

Kablosuz Erişim Noktalarına Yapılan DoS Saldırıları

Deniz Mertkan GEZGİN¹, Ercan BULUŞ²

¹ Trakya Üniversitesi, Bilgisayar Teknolojisi ve Programlama Bölümü, Teknik Bilimler Meslek Yüksekokulu, Edirne

² Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Mühendislik Mimarlık Fakültesi, Edirne

mertkan@trakya.edu.tr, ercanb@trakya.edu.tr

Özet: Kablosuz ağlar gün geçtikçe daha çok kullanılmaya başlanılmıştır. Kullanımdaki bu artış bazı sorunları da yanında getirmektedir. Sorunların en önemlisi kablosuz ağların güvenliğidir. Güvenliği etkisiz hale getirmek için kablosuz ağlara yapılan saldırılar artmıştır. Saldırıları incelendiğinde en önemli amacın kablosuz ağlarda kullanılan erişim noktalarının (AP-Access Point) hafıza kaynaklarının tüketilmesi olduğu görülmektedir. Bunun sonucunda saldırgan kolaylıkla erişim noktası cihazını ele geçirip amaçları doğrultusunda kullanabilmektedir. Bu çalışmada Servis Reddi (DoS-Denial of Service) adı verilen saldırı tipleri sınıflandırılmış ve akış şemaları yardımıyla incelenmiştir.

Anahtar Sözcükler: Erişim Noktası, Servis Reddi, Atak Şemaları, 802.11, Değişmez Eşdeğer gizliliği, Kablosuz Ağlar.

Abstract: Recently, wireless networks are used widely. This raise in using these networks brings some problems. The most important problem is providing the security of these networks. The attacks to get the security of these networks are increased. When the attacks examine, it is seen that the main purpose of these attacks is expending the memory sources of the access points (AP) used in wireless networks. As a result of this, the attackers can easily get the control of the Access point device and use it for their aims. In this study, the attack types named Dos(Denial of Service) are classified and examined with the help of the flow charts.

Keywords: Access Point, Denial of Service, Attack Schemes, 802.11, Wired Equivalent Privacy, Wireless Networks.

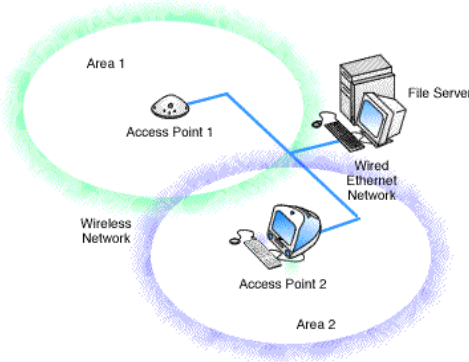
1. Giriş

Kablosuz ağların kullanımı günden güne artış göstermektedir. Bunun en önemli sebebi taşınabilirliktir. İstemciler kablo karmaşıklığına bulaşmadan ev, ofis, depo ortamlarından kolayca kablolu ağa entegre olabilirler yada internete erişim sağlayabilirler. Bazı durumlarda da bir ağ ortamı yaratabilmek için kablo kullanabiliriz. Kablolu ağa da bir Erişim Noktası (Access Point) cihazı ile entegre olunabilir. Böylece ağıımızı genişletebiliriz. Kablosuz yönlendirici olarak ta kullanılan AP'ler vardır. Bunlar daha çok ev kullanıcıları tarafından internete bağlanma amacı ile kullanılan

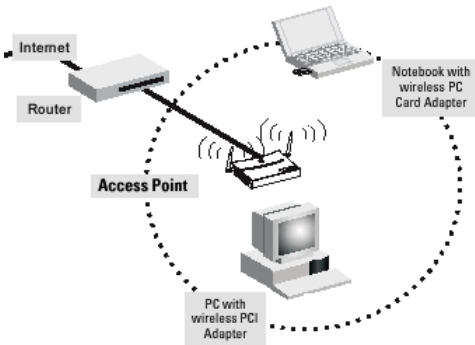
kablosuz erişim noktasıdır. AP'ler tekrarlayıcı (repeater) görevi yaparak dolaşım (roaming) işlemi ile ağı büyütüp, her yerde kaliteli sinyal almayı hedefler.

Kablosuz ağların kullanımı için pek çok önemli sebep vardır. Bunlardan en önemlisi taşınabilirliktir (mobility). Ev kullanıcıları oturdukları yerden internete bağlanabilir ya da ofislerindeki makinelere uzaktan bağlanıp işlerini görebilirler. Kablonun kullanılması tarihi eser gibi mekânlarda sakıncalıdır. Diğer taraftan ise kafe gibi değişken müşteri potansiyeli olan ortamlarda internet paylaşımı için kablosuz ağ idealdir. Endüstriyel ortamlar-

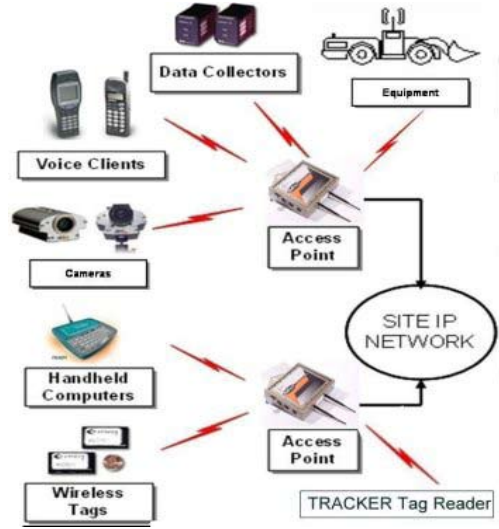
da kablosuz cihazlar olan barcode cihazlar, palm'ler ve kablosuz kameralar ve bu cihazların ağa entegre olarak çalışması üretimi ve yönetimi olumlu yönde etkilemiştir. Bu yararlı özellikler dışında, kablosuz ağların dezavantajları da tespit edilmiştir. Radyo sinyallerinin güvenliğinin sağlanması, kullanılan sinyallerin engellerden (çelik kapı, duvar gibi) kolay etkilenmesi, Sinyal bant genişliğinin düşük tutulması sıkça rastlanılan dezavantajlarından bazılarıdır. Günümüzde 802.11 protokolünü kullanan kablosuz ağ standartlarında ve cihazlardaki gelişmeler sayesinde bu dezavantajlar giderilmeğe başlanılmıştır. [1][2]



Şekil 1 - Dolaşım (Roaming) Yapısı



Şekil 2 - Ağ Geçidi Yapısı



Şekil 3 – Kablosuz Anahtar Yapısı

2. Erişim noktası (AP-Access Point) cihazları

Erişim noktası kısaca AP ya da WAP (Wireless Access Point) adıyla bilinir. Kablosuz ağlarda kullanılan basit bir cihazdır. Kablolu ağlardaki HUB isimli cihaza karşılık gösterilebilir. Düşük fiyatı ve kurulum kolaylığı sayesinde 2000 yılının başlarında Kablosuz Erişim Noktası Cihazlarının kullanımı hızlı bir şekilde arttı. İlk zamanlarda kablolu ağ ile kablosuz arasında görevi görürken, şimdilerde üç değişik işlev için kullanılmaktadır. Erişim Noktası Cihazlarının kendisine ait hafızaları vardır. İçlerinde gömülü yazılım (Firmware) bulunmaktadır. Bu yazılımlar yeni çıkan standartlara ya da gelişmelere göre güncellenebilir. Erişim Noktası Cihazları içlerinde güvenlik politikaları bulundurlar. Bunlardan bazıları WEP (Wired Equivalent Privacy) ve WPA' dır (Wi-Fi Protected Access). İstemcilere otomatik olarak IP atayan DHCP (Dynamic Host Control Protocol) mekanizmasına sahiptirler.

Üç biçimde Erişim Noktası Cihazları kullanılır:

- a)Ev ortamları için ağ geçidi(gateway)
İnternete erişmek için bir ağ geçidi gibi kullanılabilirler.
- b)Ofis ortamları için Erişim noktası
Ofiste kullanılacak kablosuz ağı oluşturmak için erişim noktası görevi görürler.
- c)Büyük şirketler için Kablosuz anahtar (switch)
Büyük ofislerde kablosuz ağlar ile kablolu ağların birbirine bağlanmasında, kablolu ağdaki switch gibi görev yapabilirler. [3]

Bunlara ek olarak, tipik bir IEEE (Institute of Electrical and Electronics Engineers) Erişim Noktası Cihazı 100 metre yarıçapında bir alanda 30 istemci ile iletişime geçebilir. Fakat bazı etkenler yüzünden sinyaller bazen azalabilir, hatta bağlantı kopabilir. Bu olumsuz etkenler; anten tipi, hava durumu, sinyal frekansının işleyişi ve aygıtın güç çıkışı olabilir. Ağ tasarlanırken alıcılar ile tekrarlayıcıların mesafeleri de ağın genişlemesi açısından dikkate alınmalıdır. Son zamanlarda Erişim Noktası Cihazları deneysel sonuçlara göre en uygun şartlarda birkaç kilometre mesafede işlem yapabilecek hale gelmiştir. Erişim Noktası Cihazları 802.11b ya da 802.11g standartlarına uygun configure edilebilirler. Bu da 11 Mbit/s ya da 54 Mbit/s hızlarında veri transferi demektir. Fakat ortalama 54 Mbit/s veri aktarımı 20 ile 25 Mbit/s arası gerçekleşir. Bu hız düşüklüğünün nedenlerinden biri ortamda bulunan duvar gibi engeller yüzünden sinyallerin geçiş yapamamalarıdır. 2006 yılında çalışmaları başlayan yeni standart 802.11n en yeni stan-

darttır ve bu standart 802.11g'ye fark atarak 248 Mbit/s (100 Mbit/s bile yüksek bir hızdır) hızda iletişim vaat etmektedir. Bu standartta karşılaşılabilecek en büyük problem 2.4 Ghz frekansını kullanan başka cihazlar tarafından yayının bozulmasıdır. Örnek: mikro dalga fırın, bebek telsizi, ya da telsiz telefon gibi.

3. 802.11 standartları

IEEE 802.11 standart takımı kablosuz yerel ağlar (WLAN-Wireless Local Area Network) iletişimi içindir. IEEE LAN/MAN (Local Area Network/Metropolitan Area Network) standart komitesi tarafından 5 GHZ ve 2.4 GHZ halk bandı (public spectrum band) içinde geliştirildi.[3] Kablosuz yerel ağlar, geniş alan değil, yerel alan uygulamasıdır. Bina içi (indoor) veya yerleşke (campus) alanında, gezici kullanıcılar (mobile user) için geliştirilmiş bir teknolojidir.

802.11 terimlerine rağmen, Wi-Fi sıklıkla kullanılan ve en çabuk ticarileşen bir isim olmuştur. Wi-Fi, Wireless Fidelity kelimelerinin ilk iki harfinin kullanılarak ortaya çıkartılmış bir kısaltmadır. 802.11b standardı Wi-Fi olarak adlandırılmış olup, kısaca Kablosuz ağ olarak kabul edilebilir.

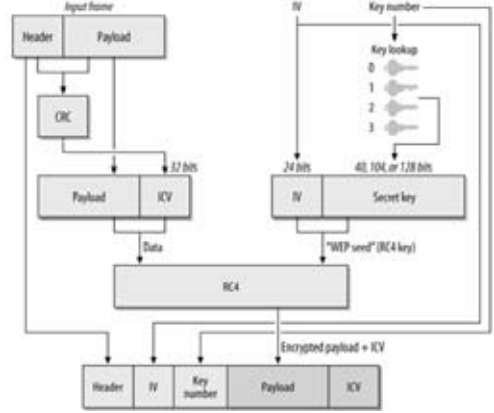
802.11 ailesi over-the-air modülasyon tekniğini içerir ki bu da aynı basit protokolü kullanır. En popüler olan kablosuz ağ standartları 802.11 b ve 802.11 g olarak tanımlanmıştır.802.11a ilk kablosuz ağ standardı olmasına rağmen 802.11 b geniş kitleler tarafından kabul edilmiştir. Bu gelişmeleri sırayla 802.11 g (şuan kullanılan) 802.11n standartları takip etmiştir.[4]

| Protokol | Yayın Tarihi | Frekans (GHz) | Net Veri Hızı (Mbit/s) | Veri Hızı (Max- Mbit/s) | Bina İçi Mesafe (metre) | Bina dışı Mesafe (metre) |
|----------|--------------|---------------|------------------------|-------------------------|-------------------------|--------------------------|
| Legacy | 1997 | 2.4 | 0.9 | 2 | 20 | 100 |
| 802.11a | 1999 | 5 | 23 | 54 | 35 | 120 |
| 802.11b | 1999 | 2.4 | 4.3 | 11 | 38 | 140 |
| 802.11g | 2003 | 2.4 | 19 | 54 | 38 | 140 |
| 802.11n | 2009 | 2.4 5 | 74 | 248 | 70 | 250 |

Şekil 2- 802.11 standartları

4. WEP(Wired Equivalent Privacy)

WEP, 802.11 kablosuz ağ güvenlik standartlarından biridir. Kablolu ağlarda eşdeğer protokolü(Wired Equivalent Privacy) geliştiricileri tarafından 802.1 olarak tanımlandı. Tam anlamıyla değişmez Eşdeğer gizliliği olarak ta adlandırılabilir. WEP 'in görevi de radyo dalgaları üzerindeki verilerin şifrelenmesini sağlamaktır. Geleneksel kablolu ağ gizliliği ile rekabet edebilmek için tasarlanan WEP, Eylül 1999'da 802.11 standardının parçası olarak onaylandı.[3] WEP gizlilik için Ron Rivest tarafından bulunan RC4 şifreleme algoritmasını ve bütünlük için CRC-32 sağlama toplamını kullanır. [5]



Şekil 3- WEP İşleyişi

WEP 'te doğrulama yöntemleri iki tanedir.

4.1. Açık anahtar kimlik doğrulaması

Açık sistem doğrulamasında, Kablosuz yerel alan ağlarının(WLAN) istemcileri doğrulama boyunca erişim noktasının güvenli bir belge sağlamasına ihtiyaç duymazlar. Doğrulama işleminde bir şifreleme yoktur. Bu yüzden herhangi bir istemci WEP anahtarlarına aldır-mayarak kendi kendine doğrulama yapıp, ağa dahil olabilir.

4.2. Ortak anahtar kimlik doğrulaması

Paylaşımlı Anahtar Doğrulamasında, WEP doğrulama için kullanılır.

Bu iletişimde istek ve cevap içi 4 yol vardır.

- 1.İstemci, erişim noktasına bir doğrulama isteği gönderir.
- 2.Erişim noktası geriye temiz bir yazı(text) gönderir.
- 3.İstemci(client) configure edilmiş kullandığı wep anahtarı ile bu texti şifreleyip tekrar geri gönderir.
- 4.Erişim noktası bu materyali deşifre eder ve gönderilen ile elindeki text'i karşılaştırır.

Bu karşılaştırmanın başarısına bağlı olarak, sonra doğrulama ve ağa dahil olma işlemi olur. Wep şifrelemesi için veri paketleri kullanılır.[6]



Şekil 5 – WEP Kimlik Doğrulaması
(WEP Authentcation)

5. DoS(Denial of Service)

Servis Reddi (Denial of Service) ataklarında, saldırgan legal istemcilerin bilgi erişimi ya da servislere erişimini engellemeye çalışır. Hedef bilgisayarınız, ağ bağlantınız, site erişimi olabilir. Örnek olarak Amazon.com adlı siteye 2000 yılında yapılan bir DoS saldırısında Server 20 dakika servis dışı (out-of-order) olmuştur. Kullanıcılar siteyi görüntülemek için site sunucusuna istek gönderirler. Sunucu bu isteklere cevap verir. Saldırgan bu istekleri devamlı göndererek sunucuya yük bindirir. Sunucu işlem yapamaz hale gelir. Kaynaklarını tüketir. Bu bir DoS ataktır. Çünkü siteye erişim yapılamaz. Dos atakları spam email mesajlarda kullanarak, kotaları şişirip, diğer mesajları ya da mail serveri şişirebilir.

DoS atak belirtileri:

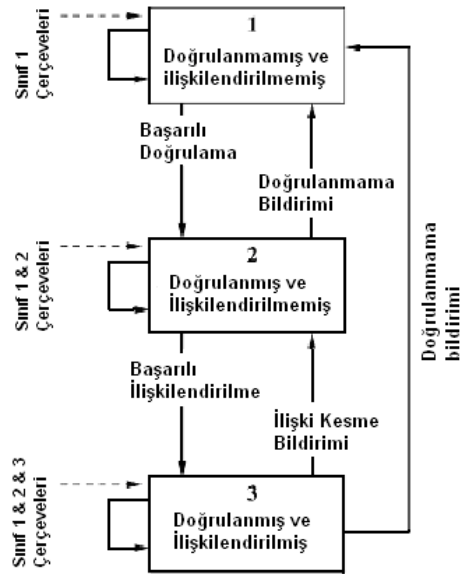
- Alışık olunmayan düşük ağ performansı
- Web sitelerinin belli bölümlerinin kullanılamaması

- Bir Web sitesine erişimde güçsüzlük
- Email kutusundaki spam e-mailerinin artışı

Son olarak tam anlamıyla DoS atakları önlemek imkânsızdır. Fakat bu durumda tavsiye edilen virüs programları, firewall programları kurarak bu ataklara müdafaa edilebilir.[7]

5. Erişim Noktalarına Yapılabilecek Saldırı Türleri

Erişim noktalarına yapılan saldırıların en önemli amaçları, sistemin kaynakları tüketerek belirli bir zaman ağ iletişiminin kesilmesidir. Böylece sisteme dâhil olan yasal istemcilerin normal iletişimi aksamış olacaktır. Bunu yaparken 3 çeşit saldırı şeması üzerinde durulmuştur. Bu üç saldırı tekniği de, erişim noktası ile istemci arasındaki etkileşim esas alınmıştır. Bu etkileşimi gösteren akış diyagramı aşağıdadır.



Şekil 6 – İstemci ile Erişim Noktası arasındaki etkileşim şeması

| Sınıf | Çerçeve Tipleri |
|-------|--|
| 1 | Araştırma İsteği/Cevabı Doğrulama, Doğrulamama |
| 2 | İlişkilendirme İsteği/Cevabı Tekrar ilişkilendirme, Ayrılma (ilişki kesme) |
| 3 | Doğrulamama |

Şekil 7 – 802.11 yönetim çerçeve sınıfları

Bu akış diyagramı üzerinden ele alınan saldırılar ise şunlardır :

5.1.Araştırma isteği taşması (Probe request Flood-PRF)

Kablosuz ağlarda, kablosuz istemciler çevredeki kablosuz erişim noktalarını keşfetmek için istek mesajları gönderirler. Erişim Noktası cihazları bir Araştırma İstek çerçevesine cevap vermelidir. Erişim noktası, bu cevabı verirken kendine özgü Araştırma Cevap Çerçevesi ile ağ hakkında bilgi verir. Böylece, bu saldırıda sahte, farklı Mac adreslerinden birçok PRF göndererek, AP'nin bunlara ağ hakkında bilgi vermekle uğraşırken diğer istemcilere ayırması gereken hafıza kaynaklarını tüketmek hedef alınmıştır.

5.2.Doğrulama isteği taşması (Authentication Request Flood - ARF)

Erişim noktası, istemciden gelen doğrulama isteklerine cevap göndererek ağın hangi doğrulama metodunu kullandığı hakkında bilgi verir.

Bu iki method önceki bölümlerde konu edilen Açık Sistem Doğrulaması ve Ortak Anahtar Paylaşımlı doğrulamasıdır. İstemci bir önceki PRF atak gibi, birçok sahte mac adresi ile doğrulama isteği gönderir. Bu isteklere hepsine AP cevap verir. Mac adresleri sahte olduğu için ve atak sayısının fazlalığı nedeniyle, iki

olayda da Erişim noktası yeni istemciler için kendi hafızasından yer saklaması gerekir. Bir önceki olay gibi ARF mesajları göndererek ve fiziksel adres yanıltma(mac spoofing) ile doyunluk seviyesine Erişim noktasının kaynaklarını kesmesi gerekir.

5.3.İlişkilendirme isteği taşması (Association Request Flood – ASRF)

ARF doğrulanmamış ya da ağa dahil olmamış durum içinde istasyon tarafından gönderilmemesi gerekir. Bu yüzden Erişim noktası tarafından asla isteklere cevap verilmemesi gerekir. Aslında ilişkilendirilmemiş doğrulanmamış çerçeve olarak gönderilen yasal olmayan ilişkilendirme istek çerçevelerine Erişim noktalarının cevap verdiğini keşfedilmiştir. Sonuç olarak, ilişkilendirme istek çerçevesi erişim noktası üzerinde hesaplanmış kaynakları, mesajla boğarak israf edebiliyor.[8]

6. Sonuç

Kablosuz ağlarda meydana gelen gelişmeler rağmen, üretilen erişim noktası cihazlarında güvenlik açısından bazı zayıflıklar görülmektedir. Özellikle DoS saldırılarına karşı görülen zayıflık üretilen cihazların ortak problemi olarak görülmektedir. Bu zafiyet hem cihazların hem de kullanılan protokollerin yapısından kaynaklanmaktadır. Çözüm olarak üretici firmalar tarafından cihazların mimarisi DoS saldırılarına karşı güçlendirilecek şekilde yeniden elden geçirilmelidir. Diğer yandan protokol zafiyeti ise halen gelişmekte olan 802.11 protokolüne yapılan eklerle gün geçtikçe azalmaktadır. Ancak protokolda yapılan yenilemeler kullanılan cihazların üzerinde gömülü yazılımlara üretici firma tarafından sık sık yansıtılmadıkça bu sorun ortadan kalkmayacaktır. Ağ yöneticilerinin ise erişim noktası cihazlarında bu güncellemeleri düzenli aralıklarla yapmalıdır.

Kaynaklar

- [1] Aravamudhan, Lachu. Getting to Know Wireless Networks and Technology. 4 July 2003. 5 Oct 2006 <http://www.informit.com/articles/printerfriendly.asp>
- [2] Goldsmith, Andrea. "Wireless Communications." Overview of Wireless Communications. 16 Oct 2006 <http://www.cambridge.org/us/catalogue/catalogue.asp>
- [3] IEEE 802.11 Working Group (2007-06-12). IEEE 802.11-2007: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ISBN 0-7381-5656-9.
- [4] ARRLWeb: Part 97 - Amateur Radio Service. American Radio Relay League.
- [5] 802.11® Wireless Networks The Definitive Guide By Matthew Gast. April 2005 ISBN: 0-596-10052-3
- [6] Nikita Borisov, Ian Goldberg, David Wagner (2001). "Intercepting Mobile Communications: The Insecurity of 802.11" 2006-09-12.
- [7] Understanding Denial-of-Service Attacks (US CERT)
- [8] Access points vulnerabilities to DoS attacks in 802.11 networks M. Bernaschi F. Ferreri L. Valcamonici 9 October 2006 Springer Science-Business Media, LLC 2006