 603 = Reddedildi
- 606 = Kabul edilemez

Yukarıda anlatılan SIP mesajlarına göre oturumun başlatılması işletilmesi ve sonlandırılması şu şekilde olmaktadır. Öncelikle VoIP sistemindeki iki kullanıcının arama yapabilmesi için REGISTER mesajını kullanarak SIP sunucusuna kayıt olmaları gerekir. Daha sonra oturum kurulabilir. Örneğin A kullanıcısı B kullanıcısını arayacağı zaman, A kullanıcısı, kayıtlı olduğu sunucuya INVITE mesajı gonderir. Bu INVITE mesajının içeriğinde aramak istediği kullanıcının bilgisi, kendi bilgileri (kullanıcı adı, oturum için gerekli IP adresi ve port bilgisi, oturumda kullanmayı tercih ettiği codec bilgisi, ne tür bir istekte bulunduğu – ses, video gibi ..) bulunur. INVITE mesajını alan sunucu, bu mesajı kendisine kayıtlı olan B kullanıcısına gönderir ve böylece A'nın görüşme isteğini B'ye iletir. (Eğer B kullanıcısı aynı sunucuya kayıtlı bir kullanıcı değilse, sunucu bu isteği, B'nin kayıtlı olduğu sunucuya yönlendirir ve mesaj bu şekilde B'ye ulaştırılır). B terminalinin çalması sırasında A'ya 180 zil çaldı mesajı gönderilir. B, isteği kabul ettiğini belirten 200 OK mesajını A'ya gönderilmek üzere kayıtlı oldugu proxy'ye gönderir. Bu mesajın içinde kendisine ait oturum için gerekli bilgileri gönderir (IP ve port bilgisi, tercih ettiği codec bilgisi,..). A kullanıcısı 200 OK mesajını aldığını belirten ACK mesajını B'ye gönderilmek üzere sunucuya iletir ve böylece üç yollu el sıkışma tamamlanmış olur. Br aşamadan sonra iki kullanıcı birbirlerinin IP adresi ve port bilgilerini öğrenmişler ve hangi koşullarda hangi seçeneklerle haberleşecekleri konusunda anlaşmışlardır. Böylece iki kullanıcı arasında gerçek-zamanlı veri ileti (ses, video..) başlar. Gerçek zamanlı verinin iletimi kullanıcılar arasında gerçekleşir, bu aşamada SIP sunucu devreye girmez. Taraflardan biri oturumu sonlandırmak istediğinde yine sunucular aracılığı ile karşı tarafa BYE mesajı gönderir. Bu mesajı alan kullanıcı mesajı aldığını, kabul ettiğini belirten 200 OK mesajını gönderir ve böylece oturum sonlandırılır. SIP mesajlarında çok sayıda gizli bilgi açık bir şekilde iletilmektedir. Örneğin bağlantıda kullanılan IP ve port bilgileri, kullanıcı adları, SIP adresleri, codec bilgisi gibi. Bu özellikleri, SIP protokolünde güvenlik açığı oluşturmaktadır [35]. Şekil 4.4'de SIP protokolü kullanımın da iki kullanıcı arasında bir proxy sunucunun olduğu durumdaki mesajlaşma gösterilmektedir.



Şekil 4.4 Proxy sunuculu SIP mesajlaşması işlem adımları

4.1.3 H.323

ITU-T tarafından iki ya da daha fazla taraf arasında IP benzeri QoS desteği olmayan bir ağ üzerinde ses ya da görüntü trafiğini taşımak için geliştirilen H.323 standardı bir protokol grubudur. Yerel ağlar üzerinde çokluortam konferansı için geliştirilmiş, fakat sonradan IP üzerinden ses uygulamasını kapsayacak şekilde genişletilmiştir. Bu standardın tanımlanmasında Microsoft, IBM, İntel, telefon operatörleri ve ISP'lerden oluşan birçok kurum ve firmanın geniş katılımı ve desteği sağlanmıştır. İnternet telefonu amacıyla kullanılan en geniş ve en etkin standartlardan birisidir [36]. Ses ile beraber tüm çokluortam (data, ses, video, resim gibi) uygulamalarını desteklemektedir. H.323 standardı bir şemsiye standart olup birçok standardı kapsamaktadır. Bu standartlar ses kodlama, video kodlama, sistem kontrol, çoklama, çokluortam yayın senkronizasyonu ve yapısını içermektedir. Bu standartlar PSTN, Mobil, ATM, F/R, LAN, WAN, IP tabanlı İnternet gibi şebekeleri içermektedir. IP telefonun etkileşmek zorunda kalacağı sistemlere ilişkin ITU standartlarından bazıları şunlardır:

H.323 LAN şebekeleri için görüntülü telefon sistemleri ve ekipmanlarının standardını içeren bir protokoldur. QoS gibi parametreler içermemektedir. H.324 PSTN şebekelerinde kullanılan görüntülü telefon sistemi ve ekipmanlarının standartlarını belirleyen bir protokoldur. H.324/M ise GSM gibi hücresel gezgin ağlar için geliştirilmiş bir standartdır. H.310 genişbantlı ses ve görüntülü iletişim sistemlerini ve terminallerini kapsamayan bir standartdır. H.321

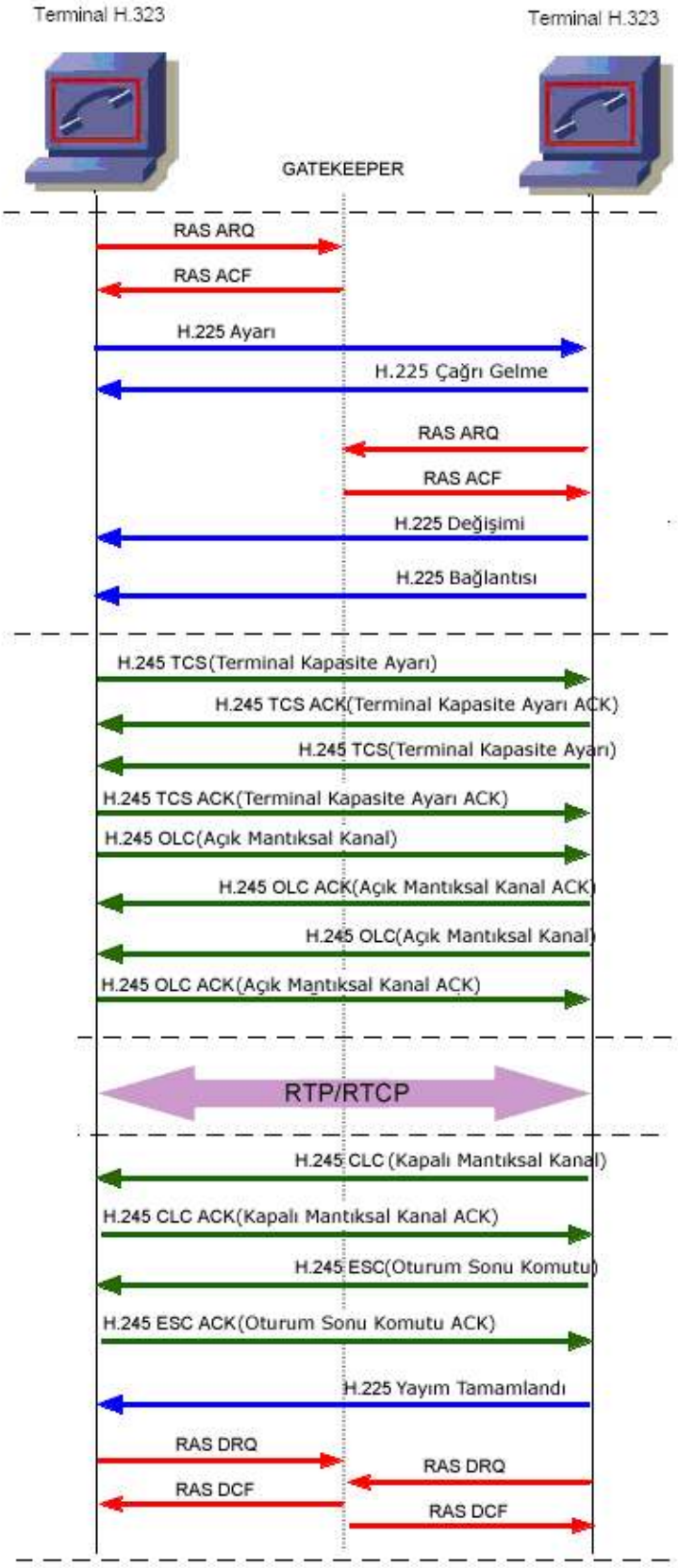
Genişbantlı ISDN şebekeleri için görüntülü telefon terminalleri standartlarını belirler. H.322 Lan şebekeleri için görüntülü telefon sistemleri ve terminallerini kapsamayan bir standardır. QoS parametreleri içermektedir. Tablo 4.3'de H.323'de hangi protokollerin hangi katmanlarda kullanıldığı gösterilmiştir.

Tablo 4.3 H.323 protokol yığını [37]

<table>
<tr><th rowspan="2">Veri</th><th colspan="2" rowspan="2">Kontrol ve İşaretleşme</th><th rowspan="2">Sistem Kontrolü</th><th>Ses Codecleri</th><th>Görüntü Codecleri</th><th>Ses ve Görüntüsel Kontrol</th></tr>
<tr><td>G.7xx</td><td>H.26x</td><td rowspan="2">RTCP</td></tr>
<tr><td>T.12x</td><td>H.245</td><td>H.225.0</td><td>H.225.0 RAS</td><td colspan="2">RTP</td></tr>
<tr><td colspan="3">UDP/TCP</td><td colspan="4">UDP</td></tr>
<tr><td colspan="7">IP</td></tr>
<tr><td colspan="7">Değişken Katman 2 Protokolleri</td></tr>
<tr><td colspan="7">Değişken Katman 1 Protokolleri</td></tr>
</table>

H.323 Mesajları: H.323 protokolünde de SIP protokolünde olduğu gibi oturumun başlatılması, yönetilmesi, sonlandırılması için çeşitli mesajlar kullanılmaktadır. Bu mesajlar Şekil 4.5'te gösterilmektedir.

- **RRQ (Request to Register – Kayıt İsteği):** GK'ye kayıt olmak için uç nokta cihazlarının yaptığı istek mesajıdır.
- **RCF (Request Confirm – İstek Onayı):** Uç birim cihazların GK'ye kayıt işleminin gerçekleştiğini söyleyen mesajdır.
- **RRJ (Request Reject – İstek Reddi):** Uç birim cihazların GK'ye kayıt işlemlerinin gerçekleşmediğini söyleyen mesajdır.
- **ARQ (Admission Request – Kabul İsteği):** Ağ geçitinin GK ile temasa geçip uç birimlerin bağlantısının nasıl yapacağını sorması işlemidir.
- **ACF (Admission Confirm – Kabul Onayı):** GK'ın hedef uç birimin bağlı bulunduğu ağ geçidi adresini kaynak taraftaki ağ geçidine vererek bağlantının kurulduğu mesajıdır.
- **RAS ARQ:** Hedef ağ geçidinin konuşmanın başlayabilmesi için uç birime gönderdiği ağ ortamının konuşma için müsait olduğunu söyleyen mesajdır.
- **Call Proceding (Çağrı İlerleme Durumunda):** RAS ARQ mesajı ile eş zamanlı olarak kaynak ağ geçidinin kendi uç birimine gönderdiği çağrı ilerleme durumunda mesajıdır.
- **Connect (Bağlantı Kuruldu):** Hedef ağ geçidinin kaynak ağ geçidine bağlantının gerçekleştiğini söylediği mesaj türüdür.
- **TCS (Terminal Capability Set – Kutup Yetenek Ayarı):** Ağ geçitleri arasında kendi yeteneklerinin ayarlanması işlemidir.



Şekil 4.5 H.323 protokolü mesajlaşma örnek gösterim

- **ACK (Acknowledge – Kabul Etmek):** Ağ geçidinin diğer ağ geçidine yetenek, durum bilgilerini verdiği mesajdır.
- **OLC (Open Logical Channel – Açık Mantık Kanalı):** Kaynak ağ geçidinin hedef ağ geçidi ile mantıksal bir kanal açılması için gönderdiği mesajdır.

4.1.4 SIP ile H.323 Protokolünün Karşılaştırılması

Tablo 4.4 SIP H.323 karşılaştırması [26]

Kategori	SIP	H.323
Uç birimler	Akıllı	Akıllı
Akıllı şebekeler ve servisler	Sunucular tarafından sağlanır.	Geçit sorumlusu tarafından sağlanır.
Kullanılan model	İnternet / www	Telefon
İşaretleme protokolü	UDP veya TCP	TCP
Medya protokolü	RTP	RTP
Kod tabanı	ASCII	İkili (Binary)
Kullanılan diğer protokoller	IP protokolleri, SDP, HTTP	ISDN, H.225, H.245 ve H.450

Tablo 4.4'de SIP protokolü ile H.323 protokolünün karşılaştırılması gösterilmektedir. Her iki protokol de VoIP sistemindeki işaretleşme işlemlerinin yürütülmesi amacıyla geliştirilmiştir. H.323 daha eski bir protokol olup ve ITU-T'nin telekomunikasyon dünyasına kabul ettirmeye çalıştığı bir protokoldür. Diğer taraftan SIP ise IETF'nin geliştirdiği bir protokoldür. Burada da bir çok konuda olduğu gibi ABD ile Avrupa'nın çekişmesi görülmektedir. SIP'in yeni çıkan bir protokol olması nedeniyle çeşitli avantajları vardır. Bunlardan bazıları, metin bazlı olmak, kolay geliştirilebilir olmak ve UDP gibi bağlantısız bir aktarım protokolünü desteklemektir. SIP modüler bir yapıya sahiptir ve görevler akıllı sunucular arasında paylaştırılmıştır. Buna karşın H.323'de daha merkezi kontrol sistemi mantığı ile hareket edilmiş olup geçit sorumlusu olan cihazlar büyük yetkilerle donatılmışlardır. Son yıllarda birçok şirket ürettikleri cihazlarda hem SIP hem de H.323 desteği vermeye başlamışlardır. Ayrıca SMC, PX, GK, Lokasyon sunuculuğu gibi birçok işlem tek bir cihazda toplanmıştır. Çok fonksiyonel bu cihazlara "softswitch" denir ve bu cihazlar iki işaretleşme protokolünü de desteklerler [23].

4.2 Veri Aktarım Protokolleri

SIP veya H.323 protokolü ile oturumun başlatılması işleminden sonra gerçek zamanlı olarak ses işaretlerinin iki yönlü olarak sağlıklı bir şekilde gönderilmesi gerekmektedir. Bu

aktarım için kullanılan veri aktarım protokolleri RSVP (Kaynak Ayırma Protokolü), RTP (Gerçek Zaman Protokolü), RTCP (Gerçek Zaman Kontrol Protokolü) protokolleridir [33].

4.2.1 RSVP

Veri trafiği üzerinde bir düzeye kadar gürültülüye ve gecikmelere tolerans gösterebilir. Buna karşılık, görüntü ve ses ile ilgili trafiğin, sürekli ve gürültüsüz olması gerekmektedir. Bu sebepden dolayı ses, video ve radyo sinyal trafiğinin ağ üzerinde, kalitesi yüksek servis gerektirdiğinden (QoS) problemlerin çıkmasına neden olmaktadır. RSVP, IP ağlar üzerinde gecikmeye duyarlı olan multimedya trafiğinin taşınmasını sağlamaktadır. RSVP'de ağ bantgenişliği önceden rezerve edilmektedir. Bu da çoklu ve tekli ağlarda kaliteli servis (QoS) garantisi verir. Önceden bantgenişliği reservasyonu yapılması, bantgenişliğinden de tasarruf sağlanmış olur. Bunun sebebi de eğer bantgenişliği reservasyonu için yeteri kadar bantgenişliği olmaması durumunda iletim de olmamasıdır. RSVP TCP/IP tabanlı ağlarda uctan-uca haberleşme sağlayan bir protokoldür.

Burada dikkat edilmesi gereken bir husus, RSVP'nin bir routing protokolü olmadığıdır. RSVP IP networkü üzerinde bir kontrol protokolüdür, OSI modeline güre iletim katmanı seviyesidir. RSVP yönlendirme (routing) protokolleri ile birlikte çalışmaktadır. Bu anlamda, RSVP Inetrnet Kontrol Mesaj Protokul'ü (ICMP) ve Internet Gateway Mesaj Protokolü (IGMP) ile benzerliklere sahiptir. RSVP ile aynı kaynağa ve QoS'e ait mesajlar sıralı bir veri akışı ile taşınırlar. Bu veri akışı da bağlantı olarak bilinir. Bir RSVP işleminde; göndericiler, yönlendiriciler ve alıcılar bulunmaktadır [37].

Tekli ortamlarda RSVP ile veri akışının şu şekilde olmaktadır. İlk başta, bir gönderici RSVP mesajını alıcıya gönderir. Bu mesaj; gönderici IP adresi, alıcı Ip adresi, veri akış ayrıntıları bilgilerini barındırmaktadır. Veri akış ayrıntılarında, başarılı bir veri aktarımı için gerekli QoS bilgisi bulunmaktadır. Alıcı, veri alacağı zaman bu isteğini belirtmek için ağdaki yönlendiricilere rezervasyon isteği gönderir. Bu reservasyon isteği içerisinde ise gönderen IP adresi, alıcı IP adresi, veri akış ayrıntıları, iki kontrol modülü içerik bilgileri bulunmaktadır. İki kontrol modülü, giriş kontrolü ve kontrol politikası olarak bilinmektedir. Giriş kontolü iyi bir QoS için yeterli bantgenişliğinin olup olmadığına karar verir. Kontrol politikası da alıcının reservasyon isteğinin kabul edilip edilmediğine karar verir. Router'lara (yönlendirici) kaynak isteği geldiğinde, yukarıda bahsedilen iki kontrol modülü kullanılır. Eğer her iki konrol de başarılı ise, gerekli bantgenişliğinin ayrılması için routerlara link layer (bağlantı katmanı) paremetreleri girilir. Sonra alıcı rezerve bilgisini alır ve verileri göndermeye başlar. Eğer yönlendiriciler yeteri kadar kaynak ayıramazlar ise, bu rezerve toplam bantgenişliğinden yer almayacaktır. Veri gönderilmemesi durumunda kaynak harcanmayacaktır [38].

Çoklu ağlarda, alıcılar ve yönlendiriciler kısa bir süre için rezerve isteğini tutarlar. RSVP'yi destekleyen alıcı sistemleri basit alıcı sistemlerden daha verimlidir. Basit sistemlerde, gönderici muhtemel tüm alıcıların özelliklerini bilmesi gerekir. RSVP ile her alıcı sadece kendi yeteneklerini ve gereksinimlerini bilmesi yeterlidir. Aslında, kaynak rezerve isteği bir yönlendiriciden bir sonrakine atlayarak tüm ağı dolaşarak gerçekleşir. RSVP'nin bu şekilde çalışması hem çoklu hem de tekli ağlarda problemlere sebep olmaktadır. Örneğin yerel yönlendirici, alıcının reservasyon isteğini kabul etmesine karşın ağdaki diğer yönlendiriciler reddedebilir. Eğer böyle olursa, RSVP paketleri ağda kilitli kalır ve veri aktarımı gerçekleştirilemez. Ağın değişmesi veya taşınması problemlere sebep olabilir. Bu problemi gidermek için, yönlendiriciler RSVP mesajlarını yeniliyebilmelidirler. Yani, göderici belirli aralıklarla RSVP rota mesajları gönderecek, alıcı da sürekli reservasyon isteğini yenileyecektir. Böylece ağ sürekli reservasyon isteklerinin varliğinindan haberdar olacaktır. Bu durumda, ağ'da meydana gelecek bir değişmeden reservasyon istekleri zarar görmeyecek ve bu istekler hesaba katılacaktır. RSVP düzenli olarak yeni reservesyon mesajlarını gözden geçirir. İşe yaramaz mesajları da siler.

RSVP Mesajları: RSVP mesajları başlık ve gövde kısımlarından oluşmaktadır. Başlık kısmı tüm mesajlaşma da ortaktır. Tablo 4.5'de RSVP başlık formatı görülmektedir.

Tablo 4.5 RSVP başlık formatı

0	1-2	3	4	5-6	7	8	9-14	15	16	17-30	31
Sürüm			Bayrak			Mesaj Türü		Kontrol Alanı			
Yaşam Süresi						Rezerve		RSVP Uzunluğu			

Tablo 4.5'de görülen sürüm başlığı kullanılan protokolün sürü numarasını, mesaj türü ise; yol kurma, yol ayırma, yol kurma hatası, yol ayırma hatası, kurulan yolu çözme, ayrılan yolu çözme, yol ayırma onayı gibi yedi değişik mesajın yayınlandığı alandır. RSVP uzunluğu alanı başlıkta dahil olmak üzere toplam mesaj boyut bilgisini byte cinsinden tutmaktadır. Yaşam süresi başlığı ise mesajın yok edilmeden önce hayatta kalacağı süreyi belirlemektedir.

4.2.2 RTP

RTP gönderici cihazdan alıcı cihaza kadar uçtan uca gerçek zamanlı ses ve görüntü bilgisinin taşınması amacı ile oluşturulmuş bir protokoldür. İnternet üzerinden sesli görüşmenin en önemli kriteri görüşmenin gerçek zamanlı, gecikmesiz ve kaliteli bir görüşme olmasıdır. RTP protokolü şebeke üzerindeki taşıma fonksiyonlarını oluşturarak bu bu fonksiyonların denetimini gerçekleştirmektedir. RTP, UDP üzerinde çalışmaktadır. UDP'yi kullanmasının sebebi çoğullama ve başlık kontrol mekanizmalarını kullanabilmektir. RTP protokolü çoklu ortamlarda

da kullanılabilmektedir. Aynı anda birden çok kullanıcının veri transferini gerçek zamanlı olarak gerçekleştirebilmektedir [39].

RTP protokolünde veri paketlere bölünerek alıcı tarafa iletilmektedir. RTP gönderim esnasında bir dizi şeklinde paketleri numaralandırmakta ve alıcı tarafta bu dizi numaralarına göre paketleri birleştirerek tüm veriyi oluşturmaktadır.

RTP Mesaj Formatı: RTP mesajları UDP protokolünü kullanmaktadır. RTP mesajları UDP 5004 numaralı port üzerinden iletilmektedir. Tablo 4.6'da RTP mesaj formatı görülmektedir.

Tablo 4.6 RTP mesaj formatı

0	1	2	3	4-7	8	9	10-14	15	16	17-30	31
V=2		P	E	CC	M	PT			Dizi Numarası		
Zaman Damgası											
Senkronizasyon Kaynak Tanımlayıcısı (SSRC)											
Ek Kaynak Tanımlayıcısı (CSRC) (Değişken)											
Veri (Değişken)											

Tablo 4.6' da görülen V (Version) versiyon numarasını belirtmektedir. P (Padding), bayrak bitidir. E (Extension), RTP başlığından sonra bir başka başlığın olduğunu söylemektedir. CC (Contributer Count), mesajda bulunan ek kaynak tanımlayıcılarının sayısını vermektedir. M (Marker), veri aktarım sınırlarının belirlenmesi için kullanılmaktadır. PT (Payload Type), hangi tür yükün taşınacağı bilgisini içermektedir. Dizi Numarası, paketlerin gönderici tarafından gönderildiği sırayı tutmak ve alıcı tarafta gelen paket numaralarına göre paketleri birleştirerek veriyi oluşturmak için gerekli olan numaralandırma işlemini gerçekleştirmektedir. Zaman damgsası, bir örnekleme saati oluşturularak senkronizasyon ve jitter kayıplarının hesaplanması amacı ile kullanılmaktadır. Senkronizasyon kaynak tanımlayıcısı (SSRC), senkronizasyon kaynağını belirtmektedir. Aynı oturum içinde senkronize olacak her kaynağın ayrı bir senkronize numarasının oluşturulması ve senkronizasyonun kontrolü için kullanılmaktadır. Ek kaynak tanımlayıcısı (CSRC), paket yüküne katkıda bulunan kaynakları tanımlamaktadır.

4.2.3 RTCP

Veri aktarım işlemi RSVP protokolü tarafından kaynak ayrılması işlemi ile başlamaktadır. Kaynak ayırım işlemini RTP protokolü uç birimler arasında veri iletiminin sağlanması ile devam ettirmektedir. RTCP protokolünün görevi ise bu iletim esnasında uç birimleri sağlayabilecekleri veya alabilecekleri hizmet kalitesi seviyesinden haberdar etmektir.

RTCP Paket Türleri: RTCP ile gönderilen bilgiler uç birimler hakkındaki çeşitli istatistikleri vermektedir. RTCP bilgisinin hangi konuda olduğunu RTCP paket numarasıdır. RTCP paket türleri tablo 4.7'de gösterilmektedir.

Tablo 4.7 RTCP paket türleri

Numara	Paket Türü	Kullanım Amacı
200	Gönderici Raporu	Aktif paket göndericilerinin gönderme ve alma istatistiklerini gösterir.
201	Alıcı Raporu	Alan taraflar için sadece alma istatistiklerini gösterir.
202	Kaynak Açıklaması	Kaynak açıklama bölümlerini içerir.
203	Sonlandırma Mesajı (Bye)	Katılımın sonunu belirtir.
204	Uygulamaya Özel	---

RTCP Mesaj Formatı: RTCP mesajları 32 bitlik mesaj katarlarından oluşmaktadır. Tablo 4.8'de aktif paket göndricilerinin gönderme ve alma istatistiklerini gösteren 200 paket numaralı örnek bir RTCP mesaj formatı gösterilmektedir.

Tablo 4.8 RTCP mesaj formatı örnek gösterim

0 1 2 3	4-7	8 9-14 15	16-23 24-31	
V=2	P	RC	PT=SR=200	Uzunluk	Başlık
Gönderen Tarafın SSRC Numarası				
NTP Zaman Damgası (En yüksek önemli kelime)				Gönderici Enformasyonu
NTP Zaman Damgası (En düşük önemli kelime)				
RTP Zaman Damgası				
Gönderen Tarafın Paket Sayısı				
Gönderen Tarafın Oktet Sayısı				
SSRC_1 (İlk Kaynağın SSRC Numarası)				1 Numaralı Rapor Enformasyonu
Kayıp Oranı	Toplam Kayıp Paket Sayısı			
Alınan En Büyük Dizi Numarası				
Aravarış Jitteri				
Son Gönderici Raporunun Zamanı				
Gelen Son Gönderici Raporu İle Aradaki Gecikme				
SSRC_2 (İkinci Kaynağın SSRC Numarası)				2 Numaralı Rapor Enformasyonu
...				
Uygulamaya Özel Genişlemeler				

Tablo 4.8'e göre; RC (Receiver Block Count), kaç bloğun mesaj içinde yer aldığını söylemektedir. PT (Packet Type), paket tipinin 200 nolu paket olduğunu ve aktif paket göndericilerinin gönderme ve alma istatistiklerini gösteren veriyi barındırdığını söylemektedir. NTP zaman damgası, sistem saatine ilişkin bilgileri içerir. Bu alan senkronizasyon amacı ile kullanılmaktadır. Gönderici paket büyüklüğü, alıcı cihazı göndericinin kaç paketlik veri gönderimi yaptığı konusunda bilgilendirmek amacı ile kullanılmaktadır. Kayıp oranı, kayıp paketlerin gelmesi düşünülen paketlere olan oranını vermektedir. Toplam kayıp paket sayısı, kayıp paketlerin sayısını vermektedir. Alınan en büyük dizi numarası, kaynaktan alınan RTCP paketlerinin en büyük dizi numarasını vermektedir. Arageliş stres bilgisi, paketlerin gelişleri arasındaki zaman bilgisini vermektedir.

5 IP ÜZERİNDEN SES İLETİMİ ESNASINDA HARİCEN OLUŞABİLECEK İSTEM DIŞI TEHDİTLER

VoIP teknolojisinde analog ses sinyalleri dijital ses paketlerine dönüştürülerek internet üzerinden telefon görüşmesi yapılması sağlanmaktadır. Bunu yaparken de eski sistemlere göre düşük maliyetli telefon görüşmesi, daha fazla özellik taşıması, gelişmeye açık olması, kolay yönetim gibi avantajlarda sağlamaktadır.

İnternet teknolojileri ile paralel olarak gelişmekte olan iletişim teknolojilerinden VoIP kullanımı gün geçtikçe artmaktadır. VoIP teknolojisi internet tabanlı bir uygulama olduğu için internet üzerinde oluşabilecek tüm güvenlik tehditleri VoIP uygulamalarını da etkilemektedir. VoIP uygulamalarında IP bazlı iletişimin kurulmasının birçok avantajları olmasına rağmen, internet üzerindeki uygulamaların hala büyük güvenlik tehditleri altında olduğuda çok açıktır. Bu saldırıların amacı finans sağlamak, bedava konuşmak, kimlik ve bilgi çalmak, maliyetsiz bir şekilde reklam yapmak, kötü şöhret edinmek veya kullanıcıları rahatsız etmektir. Genel olarak güvenli bir iletişim için bütünlük, doğruluk ve kişisel gizlilik ilkelerinin gerçekleşmiş olması benimsenmektedir. VoIP üzerinde ki güvenlik tehditleri de bu ilkeleri zedelemektedir. VoIP uygulamalarının diğer internet uygulamalarından önemli bir farkı gerçek zamanlı aktarımın olmasıdır. Ses gerçek zamanda doğru, bütün ve gizli bir şekilde aktarılmalıdır. VoIP üzerindeki güvenlik tehditleri de bu noktalarda olmaktadır. VoIP uygulamaları, görüşme esnasında kötü niyetli kişilerin uygulamaya dışarıdan müdahale ederek görüşmelerin dinlenmesi, değiştirilmesi, kopyalanması, yavaşlatılması, engellenmesi, sesli mesajların e-posta spamlar gibi diğer kullanıcılara yayılması gibi bir çok tehdit ile karşı karşıya bulunmaktadır. Bu tehditler kullanıcılara zarar verdiği gibi internet trafiğini ve bant genişliğini de olumsuz etkilemektedir.

VoIP ses akışına kelimeler sokmak en çok karşılaşılabilen güvenlik tehditleri arasındadır. Bu saldırıda saldırgan hali hazırda konuşmakta olan iki kişinin akmakta olan VoIP trafiğine müdahale ederek araya kelimeler sıkıştırmaktadır. Bunu taraflardan sadece birisi duyabilir. Yani karşı taraf araya konan kelimelerinde sizin tarafınızdan söylendiğini sanmaktadır.

Diğer bir güvenlik tehdit de istenmeyen sesli mesajlar (spam) 'dır. Ses posta kutunuza binlerce istenmeyen ses kaydıyla karşı karşıya kalabilineceği gibi IP telefonununza bir çağrı geldiğinde karşıdaki kullanıcının bir bant kaydı olarak size otomatik olarak gönderildiği durumlar ile de karşılaşabilirsiniz. Yada yapılacak olan bir DoS saldırısı ile ses kalitesinde ciddi kayıplar veya kesilmeler yaşamak mümkündür.

Bu tarz tehditlere karşı ses paketlerini şifrelemek veya IP telefonlarda dijital sertifikalar kullanılması kısa vadeli çözümler içinde görülmektedir. Çünkü ses paketlerini şifrelemek araya giren saldırganları engellese de sistemin performansını aşırı derecede etkilemektedir. Ağ geçidi

kullanmakta çok etkileyici bir çözüm olarak görülmemektedir. Güvenlik duvarı ses sistemi ile tam bütünleşik çalışmadığı sürece konuşmayı kapatacağı zamanı kestirememesi önemli bir sorun olarak görülmektedir. Güvenlik duvarı konuşma biter bitmez konuşmanın olduğu UDP portunu kapatabilmelidir.

Tablo 5.1 VoIP protokolleri ve güvenlik açıkları

<table>
<tr><th colspan="4">Ses Uygulamaları</th></tr>
<tr><td colspan="2" rowspan="2">Oturum Başlatma Protokolü (SIP)</td><td rowspan="2">RTP Kontrol Protokolü</td><td>Ses Codecleri (G.711, G.726, G.728, G.729AB ve G.729E)</td></tr>
<tr><td>Gerçek Zamanlı İletim Protokolü (RTP)</td></tr>
<tr><td>TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

Tablo 5.1'de de görüldüğü gibi; arama sinyalleşmesi (SIP), ses mesajının iletilmesi (RTP), ve kontrol protokolü (RTCP) elverişli bir kullanıcı tanımlama, uçtan uca bütünlülük ve gizlilik sağlayamamaktadır. Bu sağlanamadığı sürece saldırganlar birçok güvenlik açığı bularak sistemlere müdahale etmeye devam edeceklerdir. Oluşabilecek güvenlik tehditleri aşağıda açıklanmaktadır [35].

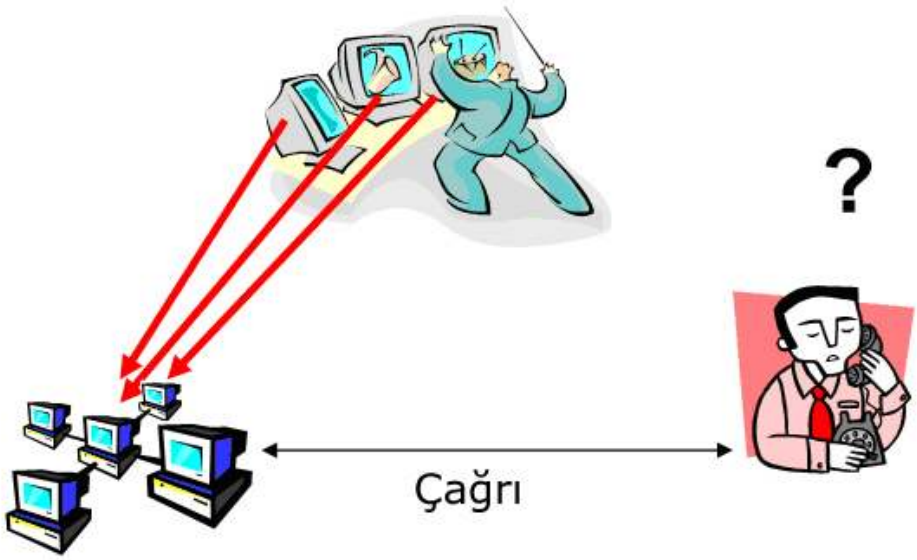
5.1 Hizmeti Engelleme (DoS) Güvenlik Tehditleri

DoS saldırısı, hizmeti engellemeye yönelik bir saldırıdır. DoS; bant genişliği, disk alanı, işlemci zamanı gibi kaynakları tüketmek; konfigurasyon bilgilerini bozmak; sistemin cevap veremeyeceği kadar çok sayıda istekte bulunmak ya da fiziksel network bileşenlerini bozmak gibi farklı şekillerde gerçekleştirilebilir.

DoS saldırısı SIP sinyalleşme protokolüne uygulanabilmektedir. TCP protokolündeki gibi kontrol paketleri (SYN, RST) bazlı bir saldırıdır. Saldırgan SIP sunucuya arama talebi veya kimlik tanımla paketleri yollayarak SIP sunucunun kaynaklarını tüketmek ve aktif aramaları düşürmek veya yeni aramalara meşgul cevabı aldırmak gibi sonuçlara kadar götürebilmektedir.

VoIP'e özel DoS saldırıları; VoIP sistemine çok sayıda yalancı SIP mesajının gönderilerek sistemin çalışamaz hale getirilmesi; SIP oturumunun sonlandırmak ya da 4xx, 5xx, 6xx cevap kodlarını kullanarak varolan SIP oturumlarını sonlandırmak şeklinde gerçekleştirilebilir. Oturumun başlamasından sonra kullanıcıya CANCEL ya da BYE mesajı göndererek oturumunu sonlandırmak şeklinde gerçekleştirilebilir. Böylece sistemin meşgul edilerek gereksiz bir trafiğin oluşması veya tamamen sistemin işlemez duruma gelmesi sağlanmaktadır.

5.1.1 SIP Bombardımanı DoS Saldırısı



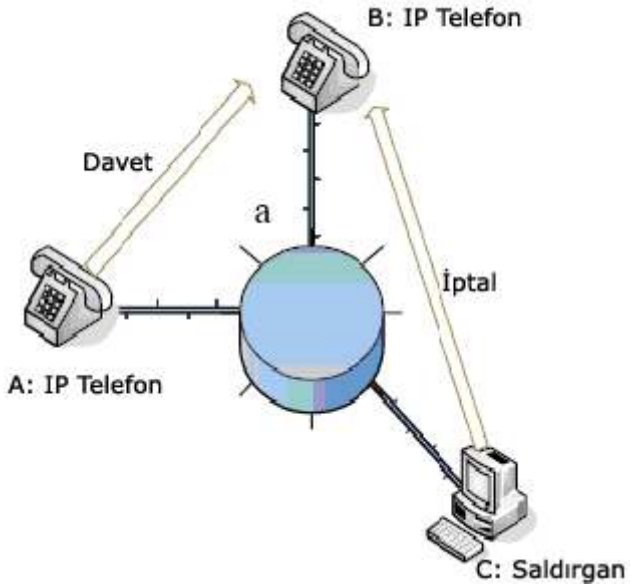
Şekil 5.1 SIP bombardımanı dos saldırısı

Şekil 5.1'de görülmekte olan SIP bombardımanı saldırısıdır. Bu saldırının amacı SIP sinyalleşme protokolünü etkisiz hale getirene kadar çok sayıda oturum başlatma talebinde bulunmaktır. Saldırgan, SIP sistemine aynı anda çok sayıda yalancı SIP mesajı ile oturum başlatma isteğinde bulunmaktadır. Gelen isteklerin sayısı, sistemin cevap verebileceğinden fazladır. Sistem kaynakları, bu istekleri işleyemeyecek şekilde meşgul olmaktadır. Aynı anda, sisteme kayıtlı olan kullanıcılar servis isteğinde bulunduğunda, sistem bu isteklere cevap verememektedir. Böylece DoS saldırısı amacına ulaşarak, sistem kullanıcılarına hizmet veremeyecek hale gelmiştir [35].

5.1.2 SIP Cancel / Bye DoS Saldırısı

Şekil 5.2'de SIP Cancel / Bye DoS saldırısına örnek bir gösterim sunulmaktadır. Şekil 5.2'de görüldüğü gibi A kullanıcısı B kullanıcısını mevcut VoIP sistemi üzerinden aramaktadır. A kullanıcısı B kullanıcısı ile çağrıyı başlatmak için INVITE mesajını gönderir. Saldırıda bulunmak isteyen C o anda ağı dinlemektedir. C, A kullanıcısından B kullanıcısına bir INVITE mesajı gittiğini farkettiği anda B kullanıcısına bir CANCEL mesajı gönderir. Böylece A kullanıcısından B kullanıcısına kurulmakta olan oturum sonlandırılmış olur. Burada saldırının başarılı olması için gerekli bazı koşullar vardır. Saldırganın göndermiş olduğu CANCEL mesajının call_ID'si ve mesaj sekans numarası, A kullanıcısının göndermiş olduğu INVITE mesajı ile uyumlu olmalı ve aynı zamanda saldırıda bulunan, B kullanıcısı, INVITE isteğine

cevap vermeden, yani iki kullanıcı arasındaki oturum kurulmadan önce CANCEL mesajını göndermesi gerekmektedir.



Şekil 5.2 SIP Cancel / Bye DoS saldırısı

Bu tür saldırının diğer bir şekli BYE mesajını kullanarak gerçekleştirilebilir. Aynı şekilde A kullanıcısı B kullanıcısını arar. Mesajlaşma tamamlanıp iki kullanıcı arasında oturum kurulur. Oturum kurulduktan sonra, kullanıcılar konuşmaya devam ederken herhangi bir anda, saldırıda bulunmak isteyen biri, kullanıcılardan birine BYE mesajı göndererek oturumu sonlandırabilir. Saldırıda bulunan, CANCEL mesajını kullanarak gerçekleştirilen saldırıdaki kriterlere dikkat etmelidir; yalnızca zamanlama konusunda diğer saldırıda olduğu gibi hız çok önemli değildir. Bu saldırı oturumun başlamasından sonlanmasına kadar ki herhangi bir zamanda gerçekleştirilebilir [35].

5.1.3 SIP 4xx, 5xx ve 6xx Mesajlaşma Kodlarını Kullanarak DoS Saldırısı

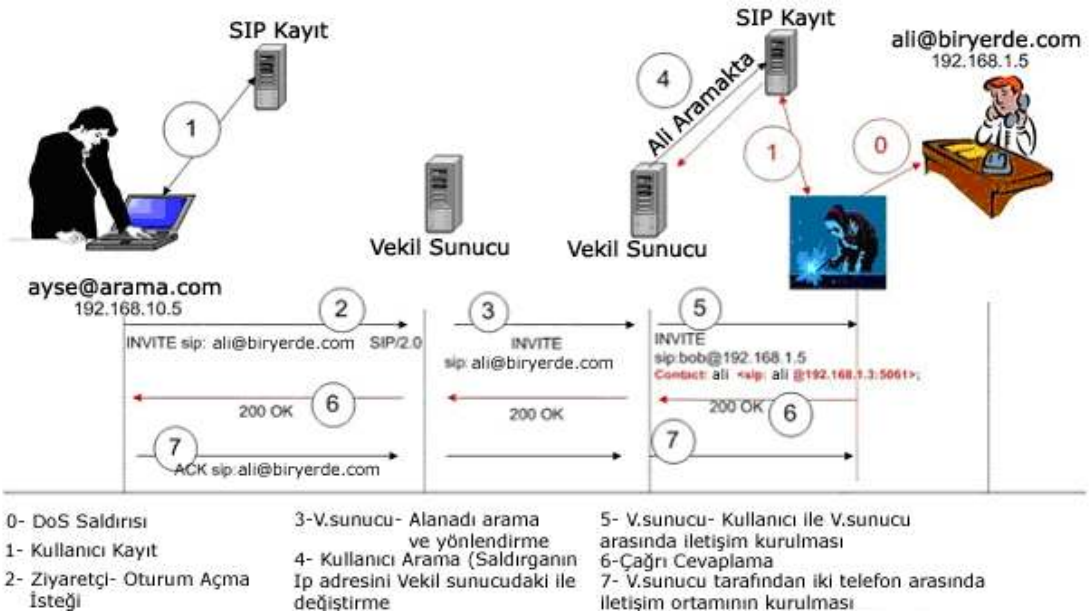
Bu saldırı tipinde, saldırgan, 4xx, 5xx ve 6xx cevap kodlarını kullanarak, mevcut bir SIP oturumunu sonlandırabilir. Sistemde varolan bir kullanıcı bir SIP isteğinde bulunduğunda, saldırıda bulunan, kullanıcıya 603-decline mesajı göndererek, isteğinin reddedildiğini bildirebilir. Böylece isteğin gerçekleşmesini engeller. Sisteme kayıtlı bir kullanıcı servis isteğinde bulunduğunda, saldırıda bulunmak isteyen biri kullanıcıya 480 temporarily unavailable mesajı göndererek istenen servisin ya da aranan kişinin geçici olarak ulaşılamaz durumda olduğunu bildirebilir. Aynı şekilde diğer cevap kodları kullanılarak da kullanıcıların servis alması engellenebilir [26].

5.2 Çağrı Kaçırma (Call Hijack) Saldırısı

Çağrı kaçırma saldırısı araya giren saldırganın, tarafların haberi olmadan iki taraf arasındaki mesajları okuyabilmesi ve değiştirebilmesi olarak tanımlanabilir. Çağrı kaçırma saldırısı, DoS ya da telekulak gibi diğer saldırı türlerini gerçekleştirmek için de kullanılmaktadır. Çağrı kaçırma saldırısı, saldırganın, taraflardan birinin yerine geçmesi durumudur. Bu saldırılar, kayıt bilgilerini değiştirmek (registration manipulation) veya 3xx cevap kodlarını kullanarak (call redirect) gerçekleştirilmektedir.

5.2.1 Kayıt Bilgilerinin Değiştirilmesi

İki kullanıcının aralarında bir oturum başlatması öncesinde ağ ortamını dinlemekte olan saldırganın sistemdeki kullanıcıların kayıt bilgilerini değiştirmesi ile kullanıcıya gelen isteklerin tümünün kendisine yönlenmesini sağlaması mümkündür. Yani kendisini iletişim kurulacak olan taraflardan birisi olarak tanıtması mümkündür. Oturumun başlatılması talebi için kullanılan SIP mesajlarının başlık kısımlarında ki kullanıcı bilgilerini değiştirerek saldırgan kendisini arayan veya aranan olarak gösterebilir. Aynı zamanda kayıt isteklerinin gönderilmesi için kullanılan UDP protokolü, bağlantısız bir protokoldür ve kolayca yanıltılabilir. SIP Registrar sunucusu, kayıt isteğinde bulunan kullanıcıları (UA), doğrulamak zorunda değildir ve genelde güvenilir olduğuna inanılan intranet içinde doğrulama yapılmaz. Doğrulama yapılsa bile, güçlü bir doğrulama algoritması kullanılmaz; yalnızca kullanıcı adı, şifre ve zaman damgasının MD5 şifreleme algıritması kullanılır. Kayıt bilgilerinin değiştirilmesi ile yapılan saldırıya bir örnek Şekil 5.3'de gösterilmektedir [35].



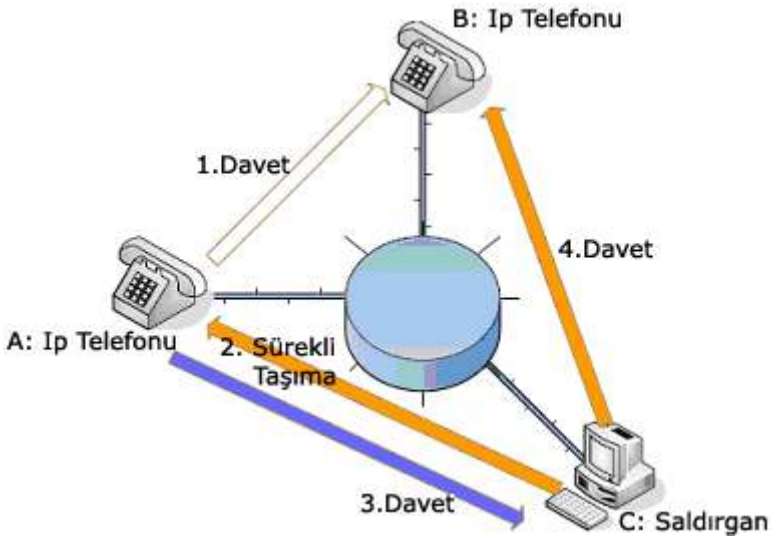
Şekil 5.3 Kayıt bilgilerinin değiştirilmesi örnek gösterim

Şekil 5.3'te, saldırgan, DoS saldırısında bulunarak bu kullanıcının terminalini iş göremez hale getirmektedir. Daha sonra SIP kayıt sunucuya Ali kullanıcısının kullanıcı adını kullanarak kayıt olma isteğinde bulunur ve böylece kayıt bilgilerini, Ali kullanıcısı saldırganın IP'sinden kayıt olacak şekilde değiştirir. Bu aşamadan sonra, Ali'nin kayıtlı olduğu SIP proxy'ye gelen tüm istekler, saldırganın IP'sine yönlendirilecektir. Örneğin şekilde görüldüğü gibi, Ayşe, Ali'yi aramak ister ve proxy'ye Ali'yi aramak üzere bir INVITE mesajı gönderir. Proxy, isteği Ali olduğunu zannettiği saldırgana gönderir, sinyalleşme tamamlanıp çağrı kurulduğunda, Ayşe, Ali ile konuştuğunu zannederken, saldırgan ile konuşmaktadır.

5.2.2 3xx SIP Mesajlaşma Kodlarını Kullanılması

SIP mesajlaşmasında 3xx cevap mesajları yönlendirme amacı ile kullanılmaktadır. Oturum başlatma isteğinde bulunan cihazın isteğin gerçekleştirilmesi için yapması gerekenler konusunda bilgilendirip ilgili yere yönlendirme işlemi 3xx mesajları ile yapılmaktadır. SIP saldırılarında 3xx cevap mesajları sahte cevaplar verilmesi amacı ile kullanılmaktadır.

SIP sistemine kayıtlı olan bir kullanıcı, bir SIP isteğinde bulunur. Ağ ortamını dinleyen kötü niyetli kullanıcı tarafından istekte bulunan kullanıcıya 3xx cevabı gönderir. Burada kötü niyetli kullanıcı, UA ya da SIP bileşenlerinden birinin yerine geçmiş bulunmaktadır. 3xx mesajını alan kullanıcının haberleşmesi, kötü niyetli kullanıcının istediği tarafa yönlenmiş olur. Bu saldırı tipine bir örnek Şekil 5.4'de gösterilmektedir.



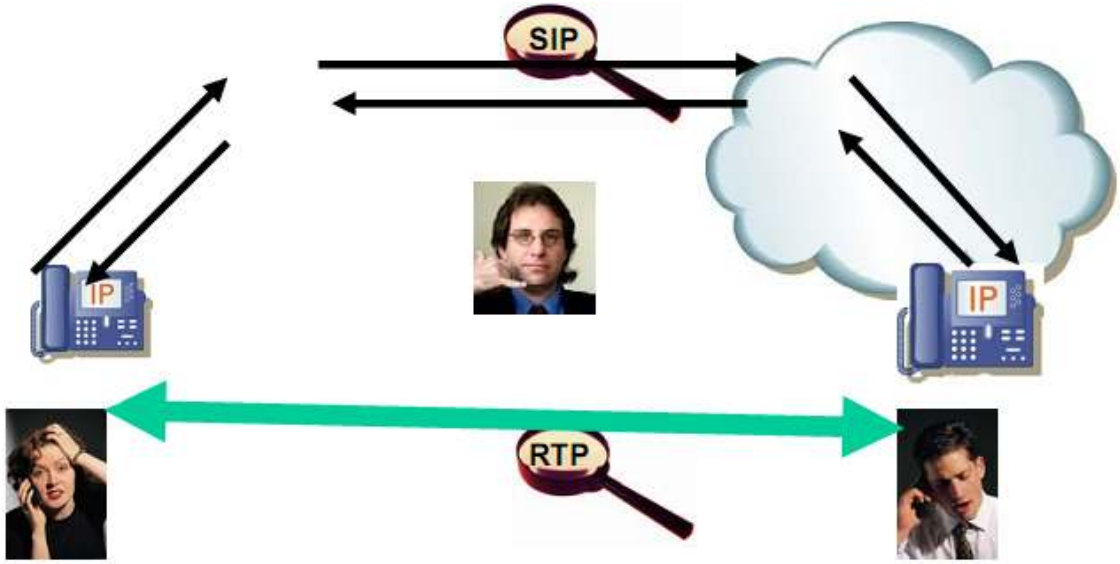
Şekil 5.4 3xx SIP mesajlarını kullanarak çağrı yönlendirme saldırısı örnek gösterim

5.3 Telekulak (Eavesdropping) Saldırısı

Bu saldırı tipi başkalarının gizli konuşmalarını gizlice dinleme anlamına gelmektedir. Bu saldırı tipinde, SIP sunucu ile SIP telefon arasındaki arama sinyalleşmesi esnasında saldırgan kullanıcının IPT kullanıcı adını, PIN numarasını ve SIP telefon numarasını çalabilir. Bunu

başarabilen bir saldırgan, her türlü kullanıcı bilgisini değiştirebilir. Mesela, bütün sesli mesajlarını silebilir, kullanıcının arama planını değiştirebilir, arama yönlendirme ayarlarını değiştirebilir veya en önemlisi konuşmayı tamamen kaydedip daha sonra dinleyebilir ve önemli bilgilere ulaşabilir, veya kullanıcının bilgilerini kendisine özel kullanarak bedava konuşma yapabilir.

IP telefon aramalarındaki bütünlülük, eğer mesaj veya paketlerde kimlik tanımlaması kullanılmaz ise sağlanamayabilir. Örneğin, saldırgan kendini arayan ve aranan arasına yerleştirerek (man-in-the-middle) gelen RTP paketlerini yollamayıp yerine kendi hazırladığı ses paketlerini yollayabilir. Özellikle kablosuz ağlarda buna araya kelimeler eklemek, gürültü yaratmak ve geciktirmek gibi saldırılarda eklenebilir. Şekil 5.5'te örnek bir telekulak saldırısı gösterilmektedir. [35]



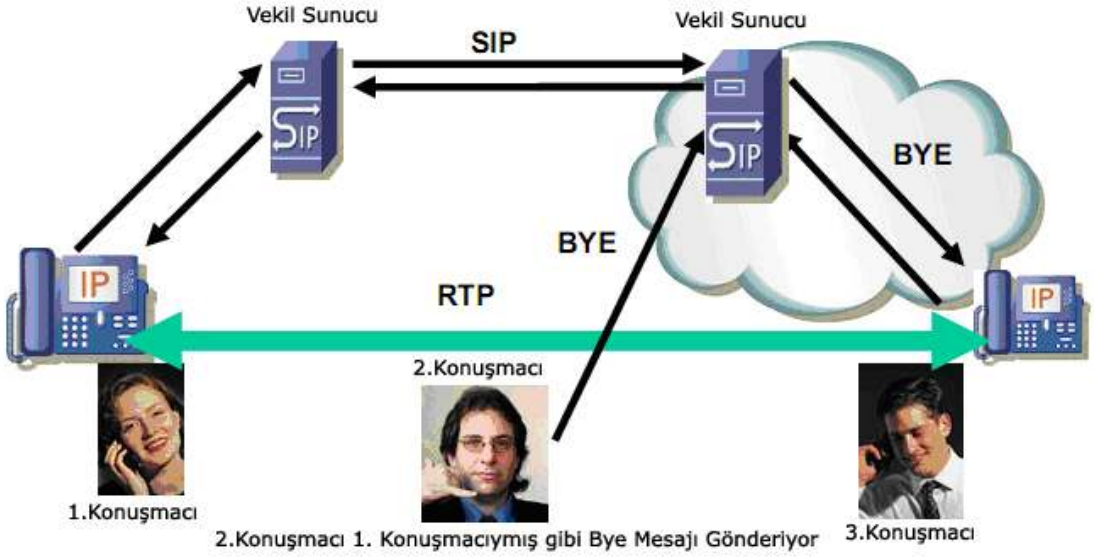
Şekil 5.5 Telekulak saldırısı örnek gösterim

VoIP ağında telekulak saldırısını kolaylaştıran etkenlerin başında, sesin iletiminde kullanılan RTP protokolünde şifreleme ya da doğrulama yapılmıyor olmasıdır. RTP başlığında PT (payload type) alanında kullanılan codec ile ilgili bilgi bulunmaktadır. İnternette kolayca erişilebilen, RTP trafiğini kaydetmeye yarayan araçları kullanarak RTP trafiğini kesip kaydeden biri, codec bilgisi de elinde bulunduğundan, bu RTP trafiğini daha sonra çözüp dinleyebilir ya da tekrarlama saldırılarısı gibi birçok saldırı amacıyla kullanabilir.

5.4 Yanıltma Saldırısı

Bu saldırı tipinde saldırgan kendi adres bilgilerini aranan kişi gibi göstererek arayan cihazı yanıltmaktadır. Saldırgan kendi kimlik bilgilerini gizleyip yanlış kaynak adresi kullanarak kendisini alıcı yada aranan olarak tanıtmaktadır. Böylece IP paketleri halinde veri doğru alıcıya değil saldırganın cihazlarına yönlenmektedir. Saldırganın bu sayede ağ trafiğini

dinleme veya tamamen trafiği ele geçirmesi mümkündür. Yani saldırgan isterse bu saldırı yöntemi ile arayan ile aranan kullanıcıların veri iletimini kendi üzerinden geçirerek sadece dinleme yapabileceği gibi tamamen trafiği kesebilir veya kendi aranan kullanıcıymış gibi arayan kullanıcı ile iletişim sağlayabilir. Bu saldırı tipi özellikle kimlik ve özel bilgilerin ele geçirilmesi için kullanılmaktadır. Şekil 5.6'da örnek bir yanıltma saldırısı gösterilmektedir. [26]



Şekil 5.6 Yanıltma saldırısı örnek gösterim

5.5 Spit (İnternet Telefonu Üzerinden Spam Gönderimi) Saldırısı

Günümüzde internet alt yapısının önündeki en büyük tehditlerden birisi istenmeyen e-postalardır. İstenmeyen metin tabanlı e-postalar internet trafiğinin büyük bir bölümünü oluşturmakta ve gün geçtikçe bu oran büyümektedir. İnternet teknolojilerinin yaygınlaşması ile birlikte ses iletimi için kullanılan VoIP uygulamaları gün geçtikçe popülerlik kazanmaya başlamıştır. VoIP uygulamalarının bir çok avantajı vardır. Bu avantajların en önemlisi IP bazlı bir iletişim teknolojisi olması sebebi ile maliyetin düşük olmasıdır. Maliyetin düşük olması, kötü niyetli kullanıcıların bu teknolojiyi farklı amaçlar ile kullanmalarına olanak sağlamaktadır. Özellikle reklam amaçlı sesli mesajların otomatik olarak VoIP cihazlarını meşgul etmesi metin tabanlı istenmeyen e-postalardan çok daha fazla tehdit oluşturmaktadır. VoIP uygulamalarının IP tabanlı bir iletişim teknoloji olması sebebi ile gelen sesli mesajların veya bant kaydı olan çağrıların kimliğini tespit etmek veya tamamen engellemek büyük bir sorundur. Bu nokta da VoIP üzerindeki istenmeyen sesli mesajlar ile metin tabanlı istenmeyen e-postalar örtüşmektedir. VoIP üzerindeki istenmeyen sesli mesajların, istenmeyen metin tabanlı e-postalardan en önemli farkı gönderilen içeriğin metin içerikli olması yerine ses içerikli bir dosya

olmasıdır. Bu içeriğin ses dosyası olması dosya boyutunun çok daha büyük olacağı ve internet üzerinde oluşabilecek trafiğin çok daha fazla olacağı anlamına gelmektedir.

VoIP üzerindeki istenmeyen sesli mesajlara SPIT (IP telefonlar üzerindeki Spam) adı verilmektedir. Spit VoIP iletişim teknolojisini kullanan kullanıcılara karşı olarak yapılan bir saldırı niteliği taşımamaktadır. Spit internet üzerindeki trafiğin artmasına yönelik çok önemli bir tehdit olarak ortaya çıkmaktadır. Asıl amaç ticari faaliyet gösteren firmaların reklamını çok düşük maliyetlere yapabilmeleri, propaganda amaçlı kullanım veya tamamen kötü niyetli kullanıcılar tarafından kullanıcıların özlük bilgilerinin elde edilerek ticari amaçla kullanmasıdır.

VoIP spam saldırısı genel olarak SIP veya H.323 işaretleme protokollerinin açıklarından yararlanılarak gerçekleştirilmektedir. Genel olarak güvenli bir iletişim için bütünlük, doğruluk ve kişisel gizlilik ilkelerinin sağlanması gerekmektedir. Ancak IP telefonların PSTN haberleşmesindeki gibi sabit bir telefon numarası yapısına değil, daha çok bir e-posta adresine benzemesi bu güvenliğin sağlanabilmesini karmaşıklaştırmaktadır.

6 IP ÜZERİNDEN SES İLETİMİ ESNASINDA HARİCEN OLUŞABİLECEK İSTEM DIŞI TEHDİTLERE KARŞI ALINABİLECEK TEDBİRLER

Beşinci bölümde VoIP uygulamalarına karşı oluşacak tehditler anlatıldı. Bu tehditler kullanıcıları etkileyebileceği gibi internet bant genişliğinin gereksiz yere kullanılarak trafiğin artması şeklinde de olabilmektedir. Bu bölümde, IP üzerinden ses iletimi esnasında oluşabilecek tehditlere karşı çözüm yöntemleri sunulacaktır. Çözüm yöntemleri incelenirken öncelikle genel olarak alınması gereken tedbirler ve çözüm yöntemleri sunulacak, internet telefonu üzerinde istenmeyen sesli mesajların (SPIT) diğer saldırı yöntemlerinden yapısal farklılıkları olduğu için ayrı çözüm yöntemleri sunulacaktır [35].

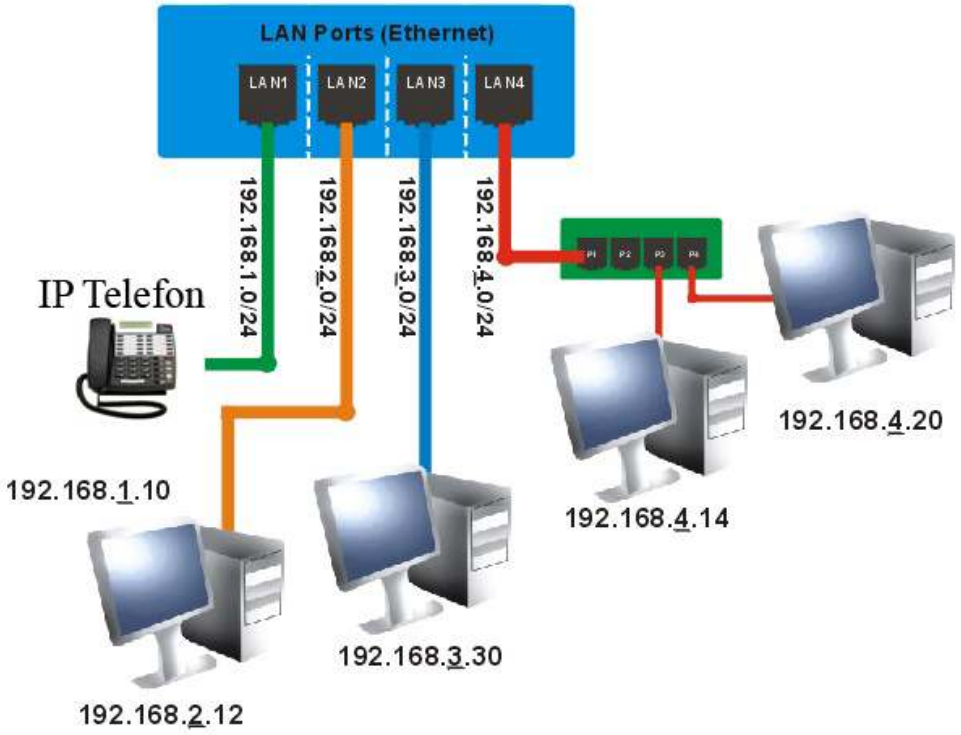
6.1 Genel Çözüm Önlemleri

İnternet ağını tehdit eden tüm tehlikeler, internet teknolojisini kullanması sebebi ile VoIP uygulamalarını da tehdit etmektedir. Bu nedenle VoIP iletişiminin güvenli yapılabilmesi için öncelikle internet ağı üzerindeki güvenlik önlemlerinin alınması gerekmektedir.

6.1.1 İnternet Ağ Güvenliği

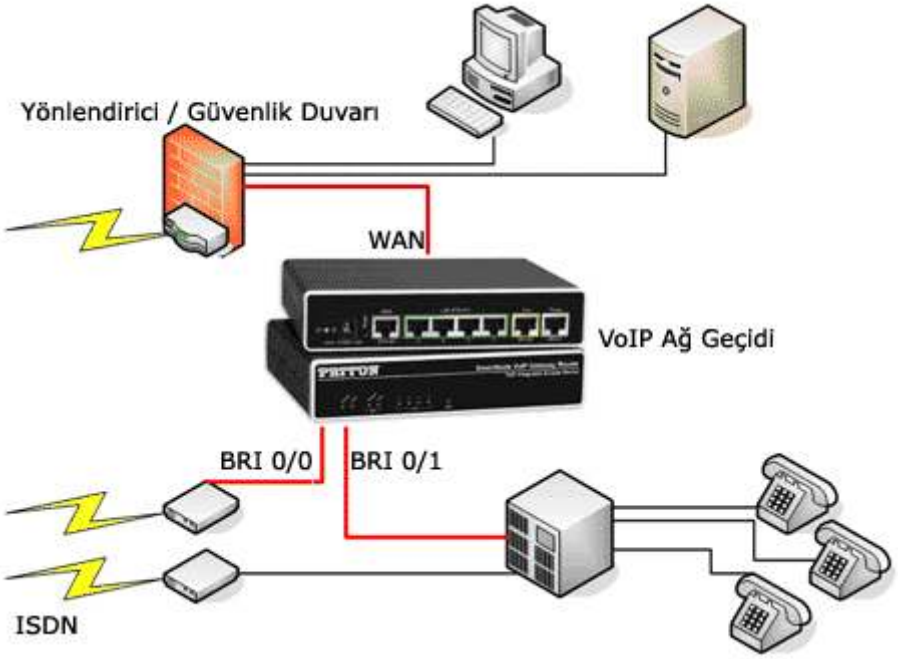
Veri iletiminin yapıldığı bir ağ ortamına yapılacak olan saldırı tüm ağ üzerindeki iletişime zarar vermesi mümkündür. Bu zarar tamamen iletişimin kesilmesi, trafiğin çok yoğun bir hale getirilerek yavaşlatılması, verilerin çalınması, silinmesi veya tahrip edilmesi şeklinde olabilir. İnternet ağ güvenliği için alınması gereken önlemler aşağıda listelenmektedir.

- VoIP güvenliği için alınması gereken ilk önlem VoIP veri akışı ile diğer veri akışlarının birbirinden ayrılması yöntemidir. Bunun için ses ve veri trafiğini bir birinden ayırmak için VLAN yapısı kullanılmalıdır. Ses ve veri iletimi için oluşturulan VLAN'lar arasındaki erişim kısıtlanarak veri trafiğine yapılacak bir saldırının VoIP uygulamalarına zarar vermesi engellenmelidir. Şekil 6.1'de ses ve veri akışını bir birinden izole eden bir VLAN yapısı gösterilmektedir [35].
- VoIP cihazları yönetilebilen cihazlardır. Bu yönetim cihazların başında iken olabileceği gibi uzaktan erişilerekte yapılması mümkündür. İnternet ağındaki önemli saldırı tiplerinden biriside uzaktaki cihaza telnet erişimi ile cihazı ele geçirmektir. Aslında telnet güvenli bir şekilde uygulama cihazlarının uzaktan yönetilmesi için geliştirilmiş uygulamadır. Ancak sistem yöneticilerinin bilgi eksikliği veya sistemdeki güvenlik açıkları sebebi ile kötü niyetli kullanıcıların açıklardan yararlanarak sisteme müdehale etmelerini kolaylaştırmaktadır. Bu yüzden VoIP ağında bulunan sunuculara kötü niyetli kişilerin erişimini engellemek amacı ile telnet erişimlerinin kısıtlanması veya tamamen kapatılması gerekmektedir [35].



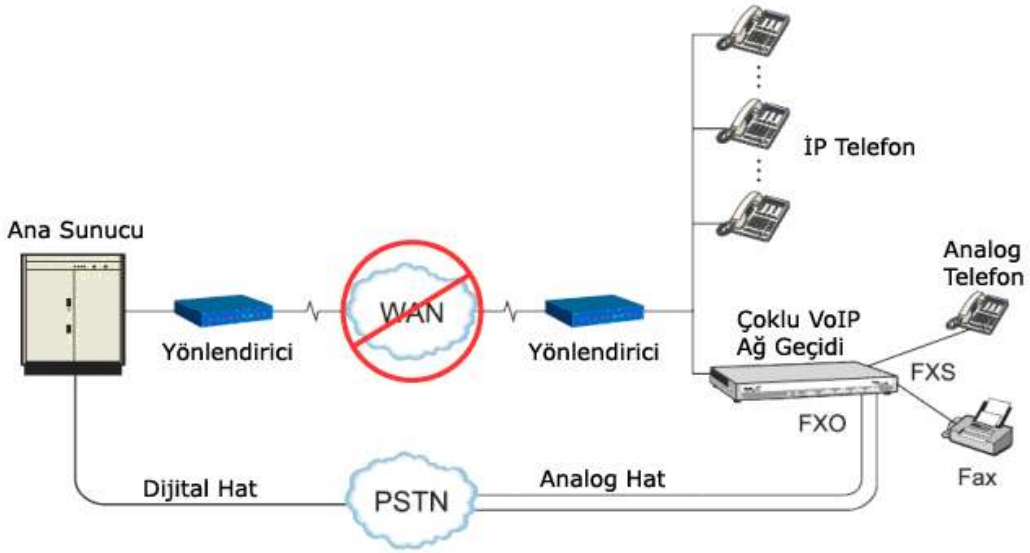
Şekil 6.1 Ses ve veri trafiğinin VLAN yapısı ile izole edilmesi

- VoIP güvenliği için alınması gereken diğer bir önlem ise güvenlik duvarı (firewall) kullanımıdır. VoIP iletişiminin kurulması için öncelikle oturumun sinyalleşme protokolleri tarafından açılması gerekmektedir. Oturumun başlatılmasından sonra ses verisinin taşınması işlemi başlamaktadır. Sinyalleşme protokolleri oturumu başlatırken paket iletimi SIP proxy ile kullanıcılar arasında olmaktadır. Ses verisinin taşıması ise uç noktalar arasında paketlerin iletilmesi şeklinde olmaktadır. Paket iletimi port bazlı bir iletişim olduğu için portların güvenlik altına alınması gerekmektedir. İletim esnasında portların dinlenmesinin önlenmesi veya ilgili porta doğru verinin iletilmesi için güvenlik duvarlarının kullanılması gerekmetedir. Aynı zamanda güvenlik duvarlarının kullanılması telekulak saldırılarına karşı alınabilecek önlemlerden birisidir. Şekil 6.2'de bir VoIP uygulamasında güvenlik duvarı kullanımına ait örnek bir gösterim sunulmaktadır.



Şekil 6.2 VoIP ağlarda güvenlik duvarı kullanımı

- Herhangi bir saldırı karşısında IP tabanlı ağın kesintiye uğraması durumunda VoIP ağ üzerindeki iletişimin PSTN ağ üzerinden devam edebilmesi sağlanmalıdır. DoS saldırıları gibi ağa yönelik saldırılara karşı ağ üzerinden iletişimin yapılamadığı durumlarda yedek bir hattın devreye girmesinin sağlanması gerekmektedir. Şekil 6.3'de internet ağının kesintiye uğraması durumunda PSTN modülü devreye girerek iletişimin kesintisiz devam etmesi durumu gösterilmektedir.

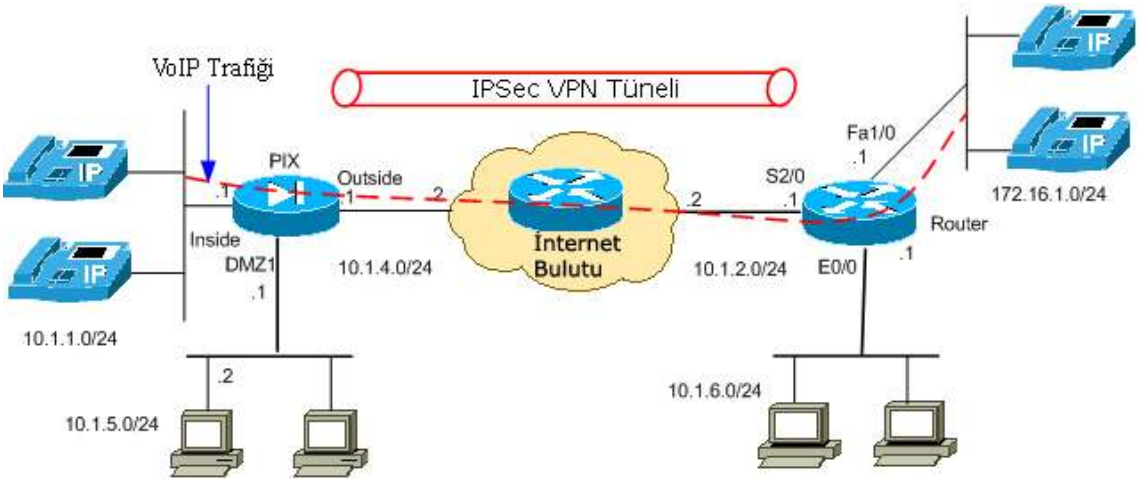


Şekil 6.3 Kesintisiz iletişim için örnek gösterim

- Ses ve sinyalleşme paketleri şifrelenerek alıcıya gönderilmeli ve alıcı tarafta şifre çözülerek veri alımı gerçekleştirilmelidir.

6.1.2 IPSec VPN Tüneli Oluşturmak

İki veya daha çok kullanıcı arasında oturumun başlatılması, yönetilmesi ve sonlandırılması için kullanılan SIP mesajlaşmasının ağ katmanında güvenli bir şekilde yapılabilmesi için IPSec VPN tünelleri kullanımı yaygın olarak kullanılan güvenlik önlemlerinden birisidir. Bu güvenlik önlemi genellikle iki ucu belli olan oturumlar için kullanılmaktadır. Bir üniversite ağında kampüsler arası iletişim veya bir kurumun şubeleri ile iletişimi için kullanılan VoIP uygulamalarında IPSec VPN tünellerinin kullanımı oldukça başarılı bir güvenlik önlemidir. IPSec, ulaşım kipi ve tünel olmak üzere iki yapıda incelemek mümkündür. Ulaşım kipinde sadece veri şifrelenirken, çok daha güvenli olan tünel yapısı paket başlığını ve verinin tümünü şifreleyerek alıcıya gönderme şeklidir. Bu yöntemde gerçekleme, mesaj bütünlüğü ve ulaşım kontrolü sağlanmış olur. Böylece verinin şifrelenerek gönderilmesinden dolayı kişisel gizliliğide sağlamak mümkün olmaktadır. IPSec VPN tünellerin kullanılması tekrarlama saldırılarına karşı önemli bir güvenlik yöntemidir. SIP mesajlaşmasının şifrelenerek IPSec VPN tünelleri üzerinden iletiminin sağlanması paket başlıklarına ek yük getireceğinden gerçek zamanlı iletişim için bant genişliğinin yeterli seviyede olması gerekmektedir. Şekil 6.4'te IPSec VPN tüneli kullanılarak gerçekleştirilen bir VoIP uygulaması görülmektedir [35].



Şekil 6.4 IPSec VPN tüneli uygulaması örnek gösterim

6.1.3 İletim Katmanı Güvenliği

VoIP uygulamalarında oturum başlatmak amacı ile kullanılan SIP protokolünün kullandığı SIP mesajlarının iletim katmanında güvenli bir şekilde aranan kullanıcıya

ulaştırılması çok önemlidir. Özellikle ağ ortamını dinleyen kötü niyetli kullanıcıların yapacağı saldırıları engelleyebilmek için arayan ile aranan kullanıcıların oturumunun başlatılması aşamasındaki mesaj trafiğinin güvenli bir şekilde işletilmesi gerekmektedir. İletim katmanı güvenliği (TLS), güvenli oturumların kurulmasına olanak sağlamaktadır. TLS protokolü SIP oturumunun kurulması için gerekli olan istemci/sunucu iletişimini kurmaktadır. Bunun için simetrik anahtarlı şifreleme algoritmaları ve istemci/sunucu arasında doğrulama ve şifreleme algoritmaları kullanmaktadır.

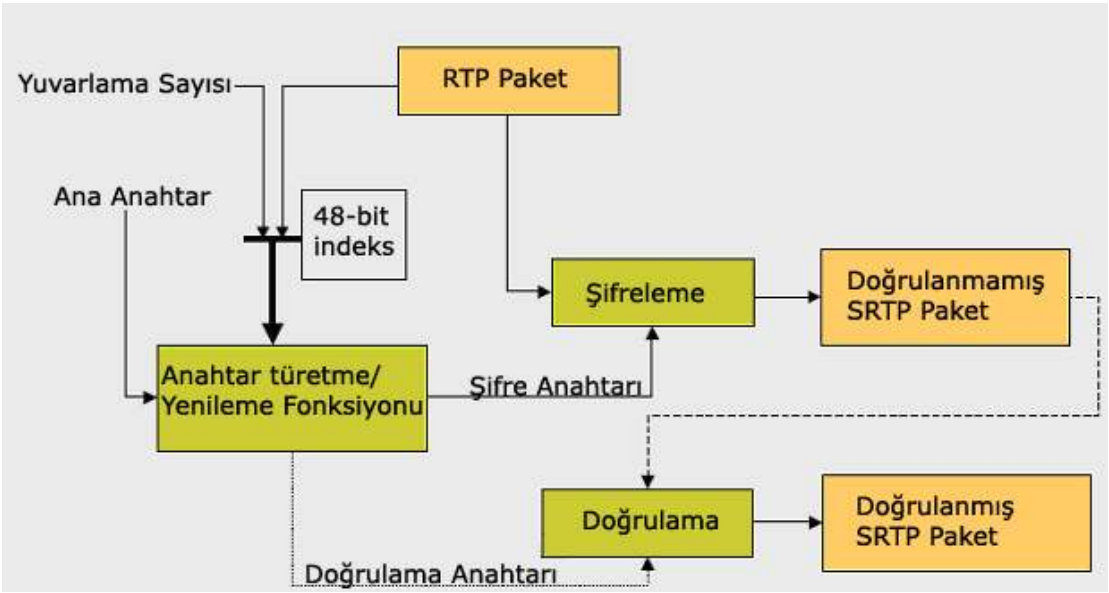
6.1.4 Güvenli Gerçek Zamanlı İletim Protokolü

SRTP, RTP protokolü kullanılarak iletilen verinin çok daha güvenli bir şekilde iletilmesi için IETF tarafından yayınlanmış bir protokoldür. Gerçek zamanlı olarak iletilmesi gereken veri RTP protokolü ile iletilmektedir. RTP protokolü, paketleri şifreleme, gizlilik, doğrulama gibi güvenlik önlemleri almadan iletmektedir. Bunun sebebi paket büyüklüğünü arttırarak sisteme ekstra yükler yüklememektir. İletilecek paket ne kadar büyük olursa sistem o kadar yavaş çalışacaktır. Bu yüzden RTP paketleri yalın halleri ile transfer etmektedir. Bu sayede veri gerçek zamanda iletilebilir. Bu şekildeki yalın paketlerin iletimi de bir çok güvenlik açığı ortaya çıkartmaktadır. Son zamanlarda gelişen internet teknolojisi ve bant genişliği miktarlarının yeterli miktarlara gelmesi paketlerin daha hızlı iletimine imkan sağlar hale gelmiştir. 2004 yılından itibaren IETF tarafından yayınlanan SRTP protokolüde bu gelişim sürecinde RTP protokolünü daha güvenli hale getirmeyi amaçlamaktadır. SRTP, doğrulama, şifreleme, gizliliğin sağlanması gibi bir çok özelliği RTP protokolüne eklenmiş halidir. Aynı zamanda SRTP paketlere gelecek olan yüküde minimum seviyeye çekmektedir. Böylece SRTP, RTP kadar hızlı aktarım yaparken aynı zamanda da güvenilir bir iletişim protokolü sunmaktadır.

SRTP'nin RTP ile karşılaştırıldığında sağladığı birçok avantaj bulunmaktadır. RTP ve RTCP için yük şifrelenmesi ile sağlanan güvenilirlik, tekrarlama saldırısına karşı koruma ile birlikte, RTP ve RTCP için mesaj bütünlüğünün sağlanması, oturum anahtarlarını periyodik olarak yenileme imkanı ile belli bir anahtar tarafından üretilmiş şifreli metin miktarını azaltmak, güvenli bir oturum anahtarı üretme algoritması (her iki uçta pseudo-random fonksiyon ile) tekli ve çoklu RTP uygulamaları için güvenlik SRTP'nin avantajları arasında sayılabilir. Şekil 6.5'de SRTP başlık yapısı görülmektedir.

Şekil 6.5 SRTP başlığı [35]

Şekil 6.6'da görüldüğü gibi SRTP, RTP mesajının sekans numarası ve ROC kullanılarak 48 bitlik index hesaplanır. Index ve master anahtar, anahtar elde etme ve yenileme fonksiyonundan geçirilerek biri şifreleme anahtarı ve diğeri asıllama anahtarı olmak üzere iki anahtar elde edilir. Şifreleme anahtarı kullanılarak RTP paketi şifrelenir. Şifrelenmiş olan metin, doğrulama anahtarı kullanılarak doğrulanmış SRTP paketi elde edilir. Böylece SRTP, RTP paketlerini şifreleme, doğrulama ve gizlilik ilkelerini uygulayarak daha güvenilir bir iletişim ortamı gerçekleştirilmiş olmaktadır.



Şekil 6.6 SRTP akış yapısı [35]

6.2 VoIP Üzerinde Oluşacak İstenmeyen Sesli Mesajlara Karşı Önlemler

VoIP iletişiminde oluşabilecek tehditlerden biriside yapısal olarak istenmeyen e-postalar ile benzerlikleri bulunan istenmeyen sesli mesajlar veya istenmeyen görüşme istekleridir. Bu tehlike sistemi kullanan kullanıcılardan çok internet trafiğinin artmasına yönelik bir tehdit oluşturmaktadır. VoIP iletişiminin diğer iletişim yöntemlerine göre çok daha uygun maliyetli olması sebebi ile bu iletişim ortamını, istenmeyen metin tabanlı e-postalarda olduğu gibi kendi çıkarları doğrultusunda kullanacak kötü niyetli kullanıcıların çıkması kaçınılmazdır.

İstenmeyen e-postalar ile VoIP üzerindeki istenmeyen mesajlar arasındaki en önemli fark mesajın içeriğidir. İstenmeyen e-postalar genel olarak metin tabanlı olarak karşımıza çıkarken VoIP üzerindeki istenmeyen mesajlar ses dosyası şeklindedir. VoIP üzerindeki istenmeyen mesajların içeriğinin ses dosyası olması, istenmeyen metin tabanlı e-postaları önlemek için kullanılan güvenlik önlemlerinin bir çoğunun VoIP üzerindeki istenmeyen mesajların önlenmesi için kullanılmasını olanaksız hale getirmektedir. VoIP üzerindeki bu tehlikenin e-posta iletişimindeki tehlikeye göre en büyük avantajı ise henüz VoIP üzerindeki uygulamaların çok yaygınlaşmamış olması ve henüz büyük çapta saldırıların gerçekleşmemiş olmasıdır. Bu yüzden VoIP üzerindeki spam tehditinin oluşmadan engellenmesi önem arz etmektedir.

İstenmeyen metin tabanlı e-postalar önlemek için geliştirilen metodların bir kısmı VoIP üzerinde oluşabilecek istenmeyen sesli mesajlara karşıda koruyucu etki göstermektedir. Bazı çözüm metodlar ise hiç fayda sağlamamaktadır. VoIP üzerindeki istenmeyen sesli mesajların önlenerek ağ üzerindeki gereksiz trafiğin önlenmesi için geliştirilen metodlar aşağıda açıklanmaktadır.

VoIP üzerindeki istenmeyen sesli mesajları yani VoIP spamları engellemek için kullanılan metodlar anlatılırken faydasız olan metodlardan da bahsedilmesinin yararlı olacağı düşünülmüştür.

6.2.1 İçerik Filtreleme

Metin tabanlı istenmeyen e-postaların önlenmesinde etkili bir metod olan içerik filtreleme VoIP spamların önlenmesinde kullanılamamaktadır. E-postaların mesaj içeriğinin metin tabanlı olması sebebi ile metin üzerinde gerekli kelimelerin veya kalıpların aranması mümkündür. Fakat VoIP iletişiminde mesaj tipinin ses içerikli olması ve çoğu zaman bu iletişimin gerçek zamanlı olarak gerçekleştirilmesi yüzünden ses içeriğinin incelenerek bir filtreleme yapılması söz konusu değildir. VoIP iletişiminde iki veya daha çok kullanıcı arasında oturumun başlatılması VoIP protokolleri konusunda anlatılmıştı. VoIP üzerinden sesli spam gönderecek olan kullanıcı oturumu başlatmak amacı ile diğer kullanıcıyı aradığında, alıcının bu oturumu kabul etmesi ile birlikte spam içerikli mesaj alıcıya iletilmiş olmaktadır. Bu noktada VoIP uygulaması üzerinden sesli spam gönderecek olan kullanıcının, bu işlemi tek tek kullanıcılara arayarak değilde metin içerikli e-posta spamlarının iletiminde olduğu gibi otomatik olarak birçok kullanıcıya aynı anda iletildiğinin unutulmaması gerekmektedir. Bu iletim esnasında kullanılacak ses analiz programları ile bir tespitin yapıllması veya ses mesajını metin tabanlı içeriğe çevirip metin tabanlı bir içerik filtreleme yönteminin kullanılarak bir önlem almaya çalışmakta kullanılan cihazlara çok fazla yük getireceğinden dolayı etkili bir yöntem değildir.

6.2.2 Girişken Spam Önleme Modeli

Girişken spam önleme modelini yanlış bilginin aktif olarak yayımı ve yanıltıcı spam saldırıları olmak üzere iki tip saldırıyı engellemek için kullanılmaktadır [40]. Bu saldırıları spam üreticisinin bilinmeyen veya yanıltıcı bir SIP adresi kullanarak bir veri tabanındaki kayıtlı kullanıcılara spam yayma işlemi olarak adlandırmak mümkündür. Kullanılan bu teknik oldukça etkili bir yöntemdir. Yanıltıcı bir SIP adresi kullanarak spam üretici kullanıcının kimliğini gizlemesi mümkündür. Bu saldırıya karşı yapılacak URL kontrolü faydalı olamamaktadır. Mesajı gönderen kullanıcının SIP adresinin sürekli değişmesi yüzünden URL adresi sürekli değişmekte ve içeriği aynı olan sesli mesajın farklı kullanıcılardan geliyormuş gibi gösterilmesi ile saldırı gerçekleştirilmektedir. Adres şaşırtarak aynı anda bir çok adresten gelen mesajlar ile bir cihaza saldırmak mümkündür. DoS saldırılarına benzerliği açısından oldukça tehlikeli bir saldırı yöntemidir ve URL kontrolü, içerik filtreleme gibi yöntemler ile çözüm bulunamamaktadır [41].

6.2.3 Hacim Tabanlı Model

Bu model e-posta veya VoIP üzerindeki istenmeyen mesajlar için kullanılabilecek ortak bir saldırı önleme metodudur. Bu metodun servis sağlayıcı kuruluşun kullanıcılara günlük belli bir oranda kullanım kotası koyması yöntemidir. Bu yöntemin avantajı her kullanıcı belli bir kotayı aşamayacağı için spam yayımının istenen limitler içerisinde kalmasını sağlamak mümkündür. Ancak her servis sağlayıcının kota koyma işlemini uygulamaması veya spam saldırısı gerçekleştiren kullanıcıların servis sağlayıcı olması durumunda bu model işlevselliğini yitirmektedir. Bu modeli tek başına bir yöntem olarak kullanmak sınırları servis sağlayıcı kuruluşlara bıraktığı için geçerli bir yöntem olarak görülmemektedir [41].

6.2.4 Kaynak Filtreleme – Kara Liste Modeli

İstenmeyen e-postaların engellenmesinde de uygulanan bu yöntem VoIP uygulamalarında da faydalı sonuçlar vermektedir. VoIP iletişiminin internet ağını ortam olarak kullanması yani IP bazlı bir iletişim yöntemi olması itibari ile tespit edilen IP adreslerinin engellenerek, engellenmiş IP adreslerinden çağrı veya oturum başlatma isteklerinin engellenmesi mümkündür. E-posta spamları anlatılırken de bahsedilen kara listelere giren IP adreslerinin erişimlerinin kısıtlanması ile bu IP adreslerine karşın bir çözüm geliştirmek mümkündür. Ancak spam yayıcı kuruluşların bu listelere girmemiş IP adreslerinden yaptıkları spam saldırıları olursa, bu saldırılar kara listeler tarafından tespit edilene kadar kaynak filtreleme metodu ile bir engelleme yapılamaz. Kara listeler uluslar arası belli kuruluşlar tarafından oluşturulmaktadır. Bu listeler tüm kullanıcıların kullanımına açıktır. Bu listelerden proxy sunucuda veya telefon üzerindeki yapılacak ayarlamalar ile yararlanmak mümkündür. Kaynak filtreleme günümüzde kısıtlı IP

adresinin olması yüzünden olumlu sonuçlar vermektedir. Ancak IPV6 ile birlikte IP adreslerinin yetersizliğinin ortadan kalkması sonucunda IP adresi değiştirmek çok daha kolay olacağı için kaynak filtreleme modelinin etkileri azalacaktır.

6.2.5 Göndericinin Tanınması ve Yetkilendirilmesi

Metin tabanlı e-posta gönderiminde VoIP iletişiminde olduğu gibi başlık kısmında kimlik bilgileri bulunmaktadır. Ancak spam saldırısı yapmak isteyen kullanıcılar genel olarak kimliklerini gizlemek için bu bilgileri gizler veya yanlış bilgiler ile bu işlemi gerçekleştirir. VoIP iletişiminde de aynı durum söz konusudur. Ancak e-posta ile VoIP iletişimi arasındaki önemli fark VoIP iletişiminde çağrı geldiğinde kullanıcı çağrıyı red edebilir. Fakat e-posta iletişiminde durum farklıdır. Bir e-posta iletişimi kurulmak istendiğinde gönderilen ileti e-posta adresine gelmektedir. Yani internet üzerindeki trafiği kullanmaktadır. Bu yüzden e-posta spam saldırılarında kimliğin gizli olup olmamasının iletişimi kesmeye olumlu bir etkisi bulunmamaktadır. VoIP iletişiminde ise kimliği belli olmayan çağrılar veya yetkilendirilmemiş kullanıcılar tarafından gelen çağrılar SIP veya H.323 protokolünde bulunan başlıklar incelenerek engellenebilir [42]. Yine SIP ve H.323 protokolleri ile oturum başlatılırken şifrelenmiş yetkilendirme algoritmaları kullanarak daha güvenli bir oturum başlatma süreci oluşturmak mümkündür [43]. Göndericinin yetkilendirilmesi ve tanınması modeli e-posta spamlarına göre çok dahi iyi sonuçlar vermektedir.

6.2.6 Beyaz Liste Modeli

Kara liste modeline zıt bir modeldir. İki tür yapılandırma söz konusudur. Birinci yapılandırma kullanıcının kendisi tarafından yapılmaktadır. Kullanıcı gelen görüşme taleplerini değerlendirerek görüşme yapmakta sakınca bulmadığı çağrıları beyaz listeye alabilir. Buna bir iletişim listeside diyebiliriz. İkinci yapılandırma ise sistem yöneticisi tarafından yapılmaktadır. Bu yapılandırma da yerel ağ içinde her kullanıcı bir birini arayabilir. Yerel ağ dışından arayan kullanıcılar için VoIP sunucu üzerinde güvenlik ayarı yapılmalıdır. Güvenli kullanıcıların bilgileri VoIP sunucuya ekleyerek, onların yerel ağ kullanıcıları ile iletişim kurmasını sağlamak mümkündür [44].

6.2.7 Gri Liste Modeli

Bu model e-posta spamlarını engellemek için kullanılan modele benzemektedir. Bu modelde çağrı geldiğinde aynı ağ içinde aynı IP adresinden N saat/dakika da gelen çağrı sayısına bakar. Çağrı sayısı limitlerin üzerinde bir sayıda ise çağrıyı engellemek mümkündür. Gri liste uygulamasına spam saldırısı yapanların yakalanmadan saldırı yapmaları mümkündür. Eğer bir yazılım ile otomatik olarak spam saldırısı yapılıyorsa, spam gönderme oranları

ayarlanarak limitlerin içinde kalınabilir. Bu yüzden gri liste modeli profesyonel spam saldırılarında çok etkili olamamaktadır [45].

6.2.8 Hafızaya Bağlı Fonksiyonlar Modeli

Spam saldırısı yapan kullanıcılar günlük milyonlarca mesaj yollayabilmektedir. Hafızaya bağlı fonksiyonlar modeli spam saldırılarını tamamen önlemek yerine oranını düşürmek için geliştirilmiş bir tekniktir. Bu modelde bir kullanıcının gün içinde gönderebileceği maksimum mesaj sayısına göre bir hesaplama zaman katsayısı ortaya atılmıştır. Bu hesaplamaya göre örnek olarak on saniyede bir mesaj gönderen bir kullanıcı gün içinde toplam 8640 mesaj gönderebilmektedir. Spam saldırıları göz önüne alındığında bu rakam çok düşük bir değerdir. Hesaplama zaman katsayısı kullanılarak belirlenen günlük limitin üzerine çıkan mesajlar engellenmektedir. Böylece spam saldırılarını tamemen engellemek yerine oranını düşürmek mümkün olmaktadır [46].

6.2.9 Arayan_ID Yaklaşımı

VoIP iletişimini normal amaçlar için kullanan bir kullanıcı ile VoIP spam saldırısı yapmak isteyen kullanıcılar arasında tipik bazı farklılıklar bulunmaktadır ve bu farklılıklar VoIP spam saldırıların önlenmesi için kullanılabilir. Normal kullanıcıların arama detaylarında genel olarak ad, adres gibi tanıtıcı bilgileri bulunmaktadır. Fakat VoIP spam saldırısı yapacak kullanıcılar bu bilgilerini gizlemeyi tercih etmektedir. Aşağıdaki SIP oturum başlatma protokolü kodları incelendiğinde arayan kullanıcının tipik bazı adres bilgilerini gizlediği görülmektedir. Normal bir çağrı başlatma işleminde bu bilgilerin doğru olması beklenmektedir. VoIP spam saldırısı yapacak kullanıcılar genel olarak kimliklerini gizleyebilmek için bu bilgileri yanlış veya eksik vermektedirler. Aşağıdaki SIP mesajı incelendiğinde “From:"kimliksiz" <sip:kimliksiz@kimliksiz.gecersiz>” satırının yanıltıcı bilgiler içerdiği açıkça görülmektedir.

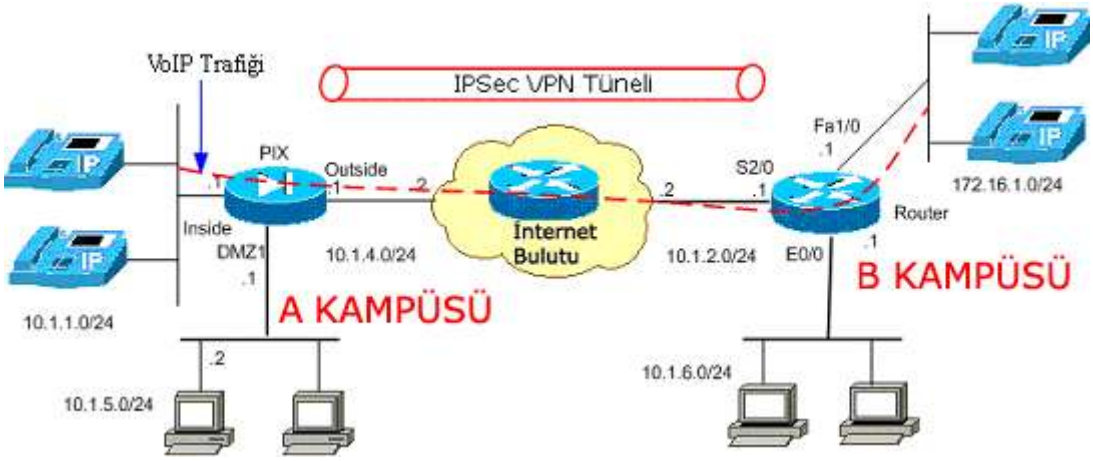
```
INVITE sip:kullanici_1@doamin_1.comSIP/2.0
To: <sip:kullanici_1@domain_1.com>
From:"kimliksiz"<sip:kimliksiz@kimliksiz.gecersiz>;tag=9802748
Remote-Party-ID: "kullanici_2" <sip:kullanici_2@domain_2.com>
    ; party=calling
    ; id-type=subscriber
    ; privacy=full
    ; screen=yes
Proxy-Require:   privacy
```

7 UYGULAMALAR

VoIP iletişiminin güvenli ve ağ üzerindeki trafiğin yeterli sınırlar içerisinde yapılabilmesi için birkaç uygulama gerçekleştirilmiştir. Uygulamalar yapılırken VoIP mimarilerinin farklı yapılarda olmasına özen gösterilmiştir.

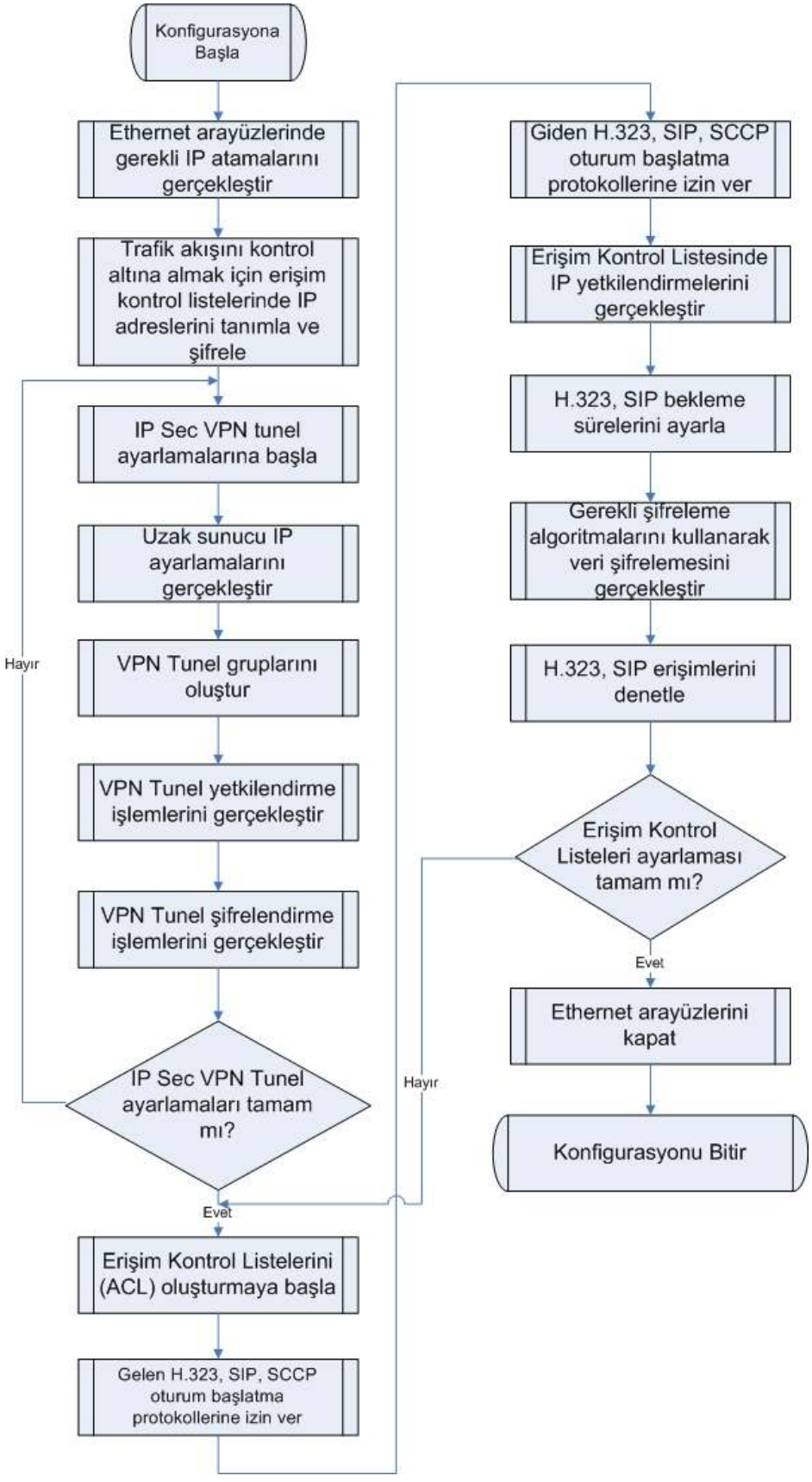
7.1 Uygulama 1: Servis Kalitesi (QoS) Göz Önüne Alınarak VPN Tünel Kullanımı ile VoIP Trafiğinin Optimizasyonu ve Güvenliği

Bu uygulamada VPN tüneli kullanımı ile iki ayrı noktada bulunan VoIP sistemi arasında noktadan noktaya güvenli bir iletişim kurulabilmesi amaçlanmaktadır. Bu uygulamada servis kalitesinin limitler içerisinde olmasına ve VoIP iletişimi esnasında ki trafiğinde optimum seviyelerde tutulması için ek önlemler alınmaktadır. Şekil 7.1'de de görülmekte olan uygulama genel olarak iki veya daha çok ayrık kampüs veya ofis yapısına sahip olan mimariler arasında iletişimin kurulması amacına yöneliktir. Bu uygulamada internet ağı üzerinden yapılan sesli iletişimin VPN tünel kullanımı ile her kullanıcının erişemiyeceği güvenli bir ortamda yapmak mümkün hale gelmiştir.



Şekil 7.1VPN tünel kullanımı ile VoIP trafiğinin güvenliği [46]

Uygulama yapılırken özellikle A kampüs ve B kampüsündeki IP telefonların IP adreslerinin segmentleri farklı seçilmiştir. Bu çalışmada öncelikle ayrık servislerin kural noktalarının (DSCP) servis kalite (QoS) konfigurasyonu gerçekleştirilmiş, bir sonraki aşamada VPN konfigurasyonu eklenmiş, erişim kontrol listeleri (ACL) oluşturularak erişim kısıtlama veya yetkilendirilme işlemleri tanımlanmış, son olarakta yönlendirici konfigurasyonları yapılarak QoS tabanlı erişim kontrol listeli VPN konfigurasyonu tamamlanmıştır. Şekil 7.2'de IP Sec VPN konfigurasyonuna ilişkin akış şeması görülmektedir.



Şekil 7.2 IP Sec VPN konfigurasyonuna ilişkin blok diyagram

Aşağıda sırası ile bu işlem adımlarına ait konfigurasyon kodları görülmektedir.

!−−−DSCP de QoS Konfigurasyon tabanını oluşturma işlemi

```
!−−− Voice adında bir sınıf yaratma işlemi.
PIX(config)#class−map Voice
!−−− Bir DSCP de ses paketlerinin kimliği kısaca "ef" olarak tanımlandı.
PIX(config−cmap)#match dscp ef
!−−− Ses trafiği politikası ayarlandı
PIX(config−cmap)#policy−map Voicepolicy
PIX(config−pmap)#class Voice
!−−− Oluşturulan Voice adındaki sınıfa öncelik tanındı
PIX(config−pmap−c)#priority
!−−− Arayüz dışındaki güvenlik politikası ayarlandı.
PIX(config−pmap−c)#service−policy Voicepolicy interface outside
PIX(config)#priority−queue outside [46]
```

!−−−DSCP de QoS tabanlı VPN Konfigurasyonunun oluşturulması

```
PIX#show running−config
: Saved
PIX Version 7.2(2)
!
hostname PIX
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
        nameif inside
        security−level 100
        ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1
        nameif outside
        security−level 0
        ip address 10.1.4.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
```

```
!−−− Erişim kontrol listelerinde trafik akışını kontrol altına almak için tanımlı
!−−−kimliklerin şifrelenmesi işlemi
access−list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
access−list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate−limit 1 burst−size 1
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 10.1.4.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half−closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp−pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip−invite 0:03:00 sip−disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp−server location
no snmp−server contact
snmp−server enable traps snmp authentication linkup linkdown coldstart
!−−− IPSec kurallarının konfigurasyonu.
crypto ipsec transform−set myset esp−des esp−md5−hmac
crypto map mymap 10 match address 110
!−−− Uzaktaki IP adreslerinin ayarlanması
crypto map mymap 10 set peer 10.1.2.1
crypto map mymap 10 set transform−set myset
crypto map mymap interface outside
crypto isakmp policy 10
authentication pre−share
        encryption 3des
        hash md5
        group 2
        lifetime 86400
!−−− Tünel gruplarının oluşturulması işlemi
tunnel−group 10.1.2.1 type ipsec−l2l
```

```
tunnel−group 10.1.2.1 ipsec−attributes
pre−shared−key *
telnet timeout 5
ssh timeout 5
console timeout 0
priority−queue outside
!
class−map Voice
match dscp ef
class−map inspection_default
match default−inspection−traffic
!
policy−map type inspect dns preset_dns_map
        parameters
                message−length maximum 512
policy−map global_policy
        class inspection_default
                inspect dns preset_dns_map
                inspect ftp
                inspect h323 h225
                inspect h323 ras
                inspect netbios
                inspect rsh
                inspect rtsp
inspect skinny
                inspect esmtp
                inspect sqlnet
                inspect sunrpc
                inspect tftp
                inspect sip
                inspect xdmcp
policy−map Voicepolicy
        class Voice
                priority
!
```

service−policy global_policy global
service−policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
!−−− Erişim Kontrol Listelerinin Oluşturulması İşlemi
!−−− Gelen H.323 çağrılarını izin verme işlemi.
PIX(config)#access−list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0 eq h323
!−−− Gelen SIP çağrılarını izin verme işlemi.
PIX(config)#access−list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0 eq sip
!−−− Gelen SCCP çağrılarını izin verme işlemi.
PIX(config)#access−list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0 255.255.255.0 eq 2000
!−−− Giden H.323 çağrılarına izin verme işlemi.
Pix(config)#access−list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0 eq h323
!−−− Giden SIP çağrılarına izin verme işlemi.
Pix(config)#access−list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0 eq sip
!−−− Giden SCCP çağrılarına izin verme işlemi..
Pix(config)#access−list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0 eq 2000
PIX(config)#access−group 100 in interface outside
PIX(config)#class−map Voice−IN
PIX(config−cmap)#match access−list 100
PIX(config−cmap)#class−map Voice−OUT
PIX(config−cmap)#match access−list 105
PIX(config−cmap)#policy−map Voicepolicy
PIX(config−pmap)#class Voice−IN
PIX(config−pmap)#class Voice−OUT
PIX(config−pmap−c)#priority
PIX(config−pmap−c)#end
PIX#configure terminal

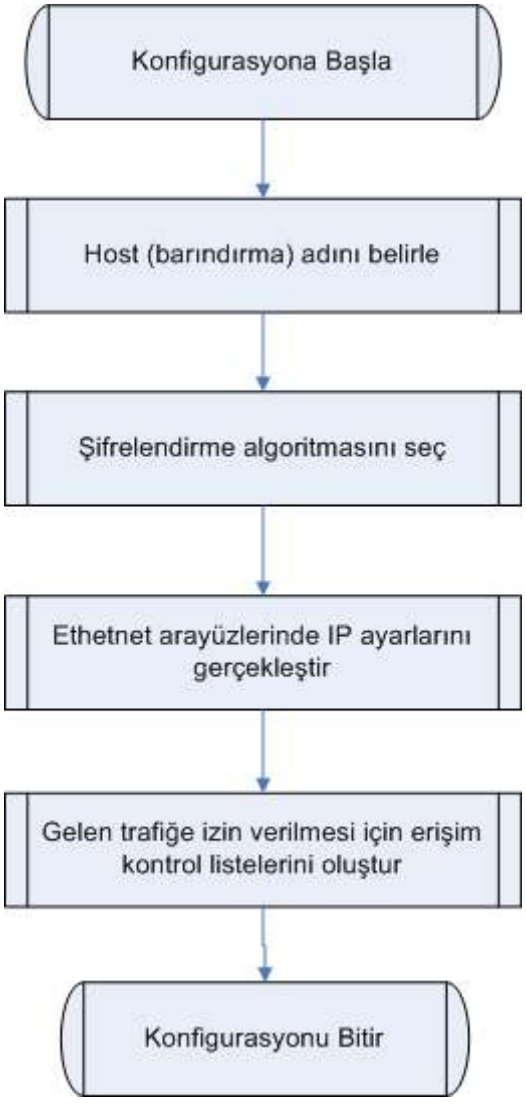
```
PIX(config)#priority−queue outside
PIX(config)#service−policy Voicepolicy interface outside
PIX(config)#end
!−−− Erişim Kontrol Listelerinin Oluşturulması İşlemi
PIX#show running−config
: Saved
PIX Version 7.2(2)
!
hostname PIX
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
        nameif inside
        security−level 100
        ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1
        nameif outside
        security−level 0
        ip address 10.1.4.1 255.255.255.0
!
interface Ethernet2
        nameif DMZ1
        security−level 95
        ip address 10.1.5.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access−list 110 extended permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
access−list 110 extended permit ip 10.1.5.0 255.255.255.0 10.1.6.0 255.255.255.0
access−list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq h323
access−list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq sip
```

```
access−list 100 extended permit tcp 172.16.1.0 255.255.255.0 10.1.1.0
255.255.255.0 eq 2000
access−list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq h323
access−list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq sip
access−list 105 extended permit tcp 10.1.1.0 255.255.255.0 172.16.1.0
255.255.255.0 eq 2000
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate−limit 1 burst−size 1
no asdm history enable
arp timeout 14400
access−group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.4.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half−closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp−pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip−invite 0:03:00 sip−disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp−server location
no snmp−server contact
snmp−server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform−set myset esp−des esp−md5−hmac
crypto map mymap 10 match address 110
crypto map mymap 10 set peer 10.1.2.1
crypto map mymap 10 set transform−set myset
crypto map mymap interface outside
crypto isakmp policy 10
        authentication pre−share
        encryption 3des
        hash md5
        group 2
```

```
        lifetime 86400
tunnel-group 10.1.2.1 type ipsec-l2l
tunnel-group 10.1.2.1 ipsec-attributes
        pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
priority-queue outside
!
class-map Voice-OUT
        match access-list 105
class-map Voice-IN
        match access-list 100
!
class-map inspection_default
        match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
        parameters
                message-length maximum 512
policy-map global_policy
        class inspection_default
                inspect dns preset_dns_map
                inspect ftp
inspect h323 h225
                inspect h323 ras
                inspect netbios
                inspect rsh
                inspect rtsp
inspect skinny
                inspect esmtp
                inspect sqlnet
                inspect sunrpc
                inspect tftp
inspect sip
```

```
                inspect xdmcp
policy−map Voicepolicy
        class Voice−IN
        class Voice−OUT
                priority
!
service−policy global_policy global
service−policy Voicepolicy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end [46]
```

Şekil 7.3'de yönlendirici için yapılacak konfigurasyonun akış şeması görülmektedir.



Şekil 7.3 Yönlendirici konfigurasyonuna ilişkin blok diyagram

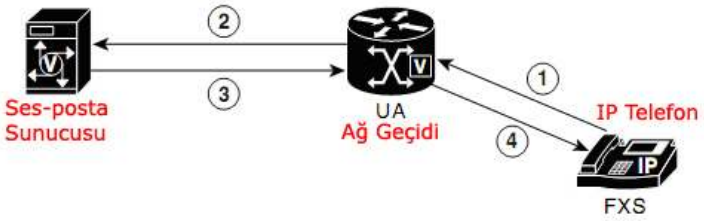
!−−− **Yönlendirici VP Konfigurasyonu**

```
Router#show running−config
Building configuration...
Current configuration : 1225 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password−encryption
hostname Router
boot−start−marker
boot−end−marker
no aaa new−model
resource policy
ip cef
!
crypto isakmp policy 10
 hash md5
 authentication pre−share
crypto isakmp key cisco123 address 10.1.4.1
crypto ipsec transform−set myset esp−des esp−md5−hmac
crypto map mymap 10 ipsec−isakmp
        set peer 10.1.4.1
        set transform−set myset
        match address 110
interface Ethernet0/0
        ip address 10.1.6.1 255.255.255.0
        half−duplex
!
interface FastEthernet1/0
        ip address 172.16.1.1 255.255.255.0
        duplex auto
        speed auto
!
interface Serial2/0
```

```
        ip address 10.1.2.1 255.255.255.0
ip access−group 100 in
        no fair−queue
crypto map mymap
!
ip http server
no ip http secure−server
!
ip route 10.1.0.0 255.255.0.0 Serial2/0
!−−− Gelen IPSec Trafiğine İzin Verilmesi İşlemi.
access−list 100 permit esp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access−list 100 permit esp 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
access−list 100 permit udp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255 eq isakmp
access−list 100 permit udp 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255 eq isakmp
access−list 110 permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access−list 110 permit ip 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
control−plane
line con 0
line aux 0
line vty 0 4
end [46]
```

7.2 Uygulama 2: VoIP İletişiminde Sesli Posta Sunucusunun Kullanımı

Bu uygulamada VoIP iletişimi esnasında gönderilecek olan sesli mesajların bir sunucu üzerinde güvenli bir şekilde tutulması ve gerektiğinde IP telefon cihazı tarafından mesajların alınması amaçlanmaktadır. Şekil 7.4'de de görülmekte olan uygulamada bir IP telefon, bir ağ geçidi ve birde Ses-posta sunucusundan oluşmaktadır. Akış incelendiğinde de anlaşılacağı gibi 1 numara ile gösterilen yolda kullanıcı ağ geçidi üzerinden MWI (Mesaj Bekleme Sinyali) servisine istekte bulunma imkanı vermektedir. 2 ile gösterilen akışta ise kullanıcı tarafından ses posta sunucusuna yapılan istek ağ geçidi tarafından iletilmektedir. Ses-postasının durumunda bir değişiklik olduğunda ses-posta sunucusu tarafından ağ geçidi 3 numaralı akışta olduğu gibi haberdar edilmektedir. 4 numaralı akışta ise durumdaki değişiklikten haberdar olan ağ geçidi, IP telefonu bilgilendirir ve kullanıcı sesli bir uyarı ile uyarılır. Böylece kullanıcıya gelen bir sesli-posta ses posta sunucusunda barındırılmış ve ses-postası geldiğinde ses-posta sunucusu kullanıcıyı haberdar etmiş olur.



Şekil 7.4 Mesaj bekleme sinyal akışı gösterimi [46]

Bu uygulamanın gerçekleştirilebilmesi için ağ geçidinin ve ses-posta sunucusunun konfigurasyonlarının uygun bir şekilde hazırlanmış olması gerekmektedir. Yapılan uygulamada sinyalleşme protokolü olarak SIP protokolü kullanılmıştır. Şekil 7.5'de ağ geçidi üzerinde yapılacak konfigurasyona ait akış şeması gösterilmektedir

Şekil 7.5 Ağ geçidi konfigurasyonuna ilişkin blok diyagram

Aşağıda ağ geçidinin ve ses-posta sunucusunun konfigurasyonları görülmektedir.

Ağ Geçidi Konfigurasyonu

```
Router# show running-config
Building configuration...
Current configuration : 14146 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service dhcp
!
boot-start-marker
boot system flash:c2430-is-mz.mwi_dns
boot-end-marker
!
card type e1 1
logging buffered 9000000 debugging
!
username all
network-clock-participate E1 1/0
network-clock-participate E1 1/1
no aaa new-model
no ip subnet-zero
!
ip domain name gb.com
ip name-server 192.168.1.1
ip dhcp excluded-address 172.16.224.97
!
isdn switch-type primary-qsig
!
trunk group  Incoming
!
voice-card 0
!
```

```
voice service voip
        fax protocol t38 ls-redundancy 0 hs-redundancy 0 fal
        h323
        sip
!
voice class codec 1
        codec preference 1 g711ulaw
        codec preference 2 g729r8
        codec preference 3 g726r32
!
voice hpi capture buffer 100000
voice hpi capture destination flash:t1.dat
!
voice translation-rule 1
        rule 1 /.*/ /8005550100/
!
voice translation-profile Out
        translate calling 1
!
controller E1 1/0
        linecode ami
        pri-group timeslots 1-31
!
controller E1 1/1
        linecode ami
        pri-group timeslots 1-10,16
!
interface FastEthernet0/0
        ip address 192.168.1.172 255.255.255.0
        no ip mroute-cache
        duplex half
        speed auto
!
interface FastEthernet0/1
        ip address 10.2.141.19 255.255.0.0
```

```
        no ip mroute-cache
        duplex auto
        speed auto
!
ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.2
!
ip rtcp report interval 30000
!
control-plane
!
! Enable MWI on voice ports 2/0 and 2/1.
!
voice-port 2/0
        mwi
        timeouts ringing 30
        station-id name SIPUser1
        station-id number 8000
        caller-id enable
!
voice-port 2/1
        mwi
        timeouts ringing 30
        station-id name SIPUser2
        station-id number 8001
        caller-id enable
!
dial-peer cor custom
!
! Configure dial peers.
!
dial-peer voice 1 pots
        preference 5
        destination-pattern 8000
```

```
        port 2/0
!
dial-peer voice 2 pots
        preference 5
        destination-pattern 8001
        port 2/1
!
dial-peer voice 3 voip
        destination-pattern .T
        voice-class codec 1
        session protocol sipv2
        session target sip-server
        dtmf-relay rtp-nte
!
dial-peer voice 7 pots
        trunkgroup Incoming
        destination-pattern 789...
!
dial-peer voice 8 pots
        trunkgroup Incoming
        destination-pattern 789...
!
dial-peer voice 22 voip
        destination-pattern 7232
        session protocol sipv2
        session target sip-server
        dtmf-relay rtp-nte
codec g711ulaw
!
gateway
        timer receive-rtcp 5
        timer receive-rtp 1200
!
```

Şekil 7.6'da ses posta sunucusu üzerinde yapılacak olan konfigurasyona ilişkin akış şeması görülmektedir.

Şekil 7.6 Ses posta sunucusuna ilişkin blok diyagram

! Ses-posta Sunucusu Konfigurasyonu

command.

!

sip-ua

authentication username Rockies password 1511021F0725 realm kampus.com

mwi-server dns:test.kampus.com expires 60 port 5060 transport udp unsolicited

registrar dns:csps-release.test.kampus.com expires 3600

sip-server dns:csps-release.test.kampus.com

!

telephony-service

max-dn 100

max-conferences 4

!

ephone-dn 1

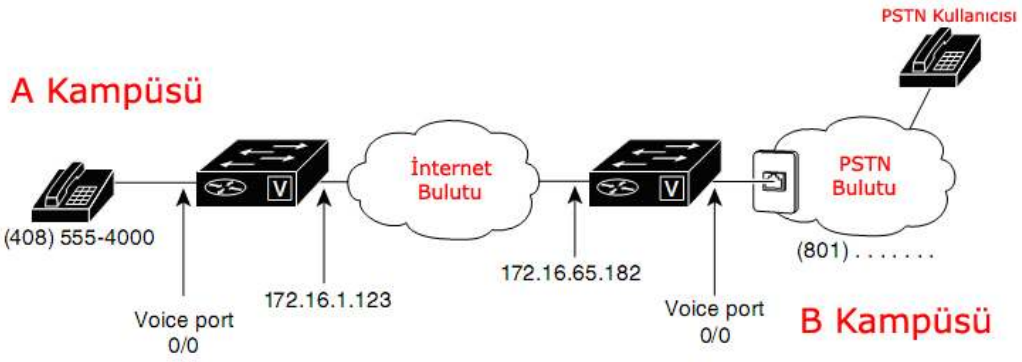
```
!
line con 0
        exec-timeout 0 0
        password 7 030D5A0F
        transport preferred all
        transport output all
line aux 0
        transport preferred all
        transport output all
line vty 0 4
        password 7 13061E010803
        login
        transport preferred all
        transport input all
        transport output all
!
End [46]
```

7.3 Uygulama 3: VoIP ile PSTN Sistemlerin İletişimi

Bu uygulamada iki ayrı noktada bulunan iletişim sistemlerinin birbirleri ile haberleşmesi amaçlanmaktadır. Uygulamada iki ayrı kampüs bulunmaktadır. Bu kampüslerden birincisinde VoIP cihazları bulunmakta ikincisinde ise tamamen PSTN iletişim cihazları bulunmaktadır. Her iki kampüste bir tane yönetilebilen anahtarlama ünitesi (switch) üzerinden internet erişimine sahiptir. Bu anahtarlama ünitelerinin üzerinde VoIP iletişiminin kurulabilmesi için gerekli olan VoIP kartlar (FXO Kart) bulunmaktadır. Böylelikle IP telefon olmadan direkt olarak mevcut sistem üzerinden iletişim kurmak mümkün olacaktır. Bu sistemde her iki kampüste bulunan kullanıcılar birbirini aramak istediklerinde internet ortamını kullanarak VoIP uygulaması ile haberleşmeleri mümkün olmaktadır. Şekil 7.7'de bu uygulamaya ait şematik gösterim görülmektedir.

Bu uygulamanın gerçekleşebilmesi için gerekli olan yönetilebilen anahtarlama ünitelerinin konfigurasyonlarının yapılması gerekmektedir. A ve B kampüslerine ait yönetilebilen anahtarlama ünitelerinin konfigurasyonları aşağıda verilmektedir. Bu uygulamada sadece gerekli olan IP yönlendirmeleri, kullanılacak bant genişliği gibi temel düzeydeki konfigurasyon yapılmıştır. Daha güvenli bir konfigurasyon için birinci uygulamada olduğu gibi

VPN tünel modeli seçilebilir. Ayrıca erişim kontrollerinin ayarlanması için erişim kontrol listeleri oluşturarak konfigurasyon yapısını genişletmek mümkündür.



Şekil 7.7 Kampüsler arası VoIP uygulaması [46]

Şekil 7.8'de A kampüsünün bağlı olduğu yönlendiricinin üzerinde yapılacak olan konfigurasyona ilişkin akış şeması görülmektedir.

Şekil 7.8 A kampüsü yönlendiricisi üzerinde yapılacak konfigurasyonun blok diyagramı

A Kampüsü Gerekli Konfigurasyon

```
hostname router KampusA
! Configure pots dial-peer 1
dial-peer voice 1 pots
destination-pattern 14085554000
port 0/0
! Configure voip dial-peer 2
dial-peer voice 2 voip
destination-pattern 1801.....
session target ipv4:172.16.65.182
ip precedence 5
! Configure serial interface 0
interface serial0
clock rate 2000000
ip address 172.16.1.123
no shutdown [46]
```

Şekil 7.9'da B kampüsünün bağlı olduğu yönlendiricinin üzerinde yapılacak olan konfigurasyona ilişkin akış şeması görülmektedir.

B Kampüsü Gerekli Konfigurasyon

```
hostname router KampusB
! Configure pots dial-peer 1
dial-peer voice 1 pots
destination-pattern 1801.....
port 0/0
! Configure voip dial-peer 2
dial-peer voice 2 voip
destination-pattern 14085554000
session target ipv4:172.16.1.123
ip precedence 5
! Configure serial interface 0
interface serial0
ip address 172.16.65.182
no shutdown [46]
```

Şekil 7.9 B kampüsü yönlendiricisi üzerinde yapılacak konfigurasyonun blok diyagramı

7.4 Uygulama 4: Güvenlik Duvarı ile VoIP Trafiğini Kontrol Altına Almak

Bu uygulamada güvenlik duvarı kullanarak VoIP iletişimi esnasında ortaya çıkabilecek istemdışı trafiğin kontrolü amaçlanmaktadır. Uygulamanın anlaşılabilirliği açısından mimari basit bir yapıda seçilmiştir. Mimari genişledikçe yapılan konfigurasyon mimariye göre genişletilmelidir. Uygulamada bir adet trafiğin kontrolü için güvenlik duvarı, bir adet üzerinde VoIP uygulamasının yapılabilmesi için FXO kartı bulunan yönetilebilir anahtarlama ünitesi ve güvenlik duvarının diğer klasik telefonların VoIP uygulamasından yararlana bilmeleri için analog telefon adaptörü kullanılmıştır. Mimari iki uç arasındaki görüşmenin VoIP protokolleri üzerinden yapılırken ağ trafiğinin limitler içerisinde kalmasını sağlamak amacı ile

tasarlanmıştır. Güvenlik duvarı ile VoIP trafiğinin kontrolünün sembolik gösterimi Şekil 7.10'de görülmektedir.

Şekil 7.10 Güvenlik duvarı ile VoIP trafiğinin kontrolü [46]

Bu uygulamada güvenlik duvarının ve yönetilebilir anahtarlama ünitesinin sistemin gereklerini yerine getirebilmeleri için konfigurasyonlarının yapılması gerekmektedir. Şekil 7.11'de güvenlik duvarı üzerinde yapılacak olan konfigurasyona ilişkin akış şeması görülmektedir.

Güvenlik duvarının ve yönetilebilir anahtarlama elemanının konfigurasyonları aşağıda verilmiştir.

(Güvenlik Duvarı Konfigurasyonu

PIX Version 6.3(1)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718−1719
!−−− H.323 protokolünün çalışabilmesi için ayarlamalar yapıldı.
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060

Şekil 7.11 Güvenlik duvarı konfigurasyonuna ilişkin blok diyagram

```
!−−− SIP protokolünün çalışabilmesi için ayarlamalar yapıldı.
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access−list 101 permit tcp host 100.1.1.2 host 100.1.1.5 eq h323
!−−− Gelen H.323 protokolü isteklerine yetki verilmesi için erişim kontrol listesi
!−−− oluşturuldu.
access−list 101 permit tcp host 100.1.1.2 host 100.1.1.5 eq 5060
!−−− Gelen SIP protokolü isteklerine yetki verilmesi için erişim kontrol listesi
!−−− oluşturuldu.
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 100.1.1.1 255.255.255.0
ip address inside 192.168.0.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
static (inside,outside) 100.1.1.5 192.168.0.2 netmask 255.255.255.255 0 0
!−−− Durağan NAT ayarlaması yapıldı.
access−group 101 in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half−closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa−server TACACS+ protocol tacacs+
aaa−server RADIUS protocol radius
aaa−server LOCAL protocol local
no snmp−server location
no snmp−server contact
snmp−server community public
no snmp−server enable traps
floodguard enable
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
end [46]
```

Şekil 7.12'de yönetilebilir anahtarlama ünitesi üzerinde yapılacak olan konfigurasyona ilişkin akış şeması görülmektedir.

Yönetilebilir Anahtarlama Ünitesinin Konfigurasyonu

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password−encryption
!
hostname Gateway
!
boot−start−marker
boot−end−marker
!
no aaa new−model
ip subnet−zero
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
ip address 100.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
```

```
speed auto
!
no ip http server
ip classless
!
voice−port 1/0/0
voice−port 1/0/1
voice−port 1/1/0
voice−port 1/1/1
!
dial−peer voice 1111 voip
destination−pattern 1111
session target ipv4:100.1.1.5
codec g711ulaw
!
!−−− H.323 çevirilecek numara ayarlandı.
dial−peer voice 2222 pots
destination−pattern 2222
port 1/0/0
!
dial−peer voice 3333 voip
destination−pattern 3333
session protocol sipv2
session target ipv4:100.1.1.5
codec g711ulaw
!−−− SIP çevirilecek numara ayarlandı.
!
line con 0
line aux 0
line vty 0 4
end [46]
```

Şekil 7.12 Yönetilebilir anahtarlama ünitesine ilişkin konfigurasyonun blok diyagramı

8 SONUÇ

Tez çalışmasında internet üzerinden ses iletişimi esnasında oluşabilecek harici trafik konusu üzerine araştırmalar yapılarak çözüm yöntemleri incelenmiştir. İlk olarak VoIP mimarisi incelenmiş, çalışma prensibi ve kullanılan protokoller üzerine araştırmalar yapılmıştır. Yapılan araştırmalar ışığında VoIP iletişimin karşı karşıya kalabileceği dezavantajlar incelenmiştir. Bu dezavantajları ortadan kaldırarak VoIP iletişiminin verimli, güvenli ve gerçek zamanlı olarak yapılmasına olanak sağlayacak çalışmalar yapılmıştır.

VoIP iletişiminde oluşacak harici trafiğin engellenmesi ve güvenliğin sağlanabilmesi için sadece uygulama üzerinde önlemler alınmasının yetersiz olduğu görülmüştür. VoIP iletişiminde bir uçtan diğer uca kadar güvenlik önlemlerinin alınmaması halinde güvenlik açıklarından yararlanan saldırganların bir şekilde iletişimi engelleyebileceği, yavaşlatabileceği, dinleyebileceği hatta başka yerlere yönlendirebileceği görülmüştür. Bu yüzden uçtan uca güvenlik önlemlerinin alınmasına yönelik çalışmalara ağırlık verilmiştir.

VoIP iletişiminde kullanıcılara, mevcut sisteme veya internet ağının yavaşlatılmasına yönelik tehlikelerin olduğu görülmüştür. Kişisel gizlilik, doğruluk ve veri bütünlüğü göz önüne alınarak bu tehlikelerin önlenmesine yönelik uygulamalar yapılmıştır. VoIP üzerindeki her tehlikeye karşı ayrı çözüm yöntemleri geliştirilmesinin uygun olduğu görülmüştür. Kullanıcıya yönelik bir saldırı varsa kullanıcı güvenliğinin ön plana çıkarılması, sisteme yönelik saldırı varsa saldırının kaynağına yönelik çalışmalar yapılarak saldırı kaynağının yok edilmesine yönelik çalışmalar yapılmıştır.

İnternet ağ trafiğini yavaşlatan saldırılar ise farklı yapılara sahiptir. İstenmeyen e-postalar da olduğu gibi VoIP uygulamasında da istenmeyen sesli mesajlar veya istenmeyen çağrılar bulunmaktadır. Aslında bu kategoriye tam anlamı ile saldırı denilmesede internet bant genişliğinin büyük bir kısmını bu mesajların oluşturduğu trafiğin kullandığı görülmektedir. İnternet telefonunda spam tehditi ülkemizde henüz çok yaygın değildir. Bunun sebebi ise VoIP uygulamalarının genellikle iki veya daha fazla ucu olan ve ticari amaçla kullanılan özel hatların olmasıdır. Özellikle ülkemizde VoIP uygulamalarının çok yeni bir teknoloji olması itibari ile ev kullanıcıları tarafından kullanımı yaygınlaşmamıştır. Ev kullanıcılarının IP telefon üzerinden VoIP uygulamalarını kullanabilmesi için servis sağlayıcı kuruluşların oluşması gerekmektedir. Bu konunun önündeki yasal düzenlemelerin henüz oluşmamış olması ülkemizde VoIP kullanımının yaygın bir şekilde kullanılmasını yavaşlatmıştır. Fakat diğer ülkelerde VoIP uygulamaları oldukça yaygınlaşmış ve ev kullanıcılarının da kullanabildiği normlara ulaşmıştır.

Tez çalışmasında VoIP spam tehlikesine karşılık yapılması gerekenler üzerinede bir çalışma yapılarak gelecekte maruz kalınabilecek olan tehlikeye karşı önlemler incelenmiştir.

Sonuç olarak VoIP iletişiminin klasik iletişim metodlarına göre bir çok avantajı olmasına rağmen çeşitli sıkıntılarının da olduğu görülmüştür. Gelecekte PSTN şebekelerin yerini alması beklenen VoIP iletişimi ülkemizde yaygın hale gelmeden önce gerekli olan güvenlik önlemlerini geliştirerek VoIP üzerinde ki sıkıntıların giderilmesi üzerine çalışmaların yoğunlaştırılması gerekmektedir.

Gelecekte yapılacak çalışmalar olarak, SIP protokol güvenliğinin arttırılması, VoIP spamların önlenmesi, servis kalitesi üzerine çalışılarak iç gecikmelerin önlenmesi, güvenli çoklu ortamda VoIP uygulamaları için VPN ağların geliştirilmesi, verilerin bir kullanıcıdan diğer kullanıcıya iletimi esnasında güvenli bir şekilde iletimin sağlanabilmesi için şifreleme algoritmalarının geliştirilmesi üzerine çalışmalar yapılabilir.

KAYNAKLAR

1- S. Goodman, L. Press, S. Ruth, and A. Rutkowski, "The Global Diffusion of the Internet: Patterns and Problems," Communications of the ACM, vol. 37, pp. 27–31, 1994.

2- T. A. Longstaff, J. T. Ellis, S. V. Hernan, H. F. Lipson, , R. D. McMillan, L. H. Pesante, and D. Simmel, "Security of the Internet," The Froehlich/Kent Encyclopedia of Telecommunications, vol. 15, pp. 231–255, 1997.

3- İTÜ Bilgisayar Mühendisliği Bölümü BLG433 Bilgisayar Haberleşmesi ders notları

4- Monkeys.com. Spam Defined. http://www.monkeys.com/spam-defined, Erişim tarihi:04.10.2005.

5- New York Library Association. I Know It When 'Obscenic'. http://www.nyla.org/ index.php?page id=768, Erişim tarihi:12.07.2006.

6- Spam, http://www.spam.org/, Erişim tarihi:04.11.2006

7- Mauro, Edward A. Unsolicited Bulk Email - The problem and some hope. Available at www.giac.org/practical/gsec/Edward Mauro GSEC.pdf, Erişim tarihi:26.08.2006.

8- SpamCop.net, Beware of cheap imitations, http://www.SpamCop.net/ Erişim tarihi:14.09.2006

9- Matt's Script Archive. FormMail. http://www.scriptarchive.com/formmail.html/, Erişim tarihi:22.10.2006.

10- Krueger, Karl A. The Spam Battle 2002: A Tactical Update. Available at http://www.sans.org/rr/catindex.php?cat id=19, Erişim tarihi:03.02.2007.

11- Prakash, Vipul V. Vipul's Razor. http://razor.sourceforge.net, Erişim tarihi:07.12.2006.

12- Rhyolite Software. Distributed Checksum Clearinghouse. http://www.rhyolite. com/anti-spam/dcc/, Erişim tarihi:14.03.2007.

13- Harris, David. (2003) Drowning in Sewage. SPAM, the curse of the new millennium: an overview and white paper. Available at http://www.internetnz. net.nz/public/committee-reports/ctte-legal-and-regulatory-affairs/larac030820spam-white-paper.pdf, Erişim tarihi:18.04.2007.

14- Brussin, David. (2004) Adaptive Behavioral Resource Allocation, Benefits and Lessons Learned From Stopping Spam. Available at http://www.turntide.com/images/pdfs/ Beyond Filters.pdf, Erişim tarihi:27.12.2006.

15- Moortgat, D., Conings, L., 2003. IP Voice at Home, Alcatel Telecommunications Review.

16- Waldron, G., J., Welch, R., 2002. Voice over IP: The Future Communications, Internet Policy Initiative, Washington.
17- Boyacı, A., 2006, İnternet Üzerinden Ses İletişimi, Yüksek Lisans Semineri, Fırat Üniversitesi Fen Bilimleri Enstitüsü
18- Hunter, P., VoIP The Latest Security Concern: DOS Attack Greatest Threat, http://www.cryptic.co.uk, Erişim tarihi:01.06.2005
19- Khosla, S., 2003. Voice over Packet: A Design Perspective, http://www.sidkhosla.com, Erişim tarihi:12.10.2006
20- Kartal, M., 2003. Mikrodalga Radyo Haberleşmesi Ders Notları, İ.T.Ü. Elektrik – Elektronik Fakültesi, İstanbul.
21- Vaudreuil, G., Parsons, G., 1998. IETF Recommendation RFC 2422, Toll Quality Voice – 32 kbit/s ADPCM MIME Sub-type Registration.
22- Fincan, E., 2002. İnternet Protokolü Üzerinden Ses Haberleşmesi, Yüksek Lisans Tezi, İ.T.Ü. Fen Bilimleri Enstitüsü, İstanbul.
23- Deva M., 2004, İnternet Protokolü Üzerinden Ses Aktarımı, Bitirme Ödevi, İ.T.Ü. Elektronik Haberleşme Mühendisliği.
24- IP Telephony Design Guide, 2003. Alcatel Telecommunications Review, California.
25- Egevang, K., Francis, P., 1994. IETF Recommendation RFC 1631, The IP Network Address Translator.
26- VoIPTürk, http://www.voipturk.com, Erişim tarihi:04.04.2005
27- Durusoy, G., 2003. Veri Haberleşmesi Ders Notları, İ.T.Ü. Elektrik – Elektronik Fakültesi, İstanbul.
28- Kara, N., ve diğ., 2000. Voice over IP, Bilişim Ağları Dairesi Başkanlığı, Ankara.
29- Rekhter, Y., 1996., ve diğ., 1996. IETF Recommendation RFC 1918, Address Allocation for Private Internets.
30- Kilmartin, L., Ranganathan, M., K., 2002. Performance Analysis of Session Initiation Based VoIP Networks, Computer Communications, Vol: 26, No: 6, pp.552-565.
31- Cambronero, D., F., Zangger, E., 2001. Voice over IP, Upgrade Magazine Vol:2 No:3, http://www.upgrade-cepis.org, Erişim tarihi:12.08.2005
32- Huitema, C., 2003. IETF Recommendation RFC 3605, Real Time Control Protocol attribute in Session Description Protocol.
33- Handley, M., Jacobsen, V., 1998. IETF Recommendation RFC 2327, Session Description Protocol.
34- CCIE - Voice over IP Fundamentals VoIP, Cisco Press 2000.
35- Örencik, M., Yavaş, S.,VoIP Güvenliği.

36- Seydim, A., Y., 1999. Voice over IP, Yüksek Lisans Tezi, Southern Methodist University, Texas.
37- Black, U., 2000. Voice over IP, Prentice Hall, New Jersey.
38- Braden, R., ve diğ., 1997. IETF Recommendation RFC 2205, Resource Reservation Protocol – Version 1 Functional Specification.
39- Shultzrinne, H., ve diğ., 2003. IETF Recommendation RFC 3550, RTP: A Transport Protocol for Real Time Applications.
40- Till Andreas Radermacher. Spam Prevention in Voice over IP Networks. Master's Thesis, University of Salzburg, November 2005.
41- Baumann ,R., Cavin ,S., Schmid ,S., Voice Over IP - Security and SPIT Swiss Army FU Br 41 KryptDet Report, University of Berne, August 24 - September 8, 2006.
42- Niccolini, Saverio et al. (2004) IP Telephony Cookbook. Available at http://www.informatik.unibremen.de-/prelle/terena/Cookbook.pdf, Erişim tarihi: 16.11.2006.
43- Rosenberg, J. et al. (2002) SIP: Session Initiation Protocol. IETF Request for Comments 3261, June 2002. Obsoletes RFC 2543.
44- Baruch Sterman. Proposal for a SPIT Prevention Security Model. White Paper, Kayote Networks, Marc 2005.
45- Dongwook Shin and Qovia Choon Shim. Voice Spam Control with Grey Leveling. In 2nd Workshop on Securing Voice over IP, 2005.
46- Cicso System, Inc, http://www.cisco.com, Erişim tarihi: 16.04.2007.

ÖZGEÇMİŞ

1978 yılında Kocaeli'nin Gebze ilçesinde doğdu. İlk ve Ortaöğretimini Gebze'de bitirdi. Lise eğitimini İstanbul'da tamamladı. Ön lisans eğitimini 1999 yılında İstanbul Üniversitesi Endüstriyel Elektronik Bölümünden mezun oldu. Lisans eğitimini 2003 yılında Fırat Üniversitesi Elektrik-Elektronik Mühendisliği Bölümünde tamamladı. 2004 yılında Fırat Üniversitesi Enformatik Bölümünde okutman kadrosu ile göreve başladı. 2005-2006 bahar yarıyılında Fırat Üniversitesi Fen Bilimleri Enstitüsü Elektrik Elektronik Mühendisliği Anabilim dalında yüksek lisans eğitimine başladı.

Halen Fırat Üniversitesi Enformatik Bölümünde Okutman olarak görev yapmakta ve üniversitenin ihtiyaç duyduğu çeşitli yazılım ve otomasyonları geliştirmektedir.