Kablosuz Ağlar İçin Bir DoS Saldırısı Tasarımı

Deniz Mertkan GEZGİN[1], Ercan BULUŞ[2]

[1]Trakya Üniversitesi Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Edirne, Türkiye
[2]Namık Kemal Üniversitesi Çorlu Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, Çorlu-Tekirdağ, Türkiye
mertkan@trakya.edu.tr, ercanbulus@gmail.com
(Geliş/Received: 24.07.2013; Kabul/Accepted: 30.12.2013)

Özet- Kablosuz ağların gelişimi ve kullanımlarının artışı ile bu ağların güvenliğinin sağlanması hususu ön plana çıkmıştır. Kablolu ağlarda bu güne dek kullanılagelmiş olan çeşitli saldırı tipleri, aynı şekilde kablosuz ağlarda da kullanılır olmuştur. En sık görülen saldırı tiplerinden biri, DoS (Denial of Service – Hizmet Reddi) şeklinde sınıflandırılmış olan saldırı çeşididir. Kablosuz Ağ donanımı imal eden belli başlı şirketler, bu DoS saldırılarına karşı güvenlik politikaları geliştirmiş ve bunları önlemeye çabalamıştır. Ancak, bu kablosuz cihazların kullanıldığı kimi sahalarda birtakım güvenlik zafiyetleri gözlemlenmiştir. Bu çalışmada ilk olarak DoS saldırı teknikleri sınıflandırılmıştır. Ardından, kamuya açık alanlardaki kablosuz ağların DoS saldırılarına karşı zafiyetlerini test etmek için Vbasic programlama dili kullanılarak bir program yazılmıştır. Gerçekleştirilen saldırı tipleri, TCP (Transmission Control Protocol) Taşma Saldırısı, UDP (User Datagram Protocol) Taşma Saldırısı ve Ping Taşma Saldırısı olmuştur. Neticede, gerçekleştirilen saldırılar başarılı olmuştur.

Anahtar Sözcükler- DoS-denial of service, hizmet reddi, ping flood, tcp flood, mac spoofing, erişim noktası, kablosuz ağlar

Designing A DoS Attack For Wireless Networks

Abstract- With the development of wireless networks and the increase in their usage, the security of wireless networks has taken the centre stage. Various attack techniques that were previously used in wired networks have started to be used also in wireless networks. One of the major attacks is the one that is generalized as DoS (Denial of Service). Several wireless device producing companies have developed security policies against DoS attacks and tried to prevent them. However, in some of the fields that these devices are used, some security vulnerabilities have been observed. DoS attack techniques have been classified initially in this study. Afterwards, a program has been developed in Vbasic programming language in order to test the vulnerabilities of wireless networks in public places against DoS attacks. The attack types that were realized are TCP (Transmission Control Protocol) Flood, UDP (User Datagram Protocol) Flood and Ping Flood. Consequently, the attacks have been successful.

Keywords- DoS-denial of service, ping flood, tcp flood, mac spoofing, access points, wireless networks

1. GİRİŞ (INTRODUCTION)

Bu çalışmada temel olarak, DoS saldırılarının amaçları ve çeşitleri incelenmiştir. Ardından, Visual Basic 6.0 görsel programlama dilini kullanarak, Windows XP ve Windows 7 sürümleri altında çalışacak şekilde geliştirilmiş bir programla TCP taşma, UDP taşma ve Ping taşma tipi saldırıları gerçekleştirecek bir program geliştirilmiştir. Programı kullanarak birkaç adet farklı erişim noktası veya kablosuz modem test edilmiştir ve sonuçlar gözlemlenmiştir. DoS, hem kablolu hem kablosuz ağlarda yasal kullanıcıların iletişimini aksatmak veya kesintiye uğratmak ve web sitelerini yahut web hizmetlerini bir süreliğine devre dışı bırakmak için kullanılan bir saldırı çeşididir [1,2].

Bir bilgisayar üzerinden yürütülen saldırıların başarısızlığa uğradığı durumlarda ise, birden fazla bilgisayar kullanarak DDoS (Distributed Denial of Service Attacks – Dağıtılmış Hizmet Reddi Saldırıları) tipinde saldırılar gerçekleştirilmiştir. Bu teknik sayesinde DoS saldırıları birden fazla cihaz yahut program ile kuvvetlendirilmiştir [3,4].

2. DOS SALDIRILARI (DOS ATTACKS)

DoS saldırıları, karşı sistemin hizmetlerini aksatmak veya çalışmasını sekteye uğratmak amacına sahip saldırılardır. Saldırıda bulunan istemci, yasal kullanıcıların bilgi veya hizmetlere erişimini engelleme amacındadır. Bu çeşit saldırılarda amaç şifre kırmak veya bilgi çalmak değildir. Bu saldırılar hizmeti iki yolla sekteye uğratmaya çalışır:

- İşlemci, bellek veya bant genişliği gibi kaynakları aşırı kullanmak vasıtasıyla,
- Protokol veya hizmetlerdeki bir zafiyetten faydalanmak vasıtasıyla.

Teknik anlamda, DoS saldırısı şu şekilde işlemektedir. Saldırı mekanizmasını çalıştıran bilgisayar web sitesine bir istek (request) yollar ve bunu sürekli tekrarlar. Bu sayede ana bilgisayarda oluşan aşırı yüklenme ile hizmetler erişilemez duruma gelir, çünkü bütün kaynaklar tüketilmiştir. Sonuç olarak, diğer kullanıcılar web sitesine veya erişim noktasına erişemezler. Dahası, DoS saldırıları spam mail'lar yoluyla kotaları doldurararak diğer üyelerden e-posta mesajları alınmasını da engelleyebilmektedir [5].

DoS saldırılarının belirtileri:

- Beklenmedik biçimde düşük ağ performansı
- Web sitelerine erişimde yavaşlık
- Ağ bağlantılarında kesilmeler
- Spam e-postaların sayısında artış
- Bir web sitesinin belli bölümlerine erişimin imkânsız hale gelmesi
- Google Analiystic gibi istatisik veriler veren sitelerde, sitenizde aniden yoğunlaşan istatistik verileri

DoS saldırılarının çeşitli tipleri ve teknikleri mevcuttur. Günümüzde birçok bilgisayar ağları konusunda faaliyet gösteren şirket DoS saldırılarını tespit edip önlemek için yazılım ve donanımlar geliştirmektedir. Ve bunu büyük ölçüde engelleyebilmektedirler. Ancak, DoS saldırıları halen kimi güvenlik zafiyetleri bulunan cihaz veya web sitelerini etkilemektedir [6]. Bunun sebeplerinin başında ağ cihazlarının güncellemelerininin yapılmaması, yanlış güvenlik politikaları ve tecrübesiz güvenlik veya IT çalışanlarınının bulunması olarak görülebilir.

3. BİLİNEN DOS SALDIRISI ÇEŞİTLERİ (KNOWN TYPES OF DOS ATTACKS)

3.1. TCP/SYN (Senkronize) Taşma Saldırısı (TCP/SYN (Synchronize) Flood Attack)

Bu klasik tipte DoS saldırısı, modern ticari bilgisayar sistemleri üzerinde artık etkili olamamaktadır; zira hepsi bu tip saldırılara karşı korunmaktadır. Bu teknikte, SYN (Synchronize) paketleri hedef sisteme ulaşarak sistemin belleğini doldurmaktadır. Belleği tamamen dolan sunucu hizmet veremez duruma gelir ve istemciler bu sistem ile bağlantı kuramazlar [7].

3.2. TCP Tekrar Taşma Saldırısı (TCP Replay Flood Saldırısı)

Bu saldırı, kablosuz erişim noktasının belleğini, açık portlarından içeri yüksek miktarda veri (paket) yollamak suretiyle doldurma mantığıyla çalışır. Bu teknikte saldırı, MAC Adresi yanıltma (MAC Spoofing) veya IP Yanıltma (IP Spoofing) ile daha da yoğun hale getirilebilir.

3.3 Land Saldırısı (Land Attack)

Land saldırısı, kurban sistemin IP ve portlarına, kaynak ve hedefin IP'lerinin yanıltma tekniği ile elde edilerek aynı hale getirildiği paketler yollanarak yürütülen bir DoS saldırısıdır. Söz konusu pakette tokalaşma (handshake) süreci ile sonuçlandırılan bir bağlantı talebi bulunmaktadır. Bu tokalaşma sürecinin sonunda, kurban system bir ACK onay talebi yollar. Hedef ve kaynak koordinatlar aynı olduğu için de kurban kendi talebini kendisi yanıtlamak durumunda kalır. Ele alınan veri, ele geçmesi beklenen veri ile eşleşmediği için de ACK talebi tekrar yollanır. Neticede bu döngü, ağ yapılanması bozulana kadar devam eder.

3.4. Kaba Kuvvet Saldırısı (Brute-Force Attack)

Brute-Force saldırılarına örnek olarak "Smurf" saldırısı verilebilir. Bu saldırı tipinde, karşı bilgisayar ağı gereksiz bilgi ile işgal edilir. Bu işgali gerçekleştirmek için, saldırganlar IP tespit yapısındaki pr yayın özelliğini kullanırlar. Bu tekniği kullanan saldırgan, paketlerin hedef adresi olarak, ağın yayın adresini gösterir. Bu durum çerçevesinde, yönlendirici (router) ağ içerisinde bulunan tüm hostlara birer ICMP talebi yollayacaktır. Ağ bünyesinde çok sayıda host bulunuyorsa da, böylece çok sayıda ICMP yankı talep paketlerinin oluşması sağlanacaktır. Bu sayede, iletişim imkânsız hale gelecektir.

3.5. Ping Taşma Saldırısı (Ping Flood Attack)

Ping Flood, temel seviyede bir DoS saldırı tipidir. Bu teknikle saldırgan, kurban sistemlere büyük boyutlu (65000) ICMP paketleri yollayarak sistemin bant genişliğini doldurur. Bu sayede, ağ iletişimi sabote edilmiş olur [6]. Bu uygulamaya örnek olarak "Ölüm Pingi" (Ping of Death) saldırısı verilebilir. Ping of Death saldırısı, PING uygulamasını kullanarak IP tespitinde izin verilen maksimum 65535 bayt'lık veri limitini aşan IP paketleri kullanılmasıyla gerçekleştirilir. Ardından, gereğinden daha büyük boyuttaki bu paketler ağa yollanır. Sistemler bu yolla bozulabilir, durdurulabilir veya yeniden başlatılabilir. Fakat günümüzde tek başına etkisini yitirmiştir.

3.6. Gözyaşı Saldırısı (Teardrop Attack)

Gözyaşı saldırısı, IP paketlerinin yeniden birleştirilmesi süresince meydana gelen zafiyetten faydalanılacak şekilde tasarlanmıştır. Veri, ağlar üzerinde bir noktadan diğerine aktarılırken, genellikle küçük parçalara ayrılır. Bu parçaların her biri orjinal bir paket görünümüne sahiptir. Ancak, bunların haricinde bir de ofset alan bulunmaktadır. Teardrop programı paket parçalarından oluşan bir küme meydana getirir. Bu parçaların genellikle birbirleriyle eşleşen ofset alanları bulunmaktadır. Söz konusu parçalar hedef sistem bünyesinde nihayet bir araya getirildiğinde sistemler bozulabilir, durabilir veya yeniden başlayabilirler.

3.7. UDP Taşma Saldırısı (UDP Flood Attack)

UDP, hızlı ancak güvenliği düşük bir iletişim protokolüdür. Zira veri yollayan host, bu esnada söz konusu verinin karşı tarafa ulaşıp ulaşmadığını doğrulamamaktadır. Yalnızca hızın birincil önceliğe sahip olduğu durumlarda tercih edilen bu protokole bir DoS saldırısı yapılabilir [8]. UDP protokolü aracılığıyla DoS saldırısı gerçekleştirmek TCP protokolü üzerinden gerçekleştirmeye kıyasla daha zor ve karmaşıktır. Prensip olarak, UDP taşma saldırıları, uzak erişim noktalarındaki rastgele portlara büyük UDP paketleri yollanılarak gerçekleştirilir. Burada en önemli nokta, paketlerin sahte IP adresleri üzerinden yollanması gerekliliğidir. Dolayısıyla IP Spoofing tekniğinin kullanılmasının zaruri olduğu söylenebilir. Örneğin, bu yöntemle taşma saldırısı gerçekleştirildiğinde önemli olan, verinin karşıya ulaşıp ulaşmadığı değil, verinin karşıya ne kadar hızlı aktarıldığıdır [9].

3.8. DDoS Saldırıları (DDoS Attacks)

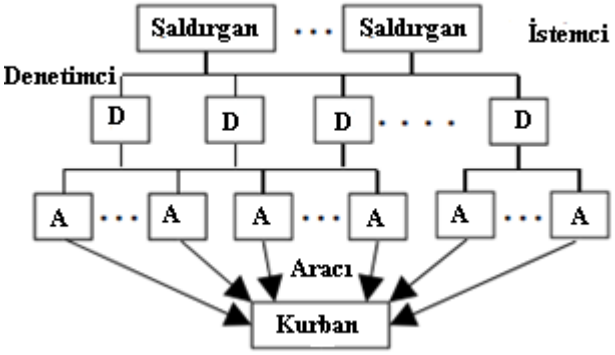
DDoS, Trojan benzeri yazılımlar aracılığıyla hedefe birden fazla sistemin aynı anda saldırıda bulunabildiği DoS saldırılarına verilen isimdir. Trojan yoluyla saldırıya katılan sistemler zombi sistem olarak tabir edilir. Bu saldırıda kurban olan sisteme binlerce, onbinlerce saldırgan ve zombileri DoS atak yapmaktadır. DDoS saldırılarının karakteristik özellikleri şöyledir:

- DDoS saldırısı birden fazla IP adresi üzerinden gerçekleştirildiği için, tespit edilmesi ve önlenmesi zordur. Ancak bir tek IP adresi üzerinden yapılan ataklar daha kolay önlenebilir.

- Bu saldırı tipinde kurban olarak seçilen birincil hedef, saldırılan sistemin hizmetleridir. İkincil kurbanlar ise, bilinçsiz biçimde ele geçirilmiş ve saldırıda kullanılacak şekilde ayarlanmış zombi sistemlerdir.

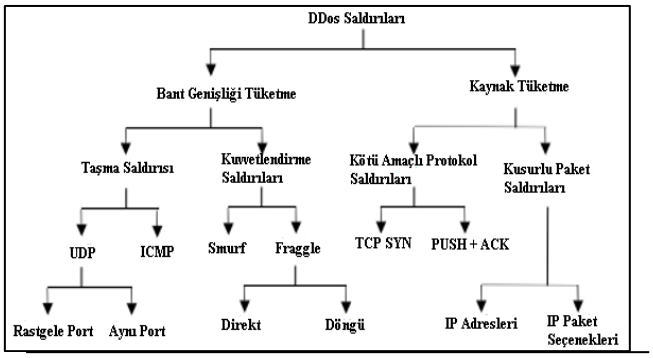
- DDoS saldırıları hedefin hizmetlerine yöneltilmiş geniş açılı ve koordineli saldırılardır [10,11].

- DDoS saldırı tipinde saldırganlar, bilgisayarı bot'a (zombi) çevirirler. Böylece bu bilgisayarların haberi olmadan internet üzerinde saldırganın saldırı programını çalışmasını sağlarlar. Bu sayede Denetimci (handler) ve Aracı (agent) olarak kullanılan cihazlar Web sistesini ya da ana makinayı çalışmaz hale getirebilir [12].



Şekil 1. DDoS Aracı - Denetimci Saldırıcı Modeli [19]
(DDOS Agent-Handler Attack Model)

- DDoS saldırılarının sınıflandırması Şekil 2'de verilmiştir. Bu makalede tasarlanan yazılım bant genişliğine yöneliktir. Kullanılan teknik ise Taşma Saldırılarıdır. Şekil 2'deki sınıflandırmada bu verilmiştir.



Şekil 2. DDoS Sınıflandırması [19]
(DDOS Taxonomy)

3.9. Kablosuz Ağlarda Kullanılan Diğer Etkili DoS Saldırı Tipleri (Other Effective DoS Attack Types Used in Wireless Networks)

Günümüzde kablosuz ağlara özgü çeşitli potansiyel tehditler ve saldırılar geliştirilmektedir. Ancak, DoS saldırıları da, kablosuz ağlar bünyesinde halen sıkça kullanılan saldırı tiplerindendir. Bir önceki bölümde yer verilmiş DoS saldırılarının yanı sıra, kablosuz ağlara özgü olan ve kimlik doğrulama kapsamına sahip aşağıdaki tipte DoS saldırıları da geliştirilmiştir:

- **802.11 Eşleştirme/Doğrulama Taşması Saldırısı,** Rastgele MAC adreslerinden yollanan sahte eşleştirme veya doğrulama istekleri ile hedef erişim noktasının eşleştirme tablosunun dolmasına yol açan saldırılardır.

- **802.11 İşaretçi (Beacon) Taşması Saldırısı,** Binlerce sahte 802.11 işaretçi yayınının yapılması ile istemcilerin geçerli bir erişim noktası bulmasını zorlaştırma amaçlı bir DoS saldırısıdır.

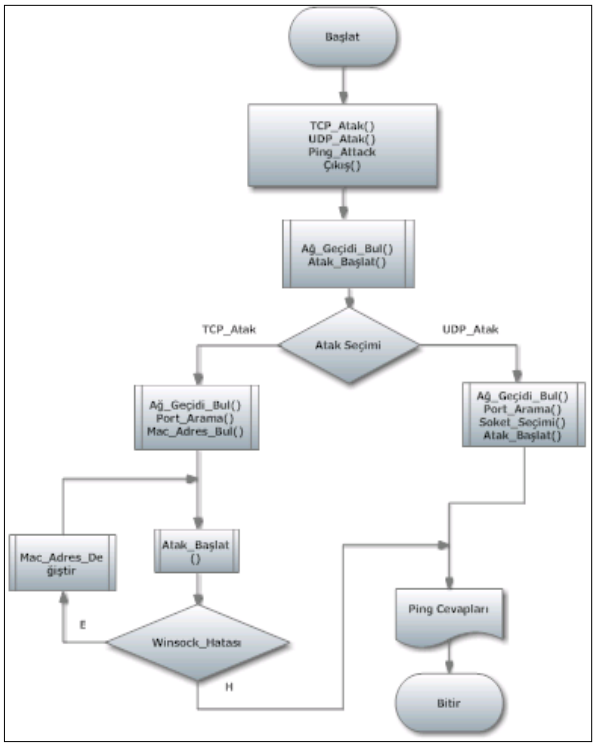
- **802.11 Kimlik Doğrulamayı Bozma (Deauthanticate) Taşması saldırısı,** İstemcilere sahte kimlik doğrulamayı bozma veya Eşleştirmeyi kırma (Disassociate) istekleri yollamak suretiyle erişim noktası ile bağlantılarını kesmeyi amaçlayan DoS saldırısıdır [13,14].

4. KABLOSUZ AĞ EKİPMANLARINA YÖNELİK OLASI SALDIRILARIN SINIFLANDIRILMASI (CLASSIFICATION OF POSSIBLE ATTACKS FOR THE WIRELESS NETWORKING EQUIPMENT)

Bu çalışmada kullanılan saldırılar, tablo 1'de görülen Netmaster Kablosuz Modem ve D-Link erişim noktası cihazlarını hedef almıştır. Bilhassa bu ürünlerin seçilmiş olma nedeni, bunların hem Kablonet ağı üzerinde hem de Trakya Üniversitesi Eğitim Fakültesi bünyesinde aktif olarak kullanılan cihazlar olmasıdır. Belirtilen saldırıların gerçekleştirilmesi için, Visual Basic 6.0 programlama dili kullanılmıştır. Bunun yanı sıra, nesne bileşeni olarak da Winsock 6.0 kullanılmıştır [15].

Tablo 1. Test Cihazları (Test Devices.)

Dizüstü Bilgisayar	Kablosuz Erişim Noktası 1
CPU: Intel Core Duo T5470 **İşletim Sistemi:** Windows Xp service pack 3 **RAM:** 2 GB **Sabit disk:** 180 GB **Kablosuz Bağdaştırıcı:** Intel Pro/wireless 3945 ABG network	• **Model:** net master cbw 560 • **Protokoller**: IEEE 802.11g • **Portlar:** 4 Ethernet Portu 10/100 Mbps, 1 USB Portu, 1 wireless (2.4 GHz) • WDS (Wireless Distribution System), WPS (Wireless Protection Setup) • WEP şifreleme, WPA/WPA2 şifreleme, MAC adres filtreleme
Kablosuz Erişim Noktası 2	
• **Model:** Dlink Dwl-2100 Access Point • **Protokoller**: IEEE 802.11 b/g, IEEE 802.3, IEEE 802.3u • **Portlar:** 1 Ethernet Portu 10/100 Mbps • WDS (Wireless Distribution System), WPS (Wireless Protection Setup) ,WEP şifreleme, WPA/WPA2 şifreleme • MAC adres filtreleme •	



Şekil 3. Programın Akış Diyagramı
(Flow Chart of the Program)

5. SALDIRIDA KULLANILAN TEKNİKLER (TECHNIQUES USED IN ATTACK)

5.1. Ping Taşma Saldırısı (Ping Flood Attack)

Ping flood saldırısını yürütebilmek için, şekil 5'de gateway_find() fonksiyonu çağırılmıştır. Ağ geçidi adresinin bulunmasının ardından, erişim noktasına şekil 4'deki fonksiyon çağrılarak saldırıyı gerçekleştirecek miktarda veri paketi yollanmıştır. Bu çalışmada, başlangıç değeri olarak 65000 belirlenmiştir. Bu adımın ardından, saldırı başlatılmıştır.

```
Gateway bul.
…
Bu AP'ye 65000 boyuntunda ping paketleri yolla.
…
Shell "ping " + (Text1.Text) + " -n1 -l " + (Text2.Text) + " & exit", vbHide
…
Devamlı Tekrarla.
```

Şekil 4. Programın Access Point'te ping saldırısını başlatması için gerekli kod
(Necesseray Code of the Program to start the ping attack)

5.2. TCP Tekrar Taşma Saldırısı (TCP Replay Flood Saldırısı)

Saldırıyı gerçekleştirebilmek için ilk olarak, Şekil 5'de Ağ Geçidi yani Erişim Noktasına ait IP adresi, MAC adresi ve SSID, Windows'un ipconfig komutu ile bulunmuştur. Bulunan ağ geçidindeki açık portlar ise yine Şekil 5'deki port_search() fonksiyonu ile taranarak elde

edilmiştir [16]. Genel olarak, erişim noktaları veya kablosuz modemlerde bu tip saldırıların önüne geçilebilmesi için cihazlar ilk satın alındığında portlar kapalı olacak şekilde ayarlanmaktadır. Bunun ardından, saldırı Şekil 4'te görülen attack_start() fonksiyonu kullanılarak başlatılmıştır. Bilgisayarın saldırıyı gerçekleştirmesinin ardından, aynı saldırı, hizmet MAC adresi değiştirilerek sistem durdurulana dek tekrarlanmıştır. Geliştirilen programın saldırı ekranı şekil 7'de verilmiştir. Saldırının gücünün yoğunlaştırılabilmesi için, diğer yandan UDP Taşma Saldırısı da aynı anda gerçekleştirilmiştir [17,18].

```
Eğer açıksa, Winsock nesnesini kapatıp tekrar aç.
...
lblportsayac. Caption = Int(lblportsayac. Caption) + 1
...
Sayacı devamlı olarak arttır ve erişim noktasına zorla bağlan.
...
Winsock2.RemoteHost = txtHost. Text
Winsock2.RemotePort = lblportsayac. Caption
Winsock2.Connect
...
Bağlanma durumunda, portun açık olduğu anlaşılır. Açık portu yazdır.
```

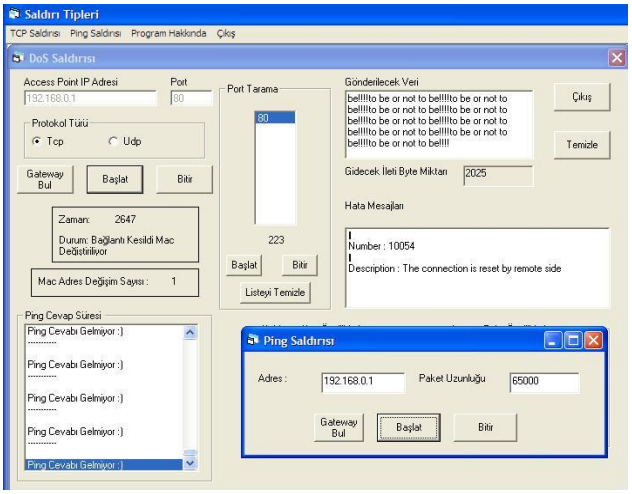
Şekil 5. AP bulma ve Açık port Arama Pseudo Kodları
(Pseudo Code of finding Access Point and researching Open port)

```
Winsock durum değeri 0 olmadığı sürece saldır.
...
If Winsock1.State <> 0 Then
...
      Winsock nesnesi içerisinden veri yolla
...
            Winsock1.SendData txtData.Text
...
Sayacı arttır.
...
            lblSent.Caption = lblSent.Caption + 1
...
Bağlantı koparsa ya da sistem bizi atarsa, MAC adresini değiştirip
tekrar bağlan.
Saldırıya devam et.
...
    lblStatus. Caption = "Durum: Bağlantı Kesildi. MAC değiştiriliyor"
...
MAC değişim fonksiyonunu çalıştır.
...
Macdegistir()
```

Şekil 6. Atağı Başlatma Pseudo Kodu
(Starting the attack of pseudo code)

5.2.1. *Saldırı Testlerinin Deneysel Sonuçları (Experimental Results of the Attack-testing)*

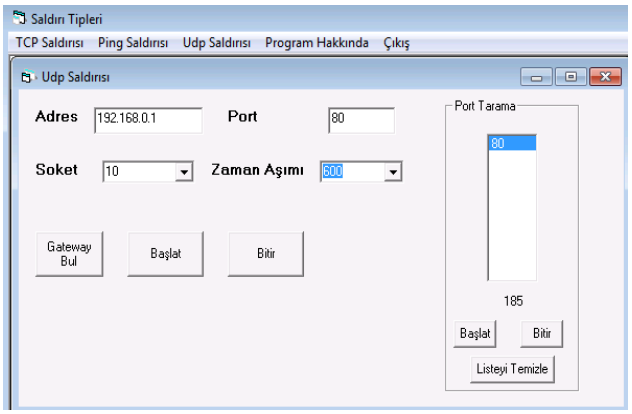
Bu saldırılarda, herhangi bir zombi sistem kullanılmamıştır ve TCP Veri Tekrarlama ve Ping saldırıları gerçekleştirilmiştir. Cihaza yollanan veri boyutuna göre değişen cihazın erişilemez hale gelme süresi incelenmiştir. Şekil 9'da, Üstel olarak azalan bir eğri göze çarpmaktadır. Yollanan veri boyutunun 256 Byte'a inmesi durumunda, cihazın servis dışı kalma süresi 18 dakikada sabitlenmektedir. Bunun yanı sıra, 64 KB'ın üzerinde verilerin kullanıldığı protokol yüzünden, veriler gönderilememiştir.



Şekil 7. DoS Saldırısı Programının Sonuç Ekranı
(Result Screen of DoS Attack Program)

5.3. *UDP Taşma Saldırısı (UDP Flood Attack)*

UDP taşma saldırısının gerçekleştirilebilmesi için, önce gateway_find() fonksiyonu tekrar çağrılmış, ardından da port_search fonksiyonu ile açık portlar tespit edilmiştir. Daha sonra, istenen soket sayısı ve zaman aşımı süresi seçenekleri ayarlanmış ve saldırı başlatılmıştır. Şekil 8'de gelişitirilen programın UDP taşma saldırısı modülü ekranı verilmiştir.



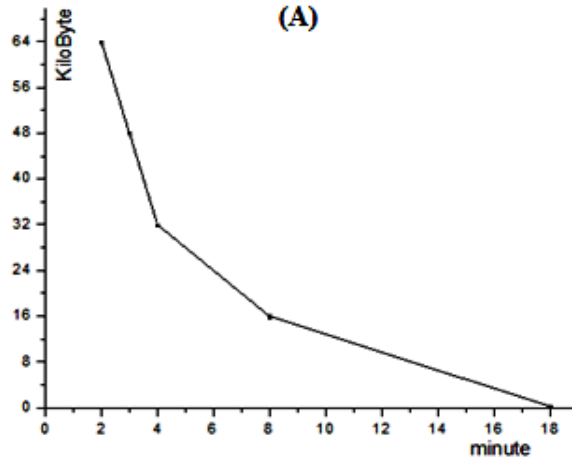
Şekil 8. UDP Taşma Saldırısı Ekranı
(UDP Flood Attack Screen)

5.3.1. *Saldırı Testlerinin Deneysel Sonuçları (Experimental Results of the Attack-testing)*

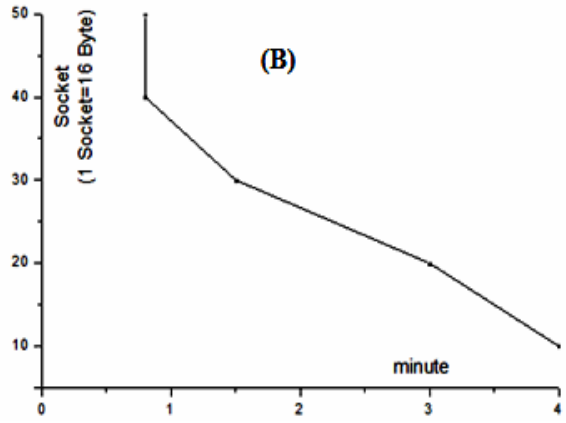
Dlink Erişim Noktasına UDP Taşma ve Ping saldırıları yapılmıştır. Şekil 10'da görüldüğü gibi yine, cihazın erişilemez hale gelme süresi, cihaza yollanan veri boyutuna göre incelenmiştir. Sonuç, doğrusal olarak azalan bir eğridir. Soketlerin sayısı 40'ın üzerine çıktığındaysa cihazın erişilemez hale gelme süresi bir dakikanın altında sabitlenmektedir.

Şekil 9 ve Şekil 10'de açıkça görüldüğü üzere, her iki saldırıda da yollanmış olan verinin miktarı arttıkça, cihazın erişilemez hale ulaşma süresi azalmaktadır. Kısa sürede başarılı saldırılar yürütebilmek için, yollanan veri

miktarı olabildiğince yüksek olmalıdır. Dahası, saldırı birden fazla bilgisayar ile yürütülüyorsa, cihazların erişilemez hali süresi daha da kısalacaktır.



Şekil 9. Netmaster Kablosuz Modem için TCP Veri Yineleme ve Ping saldırıları verileri
(TCP Data Replay and Ping attacks datas for Netmaster wireless modem)



Şekil 10. Dwl-2100 Erişim Noktası için UDP Flood ve Ping saldırıları verileri
(UDP Flood and Ping attacks datas for Dwl-2100 Access Point)

6. SONUÇLAR (CONCLUSION)

DoS, güvenlik politikaları kullanmayan veya bu tip güvenlik mekanizmaları bulundurmayan erişim noktası cihazlarını etkileyen bir saldırı tipidir. Evlerde veya kamuya açık alanlarda hizmete sunulmuş kablosuz yerel ağlara erişimi sekteye uğratmak veya tamamen kesmek için gayet etkili bir yöntemdir. Bu çalışmada kullanılmış olan saldırılar, kimseye zarar vermemek adına yerel cihazlar üzerinde gerçekleştirilmiştir. Protokol açıklarını kullanan bu atakların, bu protokollerin yapısı değişmedikçe DoS ve özellikle DDoS'un engellemesi %100 yapılamamaktadır. Aynı zamanda farklı tipte bu tip atakların web site ve servislerin yanısıra ağ cihazlarındada önemli etkileri görülmektedir [19].

Nihayetinde, bu saldırıları engellemenin kolay olmadığı görülmektedir. Bu nedenle kablsouz yerel ağların erişim güvenliğini arttırmak için aşağıdaki önerileri sunabiliriz:

1. Öncelikle billinmesi gerekn DoS ve özellikle DDoS saldırılarının tamamen önlenmesi çok zor gözükmektedir. Fakat atak sırasında önemli olan alacağınız güvenlik stratejinizin atağı tespit etmesi, ağ trafiğini hızlı bir şekilde temizlemesi ve kullanıcıların en az zararla bu ataktan kurtulmasıdır.

2. Ağ altyapımızın güçlü olması gerekmektedir. OSI katmanına göre yüksek seviyede güvenlik sağlayan akıllı cihazlar kullanılmalıdır. Planlamalar bu yönde yapılmalıdır.

3. Güvenlik duvarı (Firewall) kullanılmalıdır. Bu konuda internet servis sağlayıcılara geniş ağlar için DoS ve DDoS için belirli ücret karşılığında güvenlik iş devredilebilir.

4. Ağ Cihazlarını DoS ataklarına karşı hassas ve algılayıcı yeni cihazlarla değiştirmek etkili olabilmektedir ya da eskiye dönük cihazların Firmware güncellemeleri zamanında yapılmalıdır.

5. Ağa erişim hızının yavaşladığı tespit edildiğinde, kısa süre içinde ve tekrarlı olarak alınan taleplerin netstat gibi ağ komutları veya ağ trafiğini gözlemleyen yazılımlar kullanılarak takip edilmesi ve eğer mevcutlarsa bu talepleri yollayan sistem(ler)in IP veya MAC adreslerinin engellenmesi gerekmektedir.

6. Kablosuz ağlar için geliştirilmiş DoS ve DDoS saldırı tespit yazılımları kullanılabilir. Bu yazılımların açık kaynak kodlularıda bulunmaktadır. Ancak, bu tip yazılımların yönetim ve uygulanması zaman kaybına neden olabilmektedir [20,21].

7. Ağ içerisindeki MAC ve IP değişimlerini gözlem altında tutan bir cihaz kullanmak da güvenliğin sağlanabilmesi için son derece önemli bir adımdır. Bunun yanında DDoS ataklarına karşı sisteme etki etmeyen fakat ağda log tutan ağ cihazları(TAP) ile bu atakların tekrarlanmasına karşı çözüm üretebilinir [22,23].

8. Değişmesi gereken ve ağ cihazları üreten firmaların açıklara karşı yamaları takip edilmeli, destek vermeyen cihazlar değiştirilmelidir.

9. IT personeli ve bilgi işlem ile uğraşan akademisyenler özellikle TCP/IP protokol takımı ile DoS, DDoS atakları hakkında bilgilendirilmeli, gerekli önlemler alınmalıdır.

10. Cisco Guard, Radware Defense Pro gibi DDoS engelleyici yazılımlar yâda CheckPoint, Netscreen gibi güvenlik duvarı yazılım çözümleri kullanmak bir çözüm olarak düşünülmelidir.

KAYNAKLAR (REFERENCES)

[1]. M. Bernaschi, F. Ferreri, L.Valcamonici, "Access points vulnerabilities to DoS Attacks in 802.11 networks", Springer Science-Business Media, LLC 2006, 2006.

[2]. M. McDowell, "Understanding Denial of Servers Attacks", United States Computer Emergency Readiness Team (US-CERT), 2009.

[3]. Denial of Service, http://www.texascollaborative.org/SmithModule01/sec1_con.php, 10.06 2009.

[4]. C. Dougligeris, A. Mitrokotsa, "DDos attacks and defense mechanisms: classification and state-of-the-art", Computer Networks, 643-666, 2004.

[5]. E. Bulus, "Designing attacks for SMTP servers", International Journal of Computer Systems Science and Engineering 26-1, 43-48, 2011.

[6]. Dwl-2100 AP High Speed 2.4Ghz (802.11g) Wireless 108Mbps AccessPoint,http://www.dlink.com/products/?pid=292,02.04.2009 .

[7]. M.S. Stephen, B.L. Ruby, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures" Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems,543-550, 2004.

[8]. V. Karan, H. Hasbullah, A.Kumar, "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.

[9]. P. Payal, T. Gaurav, C. Rashmi,"Spoofing Media Access Control (MAC) and its Counter Measures", Published in International Journal of Advanced Engineering & Application, 2010.

[10]. K. R. David, "Remote Denial of Service Attacks and Countermeasures," Princeton University Department of Electrical Engineering Technical Report CEL2001-002, 2001.

[11]. Netmaster wireless gateway modem, http://www.netmaster.com.tr/urunler/cbw-560, 19.04.2010.

[12]. Microsoft Güvenlik Merkezi, "Botnet nedir", http://www.microsoft.com/tr-tr/security/resources/botnet-whatis.aspx,11.11.2012.

[13]. S. Kumar, "Ping attack-How pad is it ?", Computers&Security, 332-337,2006.

[14]. F.Y. Lee, S. Shieh, "Defending against spoofed DDoS attacks with path fingerprint", Computers&Security 24, 571-586, 2005.

[15]. Winsock.exe, SAMPLE: "Winsock.exe Getting Host Address Using Windows Sockets Article", ID:154512, http://support.microsoft.com, Microsoft, 01.03.2004.

[16]. Port Numbers, http://www.iana.org/assignments/port-numbers, last updated 29.04.2011.

[17]. P. Lisa, "A list of wirelesses network attacks", SearchSecurity.com, 2009.

[18]. Macshift.exe, " Change your MAC address" , http://devices.natetrue.com/macshift /, 10.08.2004.

[19]. R. Abramov, A. Herzberg. "TCP Ack storm DoS attacks." Computers & Security (2012), Volume 33, 12‑27, 2013.

[20]. G. Carl, R.R. Brooks, S. Rai, "Wavelet based Denial of service detection", Computers &Security 25, 600-615, 2006.

[21]. S. Han, E. Chang, T. Dillon, "Pairing-based public-key encryption schemes with backward-and-forward security", International Journal of Computer Systems Science and Engineering, Volume 23, Issue: 1, 303-308,2008.

[22]. P.K. Hussain, T. Dillon, E. Chang, F. Hussain, "Transactional risk-based decision making system in e-business interactions", International Journal of Computer Systems Science and Engineering, Volume 25, Issue: 1, 15-28,2010.

[23]. U.K. Tupakula, V. Varadharajan, "A Hybrid Model against TCP SYN and Reflection DDos attacks", International Journal of Computer Systems Science and Engineering, Volume 23, Issue: 3, 153-166,2008.