AĞ İLETİŞİMİNDE VERİ GİZLEME TABANLI BİLGİ GÜVENLİĞİ UYGULAMALARI

İsmail KARADOĞAN

Yüksek Lisans Tezi
Yazılım Mühendisliği Anabilim Dalı
Danışman: Doç. Dr. Resul DAŞ
OCAK-2016

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AĞ İLETİŞİMİNDE VERİ GİZLEME TABANLI BİLGİ GÜVENLİĞİ UYGULAMALARI

YÜKSEK LİSANS TEZİ

İsmail KARADOĞAN

(121137103)

Anabilim Dalı: Yazılım Mühendisliği

Tez Danışmanı : Doç. Dr. Resul DAŞ (F. Ü.)

Diğer Jüri Üyeleri : Prof. Dr. Asaf VAROL (F. Ü.)

Prof. Dr. Ali KARCI (İ. Ü.)

Tezin Enstitüye Verildiği Tarih: 18 Aralık 2015
Tezin Savunulduğu Tarih: 08 Ocak 2016

OCAK–2016

ÖNSÖZ

Yüksek Lisans eğitimim boyunca bilgilerinden faydalandığım, beraberinde çalışmaktan onur duyduğum ve tecrübelerinden yararlanırken hoşgörü ve sabırla desteklerini esirgemeyen değerli hocam Sayın Doç. Dr. Resul DAŞ'a, bilgilerinden istifade ettiğim tüm bölüm hocalarıma, çalışmalarım boyunca sabır gösteren ve destek olan aileme ve dostlarıma teşekkürlerimi sunarım.

İsmail KARADOĞAN

ELAZIĞ - 2016

İÇİNDEKİLER

ÖZET

Yüksek Lisans Tezi

AĞ İLETİŞİMİNDE VERİ GİZLEME TABANLI BİLGİ GÜVENLİĞİ UYGULAMALARI

İsmail KARADOĞAN

Fırat Üniversitesi
Fen Bilimleri Enstitüsü
Yazılım Mühendisliği Anabilim Dalı
2016, Sayfa: 71

Bilgi, insanlık tarihi boyunca çok kıymetli bir yer edinmiştir. Gizli bilginin üçüncü taraflarca anlaşılmadan alıcısına iletilmesi için değişik yöntemler kullanılmıştır. Bu yöntemlerin başlıcaları bilgiyi kriptografik yöntemlerle şifrelemek veya steganografik yöntemlerle gizlemektir. Bilginin işlenmesi, paylaşılması, üretilmesi gibi faaliyetler bilgisayarın icadıyla ivme kazanmıştır. Bilginin daha etkin paylaşımı için bilgisayar ağları oluşturulmuş, standartlar geliştirilmiştir.

Bu tez çalışmasında, bilgisayar ağlarında kullanılan temel iletişim protokolleri araştırılmış, bu protokollerin istismarıyla bilgi sistemlerini tehdit eden saldırı yöntemleri kapsamlı olarak incelenmiş, bilgi gizleme ve gizli kanallar hakkında bilgiler verilmiş, bilgisayar ağlarında gizli veri iletim yöntemleri araştırılıp sunulmuş ve örnek gizli veri iletimi uygulamaları gerçekleştirilmiştir. Bunlarla beraber paket zamanlama ve IP ID tabanlı yeni ağ steganografi yöntemleri önerilmiştir. Önerilen zamanlama yönteminin bant genişliğinin önceki yöntemlere göre daha yüksek olduğu; IP ID kullanan yöntemin, ID alanının benzersizliğinin sağlanmasında önceki yöntemlere göre daha etkili ve Internet üzerinden gizli veri gönderimine uygun olduğu görülmüştür.

Anahtar Kelimeler: Bilgisayar Ağları, Gizli Kanallar, Steganografi, İletişim Protokolleri, Ağ Güvenliği

SUMMARY

M.S. Thesis

DATA HIDING BASED INFORMATION SECURITY APPLICATIONS ON NETWORK COMMUNICATION

İsmail KARADOĞAN

Fırat University
Institute of Science and Technology
Department of Software Engineering
2016, Pages: 71

Information has become an invaluable place throughout human history. Different methods are used for the transmission of secret information to recipients without understanding third parties. The main of these methods are to encrypt information using cryptographic methods or to hide information with steganographic methods. Activities such as processing, sharing, production of the information have been accelerated with the invention of the computer. For more effective information sharing, computer networks have been created and standards have been developed.

In this study, basic computer network protocols are investigated. Attack methods that are threatening information systems with the exploitation of these protocols are comprehensively examined. Information is given about information hiding and hidden channels. Secret data transmission methods in computer networks are explored and presented. Examples of secret data transmission have been carried out. Additionally, new packet timing based and IP ID based network steganography methods are proposed. The bandwidth of the proposed timing method is higher than previous methods. The proposed IP ID based method is more effective to ensuring uniqueness of the ID field according to previous methods, and is suitable for sending secret data over the Internet.

Key Words: Computer Networks, Covert Channels, Steganography, Communication Protocols, Network Security

ŞEKİLLER LİSTESİ

Sayfa No

KISALTMALAR

ADS : Alternate Data Streams
ARP : Address Resolution Protocol
ASCII : American Standard Code for Information Interchange
ASP : AppleTalk Session Protocol
ATM : Asynchronous Transfer Mode
BSD : Berkeley Software Distribution
CSMA : Carrier Sense Multiple Access
CSMA/CD : CSMA with Collision Detection
DDoS : Distributed Denial of Service
DNS : Domain Name System
DoD : U.S. Department of Defense
DoS : Denial of Service
FDDI : Fiber Distributed Data Interface
FTP : File Transfer Protocol
HP/UX : Hewlett-Packard UniX
HTML : Hyper Text Markup Language
HTTP : Hyper-Text Transfer Protocol
HTTPS : Secure Hypertext Transfer Protocol
ICMP : Internet Control Message Protocol
ID : Identification
IOS : Internetwork Operating System
IP : Internet Protocol
IPSec : Internet Protocol Security
IPX : Internetwork Packet Exchange
ISN : Initial Sequence Number
ISO : International Organization for Standardization
JPEG : Joint Photographic Experts Group
MAC : Media Access Control
MIDI : Musical Instrument Digital Interface
MITM : Man In The Middle

MPEG : Moving Pictures Experts Group
MTU : Maximum Transmission Unit
NFS : Network File System
NTFS : New Technology File System
OS : Operating System
OSI : Open Systems Interconnection
POP : Post Office Protokol
RPC : Remote Procedure Call
SMTP : Simple Mail Transfer Protocol
SNMP : Simple Network Management Protocol
SQL : Structured Query Language
SSH : Secure Shell
TCP : Transmission Control Protocol
TIFF : Tagged Image File Format
ToS : Type of Service
TTL : Time to Live
UDP : User Datagram Protocol
UTP : Unshielded Twisted Pair
VoIP : Voice over Internet Protocol
WEP : Wired Equivalent Privacy
WWW : World Wide Web
XSS : Cross Site Scripting

1. GİRİŞ

Bilginin iletilmesi ve işlenmesi, bilgi ve sistem kaynaklarının paylaşımı için bilgisayarların iletişim hatlarıyla birbirine bağlandığı sistemlere bilgisayar ağları denilmektedir. Bir bilgisayar ağı oluşturmak için en az iki bilgisayar gereklidir. Ortamlarına göre farklı teknolojilere sahip olan ağ türlerinden günümüzde en çok kullanılan tür Ethernet tabanlı olandır. Dünyadaki en büyük ağ Internet ağıdır.

Şirketler, kurum ve kuruluşlar coğrafî olarak birbirinden uzak, farklı yerlerde bulunan bilgisayarların bağlandığı ağlar kullanırlar. Ağdaki bilgisayarların birbirlerine olan mesafesinden dolayı büyüklüklerine göre ağlar; Yerel Alan Ağı, Metropolitan Alan Ağı ve Geniş Alan Ağları olmak üzere genel olarak üçe ayrılır. Yerel alan ağlarında bağlantı için belli bir teknoloji ve standart kullanılırken, geniş alan ağlarında farklı teknolojiler bir arada kullanılır.

Bilgisayar ağlarına bağlı bilgisayarların haberleşmeleri için protokoller geliştirilmiştir. Uluslararası tanımlanan ve kullanılan protokollerin haberleşme biçimleri, kullandıkları veri yapıları istismar edilebilmektedir. Bu tür istismarlar ağ kaynakları ve sunucular için bilgi güvenliği ve bilgi sistemleri güvenliği sorunlarını ortaya çıkarmıştır.

Dijital dünyada bilgi sistemleri güvenliği konusunda birçok zafiyet ve bunlardan yararlanılarak bilgi sistemlerine yapılan birçok saldırı türü söz konusudur. Ağ veya uygulama seviyesinde SQL Injection, Cross-Site Scripting (XSS), Session Hijacking, Information Leakage, Denial of Service (DoS), Distributed DoS (DDoS), İşletim Sistemi Tespiti (OS Fingerprinting), Port Tarama, IP/MAC Spoofing (Aldatma), ARP Cache Poisoning (ARP Önbellek Zehirleme), DNS Poisoning, Sniffing (Dinleme), Man In The Middle (MITM) gibi saldırılar çokça bilinen saldırılardandır.

Steganografi bilgi gizleme sanatı ve bilimidir. Kriptografi, bilgiyi şifreleyip anlaşılmaz hale getirirken, Steganografi bilginin varlığını alakasız bir ortamda gizler. Bilgi gizleme, şifreleme ile beraber insanlık tarihi boyunca kullanılagelmiştir. Teknolojinin gelişimiyle beraber bilgi gizleme teknikleri de gelişmektedir. Dijital ortamda resim, ses, video, yazı, belge gibi ortamlara bilgi gizleme ile beraber bu tezde ele alınan ağ ortamına bilgi gizleme (ağ steganografi) yöntem ve teknikleri geliştirilmiştir.

Bu tez çalışmasının *birinci bölümünde* bilgisayar ağ topolojileri, referans modelleri ve ağ cihazları hakkında temel bazı bilgiler verilmiştir.

İkinci bölümde, ağ iletişiminde en çok kullanılan TCP/IP protokol kümesinde yer alan protokoller hakkında temel bilgilerle beraber işleyiş teknikleri verilmiş, bu protokollerin istismar edilebilen yönleri ve ağ saldırılarına karşı güvenlik zafiyetleri analiz edilmiştir.

Üçüncü bölümde, bilgisayar ağlarında, özellikle OSI referans modelinin ikinci, üçüncü ve dördüncü katmanlarında yer alan ve veri iletişiminde teknik altyapıyı sağlayan protokollerin istismarıyla yapılan ağ saldırı türleri hakkında kapsamlı bir araştırma yapılmış, saldırıların amaçları, nasıl ve hangi ortamlarda gerçekleştirilebildiği hakkında bilgiler sunulmuştur.

Dördüncü bölümde, steganografi, çeşitleri ve tekniklerinden bahsedilmiş, temel bilgiler verilmiştir.

Beşinci bölümde, ağ steganografi ve bilgisayar ağlarındaki gizli kanallar kapsamlı bir şekilde araştırılmış; bilgisayar ağlarında hangi tekniklerle hangi ortamlara veri gizlenerek iletilebildiği detaylı olarak sunulmuş, yanı sıra analizleri yapılarak kullanılan tekniklerin avantaj ve dezavantajlarından bahsedilmiştir.

Altıncı bölümde, araştırılan gizli kanal oluşturma yöntemleri temel alınarak, bu yöntemlerin bir kısmının uygulanabilirliği test edilmiş, bunlarla beraber ağ ortamında gizli veri gönderimi için iki yeni yöntem önerilmiş, ağ ortamında gizli veri iletimi ile ilgili bazı örnek uygulamalar gerçekleştirilmiştir.

1.1. Ağ Topolojileri

Topoloji, genel olarak bilgisayarların veya beraberinde diğer ağ elemanlarının fiziksel veya mantıksal olarak birbirlerine bağlanma şekillerini ifade etmek için kullanılan bir terimdir.

*Yol (bus) topoloji*de, bilgisayarları birbirlerine bağlamak için doğrusal bir hat mevcuttur. Bu hat boyunca her bilgisayar uygun konnektörle hatta bağlıdır. Hattın her iki ucunda sonlandırıcı konnektörler bulunur. Hattan gönderilen bir sinyal, sonlandırıcı konnektörlere

kadar gider, tüm bilgisayarlara ulaşır. Veri akışı çift yönlü olup, bilgisayarlardan biri gönderici konumunda iken başka biri veri göndermek istediğinde beklemek durumundadır.

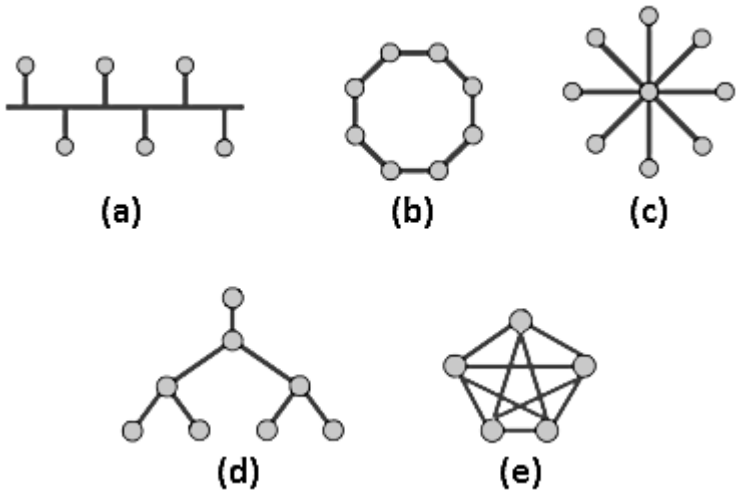
Halka topoloji, mantıksal olarak bilgisayarların bir daire üzerinde yer almasıdır. Her bilgisayar başka iki bilgisayara bağlıdır. Gönderilen sinyal tüm bilgisayarlara iletilir.

Yıldız topolojisi, en yaygın kullanılan topoloji türüdür. Bu topolojide bilgisayarlar merkezi bir cihaza bağlanır, veri iletişimi merkezde yer alan cihaz üzerinden yapılır. Merkezdeki cihaz hub, switch gibi bir cihazdır.

Ağaç topoloji, yıldız topolojideki ağların birleştirilmesi için kullanılır. Yıldız topolojiye sahip ağlar, bir omurga ile birbirine bağlanır. Omurga ağacın gövdesi, ağlar ise dallardır.

*Mesh topoloji*ye sahip bir ağda bütün bilgisayarlar veya cihazlar diğerlerine direk bağlıdırlar. Bir bilgisayardan diğerine birçok yolla ulaşılabilir, ancak ağın maliyeti yüksek olur. Bu topoloji daha çok yönlendirici cihazlar arasında kullanılır.

Temel ağ topolojileri Şekil 1'de gösterilmiştir.



Şekil 1. Temel Ağ Topolojileri
(a) Yol, (b) Halka, (c) Yıldız, (d) Ağaç (Hiyerarşik), (e) Mesh

1.2. OSI Referans Modeli

OSI (Open Systems Interconnection) modeli, ağ cihazlarında çalışan uygulamaların birbirleriyle nasıl iletişim kuracaklarını belirleyen, ağ yazılım ve donanımlarını kapsayan,

karmaşıklığı azaltan, yedi katmandan oluşan ISO (International Organization for Standardization) tarafından geliştirilen bir referans modelidir. [1]

OSI Modelinin yedi katmanı yukarıdan aşağıya sırasıyla; Uygulama, Sunum, Oturum, Taşıma, Ağ, Veri Bağlantısı Katmanı ve Fiziksel Katmandır. Bu katmanlar Şekil 2'de gösterilmiştir.

	Katman Adı	İçerdiği Protokoller
7.	Uygulama Katmanı	HTTP, HTTPS, SMTP, FTP, TFTP, UUCP, NNTP, SSL, SSH, IRC, SNMP, SIP, RTP, Telnet, ...
6.	Sunum Katmanı	ISO 8822, ISO 8823, ISO 8824, ITU-T T.73, ITU-T X.409, ...
5.	Oturum Katmanı	NFS, SMB, ISO 8326, ISO 8327, ITU-T T.6299, ...
4.	Taşıma (İletim) Katmanı	TCP, UDP, SCTP, DCCP, ...
3.	Ağ Katmanı	IP, IPv4, IPv6, ICMP, ARP, IGMP, ...
2.	Veri Bağlantısı Katmanı	Ethernet, HDLC, Wi-Fi, Token ring, FDDI, PPP, ...
1.	Donanım Katmanı	ISDN, RS-232, EIA-422, RS-449, EIA-485, ...

Şekil 2. OSI Referans Modeli Katmanları

Uygulama katmanı, son kullanıcının kullandığı uygulamaların veri iletişiminde uyacakları standartları belirler. HTTP, WWW, FTP, SMTP, SSH, Telnet gibi protokoller ve standartlar bu katmanda tanımlıdır.

Sunum katmanında, veriler bir üst katmana (Uygulama Katmanına) sunulurken gerekli kodlama ve dönüştürme işlemleri yapılır. Veri sıkıştırma ve açma, şifre kodlama ve kod çözme, karakter kodlamaları ve kümeleri arası dönüşümleri gibi işlemler bu katmanda yapılır. Bu katmanda HTML, MIDI, MPEG, JPEG, TIFF gibi standartlar tanımlıdır.

Oturum katmanı, oturumun sağlanması, oturum kontrolü ve kapatılmasını sağlar. Verinin güvenliğini ve hatasız iletimini sağlar. Bu katmanda NFS (Network File System), SQL (Structured Query Language), ASP (Appletalk Session Protocol), RPC (Remote Procedure Call) gibi protokoller çalışır.

Taşıma katmanı üst katmanlarla alt katmanlar arasında veri transferini sağlar. Üst katmandan gelen verileri segmentler halinde alt katmana iletirken, alt katmandan segmentler halinde gelen verileri birleştirerek üst katmana sunar. Bu katman, veriyi

gönderen ve alan arasında mantıksal bir bağlantının kurulmasını, veri akış kontrolünü, verinin bütünlüğünü sağlar. TCP, UDP gibi protokoller bu katmanda tanımlıdır.

Ağ katmanında, bir üst katmandan segmentler halinde gelen veri, gideceği adres bilgisini (IP adresi) bulunduran paketlere bölünür ve yönlendirme bilgisiyle alıcıya iletilmesi sağlanır. IP, IPX, ARP ve ICMP bu katmanda tanımlı protokollerdir. Yönlendiriciler bu katmanda görev yapar. Bu katmanda temel olarak adresleme ve yönlendirme yapılır.

Veri Bağlantısı Katmanında, ağ katmanından gelen veri paketleri hata bitleri eklenerek çerçeve adı verilen birimler halinde fiziksel katmana iletilir. Ağa bağlı cihazların fiziksel adresleri (Media Access Control - MAC adresi) bu katmanda tanımlanır, hattın kullanılabilirliği denetlenir. Ethernet, Frame Relay, ATM, FDDI standartları ve protokolleri bu katmanda tanımlı olmakla birlikte, Switch (Anahtar) ve Bridge (Köprü) cihazları bu katmanda görev yapar.

Fiziksel Katman (Donanım Katmanı), verilerin fiziksel olarak iletilmesinin tanımlandığı katmandır. Verinin içeriği ile ilgilenilmez. Bu katmanda, verinin taşınacağı ortam, işaretin şekli, bağlantı şekli ve konnektör türü, kablolama, bilgi gönderim hızı, maksimum transfer mesafesi gibi özelliklerle ilgilenilir. Hublar fiziksel katmanda çalışır. 10BaseT, 10BaseF, 100BaseT, UTP, RJ-45 gibi standartlar bu katmanda tanımlıdır.

1.3. TCP/IP Referans Modeli

TCP/IP Modeli, OSI Modelinden önce oluşturulmuştur. TCP/IP Protokol grubu DoD (U.S. Department of Defense) modelini referans alır. Bu model dört katmandan oluşur. Bu katmanlar Uygulama, Aktarım, Internet ve Ağ Arayüz (Bağlantı) katmanlarıdır [2]. Şekil 3'te, bu katmanlar OSI Modeli ile karşılaştırılarak verilmiştir.

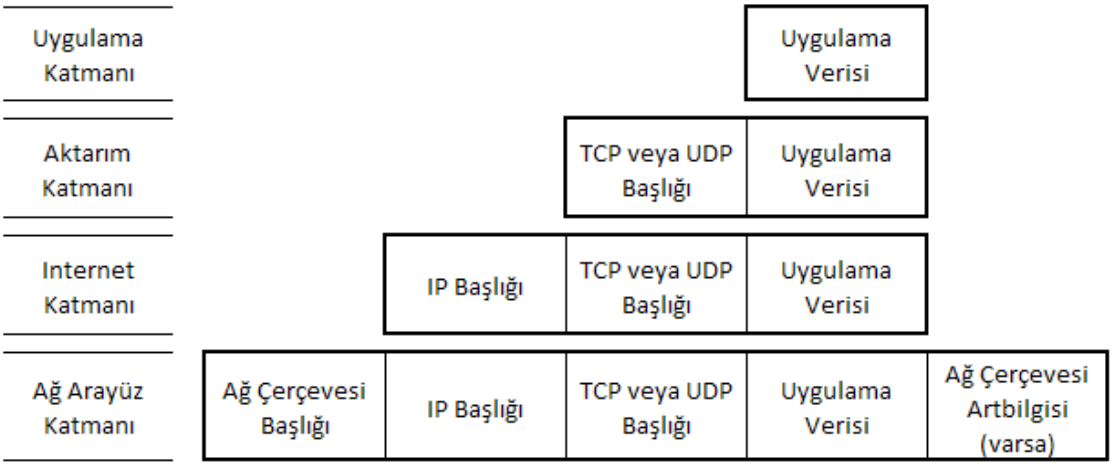
<table>
<tr><th colspan="2">OSI Modeli Katmanları</th><th colspan="2">TCP/IP Modeli Katmanları</th></tr>
<tr><td>7.</td><td>Uygulama Katmanı</td><td rowspan="3">Uygulama Katmanı</td><td rowspan="3">4.</td></tr>
<tr><td>6.</td><td>Sunum Katmanı</td></tr>
<tr><td>5.</td><td>Oturum Katmanı</td></tr>
<tr><td>4.</td><td>Taşıma (İletim) Katmanı</td><td>Aktarım Katmanı</td><td>3.</td></tr>
<tr><td>3.</td><td>Ağ Katmanı</td><td>Internet Katmanı</td><td>2.</td></tr>
<tr><td>2.</td><td>Veri Bağlantısı Katmanı</td><td rowspan="2">Ağ Arayüz Katmanı</td><td rowspan="2">1.</td></tr>
<tr><td>1.</td><td>Donanım Katmanı</td></tr>
</table>

Şekil 3. TCP/IP Modeli Katmanları ve OSI Modeli İle Karşılaştırılması

Uygulama Katmanı OSI Modelindeki Uygulama, Sunum ve Oturum katmanlarının tümüne, Aktarım Katmanı, OSI Modelindeki Taşıma (İletim) Katmanına, Internet Katmanı OSI Modelindeki Ağ Katmanına, Ağ Arayüz Katmanı ise OSI Modelindeki Veri Bağlantısı ile Donanım Katmanlarına denk gelir.

OSI ve TCP/IP Modellerinin her ikisi de katmanlarla tanımlanmaktadır. OSI Modeli uygulama gerektirmeden, resmi bir komite süreci ile daha çok iletişimde standardı belirlemektedir. Internet protokollerinin belirtimlerinde, daha az resmî mühendislik yaklaşımları kullanılır. OSI protokolleri daha yavaş geliştirilmekte, TCP/IP ve Internet hızlıca geliştirilmekte, TCP/IP Modeli daha çok uygulamaya dönük bir yaklaşım sunmaktadır. [3]

TCP/IP Protokol Kümesi, temelinde IP protokolünün yer aldığı, TCP ve UDP protokollerinin de IP üzerinden kullanıldığı ve diğer tüm üst katman protokollerinin de TCP veya UDP protokollerini kullandığı bir protokol kümesidir. Veri, göndericiden ağ ortamına iletildiğinde, Uygulama Katmanından Ağ Arayüz Katmanına indikçe ilgili protokol başlık yapıları tarafından kapsüllenerek bir alt katmana verilir. Bu durum Şekil 4'te modellenmiştir. Şekilde "Uygulama Verisi" olarak adlandırılan kısım, Uygulama Katmanında yer alan üst protokol bilgilerini de (HTTP, DHCP, DNS vs.) içerebilir.



Şekil 4. TCP/IP Protokol Kümesinde Veri Kapsülleme

Fiziksel ortamda ağ çerçevesi başlığı ile iletilen veri, alıcıya ulaştığında, her katmanda ilgili protokol başlıkları okunarak başlıktaki bilgiler değerlendirilir ve bir üst katmana üst katmandaki protokol başlığı ile verilir. En son Uygulama Katmanına çıkan veri, ilgili uygulama tarafından kullanılır.

1.4. Ağ Cihazları

Hub, en basit ağ cihazıdır. Yerel ağdaki bilgisayarlar kablolarla Hub cihazına bağlanır ve bu şekilde haberleşme sağlanmış olur. Hub, bir portundan gelen veriyi tüm portlarına gönderir, verinin geldiği ve gideceği adresle ilgilenmez.

Repeater (Tekrarlayıcı), bir giriş ve bir çıkışa sahip olup kendisine gelen sinyali kuvvetlendirip ileten cihazlardır. İşleyiş olarak iki portlu Hub gibi düşünülebilir.

Switch (Anahtar), Hub cihazından farklı olarak, adından anlaşılabileceği gibi ağa bağlı bilgisayarlar arasında anahtarlamalı bir yol sağlar, bilgisayarların adres bilgisini tutar. Herhangi bir portundan gelen veriyi sadece alıcı bilgisayarın bağlandığı porta gönderir. Switch, OSI modelinin veri bağı katmanında çalışır, ağ katmanında çalışan üst modelleri de vardır.

Bridge (Köprü), gelen verinin hangi adrese gittiğine bakar ve iletmesi gerekiyorsa iletir, gerekmiyorsa iletmez. Yerel ağların genişletilmesinde veya farklı fiziksel teknolojilere (UTP, Coax) sahip ağların birleştirilmesinde kullanılabilir. İşleyiş olarak Switch'in iki portlusu gibi düşünülebilir.

Router (Yönlendirici), OSI modelinin ağ katmanında çalışır, temel olarak paket yönlendirme yapar. Ağlar arasında (örneğin yerel alan ağı ile geniş alan ağı arasında) bağlantı kurmak, IP paketlerini yönlendirmek, güvenlik duvarı oluşturmak başlıca kullanım amaçlarındandır.

Gateway (Geçityolu), farklı teknolojilere ve protokollere sahip ağlar arasındaki bağlantıyı ve iletişimi sağlar. Örneğin bir Ethernet ağını bir FDDI ağa bağlar. Bu cihaz bir köprü, switch ya da router olabilir.

Access Point (Erişim Noktası), kablosuz erişime sahip bir cihazı kablolu bir ağa bağlamak için kullanılır.

Modem, dijital veriyi analog veriye, analog veriyi dijital veriye dönüştüren, mevcut telefon hattı üzerinden bilgisayarların haberleşmesini sağlayan cihazdır.

2. AĞ PROTOKOLLERİ VE PROTOKOL ANALİZİ

Protokol, bilgisayar ağlarında bilgisayarların ve ağ cihazlarının veri iletişimini sağlıklı bir şekilde gerçekleştirmeleri ve veriyi işleyebilmeleri için tanımlanmış kurallardır. İletilecek bilginin formatı, iletim şekli, iletim ortamı, bilginin takip edeceği yol bilgisi protokollerin tanımında yer alır. Farklı teknolojik donanımlara sahip ağ sistemleri, belirlenmiş protokollerle anlaşabilir, aynı dili konuşabilirler.

Ağ iletişiminde kullanılan cihazlar genellikle OSI modelinin veri bağı katmanı, ağ katmanı ve taşıma katmanlarındaki standartlara ve protokollere göre veriyi gönderip alırlar. Bu bölümde en çok kullanılan protokoller hakkında bilgiler sunulmuştur.

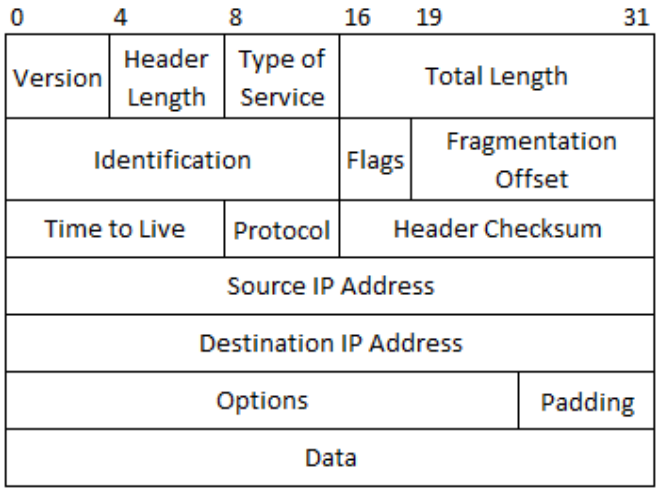
TCP/IP protokolleri endüstri standardı olarak geliştirilmiş, temel amaç güvenlik olmamış ve bu konuda esnek davranılmıştır. Bundan dolayı protokollerde istismara açık birçok durum ortaya çıkmıştır [3; 4; 5]. Bu bölümde hem protokol bilgileri sunulmakta, hem de protokollerin güvenlik analizi ve istismara açık olan bazı kısımları anlatılmaktadır.

2.1. IP

Internet Protocol (IP), günümüz Internet ağının temelini oluşturan TCP/IP Protokol kümesinin başlıca protokollerindendir. Adresleme ve yönlendirme işlemlerini yapar.

IP bağlantısız (connectionless) bir protokoldür, yani veri iletiminden önce oturum kurulmaz, tarafların anlaşması gerekmez. Verinin iletim başarısı garanti edilmez, Internet ortamında bu işlem bir üst katmandaki TCP ile sağlanır. Bu protokole göre bilgisayarlar mantıksal olarak adreslenir. Verilen adresler 32 bitten oluşur ve noktalarla ayrılmış 8'er bitlik oktetler halinde ifade edilir. Örneğin bir bilgisayarın adresi 192.168.56.101 şeklinde olabilir.

IP, verinin paketler halinde yönlendirilerek iletilmesini sağlar. Oluşturulan veri paketi başlık ve payload (veri) kısımlarından oluşur. Başlık kısmında kaynak bilgisayarın adresi ve hedef bilgisayarın adresi ile beraber verinin iletimi için gerekli olan diğer bilgiler de tutulur. IP paket başlığı Şekil 5'te verilmiştir.



Şekil 5. IP Paket Başlığı Yapısı

IP paket başlığının alanları özetle aşağıdaki gibidir [6; 7].

- *Version*: IP paketinin versiyonunu belirtir.
- *Header Length*: 32 bitlik birimler olarak paket başlığının uzunluğunu belirtir. 5'ten küçük olamaz.
- *Type of Service*: Üst katman protokolleri tarafından istenen servis kalitesini belirtir.
- *Total Length*: Başlık ve veri dâhil paketin toplam uzunluğunu belirtir.
- *Identification*: Gönderici tarafından atanan, bölünmüş paketlerin birleştirilmesi için gerekli tanımlama değeri.
- *Flags*: 3 bitten oluşan parçalanma kontrol bitleri.
- *Fragmentation Offset*: Veri iletiminde paketler parçalandığında her parçanın bütünün içindeki yerini gösterir.
- *Time to Live*: Paket ağ düğümlerinden geçtikçe bir azalan yaşam süresini gösterir. En fazla 255 olabilir. 0 olunca paket ağdan atılır.
- *Protocol*: Üst katman protokolüne ait bilgiyi içerir.
- *Header Checksum*: Başlıktaki hataları fark etmek için kullanılır.
- *Source IP Address*: Göndericinin IP adresi.
- *Destination IP Address*: Alıcının IP adresi.
- *Options*: Pek kullanılmaz. Gerektiğinde kaynak yönlendirme, zaman, güvenlik amaçlı kullanılır. Kullanıldığında 32 bit ve katlarında olmalıdır.

IP için istismara açık durumlardan bir tanesi, üçüncü bölümde detayları verilen, kaynak IP adresinin farklı gösterilmesiyle karşı tarafın aldatıldığı IP Spoofing (aldatma) işlemidir.

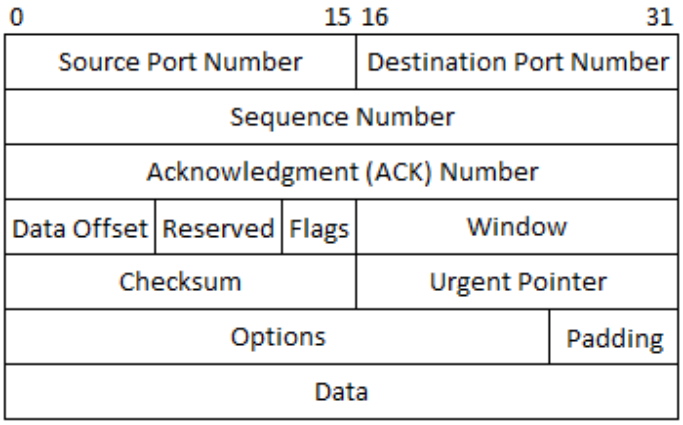
Bir bilgisayar ağında o anki iletişim için kullanılmayan IP başlığındaki bazı alanlar değiştirilerek, asıl verinin yanı sıra paket yapısının içinde farklı verilerin iletimi ile o anki iletişim veri gizleme amaçlı kullanılabilir [6; 8]. Bununla ilgili detaylar beşinci bölümde verilmektedir.

IP paketinin fragmentasyonunun (parçalanabilmesinin), yol açtığı güvenlik zafiyetleri söz konusu olabilir. Meselâ bazı saldırı tespit sistemleri parçalanmış olarak gelen IP paketinin ilk kısmına bakıp paket başlık yapısını inceledikten sonra diğer parçalarla ilgilenmeden iletirler. Bu durumda bir saldırgan paketi göndermeden önce yardımcı araçlarla paketi parçalayıp, birinci parçadan sonrakilere zararlı komut ve veriler yerleştirerek hedefe gönderebilir [9].

2.2. TCP

Transmission Control Protocol (TCP), taşıma katmanında yer alır, bağlantılı (connection-oriented) ve güvenli bir iletişim sağlar. Bağlantılı iletişim, gönderici ve alıcı tarafların oturum kurduktan (anlaştıktan) sonra veri iletişimini yapmasıdır.

TCP paketleri (segment), bir alt katmanda yer alan IP paketleri tarafından taşınır. IP, verinin gideceği adresi belirleyip paketi yönlendirirken, TCP, iletilecek verinin hangi servis ve uygulama tarafından kullanılacağını port numarası ile belirler [5]. Şekil 6'da TCP paketinin başlık yapısı gösterilmiştir.



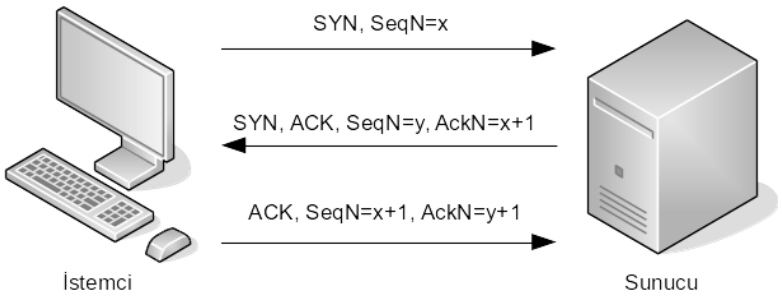
Şekil 6. TCP Paket Başlığı Yapısı **[7]**

TCP başlığının alan bilgileri aşağıdaki gibidir [7].

- *Source Port Number*: Kaynak port adresi.
- *Destination Port Number*: Hedef port adresi.
- *Sequence Number*: SYN bayrağı 1 ise ilk sıra numarasıdır, 0 ise geçerli oturum için arttırılmış sıra numarasını belirtir.
- *Acknowledgment (ACK) Number*: ACK bayrağı 1 iken alıcının beklediği sıra numarasıdır. Bağlantı kurulduğunda bu değer daima gönderilir.
- *Data Offset*: 32 bitlik birimler halinde, başlıktan sonra verinin başladığı yeri, dolayısıyla TCP başlık uzunluğunu belirtir.
- *Flags*: Kontrol bitleridir. SYN, ACK, RST, FIN, URG, PSH olarak isimlendirilen bitler bulunur.
- *Window*: Alma penceresi büyüklüğü; bu segmentin göndericisinin şu anda almak için istekli olduğu pencere boyutu birimlerinin sayısını belirtir. Akış denetimi için kullanılır.
- *Checksum*: Başlık hata kontrolü için kullanılır.
- *Urgent Pointer*: Acil bir veri iletilmek istenirse kullanılır.

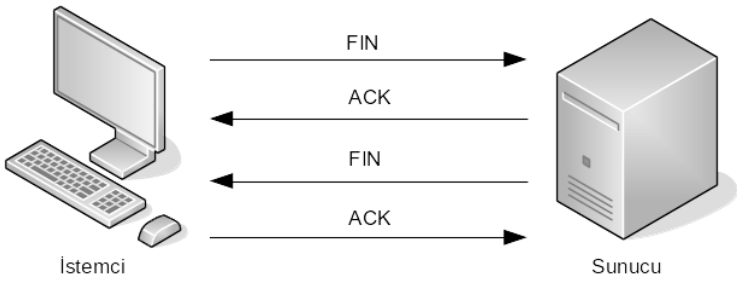
TCP'de iki nokta (node) arasında üçlü el sıkışma (handshaking) olarak adlandırılan bağlantı kurulumu Flags alanındaki SYN ve ACK bayraklarının ayarlanması ile yapılır. İstemci sunucuya bağlantı kurma isteğini SYN işaretli paketi göndererek bildirir, buna karşılık bağlantıyı kabul eden sunucu SYN ve ACK işaretli bir paketle cevap verir, istemci bu paketi aldıktan sonra ACK işaretli bir paket gönderir. Bu gönderimler esnasında

karşılıklı teyitleşme için paketlerin Sequence Number ve ACK Number alanları da ayarlanıp kullanılır. Bu durum Şekil 7'de gösterilmiştir.



Şekil 7. TCP'de El Sıkışma (Handshaking) İşlemi

TCP bağlantı sonlandırılması işleminde ise bağlantıyı sonlandırmak isteyen taraf FIN bayrağı ayarlanmış bir paketi karşı tarafa gönderir. Karşı taraf ACK işaretli bir paket ile cevap verip, peşinden FIN işaretli bir paket gönderir. Bağlantıyı sonlandırmak isteyen taraf son olarak ACK işaretli bir paket ile cevap gönderdiğinde bağlantı sonlandırılmış olur. Bu durum Şekil 8'de gösterilmiştir.



Şekil 8. TCP'de Bağlantı Sonlandırma İşlemi

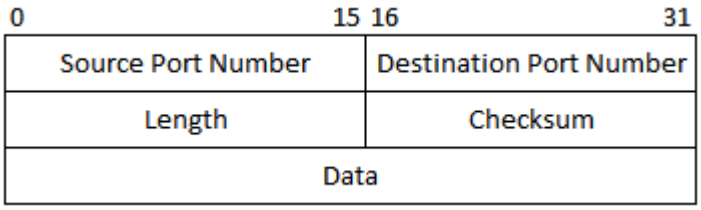
TCP bağlantı kurulumu sayesinde, TCP tabanlı servislerde ve protokollerde IP Spoofing işlemi yapılamamaktadır.

TCP'deki bayraklar ağ güvenliği alanında çokça kullanılmaktadır. TCP tabanlı saldırılardan en çok bilineni, TCP'deki el sıkışma işlemini istismar eden SYN Flood saldırısıdır. Ağ keşfinde, ICMP Ping paketlerinin engellendiği ortamlarda TCP'nin SYN, ACK, FIN bayraklarından yararlanılmaktadır [10; 11].

2.3. UDP

UDP (User Datagram Protocol), TCP'nin de bulunduğu taşıma katmanında yer alır. UDP, verinin iletimini garanti edecek mekanizmalara sahip olmadığından güvenilir bir veri aktarımı sağlamaz. Bağlantı kurma, akış denetimi, tekrar iletim gibi özellikler olmadığından ve veri paketi (datagram) başlık boyutu küçük olduğundan hızlı veri iletimi sağlar. Genellikle gerçek zamanlı gönderilecek ses ve video gibi veriler ile önemli olmayan bilgi amaçlı verilerin iletiminde kullanılır. DNS ve SNMP gibi protokollerin verilerinin iletiminde de kullanılır. Paket başlığı ve bir anda iletilen veri boyutu küçük olduğundan parçalamaya gerek duyulmaz [5].

UDP paketleri alıcıya iletilmek için TCP'de olduğu gibi IP paketlerine eklenip gönderilir. UDP paketinin başlık yapısı oldukça basittir. UDP paketinin başlık yapısı Şekil 9'da gösterilmiştir.



Şekil 9. UDP Paket Başlığı Yapısı **[7]**

UDP paket başlığının alanları şunlardır [7]:

- *Source Port Number*: Kaynak port adresi. İsteğe bağlı olarak boş bırakılabilir.
- *Destination Port Number*: Hedef port adresi.
- *Length*: Paketin toplam uzunluğunu belirler.
- *Checksum*: Hata kontrolü yapmak için kullanılan isteğe bağlı bir alandır. Kullanılmadığı zaman 0 (sıfır) değeri atanır. UDP'deki hata kontrolü sadece paketteki verinin hatasız taşınması içindir, verinin yeniden iletimi söz konusu değildir.

UDP bağlantı temelli olmadığından, istenildiği kadar UDP verileri bir sunucuya veya bilgisayara gönderilebilir. Başta UDP Flood saldırısı olmak üzere, UDP tabanlı saldırılar yapılabilir. Ayrıca bir sunucuda UDP tabanlı (DNS, SNMP gibi) protokoller veya gerçek zamanlı video ve ses akışı kullanılıyorsa, sunucu üzerinde UDP veri paketlerini almayı

tamamıyla reddetme gibi bir güvenlik önlemi düşünülemeyeceğinden farklı tedbirlere gidilmesi söz konusudur [5; 12].

2.4. ARP

Veri iletiminde hem göndericinin hem alıcının IP adresleri bilinir. Ancak yerel ağda veri iletilirken gideceği cihazın ağ bağdaştırıcısının fiziksel adresinin (MAC adresi) bilinmesi gerekir. ARP (Address Resolution Protocol), IP adresini fiziksel adrese (MAC adresine) dönüştürmek için kullanılır [5; 7].

Veri gönderecek olan bilgisayar, hedefteki bilgisayarın IP adresini bilir. Ağdaki cihazlara ve bilgisayarlara bu IP adresinin sahip olduğu fiziksel adresi soran istek paketleri gönderir. ARP istek mesajlarını alan bilgisayar veya ağ cihazları eğer hedef iseler veya hedefe giden yolda iseler bu isteğe cevap verip kendi fiziksel adreslerini bildirirler. ARP isteğinde bulunan makine, verileri gelen bilgideki adrese gönderir. Hedef olmayan bilgisayarlar ise bu isteğe cevap vermez ve mesajı çöpe atar [13].

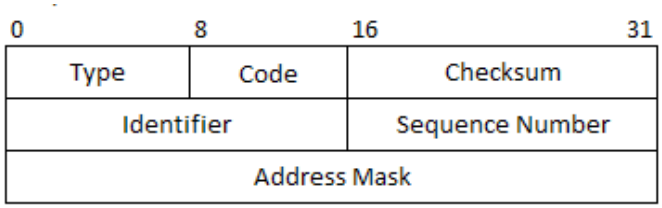
Bilgisayarlar ARP istek mesajlarını gönderip fiziksel adresleri öğrendikçe IP adresi - MAC adresi bilgilerini ARP tablosu adı verilen bir tabloda tutup, daha sonra verilerin gideceği adresi bu tabloya göre otomatik seçerler.

ARP tablosu üzerinde yapılabilecek bir değişiklikle yerel ağda ARP Spoofing veya ARP Cache Poisoning olarak adlandırılan (üçüncü bölümde anlatılan) bir saldırı şekli mevcuttur.

2.5. ICMP

Internet Control Message Protocol (ICMP), ağın işleyişi ve performansı hakkında kullanışlı bilgileri toplama ve hata raporlama için kullanılan kontrol amaçlı bir protokoldür. TCP/IP'nin işleyişine yardımcı olur.

ICMP, basit bir paket başlığı yapısına sahiptir. Veri paketinin başlığında port numarası gibi bir alan bulunmayıp, Type ve Code gibi alanlar vardır. Bu bilgilerle paketin hangi durum bilgisini verdiği anlaşılır. ICMP paket başlığı yapısı Şekil 10'da verilmiştir.



Şekil 10. ICMP Paket Başlığı Yapısı **[7]**

ICMP'nin sağladığı mesaj hizmetlerinden en önemli üçü şunlardır [14]:

- *Ping*: Başka bir IP adresinin erişilebilirliğini belirlemek için kullanılır.
- *Traceroute*: Bir IP adresine erişirken takip edilen yolu keşfetmek için kullanılır.
- *Destination unreachable*: Bir yönlendirici, kendisinden sonra herhangi bir yönlendiriciye gitmeyecek olan bir datagram (veri paketi) algıladığında "destination unreachable" (hedef erişilemez) mesajı üretir ve onu datagram kaynağına iletir.

ICMP bilgi toplama amaçlı kullanıldığından, bazı ağ ortamlarında genellikle kötü amaçlı kullanımlara karşı ICMP paketlerinin iletimine (bazı tipleri hariç) izin verilmemektedir.

2.6. IPv6

IPv6, TCP/IP'nin yeni nesil yönlendirme katmanı protokolüdür. Günümüzde kullanılan IPv4'ün bazı açılardan yetersiz kalması ve bazı iyileştirmelerin yapılması ihtiyacına binaen geliştirilmiştir [5].

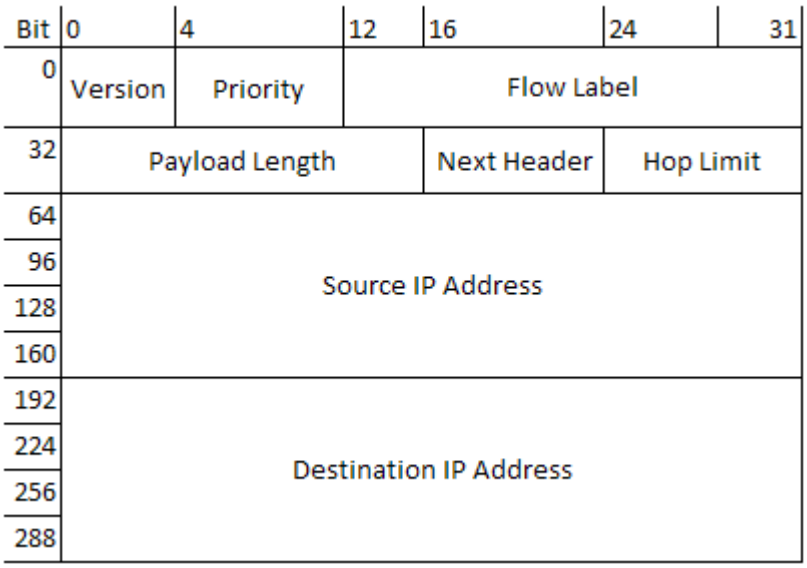
IPv6 ile beraber IPv4'te bulunan bazı az kullanılan alanlar kaldırılmıştır. IPv6'da özellikle göze çarpan değişiklik adresleme alanının genişliğidir. IPv4'de 32 bit olan IP adresleri, yeni versiyonla 128 bit olmuştur.

IPv6 ile gelen yeniliklerden bir kısmı şunlardır [2; 5; 13]:

- Daha geniş adres uzayı
- Bir ağda birçok hedefe aynı anda veri iletimi (multicasting)
- Ağ katmanı güvenliği (IPSec protokolü ile)
- Daha basit paket başlığı yapısı

- Geliştirilmiş servis kalitesi ile daha hızlı ses ve video iletimi
- Daha kolay ve verimli yönlendirme
- Otomatik adres yapılandırılması

Şekil 11'de IPv6 paket başlığı gösterilmiştir.



Şekil 11. IPv6 Paket Başlığı Yapısı **[7]**

IPv6 başlığındaki alanlar şunlardır [7]:

- *Version*: Paket versiyonu, sabit 6 (0110)
- *Priority (Traffic Class)*: IPv4'teki Type of Service alanına karşılık gelir, paketin taşıdığı veri tipine göre yönlendirmede öncelik tanınır.
- *Flow Label*: Başlangıçta gerçek zamanlı veri akışı için özel olarak konulmuştur. Servis kalitesi için farklı akışların ayırt edilmesine imkân verir. Paketin hedefe hangi yol ile ulaşacağını verir. Yönlendirme işini basitleştirir. Paketlerin çakışmaması için bir paket hedefe ulaşmadan başka bir pakete aynı akış etiketi verilmez.
- *Payload Length*: Varsa ilave başlıklar da dahil olmak üzere taşınan verinin uzunluğunu bayt (oktet) miktarı olarak verir.
- *Next Header*: Sonraki başlığın tipini belirtir. Bu alan çoğunlukla paketin payload kısmında kullanılan taşıma katmanı protokolünü belirtir. Taşıma katmanı protokollerinin en çok bilinen ve kullanılanları TCP ve UDP'dir. Bu

kullanımıyla IPv4'deki Protocol alanına benzer. Bir diğer kullanımı ise IPv6 paketinin ilave paketlerini belirtmek içindir.

- *Hop Limit*: Bu 8 bitlik alandaki sayı, paketi yönlendiren her bir noktadan (yönlendiriciden) geçtiğinde bir azaltılır. Değeri 0 (sıfır) olduğunda paket atılır. IPv4'deki Time to Live alanının yaptığı işi yapar.
- *Source IP Address*: Gönderici tarafın IP adresi.
- *Destination IP Address*: Alıcı tarafın IP adresi.

2.7. DNS Protokolü

DNS (Domain Name System – Alan Adı Sistemi), Internet uzayını bölümleme, adlandırma ve bölümler arası işleri organize etmeye yarar. Internet ağında her bilgisayar kendi IP adresine sahiptir. Bilgisayarların kolay bilinip hatırda tutulabilmesi için IP adreslerine karşılık isimler verilir. DNS, en fazla 256 karakter uzunluğa sahip olabilen host isimlerini IP adreslerine çevirmek için kullanılan bir sistemdir. Host isimleri hem bilgisayarın adını verir hem de ait olduğu domaini belirlememize yardımcı olur [13].

DNS Protokolü, DNS'in çalışması için kullanılan sorguları, bu sorguların işlenmesi için gerekli paket yapılarını vs. tanımlar. DNS Protokolü, uygulama seviyesi bir protokoldür. Ağ üzerinden veri iletiminde başlıca kullandığı aktarım katmanı protokolü UDP'dir. Ancak UDP'nin paket boyutunun yetmediği durumlarda TCP'yi kullanır.

DNS sunuculara hem DNS Flood, hem DNS Poisoning gibi saldırılar yapılabilmektedir.

2.8. SNMP

SNMP (Simple Network Management Protocol), bir uygulama katmanı protokolü olup, TCP/IP protokol kümesi içinde ağ yönetimi için tanımlanmış protokollerden en yaygın olanıdır [13]. Ağ cihazları arasında ağ yönetimi ile ilgili bilgilerin değiş-tokuşunu, ayrıca ağ yöneticilerinin ağ performansını yönetmesini, ağ problemlerini bulmalarını ve çözmelerini ve ağ büyümesini planlamalarını sağlar [5; 7].

2.9. FTP

File Transfer Protocol (FTP), kullanıcıların iki host (sunucu-istemci) arasında dosya kopyalamasına imkân tanır. Kullanıcılar FTP sunucuya bağlanırken kimlik doğrulamasından geçerler. FTP ile host üzerindeki donanımdan bağımsız olarak dosya ve klasör listeleme, silme, ekleme, değişik komutları işleme yapılabilmektedir. FTP, dosya transferinin garanti altına alınması için taşıma katmanında TCP'yi kullanır [5].

2.10. HTTP

HyperText Transfer Protocol (HTTP), HTML (HyperText Markup Language) belgelerinin iletimini sağlamak için tasarlanmış bir protokoldür. HTTP, istek (request) – cevap (response) faaliyeti tabanlıdır. İstemci taraf, web tarayıcı programı ile sunucuyla bağlantı kurarak, sunucudan bir talep metodu formunda talepte bulunur. Sunucu, durum bilgisiyle beraber cevap verir. Sunucunun cevabında hata veya başarı mesaj kodları, sunucu bilgilerini içeren mesajlar ve istenen sayfanın mümkün olan içeriği bulunur.

2.11. SMTP

Simple Mail Transfer Protocol (SMTP), varsayılan olarak TCP'nin 25 numaralı portunu kullanan Internet üzerinden elektronik posta göndermek için kullanılan bir protokoldür.

2.12. DHCP

DHCP (Dynamic Host Configuration Protocol), bir ağdaki makinelere otomatik olarak IP adresi vermek, alt ağ maskesi ayarlamak, makinelerin ağa erişimlerinde ağ geçidi bilgilerini ve DNS sunucu bilgilerini vermek için kullanılır. Uygulama seviyesi bir protokol olup, taşıma katmanında UDP'yi kullanır [2; 5].

DHCP, günümüzde neredeyse tüm ev ve işyeri ağlarında kullanılır. Bir ağa bağlı her bir bilgisayara ayrı ayrı IP adresi verilmesi çok zahmetli olduğundan sistem yöneticilerine kolaylık sağlar. Yerel bir ağda bir bilgisayar DHCP sunucusu olarak ayarlanır. Bu sunucu bilgisayar, ağdaki tüm bilgisayarlara otomatik olarak IP adresi tahsis eder.

DHCP, istek-cevap tabanlı bir protokoldür. Ağa bağlanan bir istemci ilk olarak ortama bir keşif paketi gönderir, keşif paketini alan DHCP sunucusu istemciye verilebilecek IP numarasını bir teklif paketi ile ortama gönderir. Daha sonra istemci istek paketi gönderir, sunucu, istemcinin alabileceği IP numarasını cevap paketiyle döner. Belirlenen IP adresi bir süreliğine istemciye kiralanır, kiralama süresi doldukça, istemci ağa bağlı ise adres tekrar tahsis edilir. DHCP sunucudan sadece IP adresi değil, aynı zamanda alt ağ maskesi, ağ geçidi bilgileri de istemciye aktarılır.

2.13. POP

POP (Post Office Protocol)'ün güncel versiyonu POP3'tür. POP3 iyi bilinen 110 numaralı TCP portunu kullanır. İstemcinin yerel makinede, sunucunun da uzak makinede çalışmasını sağlar. POP3'ün işlevi uzak POP3 sunucusundan e-mail alıp, yerel POP3 istemcisine getirmek, istemcinin sunucu üzerinde belli komutlar çalıştırarak e-maillerini yönetmesini sağlamaktır [15].

3. AĞ SALDIRI TÜRLERİ

3.1. Sniffing

Sniffing (Koklama-İzleme), ağ paketlerini yakalayıp takip etme ve analiz etme işlemidir. Bunun için ağ cihazları ve bilgisayarlar aracılığıyla ağ ortamındaki veri trafiğini görebilecek şekilde fiziksel veya kablosuz bir bağlantı sağlanarak, paket izleyici programlar kullanılır.

Sniffing işlemi kullanım amacına göre saldırı olarak değerlendirilebileceği gibi ağdaki veri trafiğinin takibiyle saldırı tespiti veya veri alışverişinin verimliliğinin sağlanması gibi değişik amaçlı olabilir. Kötü niyetli bir kullanıcı ağdaki paketleri yakalayıp analiz ederek kişisel ve gizli olup şifrelenmeden iletilen verileri okuyabilir. Bu veri okuma işlemi ağ düzeyinde en basit saldırı şeklidir [5].

Temel olarak art niyetli kullanıcılar şu amaçlarla sniffer programlar kullanırlar [16]:

- Kullanıcı adı ve şifre bilgilerini elde etme
- Bir ağdaki kullanıcıların ağ kullanım örüntülerini keşfetme
- Kişisel gizlilik derecesi olan bilgileri elde etme
- VoIP görüşmelerini yakalayıp tekrar oynatma
- Bir ağın düzenini haritalama
- Pasif işletim sistemi bilgilerini elde etme

Sniffer programların kullanıldığı makinelerde, ağdan gelen her verinin kabul edilmesi isteniyorsa makinenin ağ arayüzünün promiscuous (her gelen veriyi kabul eden) modu desteklemesi gerekir.

3.2. Spoofing

Spoofing (Aldatma), temel olarak, bir bilgisayar ağında bir makinaya bağlanıp veri alış verişinde bulunurken iletişim bilgilerini farklı göstererek karşı tarafı aldatma işlemidir. En basit haliyle değiştirilecek bilgiler kaynak IP adresi, kaynak MAC adresi veya kaynak port numarası olabilir.

3.2.1. IP Spoofing

İletişim kurulan bilgisayar veya cihaza veri gönderilirken kaynak IP adresini gerçeğinden farklı gösterme işlemidir. Genellikle hizmet engelleme (DoS) saldırılarında saldırgan gerçek IP adresini gizleyerek kendisinin tespit edilmesini zorlaştırır hatta imkânsız hale getirir.

TCP/IP Protokol Kümesindeki protokollerin bazı güvenlik sorunları üst katmanlardaki protokoller ile yok edilebilir, azaltılabilir. Örneğin, TCP'nin el sıkışma ile bağlantı kurulumu sayesinde, kurulmuş bir bağlantı varsa, IP Spoofing işlemi her zaman her ağ ortamında rahatça uygulanamaz. Ancak UDP ve DNS ile IP Spoofing daha kolay uygulanabilir [4].

3.2.2. MAC Spoofing

MAC Spoofing, ağ arayüz kartlarının fabrika çıkışlı MAC adreslerini farklı gösterme tekniğidir. Bunun çeşitli sebepleri olabilir. Örneğin, ağda erişim denetiminden geçme, bir bilgisayarın ağdaki varlığını gizleme, ya da bir bilgisayarın başka bir bilgisayar imiş gibi davranması, taklit etmesi gibi işlemler MAC Spoofing ile mümkündür.

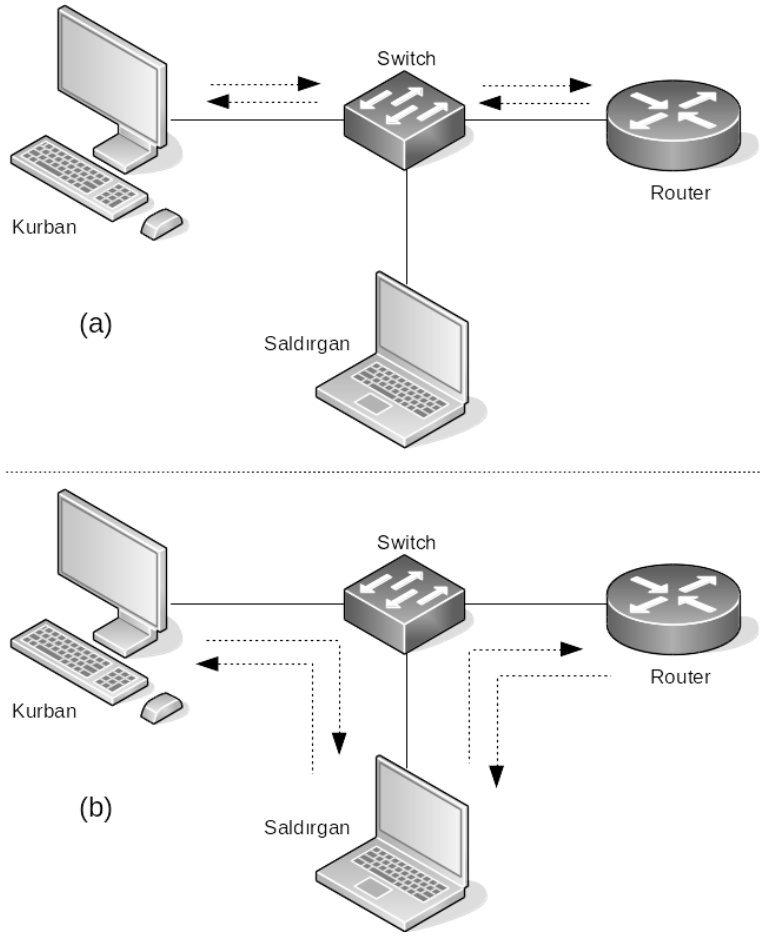
3.2.3. ARP Cache Poisoning

ARP Cache Poisoning (ARP Önbellek Zehirleme), aynı zamanda ARP Poisoning veya ARP Spoofing olarak da tarif edilir. Özellikle Switch cihazı kullanılan yerel ağlarda Man In The Middle (MITM, Ortadaki Adam) saldırılarında veya ağ izlemede kullanılır.

Yerel bir alan ağında Hub, bir portuna gelen veriyi diğer portlarına gönderir. Hub'a bağlı olan tüm bilgisayarlar ve cihazlar veriyi görür, ancak verinin sadece hedefi olan bilgisayar onu alıp işleme koyar. Switch kullanılan ağlarda, Switch, ARP tablosu olarak adlandırılan IP adresi ve MAC adresi eşleştirmelerinin tutulduğu bir tabloyu kullanarak kendisine gelen veriyi sadece hedef bilgisayara gönderir.

Adres Çözümleme Protokolü (ARP) ile IP-MAC dönüşümü yapılır. ARP Poisoning işleminde, Switch gibi cihazlarda yer alan ARP tablolarındaki IP-MAC eşleştirmeleri üzerinde değişiklikler yapılır. Saldırgan, kurban olarak belirlenen bilgisayara ait IP adresi

ile kendi MAC adresini eşleştirir. Bu durumda kurban bilgisayara gidecek olan veriler, Switch tarafından saldırgan bilgisayara gönderilecektir . ARP Poisoning ile MITM saldırısı öncesi ve sonrası ağ trafiği Şekil 12'de gösterilmiştir.



Şekil 12. ARP Poisoning ile MITM Saldırısı
(a) Normal Trafik (b) Saldırı Sonrası Trafik

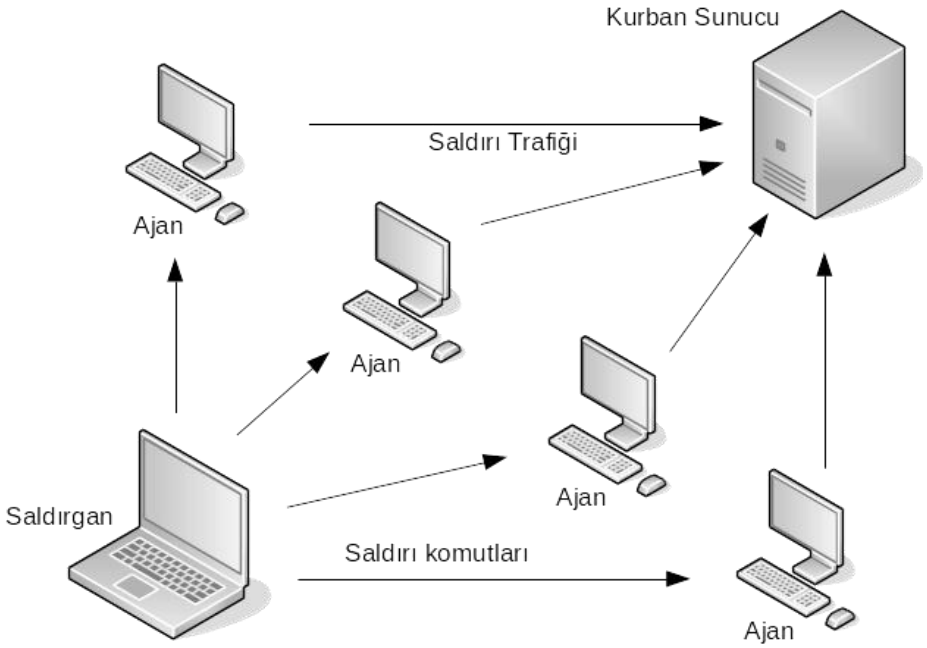
3.2.4. DNS Poisoning

DNS Poisoning işlemi, ARP Poisoning ile çok benzerdir. Saldırgan DNS sunucularındaki açıklardan faydalanarak, sunucuların Internet ortamındaki alan adlarını kaydettiği tablolarda değişiklik yapar. Belirli bir alan ismine tahsis edilmiş IP adreslerini değiştirerek, kendi sunucularının IP adreslerini bu tablolara girer. Sıradan bir kullanıcı bu alan ismi ile web sunucuya erişmek istediği zaman, saldırganın belirlediği IP adresine sahip sunucuya yönlendirilecektir.

3.3. Hizmet Engelleme Saldırıları

Hizmet engelleme saldırıları (DoS - Denial of Service) Internet dünyasında en çok karşılaşılan saldırı türüdür. Saldırgan hedefindeki sistemi (sunucuyu), protokol açıklarından yararlanıp, ya sürekli meşgul edip kaynak yetersizliğinden ya da sunucunun ağ bağlantısındaki bant genişliğini doldurup, iletişimini tıkamak suretiyle hizmet veremeyecek duruma düşürür [4].

DDoS (Distributed DoS), hizmet engelleme işleminin çok sayıda zombi saldırgan makineler kullanarak, organize bir şekilde yapılması işlemidir [4]. Yüksek bant genişliğine ve hizmet kapasitesine sahip sunucular ancak DDoS ile hizmet veremez duruma getirilebilir. Şekil 13, DDoS saldırı şeklini modellemektedir.



Şekil 13. DDoS Saldırısı

Saldırgan, DDoS saldırılarında IP Spoofing ile kendi IP adresini gizleme ihtiyacı hissedecektir, ancak bu durum üst katmanlardaki bazı protokollerin kullanımında mümkün değildir. Örneğin, SYN Flood saldırısında IP Spoofing mümkün iken, HTTP GET Flood saldırısında kurulmuş bir bağlantının gerekliliğinden dolayı bu mümkün değildir.

Hizmet engelleme saldırılarının en çok bilinenlerinden bir kısmı aşağıda açıklanmıştır.

3.3.1. SYN Flood

SYN Flood, en kolay gerçekleştirilen servis engelleme (DoS) saldırı çeşitlerinden biridir. TCP ile haberleşecek olan iki nokta arasında bağlantı kurulurken karşılıklı SYN ve ACK bayraklarına sahip TCP paketleri birbirlerine gönderilir. TCP'de el sıkışma (handshaking) olarak adlandırılan bu aşamadaki paket gönderimleri istismar edilerek SYN Flood gerçekleştirilebilir.

SYN Flood işleminde, saldırgan, hedefindeki sunucuya sürekli olarak SYN bayraklı TCP paketleri gönderir [2]. Hedef sunucu, kendisine gelen her SYN paketine bağlantı kurulumunu gerçekleştirmek amacıyla ACK paketleri ile cevap vermeye çalışır. SYN paketleri artarda geldiğinde belli bir kapasiteden sonra sunucu artık cevap veremez duruma gelir [10].

3.3.2. ACK/FIN/PUSH Flood

Veri gönderirken TCP başlığındaki ACK, FIN veya PUSH bayraklarının ayarlanıp sunucuya gönderilmesi ve sunucunun kapasitesinin zorlanmasıdır. Genellikle SYN Flooding işlemine karşı sunucuda alınan tedbirler varsa bu yöntem denenir. Ancak SYN Flood kadar etkili değildir. Engellenmesi kolaydır [5; 12].

3.3.3. UDP Flood

UDP Flood, temel olarak, saldırganın hedef sunucunun farklı port numaralarına sürekli olarak UDP paketleri göndermesidir.

UDP'de oturum kurulumu (TCP'deki el sıkışma gibi) olmadığı için, açık portlara istenildiği kadar paket gönderilebilir. Bu durumda IP Spoofing yapılması için de bir engel bulunmaz. Sunucuya gelen UDP paketi olduğunda, sunucu sonraki gelecek veriler için bağlantıyı bir müddet açık tutar. Sunucuda, sürekli bir kaynak tüketimi meydana gelir ve belli bir kapasiteden sonra artık gelen bağlantılara cevap veremez. UDP Flooding işleminde, UDP paket boyutunun küçüklüğü, belli bir zamanda gönderilebilecek paket sayısının daha fazla olmasını sağladığından dolayı avantajlıdır [5; 12].

3.3.4. DNS Flood

DNS, hem UDP hem de TCP üzerinden çalışan bir sistemdir. DNS Protokolünün saldırılara açık olan kısmı UDP üzerinden çalışanıdır.

DNS Flooding işleminde, UDP üzerinden IP Spoofing kullanımıyla birlikte, DNS istek paketlerinin gönderiminde saldırgan açısından pek bir engel bulunmaz. DNS sunucuya sürekli olarak rastgele istek paketleri gönderilerek DNS sunucu meşgul edilir [5; 17].

3.3.5. MAC Flood

Yerel bir ağda, bilgisayarlar arasındaki bağlantıyı sağlayan switch, kendisine gelen veriyi sadece ilgili makineye gönderdiğinden, switch kullanılan ağlarda sniffing (dinleme) işlemi yapılamamaktadır. Switch kullanılan ağdaki trafiği dinlemenin yollarından biri yukarıda belirtilen ARP Cache Poisoning iken, bir başka seçenek MAC Flood saldırısıdır.

Switch, kendisine bağlı makinelerin MAC adresleri ile IP adreslerini eşleştirip bir tabloda tutar. MAC-IP eşleştirme tablosu, yerel ağdaki makine sayısı arttıkça zamanla dolabilir. Tablo dolduğu zaman switch, bir hub cihazı gibi davranmaya başlar. MAC Flood işlemi bu durumu istismar eden bir saldırı tipidir. Saldırgan switch cihazına rastgele sahte MAC adres bilgileri göndererek tablonun dolmasını sağlar ve amacına ulaşmış olur [16].

3.3.6. HTTP GET/POST Flood

HTTP, web sayfalarının sunulması için kullanılan bir uygulama seviyesi protokolüdür. HTTP GET/POST Flood tekniğinde web sunucuya sürekli olarak web sayfası istek mesajları gönderilir ve sunucu meşgul edilir.

HTTP'de sayfa isteklerinin gerçekleşmesi için giden-gelen veri miktarı sadece TCP veya UDP kullanılarak iletilen veriden çok daha fazladır. Bundan dolayı HTTP GET/POST Flood saldırısı sunucunun kaynaklarını daha fazla tüketir. Ancak SYN Flood'a kıyasla daha kolay önlenebilir. HTTP, TCP'yi kullandığından, TCP bağlantı kurulumunun gerçekleştirilmesi gerektiğinden, HTTP Flood işlemiyle beraber IP Spoofing yapılamaz [5; 12].

3.4. Ağ Keşfi

Ağ keşfi, ağdaki mevcut hostları, cihazları, kullanılan servisleri, IP numaralarını, sunuculardaki açık portları tespit etme işlemidir. Amaç istismar edilebilecek bir kaynak bulmaktır.

3.4.1. IP Tarama

IP tarama, bir ağdaki açık makineleri tespit etme işlemidir. En basit IP tarama yöntemi Ping Scan'dır. Belirlenen IP adresine ICMP echo request paketleri gönderilir, IP adresi kullanımda ise ICMP echo reply paket tipi dönecektir. Bazı sunuculardaki güvenlik duvarları Ping paketlerinin geçişine izin vermemektedir. Bu durumda port tarama işlemlerinde kullanılan teknikler yardımcı olacaktır.

3.4.2. Port Tarama

Port tarama, değişik tekniklerle bir sunucunun hangi port numaralarından veri alışverişi yaptığının tespit edilmesi işlemidir. TCP, IP, ICMP, UDP gibi protokollerin bazı özelliklerinden hareketle onlarca farklı teknik ile açık port tespiti mümkündür.

Port tarama tekniklerinden bir kısmı aşağıda açıklanmıştır [16; 11].

- TCP Connect Scan işleminde, saldırgan, hedef sunucuya SYN paketi gönderir, sunucudaki port açıksa SYN+ACK döner, saldırgan ACK göndererek bağlantıyı kurmuş olur ve peşinden RST göndererek sonlandırır. Bu tür bir tarama kolaylıkla teşhis edilebilir.
- TCP SYN Scan işleminde, hedef sunucuya SYN bayraklı TCP paketi gönderilir. Paket gönderilen port açıksa, SYN+ACK paketi cevap olarak döner ve saldırgan bir RST (reset) paketi göndererek bağlantıyı kurmadan iptal eder. Port kapalı ise sunucudan RST cevabı gelecektir.
- TCP FIN Scan işleminde, saldırgan, hedef sunucuya FIN paketi gönderir, taranan port açıksa herhangi bir cevap gelmeyecek, port kapalı ise RST+ACK paketi dönecektir.
- TCP Xmas Scan işleminde, hedef sunucuya geçersiz bayrak ayarlarıyla FIN+PSH+URG paketi gönderilir. Dönecek cevap TCP FIN Scan ile aynıdır.

Ancak Microsoft Windows, Cisco IOS, BSD, HP/UX ve IRIX işletim sistemlerinde çalışmaz, çünkü port açık veya kapalı olsun dönen cevap daima RST olacaktır.

- Null Scan işleminde, hiçbir bayrağı set edilmemiş bir TCP paketi gönderilir, dönecek olan cevap FIN Scan ile aynıdır.
- UDP Scan işleminde, hedef makineye UDP paketi gönderilir, port kapalı ise dönen cevap ICMP Post Unreachabe olacaktır.

3.4.3. İşletim Sistemi Tespiti

İşletim Sistemi Tespiti (OS Fingerprinting), bir makinenin üzerinde çalışan işletim sisteminin, bu bilgisayarın ağ ortamına gönderdiği verilerin analizinden hareketle tespit edilmesi işlemidir. Bu işlem aktif ve pasif olarak yapılabilmektedir. Aktif fingerprinting işleminde saldırgan, hedef makineye bazı veri paketleri yollar ve cevap olarak geri dönen paketleri analiz ederek işletim sistemini tespit eder. Pasif modda fingerprinting ise, hedef makine ile iletişime geçmeden sadece ağ ortamındaki verilerden hareketle işletim sisteminin tespit edilmesi işlemidir. Bu durumda fingerprinting işlemi için kullanılan araç bir sniffer gibi davranır.

OS tespiti için genellikle IP paketindeki TTL ve ID değerleri, TCP başlığındaki seçenekler (genellikle SYN, SYN+ACK) ve TCP pencere boyutu, DHCP istekleri, ICMP istekleri, HTTP paketleri (genellikle User-Agent alanı) gibi veriler analiz edilir. [18]

4. STEGANOGRAFİ

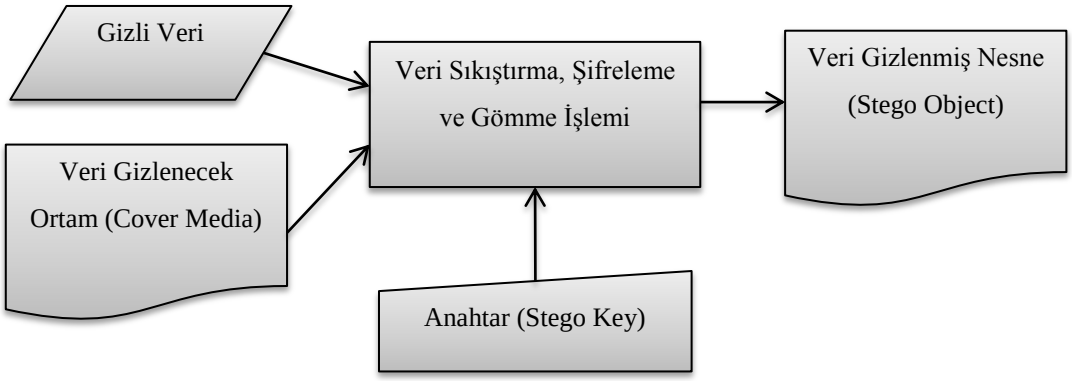
Steganografi, bilgi gizleme sanatı ve bilimi olarak tanımlanır. Steganografide, bilgi, kendisine dair hiçbir işaret içermeyen zararsız, sıradan görünümlü bir ortama gömülür. Steganografide amaç, bilginin anlaşılmamasından çok varlığının gizlenmesi, istenmeyen üçüncü tarafların dikkatinin çekilmemesidir [19].

Önemli ve gizli bilginin istenmeyen kişilerden saklanması söz konusu olduğunda, ilk akla gelen bilgiyi anlaşılmaz hale getiren kriptografi ile beraber, steganografi de çok geniş bir kullanım alanı bulmuştur. Kriptografi, bilgiyi şifreleyip, okunmasını, elde edilmesini zorlaştırır ve bilgiyi korumayı amaçlar. Ancak şifrelenmiş bilgi istenmeyen üçüncü tarafların daha çok dikkatini çeker. Bu açıdan steganografi büyük önem kazanır.

Temel steganografide sadece gizlenecek olan veri veya bilgi, *cover media* olarak bilinen ortama gömülerek, *stego object* olarak tanımlanan veri gizlenmiş nesne elde edilir. Bu durum Şekil 14'te gösterilmiştir.

Şekil 14. Temel Bir Veri Gizleme İşlemi **[19]**

Steganografik yöntemlerle gizlenen verinin varlığının istenmeyen kişilerce fark edilmesi ihtimaline karşı, gizlenecek olan veri önce kriptografik yöntemlerle kodlanıp şifrelenir daha sonra gizlenir. Şifrelemede kullanılacak olan anahtar (*stego key*), alıcı tarafta, veri gömülü ortamdan çıkarıldıktan sonra çözülürken tekrar kullanılır. Bununla beraber daha ideal bir durum için gizlenmeden önce verinin sıkıştırılması da söz konusu olabilir. Şekil 15'te steganografi ile beraber kriptografinin de kullanıldığı durum modellenmiştir.



Şekil 15. Şifreleme ile Beraber Veri Gizleme İşlemi **[19]**

Alıcı taraf, veri gizleme işleminin tersi bir işlemle tekrar veriyi elde edecektir.

Steganografinin bilimsel açıdan gelişimi insanlık tarihi boyunca devam edegelmiş, veri gizleme için farklı ortamlar denenmiş, türlü türlü yeni yöntemler geliştirilmiştir. Tarih boyunca fiziksel ortamın işlenmesiyle gelişen steganografi, günümüzde daha çok elektronik ortamda; resim, ses, video, yazı, iletişim hatları, ağ paketleri vb. veri saklama ortamlarında kendine yer bulmaktadır.

4.1. Antik ve Fiziksel Steganografi

Günümüzün elektronik tabanlı teknolojisinin gelişiminden önce, kıymetli bilgilerin gizlenip alıcıya ulaştırılması için, elle işlenen fiziksel ortamlar kullanılmıştır.

Eski Yunan'da, insanlar tahta üzerine gizli mesajı yazdıktan sonra, üzerini balmumu ile kaplarlar ve alıcıya iletirlerdi. Yine aynı çağlarda, gönderilecek olan mesaj, bir kölenin tıraşlı kafasına dövme ile yazılmış, kölenin saçları uzadıktan sonra, ilgili yere gönderilmiş ve alıcı taraf kölenin kafasını tıraş edip mesajı almıştır. Jeremiah Denton, Kuzey Vietnam'da tutuklu olduğu zamanlarda, 1966'da çıkarıldığı televizyondaki basın toplantısında, gözlerini tekrar tekrar kapatıp açarak Mors alfabesi ile *torture* (işkence) kelimesini kodlamıştır [20; 21].

Şekil 16'da metin tabanlı steganografiye basit bir örnek olarak Birinci Dünya Savaşında Almanlar tarafından gönderilen mesaj gösterilmiştir [22].

President's Embargo Ruling Should Have Immediate Notice. Grave Situation Affecting International Law. Statement Foreshadows Ruin Of Many Neutrals. Yellow Journals Unifying National Excitement Immensely.

Kelimelerin ilk harfleri gizli mesajı verir*: Pershing sails from N.Y. June 1*.

Şekil 16. Basit Bir Metin Steganografi Örneği **[22]**

4.2. Dijital Ortamda Steganografi

Elektronik ve bilgisayar teknolojisinin gelişimi ile modern steganografik yaklaşımlar geliştirilmiş ve yeni farklı ortamlara veri gizlenmeye başlanmıştır. Günümüzde veri gizleme için en çok resim, ses, video, metin dosyaları, dijital ve analog sinyaller gibi iletişim ortamları, verilerin iletişiminde kullanılan protokollerin paket başlık yapıları gibi ortamlar kullanılmaktadır.

4.2.1. Resim Steganografi

Dijital ortamda en çok kullanılan veri gizleme ortamı resim dosyalarıdır. Bunun başlıca sebepleri, veri gizlendikten sonra resim dosyalarında meydana gelecek değişikliklerin insan gözü tarafından algılanmasının zor hatta imkânsız olması ve resim dosyalarına gizlenebilecek veri miktarının çok olmasıdır.

En basit bir yaklaşımla resim dosyalarındaki her bir noktanın (piksel) renk değerlerinin çok az farkla değiştirilmesi; sayısal ifadeyle o noktanın renk kodunun en düşük değerli bitlerinin değiştirilmesi ile veri gizlenebilir.

Şekil 17'de Bitmap türündeki bir resmin veri gizlenmeden önceki ve sonraki görünümleri yer almaktadır. Resme yaklaşık 4KB veri gizlenmiş ve her iki durumda da dosya boyutu 228 KB olup bir değişme olmamıştır. İnsan gözü ile bu iki resim arasında bir fark sezilemez [19].

Orijinal Resim *Veri Gizlenmiş Resim*

Şekil 17. Orijinal Bir Resim ve Aynı Resmin Veri Gizlenmiş Hâli **[19]**

Resim tabanlı steganografide en çok LSB Replacement, LSB Matching, DCT, DFT, DWT, FFT gibi yaklaşımların bilinip kullanılmasına rağmen, resim türü ve kullanılan yöntem ve algoritmaların steganalize karşı zayıflıklarından dolayı çok daha fazla sayıda yaklaşım geliştirilmiştir [19; 23; 24].

4.2.2. Video Steganografi

Video steganografi, video dosyalarına veya canlı video akışı sırasında video sinyallerine veri gizlenmesidir. Basit bir video dosyası kare veya frame adı verilen resimlerin dizisinden oluşmaktadır. Resimler üzerinde kullanılan steganografik yöntemler ufak değişikliklerle videolar üzerinde uygulanabilmektedir [19; 25].

Videolardaki her bir kare içerisine gizli veri gömmenin yanı sıra videodaki kareler (frameler) arası ilişkiden de yararlanılmakta, gizli veri tüm videoya dağıtılmaktadır [26].

4.2.3. Ses Steganografi

Ses steganografide, ses dosyalarına veya ses sinyallerine veri gizlenir. Bilgisayar ortamında ses sinyalleri resim sinyallerine benzer bir yapıda kaydedildiğinden, ses steganografide kullanılan yöntemler resim steganografide kullanılan yöntemlerden çok farklı değildir.

İnsan kulağıyla fark edilmeyecek biçimde ses dosyalarına gizli veri gömülürken ses sinyallerindeki gürültüden ve frekanslardan faydalanılır.

4.2.4. Metin Steganografi

Metin steganografi, metin dosyalarına veri gizlenmesi işlemidir. Resim, ses ve video steganografiye göre uygulanmasının daha zor, veri gizleme kapasitesinin daha az olması dezavantajları olmasına rağmen metinler her yerde bulunduğundan dikkate değer veri gizleme işlemleri yapılabilir [19; 27].

Metin steganografi için birçok yaklaşım vardır. Bunlardan bazıları; sözdizimsel değişiklik, anlamsal değişiklik, metin kısaltma, heceleme değişikliği, satır kaydırma, kelime kaydırma, özellik kodlama, sıkıştırma ve dilbilimsel yöntem ve yaklaşımlardır. Bu yaklaşımlar genel olarak; metin biçimini değiştirme ve metnin anlamını değiştirme şeklinde iki grup altında toplanabilir [28; 29; 30].

4.2.5. Belge Tabanlı Steganografi

Belge steganografi, kelime işlemci dosyalarına, hesap tablosu yazılımlarının kullandığı çalışma kitabı dosyalarına, web sayfalarına, taşınabilir belge formatı dosyalarına vb. belgelere veri gizlenmesi işlemidir. Bu tür belgelere kaydedilen normal içerik verileri ile beraber belgelerin başlık bilgileri kısmı veri gizlenmesi için uygun alanlar bulundurur [31].

Örneğin web sayfalarında HTML etiketlerinin özelliklerinin sıraları değiştirilerek veri gizlenebilir [32].

4.2.6. Dosya Sistemi Tabanlı Steganografi

İşletim sistemlerinin dosya sistemlerinden faydalanılarak sabit disk, taşınabilir bellek gibi ortamlara normal kullanıcı dosyalarının yanı sıra gizli veriler saklanabilir. Bunun başlıca yöntemlerinden biri NTFS dosya sisteminin bilgisayar kullanıcıları tarafından pek bilinmeyen uyumluluk özelliği olan ADS'yi (Alternate Data Streams) kullanmaktır. ADS, bilgisayar korsanlarına (hackerlar) zararlı veri gizlemek için bir fırsat verir [33].

4.2.7. Ağ Steganografi

Ağ steganografi, kısaca iletişimdeki akışı bozmadan, bilgisayar ağlarında gizli veri iletimi sağlama işlemi olarak tanımlanabilir [19; 34].

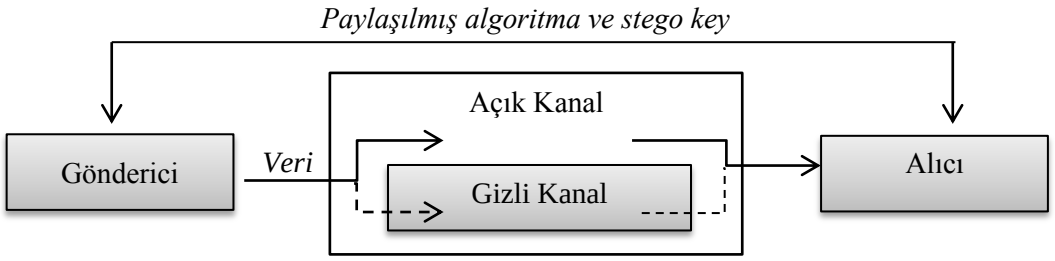
Ağ steganografide iletilen paketlerin başlık yapılarından, sınıflandırılmalarından, sıralandırılmalarından, dolgularından, uzunluklarından yararlanılarak ağ ortamında gizli veri gönderilebilir. Tüm bu ve benzeri yöntemler beşinci bölümde detaylı olarak verilmiştir.

5. GİZLİ KANALLAR ve AĞ STEGANOGRAFİ YÖNTEMLERİ

Gizli Kanallar (Covert Channels) terimi ilk olarak Lampson tarafından "bilgi iletimi amaçlı olmayan tüm kanallar" olarak tanımlanmıştır [35].

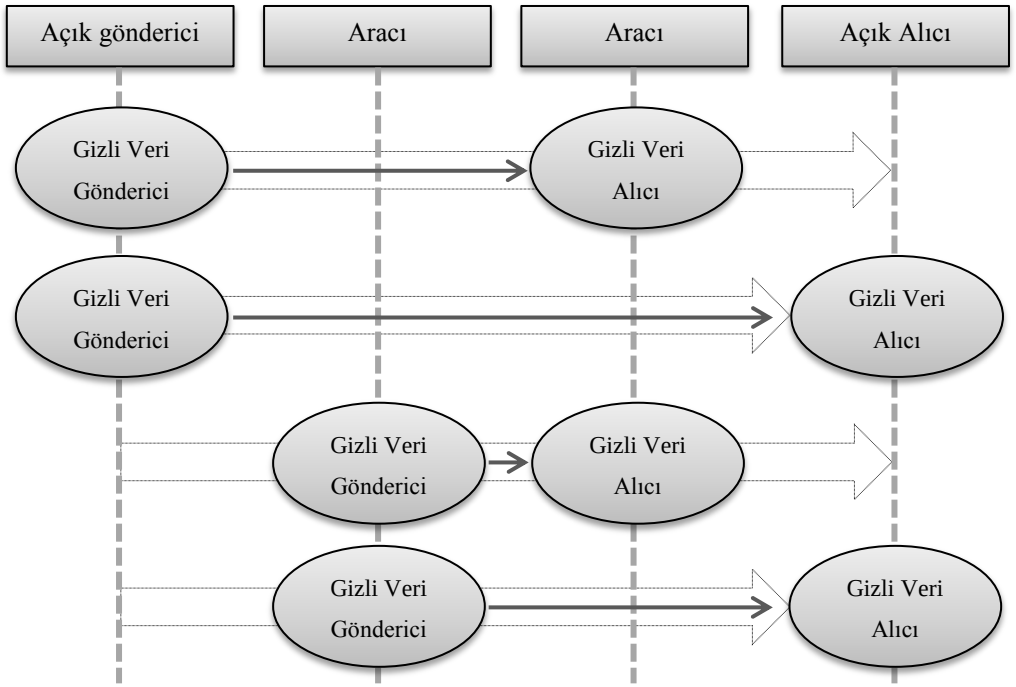
Gizli kanallar, normal veri iletişimi için kullanılan ortamlardan gizli veri gönderimini sağlayan kanallardır. Bu kanallar, iletilmek istenen gizli verinin varlığını hissettirmemeyi amaç edinir. Aslında steganografi, gizli kanal oluşturmadır. Önceki bölümde bahsedilen resim, ses, video, metin gibi steganografik ortamların kullanımı da bu kapsama girmesine rağmen, literatürde çoğunlukla gizli kanal terimi sürekli bir veri alış verişinin olduğu bilgisayar ağlarındaki iletişimle beraber anılmaktadır.

Gizli kanallar, normal veri iletimi için kullanılan açık kanalların ihlali ile oluşturulur ve açık kanaldan veri iletimi var oldukça gizli kanalın varlığından söz edilebilir. Şekil 18, gizli ve açık kanalların bir modelini göstermektedir.



Şekil 18. Gizli ve Açık Kanallar **[36]**

Gizli kanallar oluşturulurken, gönderici veya alıcının ağdaki konumları değişebilir. Uçtan uca gönderim olabileceği gibi, alıcı ve/veya gönderici, üçüncü taraf uçlar arasında da olabilir. Şekil 19, gizli veri göndericisi ve alıcısının bilgisayar ağı içerisindeki muhtemel konumlarını gösterir [36].



Şekil 19. Gizli Veri Gönderici ile Alıcının Ağdaki Muhtemel Konumları **[36]**

Bilgisayar ağlarında gizli kanallar oluşturularak gizli veri iletimine ayrıca ağ steganografi (network steganography) denilmektedir [37]. Ağ steganografide ağ paketlerine direkt veya dolaylı olarak veriler ve anlamlar yüklenir. Bunun için çoğunlukla paketlerin başlık yapıları, uzunlukları, sıraları, zamanlamaları, varsa paket uzantıları, paket dolguları ve paket trafiği manipüle edilir. Ağ paketlerinin manipülasyonu işlemi, bilgisayar ağlarında, güvenlik analizi, performans arttırma, veri gizleme, tıkanıklık denetimi, penetrasyon (sızma) testi, aldatma, saldırı gibi değişik amaçlar için yapılabildiği gibi, ağ ortamında veri gizleme amacıyla da en çok yapılan işlemdir [6].

Gizli kanallar geleneksel olarak depolama kanalı (storage channel) ve zamanlama kanalı (timing channel) olarak ikiye ayrılır [8; 38; 39; 40]. Depolama kanalı, gizli verinin gönderici tarafından paylaşılan bir alana (ağ paketlerinin başlıklarına) yazılıp, alıcı tarafından okunmasıdır. Zamanlama kanalı, gönderici tarafın sinyalleri (ağ paketlerini) modüle ederek, daha geniş kapsamda sadece ağ paketleri arasında zamanlamayı değil paketlerin sıralamasını ve diğer paketler arası ilişkileri de ele alan geniş bir tanım alanına sahiptir. Ancak literatürde sadece bu iki başlık altında incelemeler yapılmamış, kategorilerin sayısı bazen arttırılmış, bazen de hibrit yöntemler önerilmiştir. Bu bölümde gizli kanal oluşturma yöntemleri bu iki ana kategoriye bakılmaksızın başlıklar halinde incelenmiştir.

5.1. Paket Başlığı Tabanlı Steganografi

Ağ steganografide en çok kullanılan yöntem paket başlığına veri gizlemedir. Bu yöntemde genel olarak gönderilen gizli verinin bant genişliği yüksek olmasına rağmen; zamanlama, sıralama gibi diğer yöntemlere nazaran gizli verinin varlığının güvenlik duvarlarına, steganalitik yöntemlere veya saldırı tespit sistemlerine hissettirilmesi riski daha yüksektir.

Paket başlıklarına veri gizleme işleminin dayandığı temel, genel olarak veri paketlerinin iletiminde o anda kullanılmayan veya isteğe bağlı (optional) alanlara gizli veri gömmenin yanı sıra iletişimde gerekli olan yani kullanılan alanlara da işlevini bozmadan kısmen müdahaleyle gizli verinin gömülerek paketin alıcıya gönderilmesidir.

IP, TCP ve UDP, günümüz Internet altyapısında veri iletiminde en çok kullanılan protokoller olduğundan, veri gizlemek için IP paket başlığındaki Identification Number, Flags, Fragmentation Offset, Checksum, Version, ToS (Type of Service), TTL (Time to Live), Timestamp, TCP paket başlığındaki Sequence Number, Acknowledgment Number, Checksum, Timestamp, UDP paket başlığındaki Source Port, Checksum gibi alanlar literatürde veri gizleme için sıkça bahsedilen alanlardır. Bunların yanı sıra ARP, ICMP, DHCP gibi yardımcı protokollerin paket başlıkları da veri gizlemede kullanılmaktadır.

5.1.1. IP Flags Alanına Veri Gizleme

Bir IP paketinin boyutu iletildiği ağın MTU (Maximum Transfer Unit) değerinden büyükse paket parçalanıp iletilir ve alıcıda birleştirilir. Paketin boyutu MTU değerinden küçükse paket parçalanmadan iletilir. IP paketlerindeki Flags alanında DF (Don't Fragment) ve MF (More Fragments) bitleri bulunur. MF bitinin 1 (bir) olması, bu paketin parçalanmış paket olduğunu ve devamının olduğunu belirtirken; 0 (sıfır) olması, bu paketin parçalanmamış paket olduğunu ya da parçalanmış paket ise kendisinden sonra gelen bir parçasının olmadığını belirtir. MF biti 0 iken DF bitinin durumu iletişimde önemsizdir ve DF biti gizli veri gönderimi için uygundur [8]. Bu durum Şekil 20'de gösterilmiştir.

DF biti ile gizli "1" gönderimi

Identification	Flags			Fragmentation Offset
	Reserved	DF	MF	
XXX…XXX	0	**1**	0	000…000

DF biti ile gizli "0" gönderimi

Identification	Flags			Fragmentation Offset
	Reserved	DF	MF	
XXX…XXX	0	**0**	0	000…000

Şekil 20. IP Paket Başlığındaki DF Bitine Veri Gizleme **[8]**

Bu yöntemle gizli veri gönderiminde, gönderici taraf ağın MTU bilgisini bilmek durumundadır. Gönderici ve alıcının aynı yerel ağda bulunduğu durumda, MTU bilgisi kolay bir şekilde bilinir ve bu yöntem kolayca uygulanabilir. Gönderilecek olan paket başka ağ segmentlerinden ve yönlendirici, modem gibi cihazlardan geçip hedefe ulaşacaksa, her ne kadar MTU keşif yöntemleri kullanılsa bile, IP paketi farklı yollardan gidebileceğinden, paketin bölünüp bölünmemesi garantiye alınamaz.

Flags alanının kullanımında bir diğer yöntem bu alanın en önemli biti olan, IP başlığında kullanılmayan ayrılmış biti veri gizlemek için kullanmaktır [41]. Buraya gizlenecek olan veri de IP paketinin parçalanmasından dolaylı olarak etkilenecektir. Paket parçalandığı zaman bu veri paket sayısı kadar tekrar edecek, alıcı tarafında istenen veri alınamayacaktır.

Flags alanı kullanılarak gizli veri gönderiminin bant genişliği düşük olup, her IP paketi ile sadece 1 (bir) bitlik veri gönderilebilir.

5.1.2. IP Identification Alanına Veri Gizleme

IPv4 paketindeki 16 bit uzunluğundaki Identification alanı o iletişim için benzersiz bir değer tutar ve iletişimde alıcı olan tarafın gelen yeni paket parçalarının hangi pakete ait olduğunu belirlemesi için kullanılır. Bu alan sadece paket parçalanmış ise önemlidir, parçalanmamış ise dikkate alınmaz. Bu durumda gönderici, DF bitine gizleyebildiği gibi, bu alana da gizli veriler gömebilir, hatta ikisini bir arada kullanabilir [8]. Dahası, Identification değerinin eşsiz olması sadece o bağlantı için gerekli olduğundan, aynı değerler başka bağlantılarda da gönderilebilir, yani çok alıcılı bir veri gizleme işlemi yapılabilir [42].

Identification alanının benzersizliğini sağlamak için, buraya gizlenecek veri, rastgele bir değer ile birleştirilip atanabilir [8; 42]. Mesela M harfinin ASCII kodu 77'dir ve bunun

ikilik sistemdeki karşılığı 1001101'dir. İlk sekiz biti M harfinin ikilik kodu, sonraki sekiz biti rastgele bir değer seçilirse bu alana atanacak veri 01001101RRRRRRRR olacaktır. Burada R rastgele ikilik bir rakamı temsil etmektedir. Bu şekilde bir MERHABA metni gönderilmek istenirse, her bir harf yukarıdaki örneğe benzer şekilde bir pakete gömülecek ve sırasıyla alıcıya gönderilecektir. Alıcı taraf gelen paketlerin Identification alanının ilk sekiz bitini okuyup gizli veriyi elde edecektir.

Paketin hedefe ilerlerken parçalanması Identification alanına yazılan veriyi bozmaz, ancak alıcıya paket sayısı kadar tekrarlı veri iletilmesine sebep olur. Dolayısıyla Identification alanına veri gizlerken, Flags alanının kullanımında olduğu gibi, paketin parçalanmaması garanti edilmeli; alıcı ve gönderici taraf aynı ağ içerisinde olmalı veya aynı ağ içerisinde olmasalar bile MTU keşif yöntemleri ile paketin parçalanmaması sağlanmalı [43], paket boyutu iletişimin sağlandığı ağların ve cihazların MTU değerinden büyük olmamalıdır.

5.1.3. IP Fragmentation Offset Alanına Veri Gizleme

Ağda iletilen IP paketinin boyutu MTU değerini aştığında, IP paketi parçalara ayrılır. Her bir parçanın taşıdığı verinin bütün parça içerisindeki yeri 13 bit uzunluğundaki Fragmentation Offset alanında tutulur. Paket parçalanmasının olmadığı durumda bu alan ağ cihazları tarafından dikkate alınmaz ve bu alana veri gizlenebilir [44]. Ancak ağın MTU değerinin bilinmesi ve iletilecek paketin boyutunun bu değeri aşmaması gerekir.

5.1.4. IP Type of Service Alanına Veri Gizleme

Type of Service (ToS) alanının en önemsiz iki biti iletişimde kullanılmayıp rezerve edilmişlerdir. Bu bitler gizli veri iletiminde kullanılabilir [45]. Ancak rezerve edilmiş alanlara gizlenen veri kolaylıkla teşhis edilebilir. Çünkü kullanılmayan bu alanlar standart olarak daima 0 (sıfır) ile doldurulur.

5.1.5. IP Time to Live Alanına Veri Gizleme

IP paket başlığında bulunan TTL (Time to Live) alanı, paketin geçtiği her noktada bir azalan bir değer tutar. Paketin geçtiği nokta sayısı TTL değerine bakılarak hesaplanabilir. TTL değeri sıfıra ulaştığında paket ağdan düşürülür.

TTL alanına direkt olarak gizli veri gömülmesi amacıyla bir değer girilmesi şüphe uyandırıcı olacaktır. Göndericinin ortada olduğu durumda, TTL değerini kontrolsüz bir şekilde daha büyük bir değerle değiştirmesi belirsiz paket döngülerine sebep olabilir veya TTL değerini daha az bir değerle değiştirmesi paketin alıcıya ulaşmadan ağdan düşürülmesine sebep olabilir. Ayrıca TTL değerinin direkt olarak kodlanması (şüphe uyandırmasa bile), alıcının doğru değeri alması için, alıcı ile gönderici arasındaki atlanacak nokta sayısının kesin bilinmesini gerektirir. TTL alanına gizli veri gömülmesinde etkin bir yöntem [46] nolu referansta önerilmiştir. Bu yönteme göre yüksek TTL değeri mantıksal 1 (bir) olarak, düşük TTL değeri mantıksal 0 (sıfır) olarak düşünülür. Gönderilen gizli verinin algılanmaması için, ağın normal TTL varyasyonunu taklit etmek gerekir. Bunun için yüksek TTL ile düşük TTL arasında ciddi bir fark olmaması gerekir ki, bu fark 1 olarak düşünülmüştür. Bu yönteme göre bant genişliği paket başına 1 bittir.

5.1.6. TCP Sequence Number Alanına Veri Gizleme

Sequence Number (Sıra Numarası) olarak bilinen alan, gönderici tarafından atanan 32 bitlik bir sayıyı tutar ve bu sayı karşılıklı iletilen TCP paketlerinin sırasını belirler. TCP, çift yönlü iletişim sağladığından her iki taraf kendi başlangıç sıra numaralarını (Initial Sequence Number – ISN) bağlantı kurulumunda belirlerler.

TCP bağlantı kurulumunda ilk gönderilen SYN bayrağı işaretli paketin Sequence Number alanına gizli veri gömülebilir [47]. Bunun için çok farklı yöntemler düşünülebileceği gibi, en basit haliyle şu yöntem uygulanabilir; ASCII bir karakter gizlice gönderilmek istenirse, ASCII karakterin sayısal değeri 8 bit uzunluğunda olduğundan 256*256*256 sayısıyla yani 16777216 sayısıyla çarpılıp 32 bitlik bir sayıya dönüştürüldükten sonra gönderilecek olan SYN paketinin başlangıç sıra numarası (ISN) olarak ayarlanır ve paket hedefe gönderilir. Alıcı taraf, gelen SYN paketlerinin Sequence Number alanını okur ve bu sayıyı 16777216 sayısına bölerek kendisine gelen gizli ASCII kodunu elde eder. Bu basit yöntemle gizli veri gönderiminde bit dizisinde bir değişim olmamaktadır, yani ISN karmaşık bir hale gelmemektedir. Amaç ISN'yi daha gerçekçi görünen büyük bir sayı yapmaktır [47].

ISN 32 bitlik olduğundan içerisine gizlenecek veri birden fazla sayıda (2,3 veya 4) karakter de olabilir. Ancak burada aynı numarayı tekrar üretmekten çekinmek gerekir. Bunun için

ISN'nin bir kısmına rastgele değerler veya belli bir kısmını kodlama gibi yöntemlerle farklı numaralar üretme yoluna gidilebilir [42; 47].

5.1.7. TCP Acknowledgment Number Alanına Veri Gizleme

Acknowledgment (ACK) Number alanı Sequence Number alanı gibi 32 bit uzunluğunda olup, TCP bağlantı kurulumunda ve sonrasındaki veri iletiminde gelen paketlerdeki Sequence Number alanındaki sıra numarasına cevap amaçlı kullanılır.

Bağlantı kurulumunda sunucu, kendisine gelen SYN paketine bir SYN+ACK paketi ile cevap verir. Sunucu, gelen SYN paketindeki Sequence Number alanındaki değerin bir fazlasını cevap paketinin ACK Number alanına yazarak istemciye gönderir. Sunucuya gelen SYN paketi kapalı bir portu hedef almışsa, bu durumda sunucu bir RST paketi ile istemciye cevap verir ki bu RST paketinde de yine ACK Number alanını yukarıdaki gibi ayarlar. Yani her halükarda istemciye ACK Number alanı ayarlanmış olarak cevap gelir. Buradaki veri gizleme yönteminde IP Spoofing ile beraber yukarıda bahsedilen TCP bağlantı kurulumunun istismarıyla gizli veri gönderilebilir [47]. Bu yöntemle ilgili detaylar yansıma yöntemi adı altında bu bölümün Karma ve Diğer Yöntemler başlığı altında verilmiştir.

5.1.8. UDP Paket Başlığına Veri Gizleme

UDP paket başlığında 16'şar bit uzunluğunda Source Port Number, Destination Port Number, Length ve Checksum alanları bulunur. IP paketine eklenen UDP paketinin Destination Port Number ve Length alanları iletişimde zorunlu olarak kullanılırken, Checksum ve Source Port Number alanları isteğe bağlı olarak kullanılır. Checksum alanı kullanılmadığı zaman 0 (sıfır) olarak bırakılır. Source Port Number [48] ve Checksum alanları veri gizlemede kullanılabilir.

UDP paket başlığına veri gizlenmesi durumunda, UDP'nin yapısı gereği güvenilir bir iletim gerçekleşmeyebilir. İletim garantisinin istendiği durumlar için bu seçenek kullanışsızdır.

5.1.9. Checksum Alanına Veri Gizleme

Veri iletiminde değişik hata denetim mekanizmaları mevcuttur. Paket başlıklarında bulunan Checksum alanı paket başlığının bütünlüğünü sağlamak amacıyla hesaplanan bir alandır. Diğer protokollerde de bulunan Checksum alanı IP'de bir yönüyle farklıdır ki, IP'de paket her bir düğümden geçerken TTL alanındaki değerin bir azaltılmasından dolayı dolayı Cheksum alanı yeniden hesaplanıp ayarlanır. Gizli veri iletiminde IP Checksum alanı kullanıldığında, alıcı tarafta paketin ilk oluşturulduğu zamanki Checksum değeri tekrar hesaplanıp öyle dikkate alınmalıdır.

Cheksum alanına veri gizlemenin bir yöntemi bozuk paketlerden faydalanmaktır. Normalde hedefe varan bir paketin cheksum hesabı yeniden yapılır ve hesaplanan değer paketteki mevcut Checksum alanındaki değerle karşılaştırılır. Bu iki değerin farklı çıkması durumunda paket bozuk kabul edilir ve dikkate alınmadan atılır. Veri gizlenerek iletilen Checksum alanı yanlış değerle doldurulmuş olan bir paket hedefe vardığında aynı şekilde dikkate alınmaz, ancak karşı tarafta stego paket bekleyen bir program bu paketteki gizli veriyi elde eder [49].

Checksum alanına veri gizlemenin bir başka yöntemi kullanılan protokolün paket uzantılarından yararlanarak, paket uzantıları eklemek suretiyle checksum değerinin değişmesini ve gönderilecek gizli değere göre bir değer almasını sağlamak ve öylece iletmektir [50].

Bir başka yöntem olarak, Checksum alanı UDP'de isteğe bağlı olarak kullanıldığından bu alanın değerinin 0 (sıfır) olması mantıksal 0 olarak, hesaplanıp değerinin yazılması da mantıksal 1 olarak kabul edilebilir [51].

5.1.10. Timestamp Alanına Veri Gizleme

IP paketindeki Options alanı isteğe bağlı ve nadiren kullanılan bir alan olup, Options altında yer alan Timestamp alanı paketin iletildiği zaman damgasını tutar. Bu alana veri gizlenmesi mümkündür. Literatürde önerilen bir yöntemde, bu alana tek sayı olarak zaman damgası girilmesi mantıksal 1 olarak, çift sayı olarak zaman bilgisi girilmesi mantıksal 0 olarak değerlendirilmiştir [45].

Options alanının kullanımı durumunda IP paketi en fazla 20 hop (atlama) kadar gidebildiğinden, Internet ortamında kullanım için uygun bir alan olmayacak, ayrıca nadir kullanılan bir alan olduğundan veri gizleme için steganografik potansiyeli düşük olacaktır [52].

TCP paket başlığında Options bölümünde yer alan Timestamp, iki adet 32 bitlik alandan oluşur, bu alana da IP Timestamp alanına olduğu gibi veri gizlenebilir. Bu alan Linux ve Unix benzeri işletim sistemlerinin yeni versiyonlarında standart olarak kullanımda olduğundan bu alanın kullanımı diğer isteğe bağlı kullanıma sahip alanlarda olduğu gibi şüphe uyandırmaz. Veri gömme işlemi, IP Timestamp başlığında bahsedilen, bu alandaki sayının tek veya çift olmasına göre olabileceği gibi, bu sayının en önemsiz bitlerinin değerleri değiştirilerek de yapılabilir [53; 52].

5.1.11. Ayrılmış Bitlere Veri Gizleme

TCP paket başlığında, Data Offset alanı ile Flags alanı arasında ileride kullanılmak üzere rezerve edilmiş 6 bitlik bir alan bulunur. Bu alan normal iletişimde kullanılmadığı için hep 0 (sıfır) olarak bırakılır. Bu alana veri gömülebilir [45]. Ağ cihazlarının ve saldırı tespit sistemlerinin bu alanı önemsemediği durumlar için problem olmaz, ancak bu durum her zaman mümkün değildir. Saldırı tespit sistemleri bu alanı kontrol edebilir veya bazı ağ cihazları paketi iletirken bu alanı sıfırlayabilir.

5.1.12. DHCP Paket Başlığına Veri Gizleme

DHCP paket başlığında çok sayıda alan bulunur. Üstelik bu alanların kapasiteleri de oldukça büyüktür. Toplamda DHCP paketinin sadece başlık uzunluğu 500 byte'ı geçebilmektedir.

DHCP paket başlığındaki Transaction Identification (Xid) alanı, 4 byte uzunluğunda olup, o anki işlemin numarasını tutar. Bu numara istemci tarafından rastgele atanan bir değerdir. Dolayısıyla xid alanına veri gizlenebilir [54].

Seconds alanı, istemcinin ağa katılıp adres edindiği veya yenilediği andan itibaren geçen süreyi belirtir [7]. Bu alanın önemsiz bitleri üzerinde yapılacak küçük değişiklikler

potansiyel bir gözlemci tarafından pek algılanmayacağından veri gizlemede kullanılabilir [54].

Chaddr (client hardware address – istemci fiziksel adresi) alanı da veri gizlemede kullanılabilir. Burada iki yöntemden bahsedilebilir [24]. Birinci yöntem; Chaddr alanına göndericinin adresini değil de, gizli veri iletilmek istenen bilgisayarın adresini girerek, işlem süresince değeri değişmeyecek olan diğer bir başlık alanına da (örneğin Xid) gizli veriyi yazarak ağ ortamına göndermektir. Bu şekilde DHCP sunucusunun döneceği cevap belirtilen adresteki bilgisayar tarafından alınacak, beraberinde gizli veri de iletilmiş olacaktır. Bu yöntem, gönderici kendi gerçek MAC adresini kullanmadığından saldırı tespit sistemi tarafından spoofing saldırısı olarak algılanabilir. İkinci yöntem; Chaddr alanının uzunluğundan faydalanmaktır. Chaddr alanı 16 byte uzunluğunda, normalde bu alana yazılan herhangi bir MAC adresi 6 byte uzunluğunda olduğundan kalan 10 byte gizli veri gönderiminde kullanılabilir. Benzer şekilde Sname, File alanları büyük kapasitelerinden dolayı, Options alanı ise DHCP'nin yapısı gereği sunduğu farklı ve ilginç seçeneklerden dolayı veri gizlemede kullanılabilir [54].

5.1.13. ICMP Paket Başlığına Veri Gizleme

ICMP paketlerinin en çok kullanılan iki tipi Echo Request ve Echo Replay tipleridir. Tüm bilgisayarlarda standart olarak kullanılan "ping" komutu bir ağdaki bilgisayarların erişilebilirliğini belirlemek için ICMP paketlerinin bu tiplerini kullanır.

ICMP'deki 16'şar bitlik Sequence Number ve Identifier alanlarına veri gizlenebilir. Bir Echo Replay paketindeki bu alanlar ile bu paketin karşılığı olan Echo Request paketindeki bu alanlar aynı olmak durumundadır. ICMP, IP paketlerine eklenip gönderildiğinden veri iletimi garanti altına alınamazken [7], gönderici ve alıcı arasında iletilen Request ve Replay paketlerinin Sequence Number ve Identifier alanlarındaki verilerin aynı olması gerekliliğinden yola çıkarak, gönderici, veri iletimini kendi imkânlarıyla doğrulayabilir [48]. Bu yönüyle ICMP ile gizli veri gönderimi, UDP ile gönderimden daha avantajlıdır.

5.1.14. ARP Paket Başlığına Veri Gizleme

ARP paket başlığında esnek olarak kullanılabilecek üç alan mevcuttur. Bunlar Hedef MAC adresi, Hedef IP adresi ve Padding (dolgu) alanlarıdır. Hedef MAC adresi ve Padding kısmı, bazı yerel ağlarda varsayılan olarak normalize edilip sıfırlarla doldurulur, dolayısıyla bu iki kısım gizli veri gönderimi için uygun olmayabilir. Ancak Hedef IP alanı ARP isteğine cevap verecek olan hostu belirttiği için bu alan normalize edilmez. Bu durumda bu alan gizli veri gönderimi için seçilebilir [55].

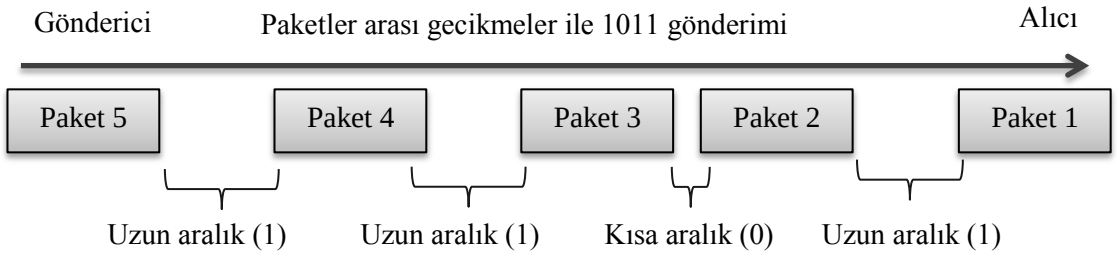
5.1.15. WIFI Çerçeve Başlığına Veri Gizleme

802.11 kablosuz ağlarda kullanılan MAC çerçeve başlığındaki Sequence Control ve Initial Vector alanlarına veri gizlenmesi mümkündür. Sequence Control alanı aslında Sequence Control ve Fragment Control olarak iki bölümden oluşur. 12 bit uzunluğundaki Sequence Control her yeni çerçevede artan bir numarayı tutarken, 4 bit uzunluğundaki Fragment Control çerçevenin parçalandığı durumda her yeni parça ile artan bir numarayı tutar. Parçalanmamış paket için Sequence Control alanına gizli veri yazılıp gönderilebilir. Initial Vector alanı taşınan veriyi şifrelemek için RC4 algoritması tarafından kullanılan 3 byte uzunluğunda rastgele bir veri tutar. Bu alana 3 byte uzunluğunda gizli veri gömülebilir ki bu veriyi ağdaki herhangi bir sniffer veya saldırı tespit sistemi rastgele değer olarak düşünecektir. Ancak WEP şifrelemenin kullanılmadığı ağlarda bu alanın bu veri gizleme amacıyla kullanılması şüphe uyandıracaktır [56].

5.2. Paket Zamanlama Tabanlı Steganografi

Gizli bilgi, gönderilen paketler arasındaki süreler ayarlanarak gönderilebilir. Paket zamanlamada taraflar önceden başlangıç zamanı, aralığı veya başlama şartını belirlerler. Başlangıç şartları oluştuğunda gizli veri iletimi başlar. Basitçe düşünülecek bir yöntem olarak, gönderici sırasıyla normal veri paketlerini gönderirken, bazı paketler arasına kasıtlı olarak gecikmeler ekler. Alıcı taraf, gelen veri paketleri arasındaki farklı gecikmeleri algılayabilecek bir konumda olacak, gizli veri göndermek isteyen kişi gönderdiği paketler arasına belirli gecikmeler ekleyerek gönderdiğinde, alıcı taraf bu gecikmelerden bilgi çıkarımı yapabilecektir [38; 39]. Alıcı tarafında paketler arasında gözlenen uzun süreler

mantıksal 1 olarak, kısa veya yok denecek süreler mantıksal 0 olarak değerlendirilir. Şekil 21, basitçe paket zamanlama tabanlı gizli veri gönderimini anlatır.



Şekil 21. Paket Zamanlama İle Gizli Veri Gönderimi

Paketler arasındaki gecikmelerle oynamak, ağ ortamında rahatsızlığa sebep olabilir, bu durumda gönderici en uygun gecikmeleri ayarlamak durumundadır. Ayrıca, ağ cihazlarının, yönlendiricilerin ve ağ geçitlerinin tamponlama, paket parçalama, birleştirme, yönlendirme gibi işlemlerinden dolayı paketler arası gecikme süreleri değişebilir, bu da yanlış veri alımına sebep olur. Bu yöntemle yerel ağda veri iletimi, büyük ağlardan veya İnternet'ten veri iletimine göre daha az risklidir. Zamanlama tabanlı gizli kanalın bant genişliği, peş peşe iletilen paketler arası bekleme süreleriyle ters orantılıdır.

Aynı anda farklı cihazlar tarafından Ethernet paketlerinin (frame) ağ ortamına gönderilmesiyle çakışmalar oluşur. CSMA (Carrier Sense Multiple Access) protokolü ve CSMA/CD (CSMA with Collision Detection) mekanizması ile bu çakışmaların önüne geçilir. Çakışma durumunda taraflar rastgele belirlenen bir süre kadar bekleyip tekrar veri gönderirler [2].

Fiziksel katman düzeyinde CSMA/CD mekanizmasının işleyişinden yararlanarak gizli veri gönderimi mümkündür. Bu yöntemde önceden belirlenmiş üçüncü bir bilgisayar veri gönderdiği anda, gizli veri göndermek isteyen taraf da veri göndermeye çalışarak Ethernet paketlerinin çakışmalarını sağlar. Gönderici, çakışmadan sonraki bekleme süresini minimuma çekerek ikinci gönderimi diğer bilgisayardan önce gerçekleştirir. Gizli veriyi alacak olan taraf ağ ortamını dinler ve bu durumu lojik 1 (bir) olarak algılar. Göndericinin çakışmadan sonraki bekleme süresini maksimuma çekip üçüncü tarafın verisinden sonra veri göndermesi durumu ise alıcı tarafından lojik 0 (sıfır) olarak algılanır. Alıcı, sürekli ağ ortamını dinleyecek ve çakışmaları takip edecektir. Bu yöntemde veri gönderiminin bant genişliği oldukça düşüktür. Çakışma sonrası paket başına bir bit veri gönderilebilir.

Fiziksel katman düzeyinde uygulanabilmesinden dolayı sadece yerel ağda veri gönderimi mümkündür [45].

5.3. Paket Uzunluğu Tabanlı Steganografi

Paket uzunluğu tabanlı steganografide, ağ üzerinden paket uzunlukları ayarlanarak gizli veri kodlanır ve gönderilir. Uzunluk tabanlı veri gizleme kavramı ilk olarak Padlibsky tarafından takdim edilmiştir [57].

Paket uzunlukları protokollere özel olarak farklılıklar gösterir [38]. Bazı protokollerin doğası gereği paket uzunlukları çok değişken iken, bazılarında paket uzunlukları varyansı düşük olabilir. Paketlerin uzunluklarından yararlanarak gizli veri göndermeye çalışan yöntemler, gizli veri gönderildiğinin anlaşılmaması için normal ağ trafiğindeki paket akışını paket uzunlukları yönüyle taklit etmeye çalışırlar. Veri gizleyen algoritma, kullandığı protokolün paket uzunluğu dağılımını dikkate almadığında, uygulamaya özel bir paket uzunluğu dağılımı söz konusu olur [58]. Dolayısıyla steganalitik yöntemler steganografi kullanımını keşfedebilir.

Uzunluk tabanlı steganografide kullanılacak olan protokol veya uygulama önemlidir. Mesela, TCP protokolü kullanan bir dosya transferi, paket boyutlarını maksimum boyutta tutar ve paket uzunlukları pek değişmez. Bu durum veri gizleme için her zaman elverişli olmayabilir. Ancak bir sohbet oturumunda veya UDP protokolü kullanan ses ve video iletiminde paket uzunlukları farklılık gösterdiğinden uzunluğa bağlı veri gizleme daha kullanışlıdır [58; 59].

Uzunluğa dayalı steganografide en basit bir yöntem olarak, veri gizleme işleminde iletilen verinin her bir byte'ının (karakterinin) değerinin direkt olarak paket veya frame uzunluklarının sayısal değeri olarak ayarlanması şeklinde düşünülebilir [57; 38]. Buna göre her farklı karakter, 256 farklı paket uzunluğu ile tanımlanır. Gönderici taraf, göndereceği her paketin uzunluğunu, göndermek istediği karakterlere karşılık gelen uzunluklar olarak ayarlar. Alıcı taraf, gelen paketlerin uzunluğuna bakarak, bu uzunluğa karşılık gelen karakteri gizli veri olarak elde eder.

Yukarıdaki yöntemin biraz geliştirilmiş bir hali olarak Yao tarafından önerilen yöntem, gizli gönderilecek veriye ait karakterlerin farklı eşsiz değerlerle eşleştirilip alıcı ve

gönderici tarafından paylaşılan bir matriste tutulmasıdır [60]. Gönderici taraf, gönderilecek gizli karakterin matristeki numarasını alıp paket uzunluğu olarak ayarlar ve alıcı taraf gelen paketlerin uzunluğunu algıladıktan sonra bu uzunluğu kendi matrisinde arayarak karşılık gelen karakteri elde eder.

Uzunluk tabanlı steganogafide Ji tarafından önerilen yöntem, önceki yöntemlerden farklı olarak, normal ağ trafiğindeki mesajların referans olarak alınması ile geliştirilen bir yöntemdir [61]. Bu yöntemde, önceden gönderici ve alıcı taraflar normal bir şekilde iletişim halinde olurlar. Her iki taraf, gönderici tarafından alıcıya gönderilen normal iletişim verilerinin paket uzunluklarını kaydeder ve bu bilgileri referans olarak tutarlar. Daha sonra iki taraf benzer rastgele algoritma ile bu referans bilgiden bir uzunluk seçerler. Gönderici taraf bu uzunluğa göre bir mesaj gönderir ve bu uzunluğu da kaydederek referans bilgiyi günceller. Alıcı tarafta da eş zamanlı olarak benzer işlemler yapılır; gelen paketin uzunluğu ile referans bilgiler güncellenir yanı sıra gizli veri elde edilir. Tüm gizli bilgi iletilene kadar, her paket veya mesaj iletiminde referans bilgiler güncellenip aynı işlemler tekrar edilir. Bu yöntemle normal ağ trafiği taklit edilerek, gizli veri gönderiminin üçüncü kişiler tarafından anlaşılmasının önüne geçilir. Bu yöntemin bir diğer önemli özelliği protokol-bağımsız olmasıdır.

5.4. Paket Sıralama Tabanlı Steganografi

Ağ ortamında iletilen paketler arasındaki sıralama bazı protokoller için değiştirilebilir. Gönderici tarafta paketlerin farklı dizilişlerine anlamlar yüklenerek, alıcıda bu anlamlar elde edilebilir. Gönderici taraf, paketlerin orijinal sırasını göndermek istediği bilgiyi kodlayacak şekilde değiştirdikten sonra alıcıya iletir, alıcı taraf ise gelen paketlerin geliş sırası ile olması gereken sırayı karşılaştırıp aradaki farka göre gizli veriyi elde eder. İdeal olarak, n adet paket sıralanarak iletilecek gizli bilginin potansiyeli $log_2 n!$ bit olabilir [8].

Ağ paketlerinin sıralanmasıyla gizli veri iletimi için paketlerin doğal sırasını belirten paket numarası gibi referans bilgilere ihtiyaç vardır. TCP'de Sequence Number ve ACK Number gibi alanlar paket numarası değildir ve verilerin oktetlerinin numarasını belirtirler. Bu durumda paket sıralama TCP ile mümkün değildir. Benzer durum IP için de geçerlidir. Ancak IPSec protokolünde kullanılan iki protokol başlığı olan AH (Authentication Header) ve ESH (Encapsulating Security Payload) 32 bit uzunluğunda Identification Number alanı

bulundurur. Burada tutulan bir paketin tekrarlı olarak iletilip iletilmediğini anlamak için paketlere sırayla artan bir numara vermek için kullanılır. Dolayısıyla bu alan paketlerin doğal sırasını vermekte olduğundan paket sıralama ile veri gizlenmesini mümkün hale getirir [8].

5.5. Paket Sınıflandırma Tabanlı Steganografi

Paket sınıflandırmaya dayalı steganografide gizli veri Internet'teki paketlerin çeşitliliğinin ayarlanmasıyla kodlanır [62]. Ağ ortamında iletilen tüm paketler belli özelliklere göre sınıflandırılır. Paketler, [62] nolu referansta önerilen yönteme göre temel olarak üç sınıfa ayrılır. Birinci sınıf, paketlerin ait oldukları protokollere göre; ikinci sınıf, paketlerin başlıklarına ve bazı alanların aldıkları farklı değerlere göre, üçüncüsü ise paketlerde kullanılmayan alanlar, başlık uzantıları ve dolgu alanlara göre ayırt edilir. Sınıflardaki özellikler belirlendikten sonra gizlenecek olan veri bitler halinde kodlanıp parçalara ayrılarak sınıflandırma vektörü (sorting vector) elde edilir, daha sonra sınıflandırma vektörü paketlerin özelliklerine eşlenir. Bu işlemler için kullanılan temel bir algoritma ve yöntem [28] nolu referansta detaylı olarak sunulmuştur.

5.6. Paket Dolgusu Tabanlı Steganografi

Ethernet protokolünde frame (çerçeve) uzunluğu CSMA/CD mekanizmasından dolayı minimum 64 oktet olmak durumundadır. Uzunluğu 64 oktetten küçük olan bir çerçeveye ilave veriler eklenerek 64 oktete tamamlanır. Bu ilave dolgu mekanizmasını belirleyen standartlardaki (RFC 894 ve RFC 1042) belirsizlikten dolayı günümüzdeki ağ arayüz kartlarında bu dolgu işlemi farklı yollarla yapılmaktadır. Üstelik bazı sürücüler çerçeve dolgusunu hatalı olarak idare etmekte, sıfırlarla doldurmaktadırlar. Literatürde Etherleak olarak adlandırılan bu durumda; bellek sızıntısının bir sonucu olarak bir Ethernet çerçeve dolgusu kernel hafızasının parçalarını içerebilir. Bu dolgu alanına değerli bilgi eklenip gönderilemez ancak steganografik veri eklenmesi mümkündür [63; 64].

5.7. Karma ve Diğer Yöntemler

Veri gizlemek ve veriyi gizlerken de bant genişliğinin yüksek olmasını sağlamak için paket uzunluğu ile beraber paketin taşıdığı yükün de kullanıldığı bir başka yöntem [65]

numaralı referansta önerilmiştir. Bu yöntemde normal trafik dağılımı göz önüne alınarak, gerçek paket uzunlukları kullanılmıştır.

TCP protokolünde alıcıya iletilen veri paketinin hedefine varması durumunda hedef bilgisayar kaynak bilgisayara onay paketi olarak ACK paketi gönderir. Kaynak bilgisayara ACK paketi gelmediği zaman, veri alıcıya iletilmemiş kabul edilir ve veri paketi yeniden gönderilir. TCP'deki bu yeniden iletim (retransmission) işleyişinden yola çıkarak gizli veri iletimi yapılmasını sağlayan yöntemler mevcuttur [34; 66]. Bu yöntemlerin temelinde kasıtlı olarak yeniden iletim yapılması sağlanarak tekrar gönderilen veri paketine gizli veriler gömülmektedir.

Yansıma (bouncing) yöntemi diyebileceğimiz bir yöntemde gönderici ve alıcı taraflar direkt olarak iletişime geçemiyorlarsa üçüncü bir taraf olan bir sunucuyu aracı yaparak gizli veriyi iletirler. TCP paket başlığındaki Sequence Number alanı gizli veri taşıyıcısı olarak, IP paketindeki Source Address alanı gizli veri gönderilmek istenen bilgisayarın adresi olacak şekilde ayarlanır (IP Spoofing). TCP SYN paketi bir sunucuya gönderilir. Sunucu, gelen SYN paketine karşılık verir ve paketin geldiği port açıksa SYN+ACK paketi gönderir, port kapalıysa RST+ACK gönderir. Her iki durumda da cevap paketinin hedefi gizli veri alıcısıdır. Alıcı taraf, ağı dinleyerek kendisine gelen paketteki TCP Acknowledgment Number alanına bakar. Buradaki değerin bir eksiği gizli verinin kendisidir [47].

Yansıma yönteminde bir anda 32 bitlik gizli veri iletilebilir. Yerel ağda herhangi iki bilgisayar bu yöntemi kullanarak gizli veri iletebilir, Internet üzerinden kullanımda herhangi bir web sunucu aracı olarak düşünülebilir, ancak alıcı tarafın Internet üzerinden direkt erişilebilir bir IP adresine sahip olması gerekir. Veri gönderimi sık tekrarlanırsa aracı olan sunucu bunu SYN Flood saldırısı olarak algılayabilir. Üstelik IP Spoofing yapıldığından, bunun tespiti durumunda veri iletişimi güvenlik duvarları tarafından engellenebilir.

6. AĞ ORTAMINDA VERİ GİZLEME UYGULAMALARI

Bu bölümde normal veri ileten ağ paketlerine ve ağ trafiğine veri gizleme işlemleri uygulamalı olarak sunulmuştur. Uygulamalar yerel ağda gerçekleştirilmiş olmasına rağmen bir kısmı Internet üzerinde de uygulanabilir niteliktedir.

Ağ uygulamalarında, özellikle paket manipülasyonunda kullanılmak için geliştirilen birçok araç olmasına rağmen, gerçekleştirilen uygulamalarda Python programlama dilinin bir modülü olarak geliştirilen Scapy aracından faydalanılmıştır [6; 67; 68]. Scapy aracı; komut satırı özelliğinin olması, Python programlama dilinin bir kütüphanesi olarak kullanılabilmesi, yazım kolaylığı, paket oluşturma, izleme, gönderilen ve alınan paketleri eşleştirme, çok sayıda protokol desteği, paket setleri oluşturma, TTL gibi alanlara varsayılan değerleri atama ve checksum gibi alanları otomatik hesaplama gibi özelliklere sahip olduğundan dolayı özellikle seçilmiştir.

Bağlantı kurulumu gerektiren uygulamalarda, sunucu olarak ayarlanan bilgisayarda sunucu soketler kullanılarak port açılmış ve bağlantı kurularak gizli veri gönderimi gerçekleştirilmiştir.

6.1. IP Don’t Fragment (DF) Biti ile Gizli Veri İletimi

Bu uygulamada, 2 byte uzunluğunda gizli veri gönderimi için, normal veri içeren 16 adet TCP paketi oluşturulmuş ve bu paketlerin her biri, gizli verinin birer bitini barındıran IP paketlerine yüklenerek hedefe gönderilmiştir.

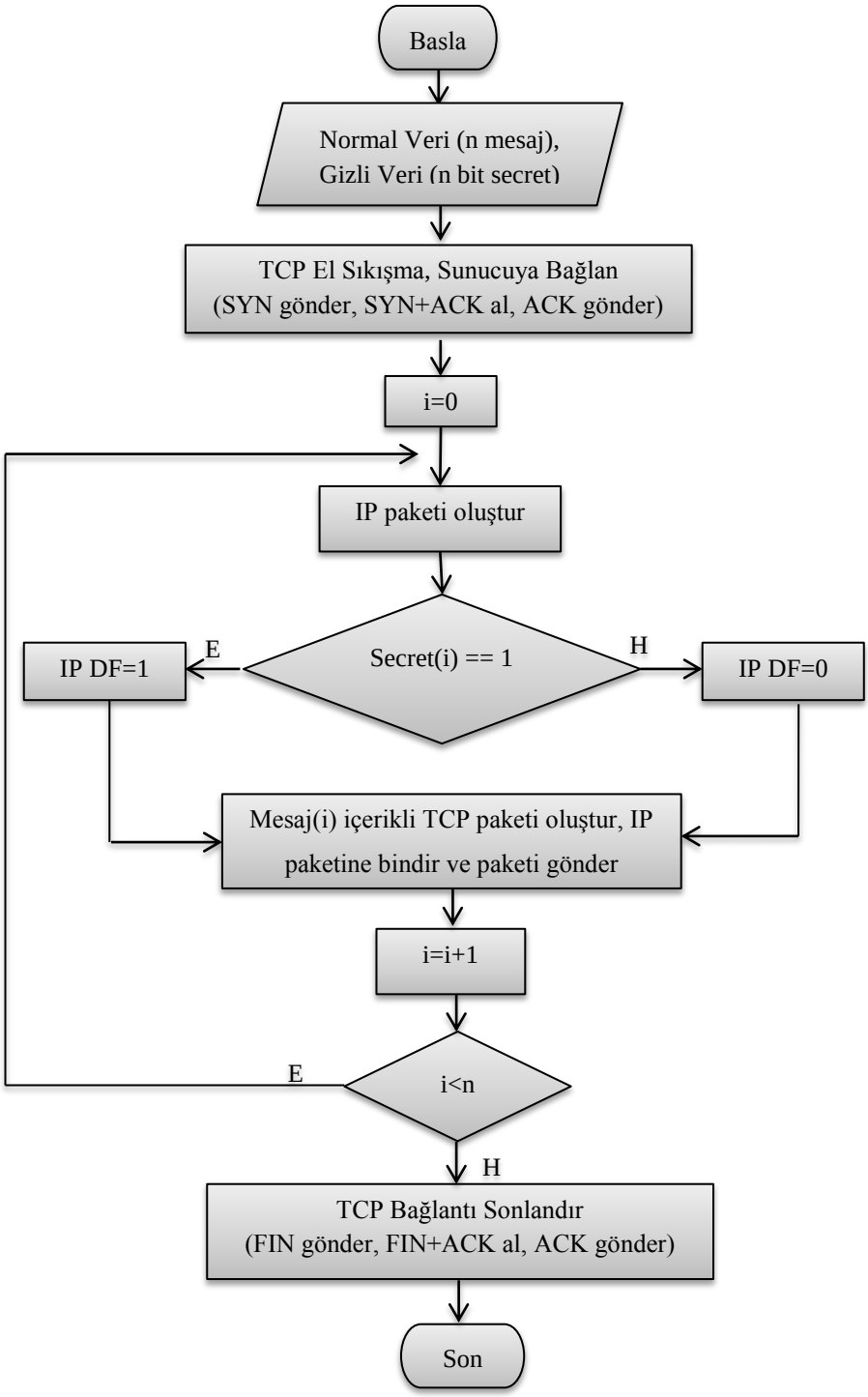
Uygulamada, öncelikle hedef bilgisayarın açık portuna erişim sağlamak için TCP el sıkışma işlemi manuel olarak gerçekleştirilmiştir. Oluşturulan TCP paketlerinin başlık alanları tek tek işlenmiştir. İlk paketin Sequence Number ve Source Port alanlarına rastgele değerler atanmış, bağlantı kurulumu için SYN paketi gönderimi, gelen SYN+ACK paketine tekrar ACK paketi ile cevap verilmesi gibi işlemler sırasıyla gerçekleştirilmiştir.

Bağlantı kurulduktan sonra normal veriler TCP paketlerine yüklenirken, bit dizisine dönüştürülmüş olan gizli verinin bitleri tek tek IP paketlerinin DF bitine gömülmüş, IP paketlerine bindirilen TCP paketleri hedefe gönderilmiştir. Normal veri için oluşturulan her pakete, gizli verinin sıradaki biti gömülmek suretiyle tüm veriler iletilmiştir.

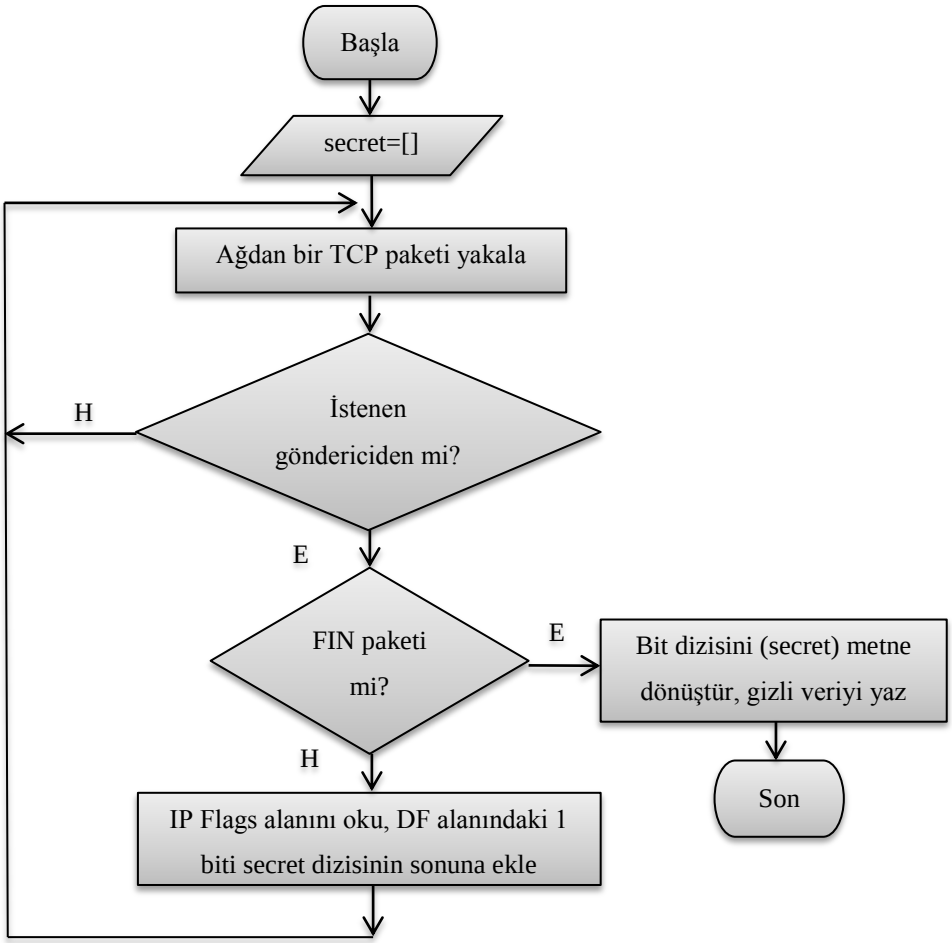
Tüm veriler iletildikten sonra TCP FIN ve ACK paketlerinin standartlara göre gönderilip alınmasıyla TCP bağlantı sonlandırma işlemi manuel olarak gerçekleştirilip sunucuyla bağlantı kesilmiştir.

Bağlantı kurulumu, veri iletimi ve bağlantı sonlandırılması işlemler gerçekleştirilirken gönderilen her TCP paketinin Sequence Number ve ACK Number alanları ile IP paketinin Identification alanı protokolde belirtilen kurallara göre arttırılıp paketlere işlenmiş, bu şekilde sağlıklı bir ağ trafiği elde edilmiştir. Şekil 22, gönderici tarafta çalışan uygulamanın işleyişinin akış şemasını verir.

Hedef bilgisayarda, gelen normal veriler, sunucuda çalışan, açık portu kontrol eden program tarafından alınmış, gizli veriyi elde edecek olan program ağ trafiğini dinleyerek seçili porta gelen TCP paketlerini taşıyan IP paketlerindeki DF bitini okuyup her paket için gizli veriye ait bir biti elde etmiştir. Şekil 23, alıcı tarafta çalışan uygulamanın işleyişinin akış şemasını verir.

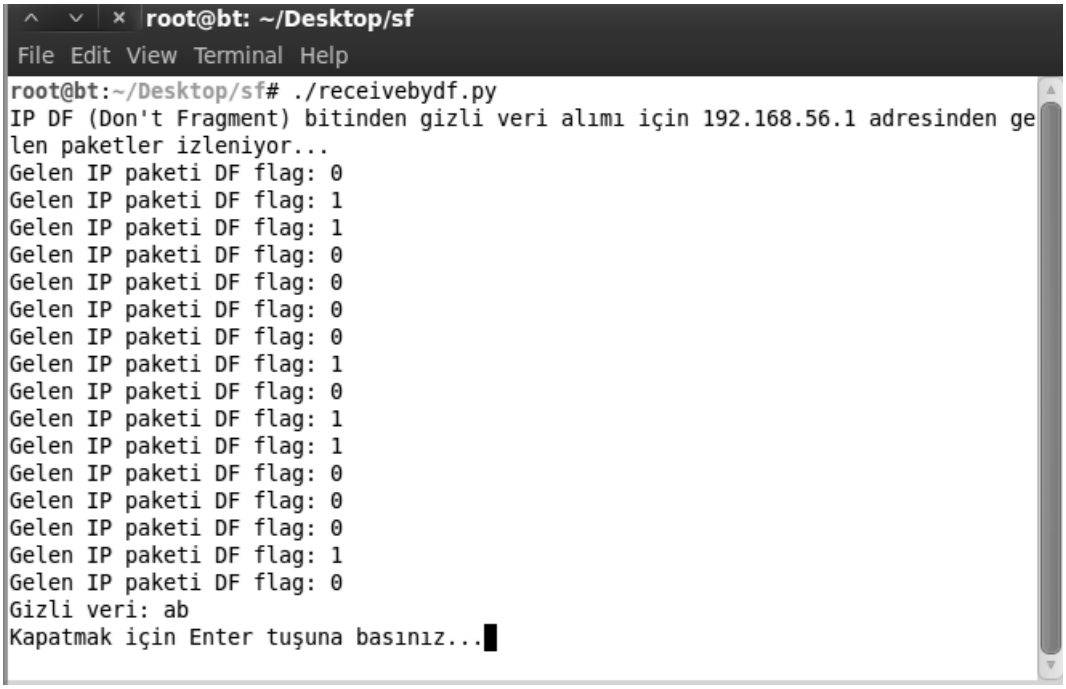


Şekil 22. IP DF Biti İle Gizli Veri Gönderimi Akış Şeması



Şekil 23. IP DF Biti İle Gizli Veri Alımı Akış Şeması

Alıcı tarafta çalışan uygulama her aldığı paketi bilgilendirmek amacıyla kullanıcıya bildirir. Paketlerde DF biti ile sırasıyla gelen gizli veriye ait bitler 8'er olarak gruplandırılarak her 8'li bit grubundan 1 byte ASCII kodu elde edilerek, iletim sonunda gelen veri ekrana yazılır. Şekil 24, örnek bir "ab" gizli metninin alıcı tarafta elde edildiği ekran görüntüsünü vermektedir.



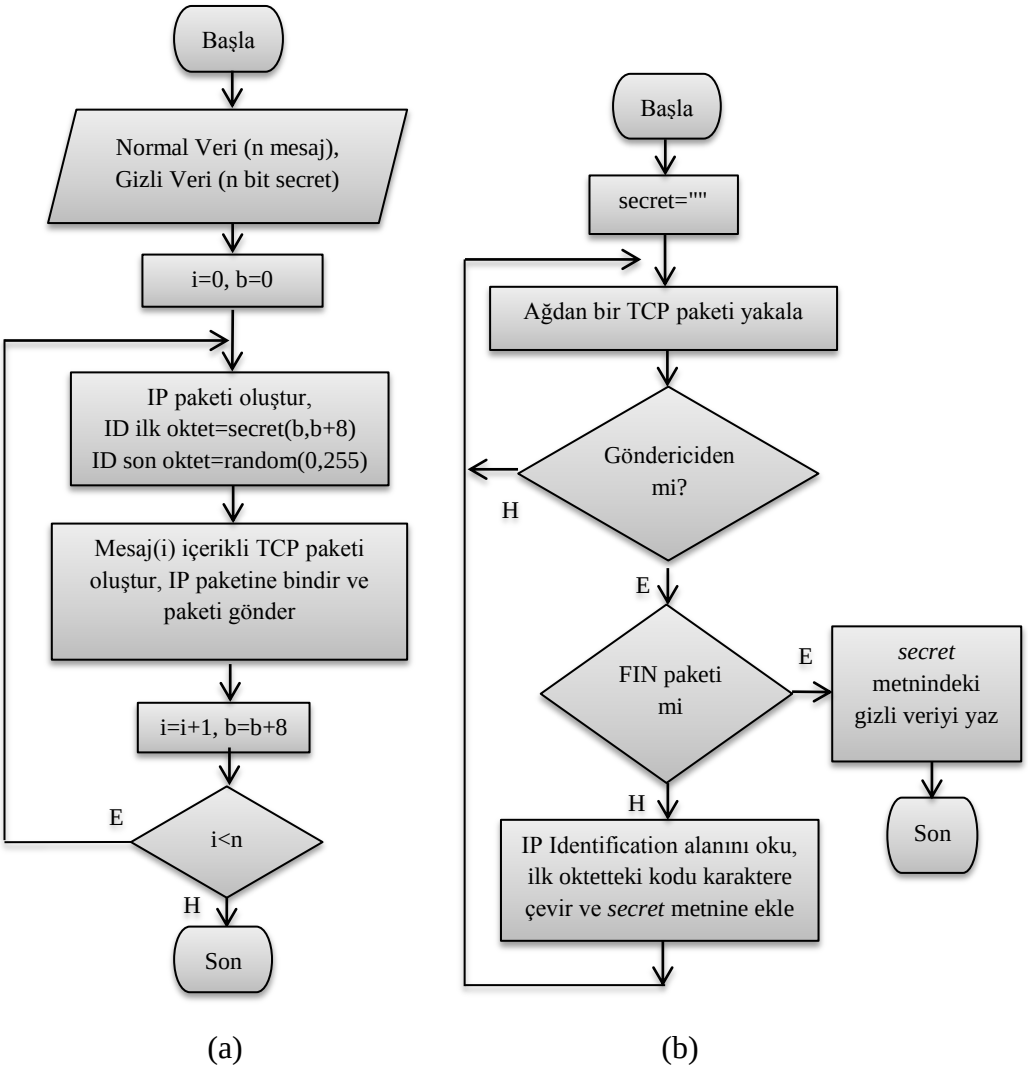
Şekil 24. IP DF Biti Kullanılarak Gizli "ab" Metni Alımı Ekran Görüntüsü

6.2. IP Identification Alanı ile Gizli Veri İletimi

IP Identification alanı 16 bit uzunluğunda olup, bu uygulamada ilk 8 biti gizli veri gönderimi için kullanılmıştır. Sonraki 8 bit ise alanın benzersizliğini sağlamak için rastgele değerlerle doldurulmuştur.

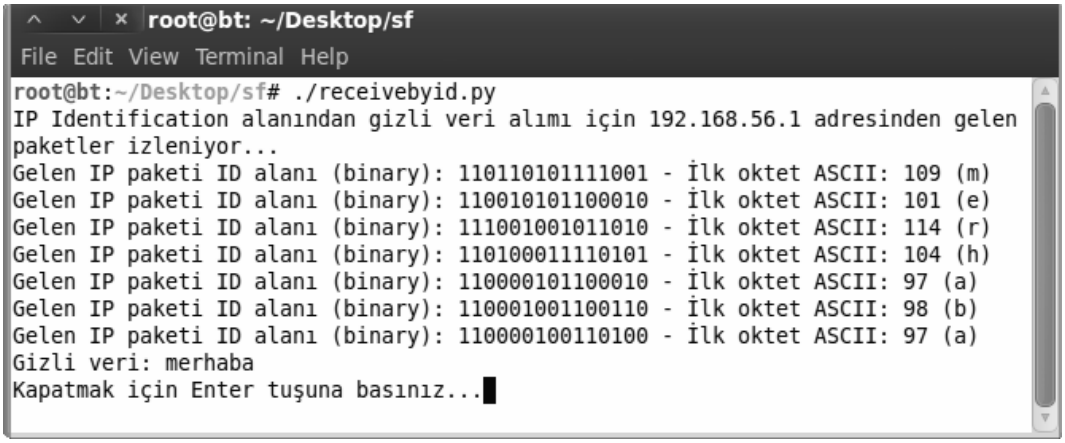
Uygulamada normal veri iletimi IP DF Bitine Veri Gizleme uygulamasında olduğu gibi TCP ile gerçekleştirilmiştir. Normal veriler TCP paketlerine eklenirken, gizli verinin her 1 byte'lık kısmı TCP paketini taşıyan bir IP paketinin Identification alanına gömülerek iletilmiştir.

Alıcı tarafta, normal veriyi alan sunucu uygulama çalıştırılırken, yanı sıra gizli veriyi elde etmek için ağı dinleyen program gelen IP paketlerini izleyerek Identification alanındaki değerin ilk 8 bitini gizli veri olarak elde etmiştir. Şekil 25, gönderici ve alıcı tarafta çalışan uygulamaların işleyişinin, bağlantı kurulu ve sonlandırma haricindeki, gizli veri gönderimi ve alımı akış şemasını verir.



Şekil 25. IP Identification Alanı İle Gizli Veri İletimi Akış Şeması
(a) Gönderici Taraf (b) Alıcı Taraf

Alıcı tarafta çalışan uygulamanın gizli "merhaba" metni iletilirken elde edilen ekran görüntüsü Şekil 26'da verilmiştir.

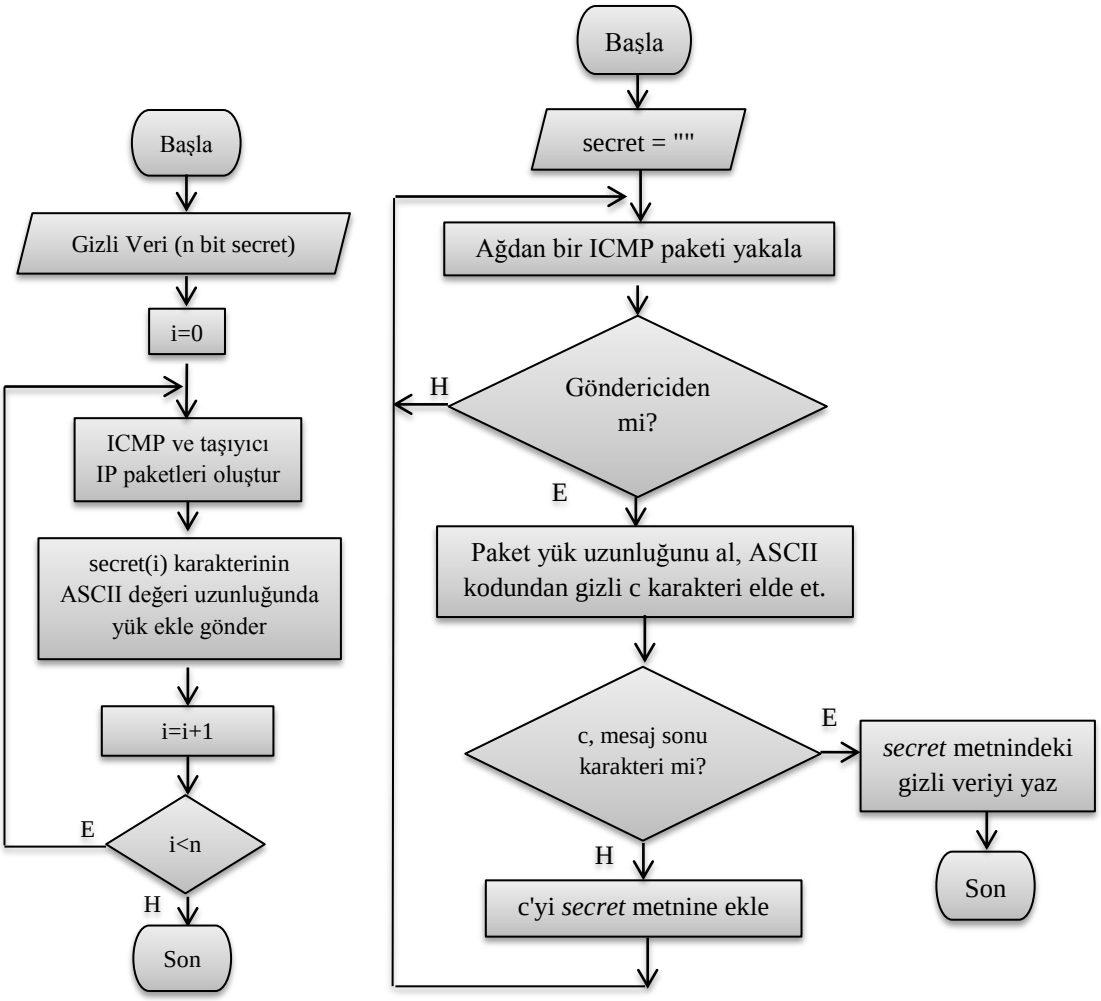


Şekil 26. IP ID Alanı İle Gizli "merhaba" Metni Alımı Ekran Görüntüsü

6.3. Paket Uzunluğu ile Gizli Veri İletimi

Bu uygulamada tüm işletim sistemlerinde kullanılabilen *ping* komutunun gönderdiği paketlerin benzerinin, organize bir şekilde Scapy aracı kullanılarak gizli veri iletimi amacıyla gönderilmesi gerçekleştirilmiştir. ICMP paketleri gönderen ping komutu, hedef bilgisayarın erişilebilir olup olmadığının anlaşılması için kullanılmaktadır. Ping komutu, işletim sistemine özgü paketler gönderirken, kullanıcıya bazı özelleştirme seçenekleri sunmaktadır. Bunlardan biri de gönderilen paketin uzunluğunun ayarlanabilmesidir. Uzunluk belirtilerek çalıştırıldığında, ping, gönderdiği ICMP paketlerine belirtilen uzunluk kadar karakter eklemektedir.

Uygulamada, gönderilmek istenen her gizli karakterin ASCII kodunun sayısal değeri sırayla paketlere eklenen normal yükteki byte miktarı olarak ayarlanmıştır. Paketlere yüklenen veriler sabit karakterlerle doldurulmayıp, işletim sistemlerinin ping komutu ile gönderdiği veriler taklit edilmiştir. Alıcı tarafta gelen paketler izlenerek, paket uzunlukları alınmış ve bu uzunluklar ASCII kod olarak değerlendirilip karşılık gelen gizli karakterler elde edilmiştir. Şekil 27, ICMP paketleri ile paket uzunluğuna dayalı gizli veri gönderimi ve alımının akış şemasını göstermektedir.



Şekil 27. Paket Uzunluğu İle Gizli Veri İletimi Akış Şeması
(a) Gönderici Taraf (b) Alıcı Taraf

Şekil 28, bu uygulamanın alıcı tarafında örnek olarak gizli iletilen "Merhaba Dunya" metninin elde edildiği ekran görüntüsünü verir.

Şekil 28. Paket Uzunluğu İle Gizli "Merhaba Dunya" Metni Alımı Ekran Görüntüsü

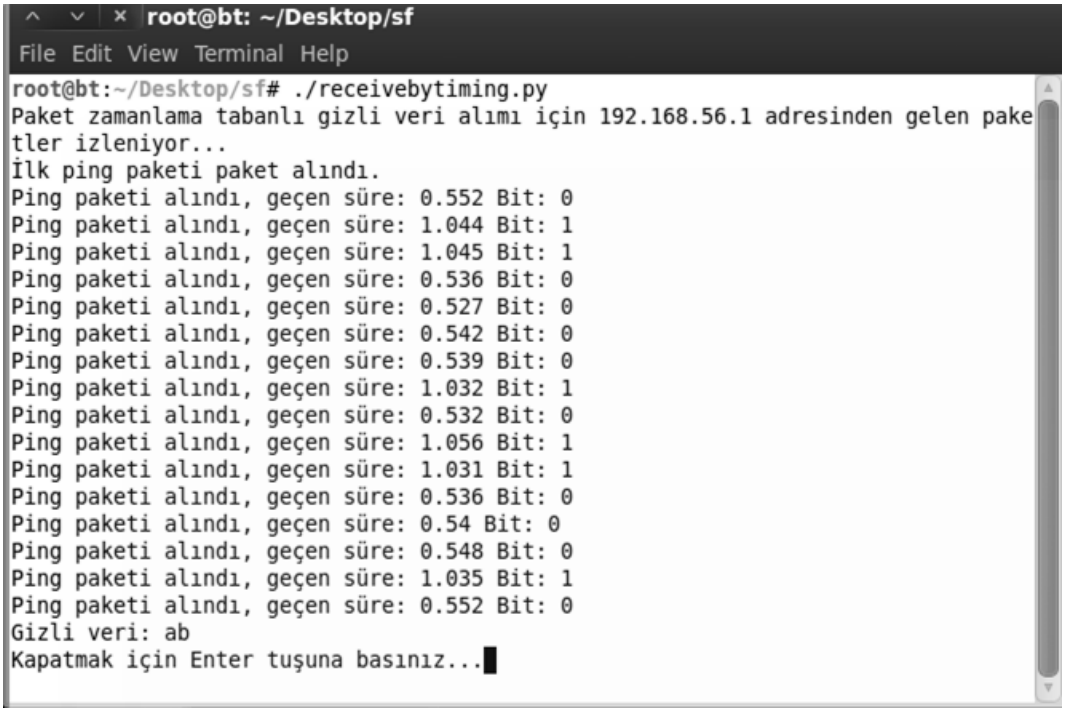
Windows işletim sisteminde ping komutuna -l parametresi, Linux işletim sisteminde ise -s parametresi gönderilerek ping paketlerinin uzunlukları belirtilmek suretiyle istenilen uzunlukta yüke sahip paketler gönderilebilir.

6.4. Paket Zamanlama ile Gizli Veri İletimi

Bu uygulamada paket uzunluğu ile gizli veri gönderimi uygulamasında olduğu gibi ICMP paketleri kullanılmıştır. Sırayla alıcıya gönderilen paketler arasına, mantıksal 1 gönderilmek istendiğinde 1 saniye, mantıksal 0 gönderilmek istendiğinde 0,5 saniye zaman aralığı bırakılmıştır.

Alıcı tarafta ise paketler yakalanırken paketlerin iletim zamanları arasında geçen süreler hesaplanmış, bu sürelerin 1 saniyeye ve 0,5 saniyeye yakınlığına bakılarak iki paket arasındaki zaman aralığı mantıksal 1 veya 0 olarak alınmış ve gizli veri elde edilmiştir.

Uygulamanın alıcı tarafının gizli "ab" metnini elde ettiği ekran görüntüsü Şekil 29'da verilmiştir.

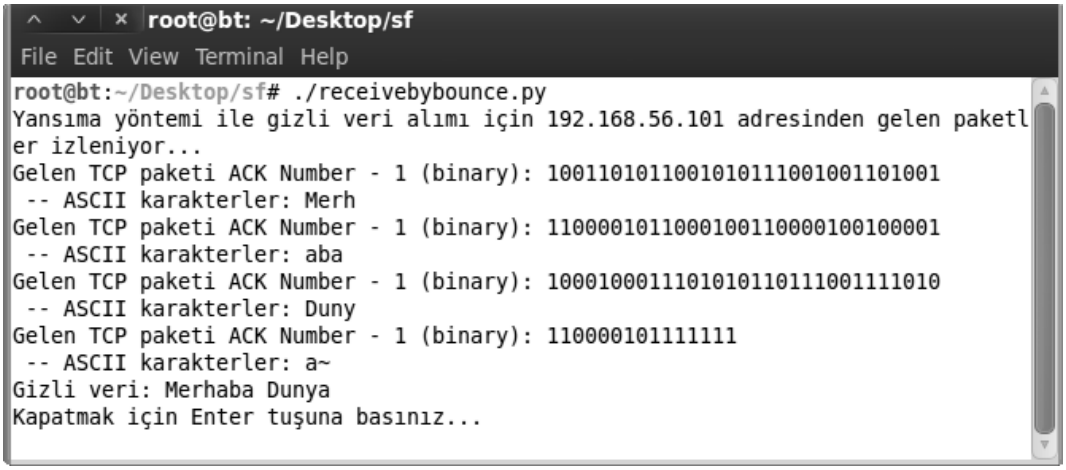


Şekil 29. Paket Zamanlama İle Gizli "ab" Metni Alımı Ekran Görüntüsü

6.5. Yansıma Yöntemi İle Gizli Veri İletimi

Yansıma (Bouncing) yöntemi ile veri gizleme uygulamasında aynı yerel ağda yer alan üç bilgisayar kullanılmıştır. Bunlar gizli veri gönderici, alıcı ve bir de veri iletiminde aracı olarak kullanılan üçüncü taraf bir sunucudur.

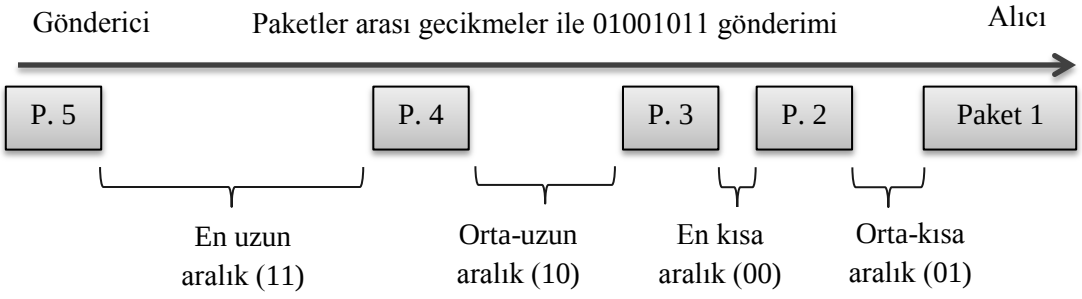
Aracı olarak kullanılan sunucunun gelen paketleri alıcıdan gelmiş gibi görmesi sağlanmış; gönderici tarafta oluşturulan IP paketlerinin Destination Address alanı sunucu adresi, Source Address alanı ise alıcı adresi olarak ayarlanmıştır. TCP bağlantı kurulumu istismar edilerek, Sequence Number alanına veri gizlenmiş, kaynak ve hedef port numaraları ayarlanmış olan SYN paketleri sunucuya gönderilmiş, sunucunun bu bağlantı isteklerine olan cevap paketleri alıcıya ulaşmıştır. Alıcı tarafta, sunucudan gelen cevap paketleri izlenerek, paketlerin TCP ACK Number alanı okunmuş, bu alandaki değerin bir eksiği hesaplanarak göndericinin Sequence Number alanına sakladığı veriler elde edilmiştir. Şekil 30, alıcının ekran görüntüsünü vermektedir.



Şekil 30. Yansıma İle Gizli "Merhaba Dunya" Metni Alımı Ekran Görüntüsü

6.6. Önerilen Paket Zamanlama Yöntemi ile Gizli Veri İletimi

Bu tez çalışmasında paket zamanlama için önerilen yöntemde paketler arası zaman aralıkları dört farklı uzunluğa sahip aralıklar olarak düşünülmüştür. Bu dört farklı zaman aralıklarından, en kısa zaman aralığı 00, orta-kısa zaman aralığı 01, orta-uzun zaman aralığı 10, en uzun zaman aralığı 11 bitlerinin gönderimi için ayarlanmıştır. Şekil 31, iletilen paketler arası dört farklı zaman aralığı ile gizli veri iletimini göstermektedir.



Şekil 31. Önerilen Paket Zamanlama İle Gizli Veri İletimi

İki farklı zaman aralığına sahip yönteme göre, bu yöntemin avantajı bant genişliğinin daha yüksek olmasıdır. Önceki yönteme göre iki paket arası sürede 1 bitlik veri iletilirken, bu yöntemde iki paket arası sürede 2 bit gizli veri iletilmektedir. Ayrıca paketler arası zaman aralıkları varyasyonunun yüksek olması sebebiyle önceki yönteme göre gizli veri iletiminin anlaşılma ihtimali daha düşüktür.

Bu yöntemin sekiz hatta daha fazla farklı zaman aralığına sahip olanı düşünülebilir. Fakat bu durumda paketler arası zaman aralıklarının ayarlanması zorlaşacaktır. Farklı zaman aralıkları sayısı arttırıldıkça paketler arası sürelerin de arttırılması gerekmektedir.

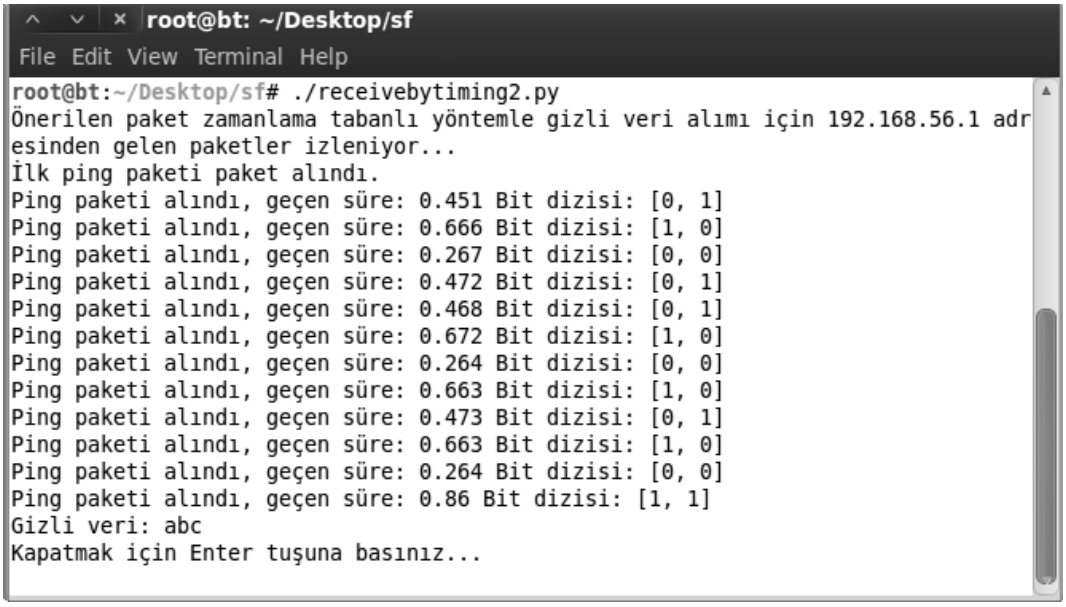
Sürelerin çok kısa tutulması, paketlerin alıcı tarafa çok yakın aralıklarla gitmesine, bu da yanlış veri alınması ihtimaline sebebiyet verebilir. Örneğin, zaman aralıklarının, 000 verisi için 0,05 saniye, 001 verisi için 0,1 saniye, 010 verisi için 0,15 saniyelik süreler olarak seçildiğini göz önüne alalım. 001 verisini iletmek için paketler arasına eklenen 0,1 saniyelik süre, sonraki paketin biraz gecikmesinden dolayı alıcıda 0,15 saniyeye yaklaşırsa, bu durumda 001 alınması gerektiği yerde 010 alınabilir. Önceki paketin gecikmesi durumunda da zaman aralığı kısalacak 001 olarak gönderilen veri 000 olarak alınabilecektir.

Sürelerin çok uzun tutulması, bant genişliğini düşürür. İletişimin sağlandığı ağ ortamının imkanları ve paketlerin üretim, işleme ve iletim süreleri de hesaba katılarak optimum sürelerin tespitinin yapılması gerekmektedir.

Önerilen yöntem kullanılarak gerçekleştirilen uygulamada sırayla alıcıya gönderilen paketler arasına; ikilik sayı sisteminde 00 gönderilmek istendiğinde 0.2 sn., 01 gönderilmek istendiğinde 0,4 sn., 10 gönderilmek istendiğinde 0,6 sn., 11 gönderilmek istendiğinde 0,8 sn. zaman aralığı bırakılmıştır.

Alıcı tarafta ise paketler yakalanırken paketlerin iletim zamanları arasında geçen süreler hesaplanmış, bu sürelerin 0,2 saniyeye, 0,4 saniyeye 0,6 saniyeye ve 0,8 saniyeye yakınlığına bakılmak suretiyle iki paket arasındaki zaman aralıkları 00, 01, 10 veya 01 bitlerine çevrilerek gizli veri elde edilmiştir.

Uygulamada, alıcı tarafın gizli “abc” metnini elde ettiği ekran görüntüsü Şekil 32’de verilmiştir.



Şekil 32. Önerilen Paket Zamanlama Yöntemi İle Gizli "abc" Metni Alımı

6.1. Önerilen IP ID Alanına Veri Gizleme Yöntemi ile Gizli Veri İletimi

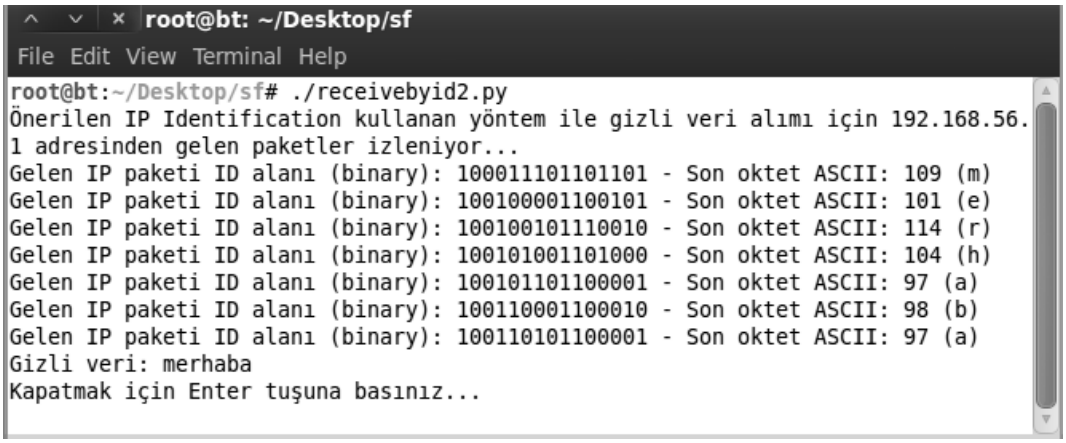
Bu çalışmada IP Identification (ID) alanı için önerilen yöntemde gönderici tarafta ID alanının önemsiz 8 bitine gizli veriye ait bir ASCII karakter; önemli 8 bitine de sırayla artan bir numara gömülmüştür. Bu yöntemde ayrıca alıcı tarafta, gelen son 256 paket için aynı ID değerine sahip birden fazla paketin gelmesi durumunda bu paketlerden bir tanesi dikkate alınmıştır.

Bu yöntemin birinci avantajı iletilen paketlerin sıralarının karışması durumunda alıcıda yine doğru sırada verilerin alınabilmesidir. Yerel ağda paket gecikmeleri pek gerçekleşmediğinden, paket sırası çok sorun olmayabilir. Internet üzerinden veri iletiminde bu ihtimalin düşünülmesi gerekir.

Yöntemin ikinci avantajı, paketlerin alıcıya ulaştığı süreler boyunca aynı ID değerine sahip olacak bir paketin üretilmemesidir. ID değeri, gönderici ile alıcı arasında o anki iletişim için paket yaşadığı sürece benzersiz olmalıdır. Bu yöntemde, aynı değerden tekrar üretilecek bir ID olma ihtimali en az 256 adet paket gönderildikten sonradır. Beşinci bölümde incelenen, altıncı bölümde de uygulaması gerçekleştirilen ID alanına rastgele değer ekleme yönteminde rastgele üretilen değerin bu yönteme göre daha kısa sürede tekrar etme ihtimali vardır. Bu durum Python dilinde random modülüyle denenmiş ve aynı sayının birkaç sayı sonra tekrar üretildiği görülmüştür.

Yöntemin üçüncü avantajı, paket parçalanmasından etkilenmemesidir. Çünkü alıcı taraf gelen son 256 paket arasından aynı ID değerine sahip birden fazla paketten bir tanesini gizli veri okumak için dikkate alacaktır. Dolayısıyla sadece yerel ağda değil, Internet üzerinden gizli veri gönderiminde de MTU keşfine gerek duyulmadan kullanılabilir.

Uygulamanın gerçekleştiriminde gönderici ile alıcı arasında TCP bağlantısı kurulmuş, gizli veriye ait bitler IP paketinin ID alanına gömülerek alıcıya gönderilmiştir. Alıcı tarafta, gelen TCP paketleri izlenerek, IP ID alanı okunmuş ve gizli veriye ait bitler elde edilmiştir. Uygulamanın alıcı taraftaki ekran görüntüsü Şekil 33'te verilmiştir.



Şekil 33. Önerilen IP ID Alanına Veri Gizleme İle Gizli "merhaba" Metni Alımı

7. SONUÇ

TCP/IP Protokol kümesi geliştirildiğinde resmî ve tam tanımlı, mükemmel güvenlikli olarak değil, uygulanabilirliğiyle ön plana çıkmıştır. TCP/IP'nin ilk ortaya çıkışından itibaren görülen bazı sorunlar çözülmüşken, çoğu problem mevcut durumda devam etmektedir. Bunların en başta geleni, günümüzde ağ seviyesindeki en basit ama en etkili saldırı şekillerinden biri olan DoS/DDoS saldırılarıdır. Protokol tasarımlarındaki eksiklikler ve istismarlara karşı zamanla önlemler alınmaktadır, mesela IPv4'ün yetersizliği ve eksiklikleri IPv6 ile giderilmeye çalışılmaktadır .

Güvenlik duvarı, saldırı tespit ve engelleme sistemleri, anti virüs yazılımları, ağ analiz araçları gibi bilgi sistemlerinin korunması için kullanılan donanım ve yazılımlar geliştikçe, karşı ataklar da gelişmekte ve bunların çoğu mevcut protokoller bazında olmaktadır. Problemlerin çözümü için güvenlik risklerine karşı alınabilecek önlemler, protokolleri, ağ altyapılarını iyi tanımak ve analiz edebilmekten geçmektedir. Ağ paket başlıklarının işlenmesi veya IP, TCP, UDP gibi belirli protokollerin istismar edilmesi genellikle uzman seviyesinde yapılan işlemlerdir. Bu işlemler teknik bilginin yanı sıra, yazılım ve donanım araçları ile mümkündür. Bir saldırganın gözünden bakılabilirse daha kolay ve etkili bir şekilde birçok problemin üstesinden gelinebilecektir.

Steganografinin fiziksel ortamlardan dijital ortama taşınması gibi, teknolojinin gelişmesiyle mevcut veri gizleme imkânlarının da daha farklı boyutlarda gelişeceği açıktır. Resim, ses, video, yazı, belge gibi nesnelerin kendisine gizli veriyi gizlemekten çok bu nesnelerin taşınırken, iletilip paylaşılırken kullanılan iletişim teknikleri ve ortamları artık gizli veri için sığınak olmuştur.

Sosyal paylaşım ağları, web, bulut bilişim gibi Internet tabanlı teknolojilerin gelişmesi ve büyümesi ağ ortamında çok büyük boyutlarda veri alışverişinin gerçekleşmesi anlamına gelmektedir. Bununla beraber, bilgisayar, tablet ve akıllı telefonların günlük hayatta aktif kullanılmaları, ağ iletişiminde gizli veri iletimi için son derece yüksek kapasiteli bir ortam oluşması demektir.

Bu tez çalışmasında, bilgisayar-bilişim ağlarındaki resim, ses, video, metin gibi ortamlarda steganografi için oluşturulan gizli kanallar incelenmiştir. Daha sonra, ağ steganografisi ile oluşturulan gizli kanallarda, hangi tekniklerle hangi ortamlara veri

gizlenerek iletilebildiği incelenmiş, iletişim protokollerinin gizli veri iletimi için ideal bir ortam oluşturdukları görülmüştür. Gizli kanal oluşturma yöntemleri ile gerçek zamanlı veri gizleme uygulamaları gerçekleştirilmiştir. Bunlarla beraber paket zamanlama ile gizli veri iletimini kullanan ve IP ID alanını kullanarak gizli veri gönderen yeni iki yöntem önerilmiştir.

Önerilen paket zamanlama yönteminin bant genişliği önceki paket zamanlama tabanlı yöntemlere göre daha yüksektir. Önceki yöntemlerde iki paket arasındaki süre aralığında 1 bit gizli veri iletilirken önerilen yöntemde iletilen veri miktarı 2 bit olarak gerçekleştirilmiştir. Ayrıca paketler arası aralıkların varyasyonunun yüksek olması gizli veri iletiminin tespitini zorlaştıracaktır.

Önerilen IP ID alanına veri gizleme yönteminin, önceki yöntemlere göre ID alanının benzersizliğinin sağlanmasında daha etkili olduğu, ayrıca bu yöntemin paket parçalanmasından etkilenmeyen, dolayısıyla Internet üzerinde de gizli veri iletimini mümkün hale getiren bir yöntem olduğu görülmüştür.

Uygulamaların gerçekleştiriminde, pratik kodlama ve ağ uygulamaları için zengin bir kütüphane sunan Python programlama dili tercih edilmiştir. Uygulamalar neticesinde, ağ iletişiminde hiç de azımsanamayacak büyüklükte bant genişliğine sahip gizli kanallar oluşturulabildiği, bu gizli kanalların bir kısmının protokolden bağımsız olduğu, bir kısmının noktadan noktaya gerçekleştiriminin mümkün olduğu görülmüştür. Gerçekleştirilen tüm ağ steganografi uygulamalarının sonucu olarak, truva atları, virüsler, solucanlar gibi zararlı yazılımların ağ steganografisini kullanabildikleri, çok büyük boyutlu verileri gizleyerek iletebildikleri ihtimali düşünüldüğünde bilgi ve bilgi sistemleri güvenliği için çok büyük tehditler olduğu aşikârdır.

Bu tez çalışması kapsamında 1 adet uluslararası dergi yayını [19], 2 adet uluslararası konferans bildirisi [6; 67], 1 adet ulusal konferans bildirisi [5] ve 1 adet poster [69] yayınlanmıştır.

KAYNAKLAR

[1] **Day, J. D. ve Zimmermann, H.** The OSI Reference Model. *Proceedings of the IEEE.* 1983, Cilt 71, 12, s. 1334-1340.

[2] **Tanenbaum, A. S. ve Wetherall, D. J.** *Computer Networks.* s.l. : Prentice Hall, 2010.

[3] **Parziale, L., et al.** *TCP/IP Tutorial and Technical Overview.* s.l. : IBM, 2006. IBM Redbooks.

[4] **Önal, H.** Bilişim Suçlarında IP Adres Analizi. *Bilgi Güvenliği Akademisi.* [Çevrimiçi] 13 Mayıs 2010. [Alıntı Tarihi: 10 Haziran 2015.] http://www.bga.com.tr/calismalar/ip_forensic.pdf.

[5] **Karadoğan, İ. ve Daş, R.** TCP/IP Tabanlı Ağlarda Protokollerin İstismarıyla Yapılan Saldırı Türlerinin Analizi. *SIU2015: Sinyal İşleme Ve İletişim Uygulamaları Kurultayı.* 2015.

[6] **Karadoğan, İ., Daş, R. ve Baykara, M.** Scapy ile Ağ Paket Manipülasyonu. *1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu.* 2013, s. 196-201.

[7] *Network Protocols Handbook.* 2nd Edition. Saratoga CA : Javvin Technologies, 2005.

[8] **Ahsan, K.** Covert Channel Analysis and Data Hiding in TCP/IP. *University of Toronto.* 2002.

[9] **Önal, H.** TCP/IP Ağlarda Parçalanmış Paketler - Parçalanmış Paketler ve Güvenlik Sistemlerine Etkileri. [Çevrimiçi] 27 Mayıs 2009. [Alıntı Tarihi: 10 Temmuz 2015.] http://www.bga.com.tr/calismalar/fragmanted_packets.pdf.

[10] **Önal, H.** SynFlood DDOS Saldırıları. *Bilgi Güvenliği Akademisi.* [Çevrimiçi] 2010. [Alıntı Tarihi: 20 Temmuz 2015.] http://www.bga.com.tr/calismalar/synflood.pdf.

[11] **Bekşen, G.** Nmap El Kitabı. [Çevrimiçi] [Alıntı Tarihi: 5 Temmuz 2015.] http://www.secwis.com/wp-content/uploads/2011/11/NMAP_guncel.pdf.

[12] **Önal, H.** Özgür Yazılımlarla DDoS Saldırılarını Engelleme. *Bilgi Güvenliği Akademisi.* [Çevrimiçi] [Alıntı Tarihi: 25 Haziran 2015.] http://www.bga.com.tr/calismalar/opensource-ddos-engelleme.pdf.

[13] **Millî Eğitim Bakanlığı.** *Meslekî ve Teknik Eğitim Programlar ve Öğretim Materyalleri.* [Çevrimiçi] 2007. [Alıntı Tarihi: 10 Aralık 2015.] http://hbogm.meb.gov.tr/modulerprogramlar/kursprogramlari/elektrik/moduller/agprotokolleriveagguvenligi.pdf.

[14] **Vacca, J. R.** *Computer and Information Security Handbook.* s.l. : Morgan Kaufman Publishers, 2009.

[15] **Reynders, D. ve Wright, E.** *Practical TCP/IP and Ethernet Networking.* s.l. : Elsevier, 2003. ISBN 07506 58061.

[16] **Orebaugh, A., et al.** *Wireshark & Ethereal Network Protocol Analyzer Toolkit.* s.l. : Syngress Publishing, 2007. ISBN-13: 978-1-59749-073-3.

[17] **Önal, H.** DNS Hizmetine Yönelik Dos/DDoS Saldırıları. *Bilgi Güvenliği Akademisi.* [Çevrimiçi] 31 01 2012. [Alıntı Tarihi: 01 Temmuz 2015.] http://www.bga.com.tr/calismalar/dns_ddos.pdf.

[18] OS Fingerprinting. *ForensicWiki.* [Çevrimiçi] [Alıntı Tarihi: 05 Ocak 2015.] http://www.forensicswiki.org/wiki/OS_fingerprinting.

[19] **Karadoğan, İ. ve Daş, R.** An Examination on Information Hiding Tools for Steganography. *International Journal of Information Security Science (IJISS).* 2014, Cilt 3, 3, s. 200-208.

[20] Steganography. *Wikipedia.* [Çevrimiçi] [Alıntı Tarihi: 10 Temmuz 2014.] http://en.wikipedia.org/wiki/Steganography.

[21] **Petitcolas, F. A. P., Anderson, R. J. ve Kuhn, M. G.** Information Hiding: A Survey. *Proceedings of the IEEE (special issue).* 1999, Cilt 7, 87, s. 1062-1078.

[22] **Kahn, D.** *The Codebreakers.* s.l. : NY: The Macmillan Company, 1967.

[23] **Cheddad, A., et al.** Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing.* 2010, s. 727-752.

[24] **Li, X., et al.** A generalization of LSB matching. *IEEE Signal Processing Letters.* 2, Şubat 2009, Cilt 16, s. 69-72.

[25] **Badem, H. ve M., Güneş.** Video Formatına Veri Gizleme Amacıyla Gömülmüş Bir Steganografi Uygulamasının Geliştirilmesi. *KSU Mühendislik Bilimleri Dergisi.* 2011, Cilt 14, 2.

[26] **Yu, S., et al.** A Novel Steganalysis Scheme of Digital Video. *International Conference on Multimedia Information Networking and Security.* 2010. DOI 10.1109/MINES.2010.203.

[27] **Clark, S. ve Chang, C.** Linguistic Steganography: Information Hiding in Text. [Çevrimiçi] [Alıntı Tarihi: 6 Haziran 2015.] http://www.cl.cam.ac.uk/~sc609/talks/ed12stego.pdf.

[28] **Singh, P., Chaudhary, R. ve Agarwal, A.** A Novel Approach of Text Steganography Based on Null Spaces. *IOSR Journal of Computer Engineering.* 4, Temmuz-Ağustos 2012, Cilt 3, s. 11-17.

[29] **Satir, E. ve Isik, H.** A Compression Based Text Steganography Method. *The Journal of Systems and Software.* 2012, s. 2385-2394.

[30] **Nechta, I. ve Fionov, A.** Applying Statistical Methods to Text Steganography. 12 Ekim 2011.

[31] **Castiglione, A., De Santis, A. ve Soriente, C.** Taking advantages of a disadvantage: Digital forensics and steganography using document metadata. *The Journal of Systems and Software.* 2007, 80, s. 750-764.

[32] **Garg, M.** A Novel Text Steganography Technique Based on HTML Documents. *International Journal of Advanced Science and Technology.* 2011, Cilt 35, s. 129-138.

[33] **Zadjmool, R.** Hidden threat: Alternate Data Streams. [Çevrimiçi] 2004. [Alıntı Tarihi: 27 Haziran 2015.] http://www.windowsecurity.com/articles-tutorials/windows_os_security/Alternate_Data_Streams.html.

[34] **Mazurczyk, W., Smolarczyk, M. ve Szczypiorski, K.** Retransmission steganography and its detection. *Soft Computing.* 2011, Cilt 15, s. 505-515. doi:10.1007/s00500-009-0530-1.

[35] **Lampson, B. W.** A Note on the Confinement Problem. *Communications of the ACM.* 1973, Cilt 16, 10, s. 613-615.

[36] **Zander, S., Armitage, G. ve Branch, P.** A Survey of Covert Channels and Countermeasures in Computer Network Protocols. *The Electronic Magazine of Original Peer-Reviewed Survey Articles.* 2007, Cilt 9, 3.

[37] **Szczypiorski, K.** Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System HICCUPS. *Institute of Telecommunications Seminar.* 2003.

[38] **Girling, C. G.** Covert Channels in LAN's. *IEEE Transactions on Software Engineering.* 1987, Cilt SE-13, 2.

[39] **Cabuk, S., Brodley, C. E. ve Shields, C.** IP Covert Timing Channels: Design and Detection. *CCS'04.* 2004.

[40] **Rohankar, N. D., Deorankar, A. V. ve Chatur, P. N.** A Review of Literature on Design and Detection of Network Covert Channel. *International Journal of Engineering Science and Innovative Technology.* 2012, Cilt 1, 2.

[41] **Almttaary, A. M. S.** Data Hiding Transmission Using Flag Field in IP Header. *Journal of Babylon University/Pure and Applied Sciences.* 2014, Cilt 22, 5.

[42] **Mehta, Y.** Communication over the Internet using Covert Channels. 2005.

[43] **Bo, X., Jia-zhen, W. ve De-yun, P.** Practical Protocol Steganography: Hiding Data in IP Header. *Asia International Conference on Modelling & Simulation (AMS'07).* 2007.

[44] **Cauich, E., Gómez, R. ve Watanabe, R.** Data Hiding in Identification and Offset IP fields.

[45] **Handel, T. G. ve Sandford, M. T.** Hiding Data in the OSI Network Model. *Lecture Notes in Computer Science.* 1996, Cilt 1174.

[46] **Zander, S., Armitage, G. ve Branch, P.** Covert Channels in the IP Time To Live Field. *Australian Telecommunication Networks & Applications Conference (ATNAC).* 2006.

[47] **Rowland, C. H.** Covert Channels in the TCP/IP Protocol Suite. *First Monday: Peer-Reviewed Journal on the Internet.* 1997, Cilt 2, 5.

[48] **Ciobanu, R, et al.** SCONeP: Steganography and Cryptography Approach for UDP and ICMP.

[49] **LuBacz, J., Mazurczyk, W. ve Szczypiorski, K.** Vice Over IP. *IEEE Spectrum.* 2010.

[50] **Abad, C.** IP Checksum Covert Channels and Selected Hash Collision. [Çevrimiçi] 2001. [Alıntı Tarihi: 10 Temmuz 2015.] http://gray-world.net/papers/ipccc.pdf.

[51] **Fisk, G., et al.** Eliminating Steganography in Internet Traffic with Active Wardens. *Proc. 5th Int'l. Wksp. Information Hiding.* 2002.

[52] **Murdoch, S. J. ve Lewis, S.** Embedding Covert Channels into TCP/IP. *Information Hiding: 7th International Workshop.* 2005.

[53] **Giffin, J., Greenstadt, R. ve Tibbetts, R.** Covert Messaging Through TCP Timestamps. *Massachusetts Institute of Technology.* 2002.

[54] **Rios, R., Onieva, A. ve Lopez, J.** HIDE_DHCP: Covert Communications Through Network Configuration Messages. *27th IFIP TC 11 International Information Security and Privacy Conference (SEC 2012).* 2012.

[55] **Ji, L., Fan, Y. ve Ma, C.** Covert Channel For Local Area Network. *2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS).* 2010.

[56] **Frikha, L. ve Trabelsi, Z.** A New Covert Channel in WIFI Networks. *Third International Conference on Risks and Security of Internet and Systems (CRiSIS)'2008.* 2008.

[57] **Padlibsky, M. A., Snow, D. W. ve Karger, P. A.** Limitations of End-to-end Encryption in Secure Computer Networks. 1978.

[58] **Nair, A. S., et al.** Length Based Network Steganography using UDP Protocol. 2011.

[59] **Zhang, L., Liu, G. ve Dai, Y.** Network Packet Length Covert Channel Based on Empirical Distribution Function. *Journal of Networks.* 2014, Cilt 9, 6.

[60] **Quan-zhu, Y. ve Peng, Z.** Coverting Channel Based on Packet Length. *Computer Engineering.* 2008, Cilt 34, 3.

[61] **Ji, L., et al.** A Novel Covert Channel Based on Length of Messages. *International Symposium on Information Engineering and Electronic Commerce.* 2009, s. 551-554.

[62] **Dong, P., et al.** A Network Covert Channel Based on Packet Classification. *International Journal of Network Security.* 2012, Cilt 14, 2, s. 109-116.

[63] **Jankowski, B., Mazurczyk, W. ve Szczypiorski, K.** Information Hiding Using Improper Frame Padding. 2010.

[64] **Wolf, M.** Covert Channels in LAN Protocols. *Proc. Wksp. Local Area Network Security (LANSEC).* 1989, s. 91-101.

[65] **Hussain, M. ve Hussain, M.** A High Bandwidth Covert Channel in Network Protocol. *International Journal of Advanced Science and Technology.* 2011, Cilt 30.

[66] **Zhai, J., Liu, G. ve Dai, Y.** An Improved Retransmission-based Network Steganography: Design and Detection. *Journal of Networks.* 2013, Cilt 8, 1.

[67] **Baykara, M., Daş, R. ve Karadoğan, İ.** Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. *1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu.* 2013, s. 231-239.

[68] **Biondi, P.** *Scapy Project.* [Çevrimiçi] [Alıntı Tarihi: 15 Ocak 2015.] http://www.secdev.org/projects/scapy/.

[69] **Karadoğan, İ ve Daş, R.** Steganografi İçin Bilgi Gizleme Araçları Üzerine Bir Araştırma. *Uluslararası Adli Bilişim Sempozyumu.* 2014. (Poster).

ÖZGEÇMİŞ

İsmail KARADOĞAN

Kahramanmaraş Sütçü İmam Üniversitesi, Elbistan Meslek Yüksek Okulu, Bilgisayar Teknolojileri Bölümü, 46300, Kahramanmaraş

E-posta: ikaradogan@gmail.com

2000 - 2005 Fırat Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği bölümünden mezun oldu.

2004- 2011 Özel Sektörde değişik pozisyonlarda bilgisayar mühendisi olarak çalıştı.

2011 - Halen Kahramanmaraş Sütçü İmam Üniversitesi, Elbistan Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümünde Öğretim Görevlisi olarak çalışmaktadır.

2012- Halen Fırat Üniversitesi, Fen Bilimleri Enstitüsü Yazılım Mühendisliği Anabilim Dalında Yüksek Lisans eğitimine devam etmektedir.