POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Nesnelerin interneti (IoT) ve kablosuz algılayıcı ağların güvenliğine yapılan saldırıların tespit edilmesi ve önlenmesi

Detection and prevention of attacks on the internet of things (IoT) and wireless sensor networks

***Yazar(lar) (Author(s))**: Oğuzhan TAŞ[1], Farzad KIANI[2]*

ORCID[1]: 0000-0001-5019-3574

ORCID[2]: 0000-0002-0354-9344

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Taş O. ve Kiani F., "Nesnelerin interneti (ıot) ve kablosuz algılayıcı ağların güvenliğine yapılan saldırıların tespit edilmesi ve önlenmesi", ***Politeknik Dergisi***, 24(1): 219-235, (2021).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: **10.2339/politeknik.627825**

Nesnelerin İnterneti (IoT) ve Kablosuz Algılayıcı Ağların Güvenliğine Yapılan Saldırıların Tespit Edilmesi ve Önlenmesi

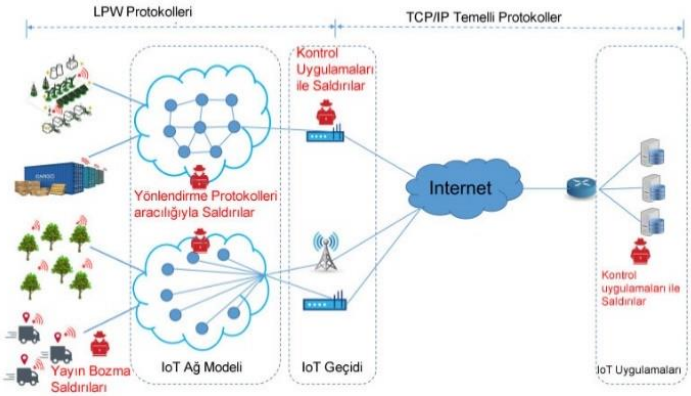
Detection and Prevention of Attacks on the Internet of Things (IoT) and Wireless Sensor Networks

Önemli noktalar (Highlights)

- *IoT Güvenliği (IoT Güvenliği)*
- *Nesnelerin İnternetinde Güvenlik (Internet of Things Security)*
- *Saldırıları tespit etme ve önleme (Detection and prevention of attacks)*

Grafik Özet (Graphical Abstract)

Bu çalışmada, IoT cihazların güvenliğini tehdit eden saldırılar incelenerek, ağ katmanlarına göre detaylı şekilde sınıflandırılmış ve savunma teknikleri önerilmiştir. In this paper, attacks that threaten the security of IoT devices are examined and classified according to network layers and defense techniques are proposed.



Şekil. Tipik LPW ağlar ve EDA saldırıları. /**Figure**. Typical LPW networks and related EDA

Amaç (Aim)

Bu çalışmada IoT güvenliğine yapılan saldırıların tespit edilmesi ve önlenmesi için katman bazlı çözümler amaçlanmıştır. / In this study, layer-based solutions are aimed to detect and prevent attacks on IoT security.

Tasarım ve Yöntem (Design & Methodology)

Şimdiye kadar yapılan tüm saldırılar incelenmiş ve bu saldırıları tespit etme ve önleme yöntemleri sunulmuştur. /All of the attacks which are maden so far have been examined and methods of detecting and preventing these attacks are presented.

Özgünlük (Originality)

Geçmişten günümüze IoT güvenliği hakkında çalışmalar IoT katmanlarına göre detaylı şekilde incelenip, şimdiye kadar sunulan savunma tekniklerine ilave olarak savunma teknikleri de önerilmiştir. / Studies on IoT security from past to present have been examined, and defense techniques presented so far.

Bulgular (Findings)

IoT sistemler internete bağlı olmaları yanında farklı ağ yapılarından ve heterojen teknolojilerin birleşiminden oluşması nedeniyle birçok saldırıya açıktır. / IoT systems are vulnerable to many attacks due to the combination of different network structures and heterogeneous technologies, as well as being connected to the internet.

Sonuç (Conclusion)

IoT cihazlarda gerekli güvenlik önlemleri alınmadığında, veri kaybı ve yetkisiz erişimler olabilmektedir. /When necessary security measures are not taken on IoT devices, data loss and unauthorized access can ocur

Etik Standartların Beyanı (*Declaration of Ethical Standards*)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler. / The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Nesnelerin İnterneti (IoT) ve Kablosuz Algılayıcı Ağların Güvenliğine Yapılan Saldırıların Tespit Edilmesi ve Önlenmesi

Araştırma Makalesi / Research Article

Oğuzhan TAŞ[1*], Farzad KIANI[2]

[1]Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Müh. Bölümü, İstanbul Sabahattin Zaim Üniversitesi, Türkiye
[1]Mühendislik Fakültesi, Bilgisayar Müh. Bölümü, İstinye Üniversitesi, Türkiye
[2]Mühendislik Fakültesi, Bilgisayar Müh. Bölümü, İstanbul Arel Üniversitesi, Türkiye

(Geliş/Received : 01.10.2019 ; Kabul/Accepted : 10.03.2020)

ÖZ

IoT (Internet of Things) ya da diğer adıyla Nesnelerin İnterneti kavramı, internete bağlanan ve diğer cihazlarla iletişimde olan her nesneyi kapsamaktadır. Artık hayatımızın bir parçası haline gelecek otonom araçlar, akıllı buzdolabılar, akıllı çamaşır makineleri, akıllı tost makineleri, akıllı saatler gibi birçok IoT cihazı birbiriyle farklı kablosuz ağ teknolojilerini kullanarak haberleşebilirler. IoT cihazların birçok kritik alanda kullanılmasıyla birlikte IoT güveniğine karşı yapılan saldırılar da artmıştır. Bu saldırılarda IoT katmanlarına yapılarak veri gizliliği, veri bütünlüğü, veri tazeliği, veri erişilebilirliği, kimlik doğrulama gibi kriterler ihlal edilebilmektedir. Bu saldırıları önlemek amacıyla birçok güvenlik çözümü önerilmiştir, fakat sınırlı enerji, kısıtlı batarya süresi, zayıf işlemci gücü ve sınırlı hafıza gibi sınırlamalardan dolayı düşük güçlü IoT cihazlar üzerinde geleneksel güvenlik yöntemlerinin uygulanması mümkün değildir. Bu çalışmada, IoT cihazların güvenliğini tehdit eden saldırılar incelenerek, ağ katmanlarına göre detaylı şekilde sınıflandırılmış ve savunma teknikleri önerilmiştir..

Anahtar Kelimeler: Nesnelerin interneti, nesnelerin internetinde güvenlik, kablosuz algılayıcı ağların güvenliği.

Detection and Prevention of Attacks on the Internet of Things (IoT) and Wireless Sensor Networks

ABSTRACT

Internet of Things (IoT) covers every object that connects to the Internet and communicates with other devices. Many IoT devices, such as autonomous vehicles, smart refrigerators, smart washing machines, smart toasters, smart watches that can become part of our lives and they can communicate with each other using different wireless network technologies. Because of using IoT devices in many critical areas, attacks against IoT security have increased. By making these attacks on IoT layers, criteria such as data privacy, data integrity, data freshness, data accessibility and authentication can be violated. Some security solutions have been proposed to prevent these attacks, but it is not possible to apply traditional security methods on low-power IoT devices due to some constraints such as limited energy, limited battery time, limited computational power and limited memory. In this paper, attacks that threaten the security of IoT devices are examined and classified according to network layers and defense techniques are proposed.

Keywords: Internet of things, internet of things security, wireless sensor networks security.

1. GİRİŞ (INTRODUCTION)

IoT(Nesnelerin İnterneti) son zamanlarda ortaya çıkan Bluetooth, Zigbee, GSM ve WiFi gibi çeşitli haberleşme çözümleri sunan nesnelerin ve cihazların birbiriyle bağlantısını ifade eden bir bilgisayar paradigmasıdır, IoT geleceğin haberleşme teknolojisi olarak kabul edilmektedir[1]. IoT tanımındaki "şey(things)" ifadesi, bir insan, hasta izleyen bir cihaz, akıllı bileklik, akıllı çatal, akıllı saat, akıllı telefon, otonom araçlar, akıllı şebeke istasyonu veya akıllı ev uygulamaları vb. birçok nesneyi ifade eder.

IoT teknolojisinin içeriğine bakıldığında Kablosuz Algılayıcı Ağlar(KAA), Makineden Makineye İletişim(M2M), Düşük güçlü Kablosuz Kişisel Bölge Ağları(LoWPAN) gibi ağlardan oluşmaktadır[2]. FANET(Tasarsız Hava Taşıt Ağları) ve VANET(Araçlar arası Tasarsız Ağlar) gibi ağlardan da IoT ağı oluşabilir. IoT teknolojisi, günden güne kullanım alanları artan dijital teknolojinin lokomotifi olacak teknolojilerden biridir. Gartner'in raporuna göre 2019 yılında 14,2 milyar cihaz kullanımda olacağı, 2021 yılında ise 25 milyar cihazın internete bağlanacağı tahmin edilmektedir[3]. Makineden Makineye bağlantı (M2M) sayısının 2022 yılında 12,3 milyara ulaşacağı, kişi başı 1,5 mobil cihaz düşeceği tahmin edilmektedir[4].

Sayısız uygulama alanına sahip olan IoT cihazlar, doğada vahşi yaşamın izlenmesinde, endüstride makinelerin performanslarının değerlendirilmesinde, şehir içi trafik yoğunluğunun takip edilmesinde, yapıların güvenliği ve deprem tespitinde, askeri alanda sınır güvenliğinin

*Sorumlu Yazar (Corresponding Author)
e-posta : oguzhantas@gmail.com

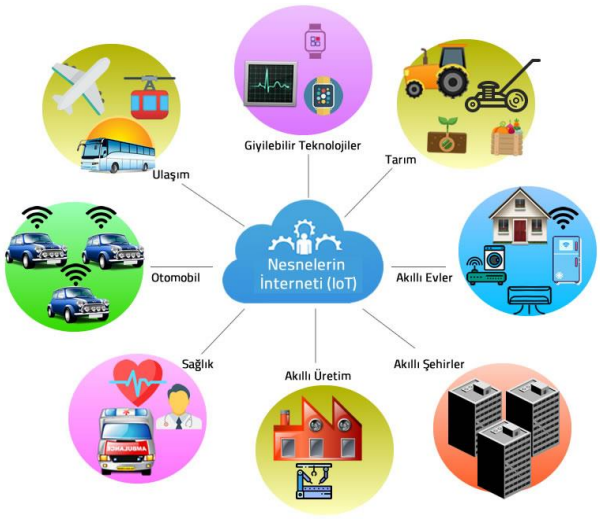
sağlanmasında vb. birçok görevde karşımıza çıkmaktadır. Ayrıca sağlık alanındaki uygulamaları popülerliğini korumaktadır, örneğin uzaktan hastaların izlenmesinde, görme özürlü insanların çevrelerindeki nesneleri hissetmelerinde, hasta kalp atışlarının takibinde, hastanın ilacını alıp almadığının kontrolünde vb. sağlık alanlarında IoT uygulamaları geniş olarak görülmektedir.

IoT cihazların kendi yapılarından kaynaklanan güvenlik, gizlilik problemleri araştırma konusudur. IoT sistemde güvenlikten bahsedildiğinde İnternet, Hücresel Ağlar, Kablosuz Algılayıcı Ağlar(KAA) gibi ağlardan kaynaklanan sorunlar olabilir. Ayrıca, IoT cihazların kendilerine gelen büyük miktarda bilgiyi depoladıkları Bulut Sistemlerin güvenliği de IoT güvenliği bünyesinde incelenen önemli bir konudur.

IoT şemsiyesi altında yer alan Kablosuz Algılayıcı Ağların(KAA) üç anahtar elementi olarak; algılama, işleme ve haberleşmeyi sayabiliriz. KAA'ın avantajları arasında; düşük maliyetli olmaları, az yer kaplamaları ve küçük hacimde olmaları söylenebilir, bu özelliklerinden dolayı KAA'lar geçmişten günümüze birçok uygulama alanı bulmuştur. Ayrıca, algılayıcı ağlar kendi kendini organize eden bir yapıya sahiptir, bu özellik ile de işleme ve haberleşme kapasitesini paylaşabilme gibi avantajları bulunmaktadır.

Bir algılayıcı ağ donanımsal olarak; batarya, mikro-kontrolcü, radyo iletişim ünitesi ve algılayıcıdan oluşur. Kablosuz Algılayıcı Ağların(KAA) ve kısıtlı batarya süreli IoT cihazların bazı dezavantajları bulunmaktadır. Sınırlı enerji, zayıf işlemci gücü, limitli saklama kapasitesi, sınırlı bant genişliği gibi dezavantajlar, karşılaşılan en önemli zorluklardır. Bu nedenle, klasik ağ teknolojilerinden farklı olarak, özel yönlendirme protokolleri, az sistem kaynağı tüketen, hafif şifreleme algoritmaları, bu cihazlar için özel olarak tasarlanmış hafif güvenlik protokolleri uygulanmaktadır.

Geleneksel kriptografide kullandığımız büyük anahtar boyutuna sahip(şifreleme güvenliğini artırmak için) AES, DES gibi güçlü simetrik şifreleme algoritmaları algılayıcı ağlarda ve küçük ölçekteki IoT cihazlarda uygulamak pratik değildir. Ayrıca, güvenlik için oldukça sık kullanılan RSA gibi asimetrik yapıdaki güçlü genel anahtar algoritmaları, SHA-256 ve RIPEM-D gibi mesaj özütü algoritmaları, Diffie Hellman gibi güvenliği büyük asal sayılara dayanan anahtar yönetimi teknikleri kullanılması uygun değildir. Klasik teknikler, hesaplama karmaşıklığı bakımından verimli değildir, çünkü hesaplamalar güçlü işlemci ve bellek birimi gerektirmektedir. Sistem kaynaklarının sınırlı olmasından dolayı, güvenlik gereklerinden olan gizlilik, kimlik doğrulama, inkâr edememe, erişilebilirlik bahsedilen bu güçlü algoritmalarla ve tekniklerle sağlanamamaktadır, dolayısıyla cihazlar saldırılara karşı zayıf hale gelmektedir. Özellikle askeri alanda ve tıp alanında algılayıcıların güvenliği önem arz etmektedir. Çünkü IoT ağları, geleneksel ağlar gibi erişilemez veya ulaşılamaz durumda değildir. Geniş bir coğrafi alana bırakılan kablosuz algılayıcıların düşman tarafından ele geçirilip, yeniden programlanması gibi riskler mevcuttur.



Şekil 1. Nesnelerin internetinin kullanıldığı bazı alanlar (Some areas where the Internet of Things is used)

IoT ve WSN katmanlarına geçmeden önce MANET, VANET ve FANET kavramlarını kısaca açıklayalım. MANET(Mobil Tasarsız Ağlar) tanım olarak, serbest şekilde ağa dâhil olan ve ağdan ayrılan mobil düğümlerden oluşan sınırlı iletişim gücüne, bataryaya ve işleme gücüne sahip ağlardır. MANET düğümlerinin belli bir yapısı yoktur. Kendi kendine organize olan bu yapı, özellikle askeri alanda ve felaket yönetimi uygulamalarında tercih edilen popüler hale gelmiştir. MANET'in alt kolu olan FANET(Tasarsız Hava Taşıt Ağları) ise tanım olarak, insan yönetimi olmadan verilen işi, işbirliği yaparak tamamlayan bir grup insansız hava aracının oluşturduğu ağ yapısıdır. MANET'in diğer bir alt kolu olan VANET(Araçlar arası Tasarsız Ağlar) ise verimli ve güvenli taşıma amacıyla araçlar arası ve araçlar ile yol kenarındaki baz istasyonları arası haberleşmeyi ifade etmektedir.

IoT ve KAA sistemde katman mimarisi birbirine benzemekle birlikte farklı kaynaklarda farklı şekilde ifade edilmektedir, KAA sistemde aşağıdaki gibi beş katmanda[5], IoT sistemde ise dört katmanda[6] ifade edilmektedir, fakat heterojen yapıdaki tüm IoT sistemleri için bu katman yapısı geçerli değildir, farklı IoT teknolojilerinde katmanlarda farklılıklar olabilmektedir.

Nesnelerin İnterneti Uygulamalarında farklı kaynaklarda farklı gösterimler mevcut olmakla birlikte genelde dört katmanla ifade edilmektedir.

Bazı kaynaklarda Uygulama ve Ağ Katmanı arasında Veri İşleme Katmanı (Data Processing Layer) da ifade edilmektedir. Bu katmanın alt katmandan aldığı bilgileri işleme, analiz etme, değerlendirme, sonuca göre karar alma diğer cihazlarla paylaşma gibi görevleri vardır. Akıllı saat, akıllı ev hub'ı gibi cihazlarda daha önce analiz edilip ve kaydedilen verilerden yola çıkarak kullanıcı deneyimini artırılır[7]. Biz bu katmanı da Uygulama katmanı bünyesinde değerlendireceğiz.

Çizelge 1. KAA katman mimarisi (layered architecture for WSN)

UYGULAMA KATMANI	Veri birleştirme, son kullanıcıyla etkileşim yapılır.
TAŞIMA KATMANI	Güvenilir veri taşıma işlemi bu katmanda yapılır.
AĞ KATMANI	Yönlendirme, ağ topoloji yönetimi yapılır.
VERİ BAĞI KATMANI	Hata Kontrolü, Veri çerçevesi tespit etme, çoğullama
FİZİKSEL KATMAN	Modülasyon, frekans ve kanal seçimi, sinyal işleme

Çizelge 2. Nesnelerin İnternetinde katman mimarisi (layered architecture for the Internet of Things)

UYGULAMA KATMANI	Son kullanıcıyla etkileşim kuran soyutlanmış çözümler.
ORTA KATMAN	API, Web Servis ve Bulut vb.
AĞ KATMANI	Kablolu ve kablosuz sistemlerden oluşur. Algılama katmanından gelen veriyi işleme ve iletme işlemleri.
ALGILAMA KATMANI	Ortam verisini algılama işlemleri. mekaniksel, elektriksel, elektronik ve kimyasal algılayıcılar

IoT sistemlerde Algılama(Sensing) Katmanında, fiziksel ortamda algılanan veriye bağlı olarak eylemler gerçekleştirilir. Çeşitli algılayıcılar tarafından farklı türde veriler gerçek dünyadan algılanmaktadır. Bu katman birkaç algılayıcıdan oluşur, uygulamalarda çoğul algılayıcı kullanımı IoT cihazların en temel özelliklerinden birisidir. Hareket Algılayıcılar(doğrusal ve açısal), Çevresel Algılayıcılar(basınç, ışık, sıcaklık, nem, kamera, ultrasonik), Pozisyon Algılayıcılar(manyetik, GPS vb.) örnek verilebilir. Mekaniksel, elektriksel, elektronik ve kimyasal algılayıcılar fiziksel ortamda kullanılabilir. Farklı IoT Uygulamaları örneğin GPS, RSN vb. farklı algılama katmanı teknolojileri kullanır. Düğüm ele geçirme, Yayın Bozma, Zararlı Kod Aşılama, Yan Kanal Saldırısı, Uykudan Yoksun Bırakma gibi saldırı teknikleri bu katmana yapılmaktadır.

IoT sistemlerde Ağ(Network) Katmanı, algılama katmanından alınan bilginin işleme amacıyla hesaplama birimine gönderilmesini sağlayan, adeta haberleşme kanalıdır. DDoS/DoS Saldırıları, Gider Deliği(Sinkhole), Kara Delik(Blackhole), Solucan Deliği(Wormhole), Sybil, Yönlendirme Saldırıları vb. saldırılar bu katmana yapılmaktadır.

IoT sistemlerde diğer bir katman olan Orta-Katman(Middleware), Ağ ve Uygulama katmanı arasında soyut bir katman oluşturarak güçlü hesaplama ve saklama yeteneği sağlamaktadır. Kuyruklama sistemleri, uygulama katmanın isteğini yerine getiren API'ler, web servisler, kalıcı veri depoları vb. bu katmanda yer almaktadır. Ağ Geçidi(Gateway) ise çoklu cihaza, kullanıcılara, bulut servislere bağlantıda önemli görev üstlenmektedir, bu katman IoT cihazlarda yazılım ile donanım çözümleri sunmaktadır. Farklı katmanlar arasında IoT verisinin şifrelenmesi ve çözülmesi işlemleri için de geçitler kullanılmaktadır. Heterojen IoT sistemleri(Zigbee, KAA, LoraWin, Z-Wave, LoRa, WiFi, Bluetooth, hücresel ağlar vb.) arasında güvenliğe yönelik saldırılar olabilmektedir. Veritabanlarına yönelik SQL Aşılama Saldırısı, IoT sistemlerde yayınlama-üyelik haberleşme modeli sunan MQTT protokolüne Ortadaki Adam Saldırısı, web servislerinde kullanılan İmzalara Yönelik Saldırılar, bulut sistemlere Zararlı Yazılım Aşılama, DoS saldırısının bir benzeri olan servis kalitesini (QoS) düşüren Bulutta Akın Saldırısı bu katmanda gerçekleşir.

Uygulama(Application) Katmanı ise IoT sistemlerde son kullanıcıya hizmetler sunmaktadır. Akıllı evler, akıllı sayıcılar, akıllı şebekeler, akıllı taşımacılık, kişisel bakım, sağlık vb. uygulamalar bu katmanda yer almaktadır. Veri Çalma, Erişim Kontrol Saldırıları, Servis Kesintisi Saldırıları, Zararlı Kod Aşılama Saldırıları, Dinleme Saldırıları ve Yeniden Programlama Saldırıları bu katmanda gerçekleşir.

Bu çalışmada, yapılan saldırılar sınıflandırılarak detaylı şekilde incelenmiş ve bu saldırılara karşı savunma stratejileri geliştirilmiştir. Geçmiş çalışmalara bakıldığında, saldırıların sınıflandırılmaları farklı kategorilere ayrılarak incelenmiştir. Örneğin Chelli[8]'e göre saldırılar; hedef yönelimli, performans yönelimli ve katman yönelimli olmak üzere üç temel gruba ayrılmaktadır. Bu çalışmada bazı saldırılar tanımlanmış ve kategorize edilmiş ama savunma stratejileri sunulmamıştır. Bisvas ve arkadaşları[9] ise bu saldırılara ilave olarak, veri iletilirken yapılabilecek Ağ iletimini Kesme, yetkisiz olarak algılayıcıya veya veri saklanılan birimine erişme, Mesajın kimden geldiği bilgisinin değiştirme gibi saldırı yöntemlerini incelemiştir. Bu çalışmada bazı savunma tekniklerine değinilmesine rağmen tüm saldırılar detaylı olarak incelenmemiştir. Bu çalışmalara benzer olarak farklı çalışmalarda[10-14] algılayıcılara yapılan saldırılar katmanlara göre sınıflandırılarak incelenmiş, fakat kısıtlı sayıda saldırı tekniğine çözüm getirilmiştir. Ayrıca, algılayıcılara saldırılar katmanlara göre detaylı olarak incelenmiş, saldırılara karşı çözüm önerileri getirilmiştir. Heterojen yapıdaki tüm IoT sistemlerine göre katmanlar tam olarak belirlenmediği için, IoT sistemi çatısında yer alan Kablosuz Algılayıcı Ağların katman yapısına göre saldırıları tasnif edilmiştir. IoT katman yapısındaki Orta-Katman ise KAA'lardaki Uygulama Katmanına dâhil edilmiştir.

II. Bölümde Fiziksel Katmana Saldırılar, III. Bölümde Veri Bağı Katmanına Saldırılar, IV. Bölümde Ağ Katmanına Saldırılar, V. Bölümde Taşıma Katmanına Saldırılar ve VI. Bölümde Uygulama Katmanına Saldırılar, VII. Bölümde Diğer Saldırılar incelenmiştir. Her bir saldırı türü için ilgili bölüm içinde savunma stratejileri önerilmiştir. Sonuç bölümü olan VIII. Bölümde özet ve gelecekte yapılması planlanan çalışmalar üzerinde durulmuştur.

2. FİZİKSEL KATMANA SALDIRILAR (ATTACKS TO PHYSICAL LAYER)

2.1. Yayın Bozma Saldırısı (Jamming Attack)

Bu saldırıda düşman güçlü bir anten ile sinyal üreterek iletişimde parazit yapmaya çalışır, bu saldırının farklı türleri bulunmaktadır.

- Sabit olarak yayını bozma(Constant jamming) işleminde sürekli olarak radyo sinyali gönderilir veya MAC katman etiketi olmadan rastgele bitler kanala gönderilir[15].
- Aldatıcı yayın bozma(Deceptive Jammer) işleminde ise, sürekli aldatıcı paketler göndermek yerine, düzenli paketlerin arasına aldatıcı paketler yerleştirilir, iletişim kuran taraf her şeyin yolunda gittiğini zanneder.
- Rastgele yayın bozmada(Random jammer) ise sürekli radyo sinyalleri göndermek yerine bir süre gönderilir sonra uyuma moduna geçilir, belli bir süre sonra uyku modundan çıkılarak tekrar göndermeye devam edilir. Uyku modunda, sabit veya aldatıcı yayın bozma gibi davranılır.
- Tepkili yayın bozma(Reactive Jammer) saldırısında ise, daha önce değinilen üç aktif yayın bozma tekniğinden farklı olarak, ağda trafik olup olmadığına bakılır, trafik yoksa bekleme moduna, trafik varsa aktif moda geçilir, tespit edilmesi zor bir saldırıdır[14-18].

Yayın bozma saldırıları, tüm algılayıcı ağ tiplerine yönelik olduğundan oldukça etkili bir saldırılardır. Bazı kaynaklarda servis yalanlaması (DoS) kategorisi altında gruplandırılmıştır. Bu saldırı her bir katman için de tehlike oluşturmaktadır, dolayısıyla bu saldırı için her katmana yönelik alınan önlemler farklılaşmaktadır. Fiziksel katmanda, haberleşme sırasında sinyalin veya paket bitlerinin değiştirilmesi şeklinde de gerçekleşmektedir. ACK paketlerine yönelik saldırılar Veri Bağı katmanını ilgilendirdiğinden, ilgili bölümde incelenecektir.

Savunma stratejisi olarak, ağ performansını ölçen istatistiksel teknikler uygulanabilir. Sinyal gücü, taşıyıcı algılama süresi, paket teslim oranı gibi bilgiler kullanılarak yapılan hesaplamalarla sinyalde bozulma olup olmadığı anlaşılır.

Diğer bir savunma tekniği olarak, algılayıcı düğümlerde frekans karıştırma teknikleri ile yayın bozma saldırısı önlenebilir. FHSS(Frekans Atlamalı Dağınık Yayılma) ve DSSS(Düz Sıralı Dağınık Yayılma) dağınık yayılma teknikleri kullanılabilir. FHSS, hem verici hem de alıcı tarafından bilinen bir rastgele dizi ile birçok frekans kanalı arasında bir taşıyıcıyı hızla değiştirerek radyo sinyallerini iletir. DSSS ise orijinal sinyali temsil etmek için çok miktarda bitten oluşan bir örüntü(pattern) kullanır. Haberleşme sırasında bir ya da iki bit bozulursa, istatistiksel tekniklerle haberleşmeyi tekrarlamadan orijinal veriye geri dönüş mümkündür.

Kablosuz ve kızılötesi haberleşme sistemlerinde, haberleşmenin modu değiştirilerek yayın bozma saldırısında bulunan düşman atlatılabilir.

Bölgesel Planlama(Regional Mapping) ile yayın bozma tekniği uygulanan bölgeler tahmin edilir ve etkilenebilecek düğümlerden bir grup oluşturulur. Eğer mevcut kanalda algılayıcı düğümler saldırı tespit ederse, çalışılan kanal değiştirilecek ve düşman atlatılacaktır.

2.2. Kurcalama Saldırısı (Tampering Attack)

Düşmanın algılayıcı alanına girerek, düğümlerine fiziksel müdahalede bulunduğu saldırı türüdür. Cihazın yazılımının değiştirilmesi, yeni yazılım yüklenmesi gibi saldırılar yapılabilir. Hiyerarşik yapıdaki bir algılayıcı ağında en kritik seviyedeki algılayıcıya ulaşılabilir ve sadece bu algılayıcıya saldırılarak ağ çökertilebilir.

Mekaniksel veya kimyasal yollarla yongaya zarar verilmeden yuvadan çıkarılması(de-packing of chip), ters mühendislikle baskı devrenin tekrar çıkarılması[19], hafıza okuma, ROM ve RAM içeriğinin tekrar inşa edilmesi, yongada araştırma(on-chip probing), elektromanyetik tarama, derin alt-mikron saldırıları[20] gibi donanım birimlerine saldırılar yapılabilir.

Savunma stratejisi olarak, bilgi sızıntısını önlemek için hafıza içeriği müdahale olduğunda silinebilir. Kayıtları yonga üzerinde dağıtmak için rastgele yer ve rota belirlenebilir, hafıza içeriği şifrelenebilir, fakat şifrelenirken performans kaybı olmamalıdır. Algılayıcılar ortama gizlenerek fiziksel olarak bulunması zorlaştırılabilir. Düşman eline verinin geçmesini önlemek için yazılım koruma teknikleri de kullanılabilir. Örneğin kod gizleme(obfuscation) ve şifreleme ile kod değiştirilmesi önlenebilir.

Anahtar Yönetim(key-management) teknikleri ile de algılayıcılar arası ile de devre dışı kalan veya algılayıcını yerine başka algılayıcının yerleştirildiği durumların farkına varılabilir.

2.3. Zararlı Kod Aşılama Saldırısı (Malicious Code Injection Attack)

Ağdaki düğümün belleğine zararlı kodların saldırgan tarafından yerleştirildiği saldırı tekniğidir. Belli aralıklarla IoT cihazların yazılımlarının güncellenmesi gerekebilir, gerekli güvenlik önlemleri alınmamışsa bu durum, saldırganın zararlı kodları yerleştirmesine imkân tanır. Daha sonra saldırgan, istenmeyen fonksiyonları

gerçekleştirmesi için IoT cihazı zorlar veya IoT sistemin tamamını kontrol altına alarak erişim sağlar.

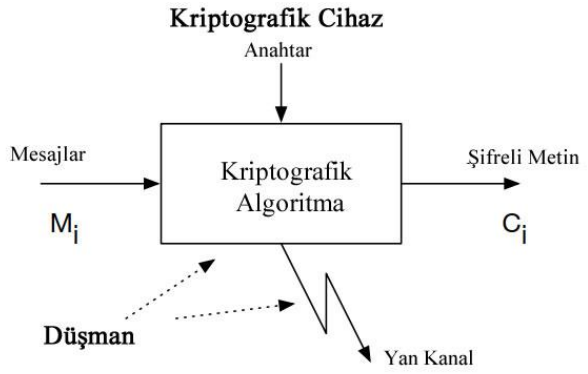
Savunma stratejisi olarak, teorik olarak en güçlü yaklaşım Komut Seti Rasgeleleştirme(ISR) tekniğidir. Rasgeleleştirme algoritmalarıyla işleme özel komut seti oluşturularak ve kullanılarak IoT cihaza zararlı kod yerleştirilmesine önlem alınmasıdır. Rasgeleleştirme anahtarını bilmeyen saldırganın yerleştirdiği kod, işlemci tarafından engellenecektir. Hu ve arkadaşları tarafından önerilen yaklaşımda[21] AES şifreleme algoritması kullanılarak rasgeleleştirme gerçekleştirilmiştir.

2.4. Yan Kanal Saldırısı (Side Channel Attack)

Şifrelenecek metin veya şifreleme sonucu elde edilen metin gibi bilgilere sahip olmadan sadece şifreleme yapılan fiziksel cihazdan elde edilen bilgiler kullanılarak yapılan saldırı şeklidir.

Saldırgan tarafından mikro işlemci mimarileri, elektromanyetik yayılma ve güç tüketimi yoluyla fiziksel cihaz tarafından yapılan şifreleme ve çözme esnasında hassas bilgiler ele geçirilebilir[19]. Hassas verilerin ele geçirilmesi için birçok yan kanal saldırı tekniği bulunmaktadır. Örnek olarak lazer tabanlı saldırılar, zamanlama saldırıları, güç tüketimi saldırıları, hata analiz saldırıları, elektromanyetik saldırılar verilebilir. Acıiçmez ve arkadaşları[22] tarafından yapılan çalışmada modern mikroişlemcilerin Dallanma İşlem Birimine(BPU) yan kanal saldırısı yapılmıştır, ünlü asimetrik anahtar algoritması olan RSA ve bu algoritmanın kullanıldığı OpenSSL uygulamasına dört farklı senaryo ile saldırı gerçekleştirilmiştir.

Savunma tekniği olarak, işlemci bünyesine eklenecek kriptografik modüller aracılığı ile bu saldırı önlenebilir.



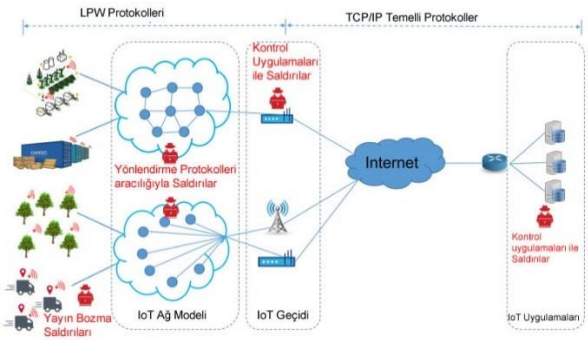
Şekil 2. Yan Kanal Saldırısı (Side Channel Attack)

2.5. Uykudan Yoksun Bırakma Saldırısı (Sleep Deprivation Attack)

IoT cihazlar kullanılmadıklarında kendilerini uyku moduna alarak güç tüketimini azaltır ve batarya ömürlerini artırırlar. Bu saldırıda, düşman düşük güçlü IoT cihazları sürekli meşgul ederek batarya sürelerini tüketir ve kısa sürede düğümlerin yaşam sürelerinin sona ermesine ve işlevsiz kalmalarına neden olur. Batarya ömürleri biten düğümler bir daha ağa dâhil olamayacaklarından bu saldırı "Servis Reddi" saldırısının bir türevi olarak da ifade edilebilir.

Zararlı kodlar kullanılarak sonsuz döngüye sokulan işlemler neticesinde, artırılan güç tüketimi sonrası zaten sınırlı olan IoT cihazın bataryası devre dışı kalır.

Savunma mekanizması olarak, uykudan yoksun bırakma problemi için hiyerarşik çatı tabanlı dağıtık işbirlikçi mekanizma önerilmiştir[23]. Önerilen model ile algılayıcı ağlarda anormallik tespitinde yanlış ihlallerin olasılığı iki adımda azaltılmıştır. Böylece düğümlerin enerji tüketimini koruyarak, ağın yaşam süresi uzatılmıştır. Diğer bir çalışmada[24], Düşük Güçlü Kablosuz Ağlar(LPW) için enerji tüketim saldırıları(EDA) Fiziksel, MAC, Ağ ve Uygulama katmanı olarak incelenmiştir. Fiziksel katmana yapılan saldırılar Yayın Bozma başlığı altında incelendiği için tekrar değinmeyeceğiz, MAC katmanına yapılan saldırılar ise Tekrar Gönderme Korunması (Replay Protection) başlığı altında incelenmiştir. Uygulama katmanına yapılan Yeniden Programlama ve Kod Aşılama saldırıları da incelenmiştir.



Şekil 3. Tipik LPW ağlar ve EDA saldırıları[24]. (Typical LPW networks and related EDA)

3. VERİ BAĞI KATMANINA SALDIRILAR (ATTACKS TO DATALINK LAYER)

3.1. Çakışma Saldırısı (Collision Attack)

Eş zamanlı olarak iki algılayıcı düğüm, aynı frekansta paket göndermeye kalkıştığında çakışma meydana gelir. Paketler çakıştığında, veri bölümünde değişiklik olur ve sinyalin doğru gidip gitmediğini kontrol etmek için kullanılan CRC(Cyclic Redundancy Check) tekniği uyuşmazlık olduğunu belirler. Sonuçta CRC sonucuna göre, paket geçersiz sayılarak yok edilecektir. Diğer bir saldırı türünde ise, saldırgan sürekli gönderdiği ACK kontrol mesajı ile paketlerde çarpışmaya neden olabilir, sonuçta etkilenen paketler tekrar tekrar iletilir ve bu durum algılayıcının gereksiz enerji tüketmesine ve zaman kaybına neden olur [25].

Savunma stratejisi olarak, ağda baz istasyonuna giden paket akış miktarını temel alan çeşitli tespit algoritmaları kullanılabilir.

3.2. Tükenme Saldırısı (Exhaustion Attack)

Kötü niyetli algılayıcı düğümü tarafından gerçekleştirilen bu saldırıda, kanal üzerinden sürekli

istek-iletimi yapılarak, MAC protokolü bozulur. Tekrarlanan çarpışma saldırıları belli bir süre sonra aşırı kaynak tüketilmesine neden olur. Sonuç olarak bu saldırı türü, algılayıcı düğümün bataryasının kısa sürede bitmesine neden olur dolayısıyla cihazın gücü üzerine etkilidir.

Savunma stratejisi olarak, birinci teknikte MAC kabul kontrol birimine konulacak oran limiti ile aşırı isteklerin yok sayılması sağlanabilir[25]. İkinci teknik olarak, zaman bölmeli çoğullama kullanılabilir[26].

3.3. Yayını bozma Saldırısı (Jamming Attack)

Veri bağı katmanındaki yayın bozma saldırısı, fiziksel katmandakinden daha karışık ve enerji bakımından daha etkili saldırılardır. Fiziksel katmanda hedef sadece veri paketleri iken bu katmanda herhangi bir paket olabilir, dolayısıyla tespit edilmesi daha zordur.

Bu saldırıda düşman, düğümlerin veri iletim zamanında veri bağı katmanına paketler göndererek tıkanıklığa neden olur, normal kullanıcıların ağı kullanmasını engellenir. Farklı MAC protokol tipleri var olduğundan dolayı, saldırgan tarafından KAA'da kullanılan MAC protokol tipine yönelik olarak hazırlanmış tıkama yapılır. Yayını bozma saldırısında, veri paketlerinin ulaşım zamanını tahmin etmek saldırgan için en önemli zorluklardan birisidir. Law ve arkadaşları tarafından, veri paketlerinin zaman aralıklarının olasılık dağılımını kümelere ayırarak ve gözlemlenerek bir yayın bozma saldırısı önerilmiştir[27].

Savunma stratejisi olarak, çoğu veri bağı katmanında yer alan eşzamanlı veri iletiminin başlangıç aşamasında iken düğümlerle mesaj iletim çizelgesi paylaşılır. Bu mesaj iletim çizelgesindeki, paket anahtar yönetim teknikleri kullanılarak paketler ayrı ayrı şifrelenebilir.

3.4. Geri Çekilme Saldırısı (Back-off Manipulation Attack)

Birçok veri bağı protokolünde düğümlerin aynı zamanda erişimini önlemek için bir geri çekilme zamanı(back-off time) konulmuştur. Saldırgan hile yapıp, bir küçük bir geri çekilme zamanı seçerek, daha az uyku modunda kalıp ağdaki diğer düğümlere göre daha avantajlı hale gelebilir. Ayrıca geri çekilme zamanının kendisi belirlerse istediği zaman diğer düğümler iletişim kurabilir[28,29].

Savunma stratejisi olarak, CSMA-CA tabanlı protokoller (IEEE 802.11, IEEE 802.15.4 gibi) kullanılarak bu saldırıya karşı önlem alınmış olur. Diğer bir savunma tekniği olarak, geri çekilme zamanı gerçekten rastgele olarak belirlenebilir, düğümün kendi kendine belirlemesine izin verilmeyebilir. Ayrıca, geri çekilme ile ilgili protokol paketleri üzerinde şifreleme yapılırsa saldırganın geri çekilme zamanı ile istediği gibi oynamasına izin verilmez ve güvenlik sağlanmış olur.

3.5. Aynı Tek Kullanımlık Sayı Saldırısı (Same Nonce Attack)

Ağ güvenliği ve kriptografi teknolojilerinde nonce (number used once) ifadesi, bir defa kullanılan sayı(bks) anlamına gelir. Algılayıcı düğümleri hedef adres, anahtar ve bks bilgisini, erişim kontrol listesinde şifreleyerek tutabilirler. Eğer iki iletimde aynı anahtar ve bks bilgisi kullanılırsa, saldırgan bu şifreli metinlerde işine yarar bilgiler elde edebilir.

Savunma olarak, mesaja yeni alanlar eklenebilir, çerçeve sayıcısından bks değeri ayrılabilir[30]. Literatürdeki birçok çalışmada çerçeve sayacı yerine sürekli değişen bir bilgi olarak, zaman damgası(timestamp) kullanılması önerilmiştir, bu şekilde iletim zamanı hesaplanabilir, saldırganın paketlerin indirip incelemesi gibi pasif saldırılar zaman damgası tekniği ile önlenebilir.

3.6. Garantilenmiş Zaman Slotu Saldırısı (GTS-Guaranteed Time Slot Attack)

MAC katmanına yapılan saldırılardan biridir. IEEE 802.15.4 MAC standardı, PAN koordinatör tarafından yönetilen süper çerçeve yapısına sahiptir, bu yapıyla kaynakları kapma için çekişmeli ya da çekişmesiz olarak servisler yönetilir. IEEE 802.15.4 standardında, PAN(Kişisel bölge ağı) koordinatörü aracılığı ile her bir ağ cihazı için ayrı bir oluk(slot) atanarak, çarpışma olmadan mesaj iletimi sağlanmaktadır.

Bu saldırıda, saldırganın GTS oluklarda cihaz ve PAN koordinatörü arasındaki haberleşmeyi bozmasına neden olan zayıf bir nokta vardır. Düşman kendini diğer algılayıcı düğümleri ile birlikte senkronize ederek, ağ hakkında tüm bilgileri içeren fener(beacon) mesajlarını alır. Önce bir düğüm, kendisine bir GTS oluğu ayrılması için PAN koordinatöre istekte bulunur, bunun için GTS isteği ve GTS açıklama bilgisi gönderir. Koordinatör burada ya isteği olumlu cevap vererek GTS oluğu ayırır, ya da isteği reddeder. Olumlu cevap verilen GTS isteği "fener" ismi verilen mesaj ile tüm düğümlere bildirilir. Saldırgan GTS oluk zamanını, GTS açıklama bilgisinden anlar ve araya girerek yasal GTS düğümü ile koordinatör arasındaki veri paketlerinde bozulmalar ve çarpışmalar meydana gelmesine neden olur[30].

Savunulması ve tespit edilmesi zor saldırılardan biridir. Bilgi sızıntısını önlemek için GTS istek mesajları şifrelenebilir ve kimlik doğrulama ile saldırganın sahte mesaj yayınlaması önlenebilir. MAC komut çerçeveleri şifrelenmelidir. Sajjad ve arkadaşları tarafından yapılan çalışmada [31], IoT için gerekli olan düşük enerji tüketiminden IEEE 802.15.4'ün önemli rol oynadığı ve güvenliğinin hayati önem taşıdığı belirtilmektedir. İlgili çalışmada, tamamen güvenli IEEE 802.15.4 alanı nasıl oluşturulacağı, anahtarların nasıl oluşturulacağı ve değiştirileceği, macKeyTable'in nasıl oluşturulacağı gibi eksikliklere dikkat çekilmiştir. IEEE 802.15.4e (6TiSCH)'nin TSCH modu üzerinden IPV6 bütünleşme çalışmalarının güçlü MAC için düşük güçlü ağlar için yapıldığı belirtilmektedir.

3.7. Tekrar Gönderme Korunması Saldırısı (Replay Protection Attack)

Kablosuz ağ standardına göre, tekrar gönderme saldırılardan korunmak için son gönderilen mesajın çerçeve numarası öncekilerden büyük olmalıdır. Fakat bu durumu bilen saldırgan, büyük çerçeve numarasına sahip

büyük sayıda mesaj göndererek sisteme saldırıda bulunabilir[32, 33].

Savunma olarak, çerçeve numarası yerine zaman damgası kullanılmalıdır, çünkü zaman damgası, çerçeve sayacından daha büyük bir sayı uzayı içerir ve tekrarlanması imkânsızdır.

3.8. Tam Hakimiyet Saldırısı (Full Domination Attack)

Saldırganın MAC katman protokolü üzerine detaylı bilgiye sahiptir ve ağa nüfuz edebilir. Bu saldırı türü en yıkıcı KAA saldırılarından biridir. Saldırgan güvenilir trafik üreterek, uyku yalanmasından (denial of sleep) maksimum kazanç sağlayabilir. Saldırgan, ağdaki bir veya daha fazla düğümü kullanarak yerleşebilir. Tüm MAC katmanı saldırıları bu saldırıya karşı zayıftır[32].

Savunma olarak, protokol paketleri şifrelenerek bu saldırının üstesinden gelinebilir.

3.9. Zeki Olmayan Tekrarlama Saldırısı (Unintelligenet Replay Attack)

Saldırgan MAC protokolü hakkında detaylı bilgiye ve ağa nüfuz etme yeteneğine sahip değildir. Kaydedilen olaylar ağda tekrar tekrar meydana getirilerek, algılayıcı düğümlerinin uyku moduna girmesi önlenir ve böylece algılayıcılar paket alarak ve işleyerek çok fazla enerji harcarlar[33,34].

Savunma olarak, paketlerin ulaşım zamanı zaman damgası ile takip edilebilir, böyle bu tekrarlama saldırısı da bertaraf edilebilir.

3.10. Asıllanmamış Yayın Saldırısı (Unauthenticated Broadcast Attack)

Saldırgan MAC protokolü hakkında detaylı bilgiye sahiptir ama ağa nüfuz edememiştir. MAC kurallarına uyarak, saldırgan ağda kimliği belli olmayan bir trafik yayınlar. Bu gereksiz yayınlar, algılayıcıların normal uyku modunu ve dinleme döngüsünü(listen cycle) bozar[35]. Sonuçta bu durum, ağda aşırı enerji tüketimine ve ağ yaşam süresinin azalmasına yol açar.

Savunma olarak, paketlerin şifrelenmesi ve paketlerin kimliğinin doğrulanması için her bir pakete zaman damgası eklenebilir. Her bir düğüme gönderilme geçmişini düğümün iletim tablosunda tutarak, paketin düşürüleceğine ya da iletileceğine karar veren AT2A metodu önerilebilir[36]. Ayrıca SPINS[37] güvenlik sisteminde, algılayıcı ağında kimlik doğrulamadan sorumlu olan µTesla benzeri bir yapı önerilebilir.

3.11. aMacBattLifeExt Saldırısı (aMacBattLifeExt Saldırısı)

Bazı MAC katmanı algoritmaları aMacBattLifeExt tekniği kullanır. Bu tekniğe göre bataryası bitmeye yakın düğümlere öncelik verilmektedir. Diğer bir deyişle, ölmeye yakın düğümler, paket göndermede önceliğe sahiptir. Düşman düğüm kendi aMacBattLifeExt değerini doğru(true) ayarlayarak veri göndermede diğer düğümlere göre daha yüksek öncelik avantajı elde eder ve sonuçta ağda adaletsizliğe neden olur[38].

Savunma mekanizması olarak, aMacBattLifeExt tekniği kullanan MAC katmanlarında, düğüm etrafında yer alan en yakın komşu düğüm ilgili düğümün "batarya seviye bilgisini" tutulabilir, eğer yakınlığı eşit birden fazla düğüm varsa enerjisi en yüksek olan tutar. Diğer bir yöntem de sink'te bu bilginin tutulması olabilir. Ayrıca bu bilgi şifrelenerek tutulursa, düğüm kendi kendine değiştiremez.

4. AĞ KATMANINA SALDIRILAR (ATTACKS TO NETWORK LAYER)

Bu saldırılar, yönlendirme saldırıları olarak da bilinir. Aşağıdaki saldırılar, özellikle mesajlar yönlendirilirken meydana gelmektedir.

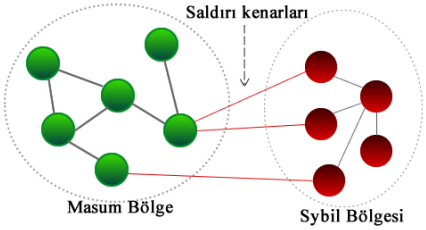
4.1. MERHABA Akını Saldırısı (HELLO Flood Attack)

Birçok ağ protokolünde komşuların keşfi için HELLO paketleri yayınlanır, paketi alan düğüm göndericinin radyo alanından geldiğini zanneder. Güçlü iletim gücüne sahip bir saldırgan, ağdaki tüm düğümlerin HELLO mesajı cevabı üretmesine neden olur ve sonuç olarak düğümler aşırı enerji tüketirler[39]. Bu durum, ağdaki düğümlerin kısa sürede devre dışı kalmasına ve ağ başarısının düşmesine neden olur.

Savunma stratejisi olarak, iki yönlü doğrulama sağlanarak önlenebilir. Diğer bir yol da kimliklendirilmiş yayın protokolleri kullanmaktır. HELLO Akını saldırısı için, formal metotlarla, bilgisayar benzetimi ve donanım uygulaması ile saldırılara dayanıklılığı test edilen RAEED[39] isimli protokol önerilmiştir. Bu protokol iki yönlü doğrulama gerçekleştirmektedir ve INSENS[40] ile LEAP[41] anahtar değişim karakteristiklerini göstermektedir. Az sayıda mesaj alınıp verildiği için ağ trafiğini hafiflemekte ama güvenlik seviyesi korunmaktadır. RAEED'in kötü tarafı, INSENS/LEAP protokollerinden kaynaklanan evrensel anahtar iptali konusundaki zayıflığıdır. Diğer bir savunma mekanizmasında[42], LEACH protokolü değiştirilip, daha az enerji ve zaman harcanarak MERHABA akını saldırısı tespit edilmiştir, ayrıca LEACH protokolünün haberleşme yükü de azaltılmıştır. Fakat bu çalışmada düşmanın tam anlamıyla soyutlanması sağlanamamıştır.

4.2. Sybil Saldırısı (Sybil Attack)

Bu saldırıda, bir düğüm sahte olarak üretilen çoklu sahte kimliklerle veya mevcut düğüm kimliklerinin çoğaltılması ile ağa giriş yapar. Dağıtık algoritmaların başarmaya çalıştığı veri bütünlüğünü, güvenliği ve kaynak yararlanmasını düşürür. Dağıtık depolama ünitelerine, yönlendirme mekanizmalarına, veri bütünleştirmeye, yanlış kaynak ayırmaya karşı saldırılarda Sybil saldırısı etkili olabilir.



Şekil 4. Sybil saldırısı (Sybil attack)

Temel olarak, herhangi bir eşler arası ağ (peer-to-peer), Sybil saldırısına karşı zayıftır. Yukarıdaki şekilde sağ taraftaki kırmızı düğümler yapay olarak üretilmiş ya da ağdaki bir düğümün aynısından kopyalar üretilerek oluşturulmuş Sybil düğümleridir[43].

Savunma stratejisi olarak, kimlik doğrulama ve şifreleme teknikleriyle dışarıdan Sybil saldırısının başlatılması önlenebilir.

4.3. Gider Deliği Saldırısı (Sinkhole Attack)

Bu saldırıda, ağdaki baz istasyonun doğru ve tam bilgi elde etmesi saldırgan tarafından önlenmeye çalışılır. Saldırgan, tüm trafiği belli bir bölgeye çekmeye çalışır. Örneğin yanlış olan en uygun yönlendirme bilgisi paylaşarak, çekmek istediği yönlendirme yolunu cazip hale getirir. "Yüksek bant genişliği" ve "düşük gecikme" avantajlı yönlendirme olduğunu belirtir.

Bu saldırının etkilerinden biri de; seçici yönlendirme (selective forwarding), sızdırma bilgisi (acknowledge spoofing) ve yönlendirme bilgisinin değiştirilmesi gibi diğer saldırı şekillerini başlatmak için kullanılmasıdır.

Savunma olarak, önerilen algoritma ile veri tutarlılığı kontrol edilerek şüpheli düğümlerin listesi bulunur ve ağ akış grafiği analiz edilerek, davetsiz misafir etkin şekilde tespit edilir[43,44]. Ayrıca, düğümlerin komşularındaki trafiği gözetleyebildiği izinsiz giriş tespiti sistemleri (intrusion detection) uygulanabilir. Her düğümde belli kurallar ile anormallik tespiti yapılır.

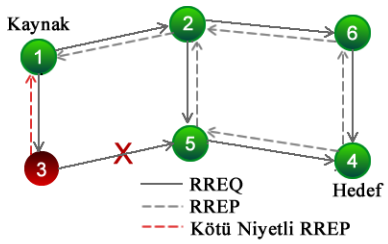
4.4. Gri Delik Saldırısı (GreyHole-Selective Forwarding Attack)

Bu saldırıda, düşman düğümler bazı mesajları iletmez ve paketleri ağdan düşürerek yayılmasını engeller. Tespit edilme ihtimalini azaltmak için, dilediği paketin içeriği seçer ve değiştirirken diğerlerini değiştirmeden gönderir. Bu nedenle tespit edilmesi zor saldırılardan biridir.

Savunma olarak, AODV(Ad hoc On-Demand Distance Vector) yönlendirme protokolü tabanlı bir algoritma önerilmiştir[43,49], algoritmanın ilk aşamasında paket sayıcısı ve tespit eşik değeri kullanılır. İkinci aşaması sorgu tabanlıdır ve ara düğümlerden saldırganın yeri belirlenir.

4.5. Kara Delik Saldırısı (BlackHole Attack)

Bu saldırıda, ağa eklenen kötü niyetli düğüm, yönlendirme tablosunu değiştirerek komşu düğümleri kendisine veri göndermeye zorlar. Sonra uzayda içine aldığı her şeyi içine çeken gerçek bir kara delik gibi davranır ve kötü niyetli düğüm tarafından ele geçirilen paketler asla geri gönderilmez, hiçbiri yönlendirilmez ve hepsi ağdan düşürülür[47,48]. Diğer bir ifadeyle Kara delik saldırısı, bir düğümün yönlendirdiği paketler arasından seçtiği belli paketleri veya tüm paketleri ağdan düşürmesi nedeniyle aslında bir Servis Yalanması (DoS) türüdür. Bu saldırı ile ağ, baz istasyonuna bilgi gönderemeyerek tamamen devre dışı kalabilir.



Şekil 5. Kara delik saldırısı (Blackhole attack).

Şekil 5'de 1 numaralı düğüm kaynak, 4 numaralı düğüm ise ulaşılmak istenen hedef düğümdür. 1 numaralı paket RREQ paketini yayınladığında, düğüm 2 ve düğüm 3 paketleri alır. 3 numaralı düğüm, kötü niyetli düğüm olup, kaynak düğümden gelen RREQ mesajını en hızlı şekilde cevaplar. Kendi rota tablosuna bakmadan, en kısa rotanın kendisi üzerinden olduğunu konusunda yanlış bilgi verir. Bunun üzerine 1 numaralı düğüm, veri paketleri 3 numaralı düğüme göndermeye başlar. 3 numaralı düğüm gelen paketleri tıpkı bir kara delik gibi içine çeker ve yok eder.

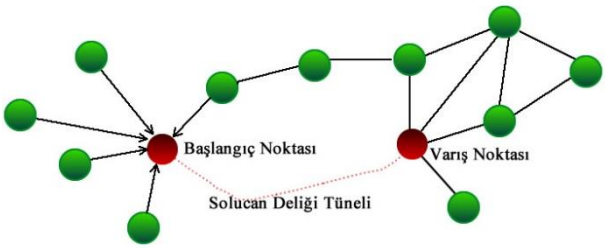
Ağda birden fazla kötü niyetli düğüm olabilir, bu duruma Çoklu Kara Delik Saldırısı ya da İşbirlikçi Kara Delik Saldırısı ismi verilir.

Sürekli ağ trafiği gözlemlenerek, ağda kaybolan paketlerden şüpheli düğümler tespit edilerek, ağdan izole edilebilir.

4.6. Solucan Deliği Saldırısı (Wormhole Attack)

Coğrafi olarak iki tarafa ayrılmış algılayıcı ağında, iki düşman düğüm arasında yapılan düşük gecikme süreli bağlantıya(tünelleme) solucan deliği saldırısı denir. Bağlantı fiber ya da daha güçlü kablosuz bir bağlantı olabilir. Bu saldırıda, düşman düğümler aldıkları paketleri tünelin diğer ucuna gönderirler, böylece tünelin diğer ucunda yer alan düğümler, haberleştikleri düşman düğümün komşu ya da bir atlama(hop) mesafesinde olduğunu sanırlar. Bundan sonra kablosuz ağın çökmesi için, düşman düğümler tarafından paketler ele geçirilip tekrar tekrar solucan deliği tüneli üzerinden gönderilmektedir. İki düşman düğüm arasından geçen paketler istenirse değiştirebilir, bundan sonra saldırgan isterse DOS(servis yalanlaması-servis reddi) gibi başka bir saldırı başlatarak, tüm paketleri düşürebilir. Ayrıca, solucan deliği tüneli üzerinden giden mesaj trafiğindeki istatistiksel bilgileri paketleri analiz ederek elde edebilir.

Bu saldırı, özellikle düğümler arası en kısa mesafeyi hesaplayan yönlendirme protokolleri ve komşu değişiminde bulunan MAC teknikleri için tehlikelidir[48]. Ayrıca tüm paketler solucan deliği tüneli üzerinden gittiğinden ağ verimliliği de ciddi oranda düşmektedir.



Şekil 6. Solucan deliği saldırısı (Wormhole attack).

Savunma tekniği olarak, Packet Leash[49], DelPhi[50], LiteWorp[51] ve MobiWorp[52] teknikleri önerilmiştir. Packet Leash savunma tekniğinde her düğümün konum bilgisinin doğru alınması şarttır, düğüm zaman damgasını gönder/al yaparak kendi kendine hızı türetmekte ve önceki düğümle arasındaki mesafeyi hesaplamaktadır. Eğer mesafe daha önce belirlenen üst sınırın üzerindeyse, solucan deliği saldırısı olduğu anlaşılmaktadır.

DelPhi[50] savunma tekniği ise basit gecikme analizi yaklaşımı kullanmaktadır. Bu yaklaşımda olası her yönlendirme için, gönderici paket başlangıcına (örneğin RREQ yönlendirme isteği ve alınan her bir paket için alıcının cevabı) bağlı olarak her atlamadaki gecikmenin ortalama değeri hesaplanır. Tüm cevaplar toplandıktan sonra, gönderici her paket için her bir atlamadaki gecikmenin ortalamasını hesaplar. Burada solucan deliğinin belirtilen atlama sayısından daha fazla atlamaya sahip olacağı farz edilir. Daha sonra hesaplanan gecikmeler şemada analiz edilir ve herhangi iki değer arasında büyük fark olup olmadığına bakılarak saldırı tespit edilir.

Khalil ve arkadaşları solucan deliği saldırısı için iki tespit ve cevap metodu önermiştir. LiteWorp[51] metodu statik tasarsız ağlar için, MobiWorp[52] metodu ise mobil tasarsız ağlar içindir. Bu metotlarda bilgi düğümün iki atlama mesafesinden toplanır. Her düğüm, hemen bitişiğindeki ve onun sonraki komşusunu dinlediği için iletilen iki paket kümesini de gözetler ve ikisinin de aynı olduğundan emin olur. Bu yaklaşımda, gözetleyici bağlantıların bazıları için aktif olmalıdır ve paket dağıtıldığında depolamak üzere tampon hafızaya sahip olmalıdır.

Solucan deliği saldırısına karşı savunma için yukarıda anlatılan bu teknikler verimli değildir, çünkü aşırı haberleşme yüküne ya da daha yüksek hesaplama gücüne gereksinim duyulmaktadır.

Seo ve arkadaşları[53] tarafından önerilen çalışmada, savunma mekanizması iki kısımdan oluşmaktadır. Solucan deliği saldırısının tespiti için bir metot ve bu saldırıya verilecek cevap için başka bir metot önerilmiştir. Solucan deliği saldırısı tespiti için her düğümün komşusunda yer alan bilgi kullanılmaktadır. Her paket, onu gönderen düğümün kimliğinin kanıtını taşır. Ara düğümler mesaj iletirken, bu kanıtların yalnızca komşu düğümlerle ilişkili kimlikleri içerip içermediğini doğrulayarak, yönlendirmede solucan deliğini tespit edebilir.

4.7. DüğümTekrarlanması-Kimlik Sahtekarlığı Saldırısı (Node replication-Identify Spoofing Attack)

Uygulamadan bağımsız olarak gerçekleştirilen bu saldırıda, saldırgan kendi düşük maliyetli düğümleri hazırlayarak ağın gerçek düğüm gibi kabul etmesine sebep olur. Bunu yapmak için saldırganın sadece bir düğümü fiziksel olarak ele geçirmesi yeterlidir. Bu açıdan Fiziksel Katmana yapılan bir saldırı türü olarak da değerlendirilebilir. Ele geçirilen düğümdeki kriptolanmış bilgiler ve kodlar açığa çıkarılır ve düğüm yeniden programlanır. Ardından saldırgan tarafından sahte düğümler kopyalanarak çoğaltılır ve ağda planlanan yerlere yerleştirilir. Sürekli tekrarlanan yeni oturumlar açılıp ağ meşgul edilir ve ağın çökmesine neden olur. Böylece saldırgan düşük bir çaba sarf ederek ağı bozar.

Bu saldırıya karşı, statik ağ yapıları için "Komşu Tabanlı Saldırı Tespit Şemaları önerilmiştir[54-58]. Ko ve arkadaşları[57] tarafından önerilen şema ise önceki tespit şemalarından farklı olarak düğüm hareketliliğini de göz önüne alarak çalışır ve dağıtık olarak tespit etmede protokol iterasyonundan kaçınma özelliğine sahiptir.

4.8. Yeni Gelen Saldırısı (NewComer or WhiteWasher Attack)

Başlangıçta pozitif veya nötr olan düğümlerin itibar puanları yaptıkları kötü eylemlerle düşer ve şüpheli hale gelirler. Sabıkalı düğümler ağdan izole edilirler ve yönlendirme bağlantılarına katılmalarına izin verilmez. Bu durumu değiştirmek ve silmek için düğüm ağa yeni bir kimlik numarası ve yeni bir tanımlama bilgisi ile yeniden katılırlar.

Savunma olarak, kimlik kanıtlama(authentication) protokolleri ve erişim kontrol mekanizmaları ile bir düğümün ağa sürekli katılarak yeni kimlik numarası alması önlenebilir. Diğer bir çalışmada[59], hem Yeni Gelen hem de Sybil saldırılarının da bertaraf edilmesi için bir yaklaşım önerilmiştir. Her düğüm ağ kaynaklarını tüketmek için bir bedel ödemek zorundadır. MANET'ler için ücreti yönetim karmaşıklığından dolayı ücretlendirme uygun değildir. Fakat belirtilen çalışmada işbirliği şeklinde bir ücret sistemi belirlenmiştir. Bir düğümün itibar puanı Y seviyesine ulaşıncaya kadar işbirliği yapar daha sonra ağ hizmetlerinden yararlanır. Normal bir bencil düğüm için WhiteWasher saldırısını gerçekleştirmek avantajlı değildir, çünkü ağa giriş için her defasında ücret ödeyecektir.

4.9. Yanlış Bildiri Saldırısı (Bad Mounting Attack)

Güven mekanizmasına yapılan bir saldırı şeklidir. Saldırgan düğümler tarafından gerçek olmayan, aldatıcı

bilgiler verilerek kötü niyetli düğümlerin tespit edilmesi engellenir.

Savunma mekanizması olarak, Sun ve arkadaşları tarafından önerilen çalışmada[60], A düğümünün ilgilendiği her C varlığı için, ilgili düğümün daha önce yapmış olduğu eyleme ve diğer düğümler tarafından verilen tavsiyeye dayalı güven puanlarına bakılır. Eğer düğüm yüksek oranda tavsiye edilmişse tavsiye puanı yüksektir, tavsiye edilmemişse ise tavsiye puanı düşüktür, eylemleri dürüst olarak gerçekleştirip gerçekleştirmediklerine bakılmaz.

4.10. Aç/Kapa Saldırısı (On/Off Attack)

Bu saldırı da güven mekanizmasına yapılmaktadır. Şüpheli düğümler önce iyi sonra kötü davranışlar sergileyerek, yakalanmadan saldırı gerçekleştirmeyi ve ağı çökertmeyi amaçlarlar. Güven puanı dinamik olarak değişmektedir. Örneğin iyi olarak görülen bir düğüm değişebilir ve kötü niyetli bir düğüm haline gelebilir. Yetkisiz olmayan bir düğüm, zamanla çevresel şartlardan dolayı yetkili hale gelebilir. Dolayısıyla uzun zaman önce bir düğüm hakkında yapılan gözlemin, yakın zamanda yapılanla aynı ağırlığa sahip olması beklenemez.

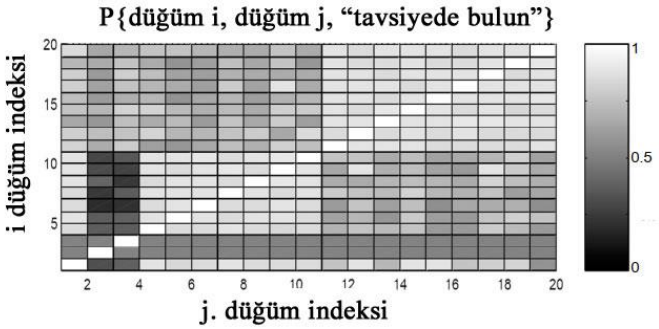
Savunma mekanizması olarak, hesaplanan "Adaptif Unutma Katsayısı" ile bir düğümün iyi veya kötü niyetli olup olmadığına karar verilir[60]. Klasik "Unutma Katsayısı" şöyle hesaplanır t_1 zamanında gerçekleşen K tane iyi eylem, t_2 zamanında gerçekleşen $K\beta^{t_2-t_1}$ iyi eyleme eşittir ve β değeri $0< \beta \leq 1$ arasında ifade edilir. Birçok şemada önerilen unutma katsayısı Aç/Kapa saldırısına uygun olmadığından "adaptif unutma katsayısı" değeri ise $\beta = 1 - p$, burada p olasılık ifade eder, $p = P\{\text{Kimden: Kime, "eylem"}\}$ veya $\beta = \beta_1$ ($p \geq 0,5$ için) ve $\beta = \beta_2$ ($p < 0,5$) şeklinde ifade edilir. β_1 ve β_2 değerleri $0 < \beta_1 << \beta_2 < 1$ arasındadır. İlgili çalışmada yapılan benzetiminde β_1=0,01, β_2=0,99 seçilmiştir. Bir varlığın birkaç kötü davranıştan sonra güven değerini normal seviyeye çekebilmesi için çok fazla iyi eylem yapması gerekmektedir.

4.11. Çakışan Davranış Saldırısı (Conflicting Behaviour Attack)

Güven mekanizmasını ilgilendiren bu saldırı şeklinde, saldırgan farklı ağ ortamlarında farklı davranışlar gösterir. Örneğin saldırgan bir grup kullanıcıya iyi davranışlar gösterirken, diğer grup kullanıcıya kötü davranışlar gösterir. Bu iki gruptaki kullanıcıların kötü niyetli düğüm hakkındaki fikirleri çakışır. Sonuçta bir gruptaki kullanıcıların diğerlerine karşı "düşük güvenlik puanı" atar. Bu duruma çakışan davranış saldırısı adı verilir.

Savunma olarak, her düğüm için kaybettiği veya başka bir gruba gönderdiği paket için bir güven değeri hesaplanır[10]. Eğer güven değeri düşükse ve kötü niyetli düğüm komşuları hakkında kötü davranışlar gösteriyorsa hemen tespit edilir, aksi takdirde tespiti zordur.

Diğer bir çalışmada[61], her bir zaman aralığında paket transferi için rastgele paket seçer, farz edelim ki A düğümü paket göndermek için B düğümünü seçsin. Bu olaydaki olasılık gösterimini şöyle ifade edelim; $P\{\text{Kimden: Kime, "Eylem"}\}$. Eğer A düğümü daha önce B düğümü ile karşılaşmamışsa veya güven değeri olasılığı $P\{\text{A:B, "iletilen paket"}\}$ eşik değerinden düşükse, düğüm A, B düğümü hakkında diğer düğümlere danışır, sonra düğüm A, B'ye n tane paket iletmek istediğini bildirir. Burada, düğüm B'nin kaç tane paket gönderdiğini, düğüm A'nın gözlemleyebileceğini farz ediyoruz. Daha sonra, A güven değerini kendi gözlemlerine göre ve B'nin davranışına göre diğer düğümlerden gelen bilgilere göre günceller.



Şekil 7. Düşmanlar iyi kullanıcıların yarısına saldırdıklarında güven tavsiyesi[61] (Recommendation trust when malicious users attack half of good users[61])

Şekil 7'da 20 düğüm bulunan bir ortamda kullanıcı 2 ve kullanıcı 3'ün saldırgan olduğu, paket düşürme oranı rastgele olarak %0 ile %40 arasında seçilerek 1'den 10'a kadar kullanıcıların paketleri ağdan düşürülüyor, fakat 11'den 20'ye kadar olan kullanıcıların paketlerine karışılmıyor. *i.* satır *ve j.* sütun değerleri, *j.* kullanıcının *i.* kullanıcı kaydındaki tavsiye güven değerini gösteriyor. Renk ne kadar açıksa, güven değeri o kadar yüksektir. Düğüm 1 ile 10 Aralığı düşük tavsiye, düğüm 11 ile 20 Aralığı ise yüksek tavsiye değerini gösteriyor.

4.12. Akıllı Davranış Saldırısı (Intelligent Behaviour Attack)

Saldırgan güven değeri gibi önemli bilgileri tespit etmeye çalışır, "şüpheli düğüm eşik değeri" civarında normal hareketlerde bulunur, bu bilgiye göre davranışını değiştirir. Bu gibi saldırıların tespiti oldukça zordur ve uzun zaman gerektirir.

Savunma olarak, güven derecesi gibi değerlerin ele geçmemesi için şifreleme yapılabilir.

5. TAŞIMA KATMANINA SALDIRILAR (ATTACKS TO TRANSPORT LAYER)

5.1. SYN Akını Saldırısı (Syn Flood Attack)

Bu saldırıda düşman büyük sayıda SYN isteğini kurbana gönderir. Cevap olarak kurban düğüm, kurulan bağlantının on anki durumunu kaydeder ve SYN/ACK ile cevap verir. Saldırgan daha ileri eylemler gerçekleştirmez, fakat daha sonra diğer bir bağlantı isteğini kurbana gönderir. Bu şekilde, birçok yarım kalmış TCP bağlantısı meydana gelir. Ağ bağlantısı bu şekilde meşgul edilerek, iş göremez hale getirilir[62].

Savunma olarak, SYN çerezleri(cookie) kullanılarak SYN akını saldırısı önlenebilir. Bağlantı istekleri hedef tarafta tutulmaz, hedef düğüm bağlantı durumunu tekrar saldırgana gönderir ve bu düğümdeki bir çerezde saklar. Bu şekilde SYN akını saldırısı yapılamaz ve kurban düğümün de bellek taşması önlenmiş olur, ağ trafiği normal düğümlerle aksamadan devam eder.

5.2. Eşleme Bozulması Saldırısı (Desynchronization Attack)

Eşlemenin sağlanması için gönderi ve alıcı arasında bir sıra numarası kullanılır. Saldırgan, gönderici ve alıcı arasına girip bağlantıyı keserek, sıra numarası ya değiştirir ve da bağlanılan düğümlere sahte sıra numaralı veri paketleri gönderir[62]. Böylece düğümler arasındaki eşleme bozulur ve düğümler veri paketlerini tekrar tekrar birbirlerine iletirler.

Savunma olarak, paket başlıklarına bir doğrulama imzası eklenerek bu saldırı bertaraf edilebilir.

6. UYGULAMA KATMANINA SALDIRILAR (ATTACKS TO APPLICATION LAYER)

6.1. Kopyalama Saldırısı (Cloning – Replication Attack)

Düşmanın algılayıcı düğümlerini ele geçirip ve bu düğümlerin kopyalarını oluşturduğu saldırı tipidir. Ele geçirilen düğümler üzerinde yeniden programlama da yapılabilir. Kopyalanan sahte düğümler, diğer düğümler gibi, normal bir şekilde algılayıcı ağına erişebilir. Saldırgan, bu düğümler vasıtası ile istediği gibi algılayıcı ağı ile ilgili operasyonlara katılabilir. Bu kadar sistemin içinde olan saldırgan daha büyük bir saldırı yapabilir hatta ağı tamamen ele geçirebilir. Eğer kopyalanan düğümler algılayıcı ağda tespit edilemezse veya geç tespit edilirse algılayıcı ağ güvenliği için bu durum bir zafiyet oluşturur. Kopyalama saldırısının verdiği hasarı kısıtlama ve tespiti için verimli ve etkili çözümler gereklidir.

Savunma stratejisi olarak, bu saldırıyı tespit edecek aktif araştırma sisteminin ağın çalışmasını aksatmayacak şekilde olması, geliştirilen tekniğin hafif, hızlı, verimli bir çözüm olması gerekmektedir. Sathish ve Kumar tarafından, merkezi ve dağıtık olarak çalışan birçok şema incelenmiş ve mobil ajan tabanlı yeni bir saldırı tespit şeması önerilmiştir. MABCAD(Mobil Ajan Tabanlı Kopyalama Saldırısı Tespiti) ile "α" düğümünün her bir komşusu imzayı doğrular ve konumun uygunluğunu kontrol eder. Bir düğüm çakışma olduğunu algılarsa, örneğin iki farklı yerde aynı kimlik numarası olduğu saptanırsa bunu ağdaki diğer düğümlere bildirir. Ağda kopya düğüm olduğunu anlayan düğümler şüpheli veya ele geçirilmiş düğümün isteğine itibar etmezler, bu yaklaşım ancak mobil ajan tabanlı bir yapı ile sağlanabilir. Komşu iki düğüm arası mesafe, D= (TR-dt)/V denklemi ile hesaplanır. Burada TR iletim aralığı, dt iki düğüm arası uzaklık, V ise düğümün ortalama hızıdır. Bir düğümden diğer düğüme bilgi taşıyan mobil ajanlar en az gezilen komşuya öncelik vererek dolaşırlar, her düğümün ön belleğindeki bilgiyi güncellerler ve yer, düğüm kimlik numarası(nodeID) gibi bilgilerin özüt algoritmasından geçirilerek imzalanır, imzası doğrulanamayan ağdan çıkarılır. Düğüm i'nin ön belleğinde tüm düğümlerin sayaçları saklanır, ajan kendi taşıdığı bilgi ile düğümdeki bu bilgileri karşılaştırır, ajanın taşıdığı bilgiden küçükse ajanın düğümler hakkında güncel bilgiyi taşıdığı anlaşılır, düğüm bilgisi güncellenir[63].

Farklı kimlik doğrulama ve şifreleme teknikleriyle aynı kimlik numaralı düğümler tespit edilip kopyalama saldırısı önlenebilir.

6.2. Algılayıcı düğümünün boğulması Saldırısı (Overhelming Sensor Node Attack)

DoS/DDoS saldırısının bir nevi türevidir. Bu saldırıda algılayıcı düğüme karşı, yoğun şekilde mesajlar üretilerek gönderilir. Saldırgan, böylece ağ bant genişliğinin tüketilip ağın çökmesine, algılayıcıların enerji tüketiminin artmasına, dolayısıyla ağ yaşam süresinin azaltılmasına neden olur.

Savunma olarak, uygulamalarda kullanılan algoritmalar özenle seçilmelidir, örneğin yönlendirme için enerji verimliliğini ön planda tutan algoritmalar kullanılabilir. Paket şifrelemesi yapılabilir. DoS/DDoS saldırıları bölümünde de inceleyeceğimiz Yapay Zekâ tabanlı saldırı tespit sistemleri kullanılabilir.

6.3. Yol Tabanlı Servis Yalanlaması Saldırısı (Path based DoS Attack)

Bu saldırı tipinde, hiyerarşik ağaç yapısındaki bir algılayıcı ağında, en alttaki yaprak düğüm ağa tekrar tekrar mesajlar gönderir. Bu durum, sink'e kadar bir yol(path) boyunca gidebilir. Ağın bu kadar işgal edilmesi, aşırı enerji tüketimine, bant genişliğinin gereksiz tüketilmesine ve sonuçta ağ yaşam süresinin azalmasına neden olur.

Savunma olarak, paket kimlik doğrulaması, zaman damgası kullanımı, yeniden tekrarlamaya karşı koruma(anti-replay) gibi teknikler kullanılabilir.

6.4. Yeniden Programlama saldırısı (Reprogramming Attack)

Bu saldırıda, eğer programlama süreci yeterince korunmamışsa, düşman sistemdeki açık noktaları kullanarak algılayıcı düğüme uzaktan erişip, yeniden programlayarak ağın büyük bölümünü kontrol altına alabilir. Ağ Katmanına saldırılar kısmında incelediğimiz "Düğüm Tekrarlanması" saldırısında da fiziki olarak ele geçirilen düğüme yeniden programlama yapıldığından bu saldırının bir türevi olarak sayılabilir.

Bu saldırıya karşı savunma stratejisi olarak, önceki bölümlerde anlatıldığı gibi fiziki kurcalamaya karşı önlemler alınabilir. Erişim noktasına (Sink veya Access Point) girişte, kimlik doğrulama için direkt şifre kullanımı güvenlik zafiyeti oluşturur.

6.5. Ortadaki Adam Saldırısı (Man in the Middle Attack)

Tanım olarak, iki taraf arasındaki haberleşmenin saldırgan tarafından dinlendiği saldırı türü olarak ifade edilir. Klasik ortadaki adam saldırısında istemci sunucu arasına girerek dinleme yapılır. Dsniff, Cain, Ettercap, Wsniff, Airjack gibi saldırılar örnek verilebilir. Diğer taraftan, hem IoT cihazların kullandığı bulut teknolojisine karşı hem de IoT sistemlerde Orta-Katmanda yer alan MQTT protokolüne yönelik olarak bu saldırı gerçekleştirilebilir.

Yayınlama ve Üye Olma prensibine göre çalışan MQTT protokolü, istemciler ve üyeler arasında MQTT Aracısı(MQTT Broker) yani vekil gibi işlem görür. Bu sayede, hedef hakkında hiçbir bilgiye sahip olmadan yayınlayan ve üye olan istemcileri birbirinden ayrılıp, mesajlar gönderilir. Fakat bu özellik saldırgan için bir güvenlik açığı doğurur. Saldırgan, MQTT Aracısını kontrol ederek, ortada gelip giden mesajları gözleyerek, istemciler hakkında hiçbir bilgiye sahip olmadan haberleşmenin tamamını denetimine alır.

Çok eski olan fakat halen güncelliğini koruyan bu saldırı türü gelişmiş anahtar yönetim protokolleri ve kullanılarak önlenebilir. Fakat ağ yapısına özel anahtar yönetim protokolü geliştirilmelidir ve internet gibi dinlemeye müsait bir ağ yapısı üzerinden gönderilmeden önce gizliliğin sağlanması amacıyla şifrelenmeli, bütünlüğün korunması amacıyla mesaj özütü teknikleri kullanılmalıdır.

6.6. Çapraz Site Betiği Saldırısı
(XSS-Cross Site Scripting Attack)

Uygulama katmanında gerçekleşen genel saldırı türlerinden biridir. Saldırgan, hazırladığı betik ifadelerini tarayıcıda form girişi yapılan kısımlara yerleştirerek farklı bir kullanıcının makinesinden bilgi alınmasını gerçekleştirir. Javascript, VBScript gibi betik dillerini kullanabilir. Bazen kullanıcının doğru olarak girdiği web adresini (URL) kendi istediği farklı bir web adresine yönlendirir ve kullanıcı farkında olmadan şifre, TC kimlik no vb. özel bilgilerini saldırganın istediği web sitesine girer.

Bu saldırıya karşı savunma olarak öncelikle veri girişi yapılan ekranlara betik komutları girilmişse filtreleyen özel güvenlik fonksiyonlarından geçirilmelidir. Sun ve He[67] tarafından yapılan çalışmada, Web sitesindeki illegal metotları sezinleyen bir model kontrol metodu önerilmiştir. HTML için otomatik bir modelleme algoritması geliştirerek XSS saldırısına karşı çözüm önermişlerdir.

6.7. XML Sayısal İmza Saldırısı (XML Signature Wrapping)

Bu saldırıda, saldırgan web servislerinde kullanılan XML imza algoritmasının kırarak, tüm bilgileri ele geçirebilir ve sisteme zarar verebilir. Basit Nesne Erişim Protokolü(SOAP) mesajları saldırılara karşı zayıftır. SOAP mesajları, kullanıcı web tarayıcısı(istemci tarafında) aracılığı ile istekte bulunduğunda sunucu tarafından üretilen mesajlardır. Web sunucu güvenlik protokolünde bir açık bulunduğunda, saldırgan XML imzalarını kullanarak, dijital olarak imzalanmış SOAP mesajını istediği bir mesaj ile değiştirebilir.

Savunma tekniği olarak, web servislerinde veri gönderilirken ve alınırken iletim zamanının uzatsa da mutlaka şifrelenmelidir. Önerilen UNWRAP[64] isimli çalışmada ontoloji kullanılarak SOAP mesaj element yapısı ilk önce inşa edilip sonra SOAP mesaj başlığına eklenmektedir. Alıcı tarafta ontolojinin doğrulanmasıyla saldırı tespit edilebilmektedir. Ayrıca, tüm SOAP mesajları bir kütüğe(log) yazılmaktadır, eğer bir güvenlik ihlali oluşursa bu kütük kontrol edilip kurtarma yapılabilmektedir.

6.8. SQL Aşılama Saldırısı (SQL Injection Attack)

Web tabanlı yapılan saldırılarda SQL Aşılama ve daha sonra değineceğimiz XSS saldırısı, bilinen genel saldırı tipleridir. Saldırgan, metin girişi yapılan herhangi bir ekranda, özel karakterler veya sorgular girerek SQL kodlarının istediği gibi çıktı verdirir ve vertabanındaki bilgileri ele geçirir. IoT cihazlarda kullanıcının özel anahtarını ele geçirerek, programa zararlı SQL ifadelerini gömülü olarak yerleştirip, veritabanındaki gizli bilgileri ele geçirebilir, istediği bilgiyi değiştirebilir veya silebilir. Bilgi girişi yapılan kısımların yanısıra, AJAX ve URL arayüzleri de saldırılara karşı zayıf noktalar içerebilir. Bulut sistemlerde dahi güvenliği tehdit eden bir saldırı türüdür.

Savunma mekanizması olarak, bilgi girişi yapılan nesnelerden alınan bilgiler filtrelenmeli, daha sonra SQL ifadeleri ile birleştirilmelidir. Örneğin kullanıcı adı ve şifre girişi yapılan bölümlerden alınan veriler SQL ifadesi ile birleştirilmeden önce filtrelenmelidir. DetAnom ismi verilen çalışmada[65] veritabanı erişim katmanına uygulamaların yetkisine göre veritabanına erişimini imza tabanlı bir yöntemle koruma altına alan bir yaklaşım önerilmiştir. Sorgu veritabanına ulaşmadan önce imza ve kısıtlama doğrulaması yapılmakta, eğer bir uyuşmazlık varsa şüheli olarak işaretlenmektedir. Uwagbole ve arkadaşları[66] tarafından yapılan çalışmada makine öğrenmesi yaklaşımı kullanılarak bilinen saldırı örüntüleri Destek Vektör Makineleri ile tespit edilmiştir. Son olarak, güvenlik açığı bulma araçları ile tüm sistem taratılıp, sızıntı olabilecek noktalar tespit edilebilir.

6.9. Bulutta Akın Saldırısı (Flooding Attack in Cloud)

Ağ Servis Kalitesini(QoS) olumsuz olarak etkileyen DoS saldırısının benzeri olan bu saldırıda amaç, sürekli çoğul istek göndererek bulut sistemin kaynaklarını tüketmektir. Bulut sunucuda aşırı yüklenmeye neden olan bu saldırı sonucunda kullanıcılar hizmet alamaz hale gelebilmektedir.

Savunma olarak, DoS/DDoS saldırılarında kullanılan yapay zekâ ve istatistiksel teknikler bu saldırıyı bertaraf etmek için kullanılabilir.

6.10. Bulutta Zararlı Yazılım Aşılama Saldırısı
(Malware Injection in Cloud)

Bu saldırı tekniğinde saldırgan, buluta kötü amaçlı yazılım(malware) bulaştırarak, bulut sistemin yönetimini ele geçirir. Daha sonra zararlı sanal makine ya da zararlı kod modüllerini bulut sistemine yerleştirerek, normal kullanıcıların hizmet almasına engel olabilir, kullanıcı isteklerini gözlemleyerek hassas bilgileri yakalayıp, değiştirebilir.

6.11. Servis Yalanlaması Saldırısı
(Denial of Service-DoS Attack)

Servis Yalanlaması ya da Servis Reddi olarak isimlendirilen bu saldırı tipinde, ağı ortadan kaldırma veya yok etmek amaçlanmaktadır. DDoS/DoS saldırısında, beklenildiği gibi düğümün fonksiyonu azaltılabilir veya tamamen ağdan elimine edilebilir. Ağın herhangi bir OSI katmanında bu saldırı türü meydana gelebilir. DDoS/DoS saldırısı hedeflenen ağa nüfuz ederek kaynak(bellek, işlemci, batarya, bant genişliği) tüketimini artırır, altyapı ayarlarını değiştirerek veya yok ederek, fiziksel olarak ağ bileşenlerine zarar verir.

DoS/DDoS saldırısını tanımlamak, hafifletmek ve önlemek amacıyla farklı çalışmalar yapılmıştır. Bu saldırı farklı şekillerde yapılabileceği için, her DDoS/DoS saldırısını önlemek için kesin bir yöntem bulunmamaktadır. Örneğin merkezi yapıdaki bir sunucuya yoğun şekilde paket gönderilerek bant genişliği tüketilmesine karşı dağıtık şekilde birden fazla sunucu ile saldırı hafifletilmeye ve saldırı yükü dağıtılmaya çalışılabilir. DoS saldırısı tek kaynaktan gelebileceği gibi dağıtık şekilde birden fazla kaynaktan aynı anda da gelebilir, bu şekilde saldırı DDoS olarak adlandırılır. DDoS saldırılarına karşı sınırlı sayıda sunucu ile karşı koymak da etkin bir çözüm değildir.

Hızlıca değişen örüntülerin, portların, protokollerin veya işlem mekanizmalarının dinamik olarak analiz edilmesi gerekmektedir. Bu nedenle yapay zekâ ve istatiksel yaklaşımlar önerilmektedir. Sistemin saldırı yapıldığında kendi kendine bir savunma mekanizması geliştirerek saldırının önce tespit edilmesi(tanımlanması), sonra hafifletilmesi, sonra da tamamen önlenmesi amaçlanmaktadır.

Yapay Zekâ tabanlı yaklaşımlarına örnek olarak Bayesian Ağları, Bulanık Mantık(Fuzzy Logic), Genetik Algoritmalar, K-En Yakın Komşu Algoritması(K-nearest Neighbour), Derin Yapay Sinir Ağları, Destek Vektör Makineleri(Support Vector Machine) önerilmektedir.

Çizelge 3. Katmanlara göre saldırılar (Attacks by layers)

Fiziksel Katman	Radyo yayını bozma, Kurcalama Saldırısı, Zararlı Kod Aşılama, Yan Kanal Saldırısı, Uykudan Yoksun Bırakma Saldırısı
Veri Bağı Katmanı	Çakışma, Tükenme, Yayın Bozma,
	Geri Çekilme, Aynı Tek Kullanımlık Sayı Tekrar Gönderme Korunması Tam Hâkimiyet, Zeki Olmayan Tekrarlama, Asıllanmış Yayın, GTS
Ağ Katmanı	Merhaba Akını, Solucan Deliği, Sybil, Gider Deliği, Gri Delik, Kara Delik, Düğüm Tekrarlanması, Yeni Gelen, Yanlış Bildiri, Aç/Kapa Saldırısı, Çakışan Davranış, Akıllı Davranış
Taşıma Katmanı	SYN Akını, Eşleme(Senkronizasyon) Bozulması
Uygulama Katmanı	Servis Yalanlaması, Kopyalama Saldırısı, Algılayıcı düğümünün boğulması Yol Tabanlı Servis Yalanlaması Yeniden Programlama SQL Aşılama Saldırısı Çapraz Site Betiği (XSS) Saldırısı Sayısal İmza Saldırısı Ortadaki Adam Saldırısı Bulutta Akın Saldırısı Buluta Zararlı Yazılım Aşılama

İstatiksel yaklaşım olarak Paremetrik (Operasyonel, Spektral, İstatiksel Moment) ve Parametrik olmayan metodlar (CATs, D-WARD, FFV, Markov, Regresyon Analizi, İstatiksel Ayrım, Zaman Serileri) önerilmektedir[68]. Fakat bu teknikler daha önce belli olan sınırlı bir veri kümesi üzerinde çalışılmaktadır, yapay zekâ tekniklerinden verimli sonuçlar alabilmek için hemen her saldırı türünü içeren oldukça geniş bir veri kümesinde çalışılması gerekmektedir. Sağlıklı sonuçlar alabilmek için de güçlü bir bilgisayar ağında denemeler yapılmalıdır. Kurumların mevcut yapılarında DDoS saldırılarını analiz edecek bir yapı olmadığından ancak saldırılar daha güçlü sistemlere yönlendirilerek çözülür.

7. DİĞER SALDIRILAR (OTHER ATTACKS)

IoT cihazlarda kullanılan çeşitli işletim sistemlerinden (Android, Blackberry OS, iOS, Windows Phone OS, WearOS, Contiki vb.) kaynaklanan sistem açıkları, IoT cihazlardaki algılayıcılara yönelik tehditler olabilir.

Güvenlik için kullanılan algoritmalardaki zayıflıklar da IoT cihazların güvenliğini tehdit edebilir. Örneğin, bir akıllı ev otomasyonunun kontrol edildiği programa girilen şifrenin direkt olarak sistemin veritabanında

saklanması önemli bir güvenlik açığıdır. Şifre ile tuz(salt) değeri birleştirildikten sonra özüt algoritmasından geçirilip saklanmalıdır. Burada dikkat edilmesi gereken SHA-1 veya daha üstü güvenliğe mesaj özütü algoritmaları kullanılmalıdır. Diğer taraftan, özüt algoritmalarında çakışma meydana gelebilir. Matematiksel olarak ifade edecek olursak; m ve m' farklı mesajlar, h() özüt fonksiyonu olsun h(m)=h(m') ise çakışma meydana gelmiştir. Bu durumda özüt fonksiyonu artık kullanılamaz[69].

Bilgi gizliliği için kullanılan şifreleme algoritmaları da hem güçlü olmalı hem sistemin işleyişini aksatmayacak kadar hızlı olmalıdır. IoT çatılarında genel olarak AES simetrik şifreleme algoritması kullanılmaktadır. Fakat gelişen işlemci ve GPU(grafik işlem birimi) teknolojisi nedeniyle güvenlik algoritmalarının çözülme zamanının zamanla kısalması veya açıklıklar tespit edilmesi sonucunda değiştirilmesi gerekebilir. Bu nedenle IoT cihazlarında güvenlik güncellemeleri de belli aralıklarla sızıntıya imkân vermeden yapılabilmelidir.

IoT uygulamalarından kaynaklanan hatalar(bugs) örneğin bellek taşması (buffer overflow), Web API'lerdeki güvenlik problemleri saldırganın tam erişimine neden olabilir.

IoT sistemlerde anahtar dağıtımı ve yönetimi, IoT güvenliği için üzerinde çalışılan ayrı bir konudur. Heterojen yapıdaki bir IoT sisteminde farklı teknolojiler, farklı anahtar yönetim protokolleri kullanmaktadır; 1) Bulut tabanlı çözümlerde, 2) Edge ve Fog tabanlı çözümlerin olduğu yapılar için farklı anahtar yönetim protokolleri geliştirilmektedir.

Diğer bir güvenlik tehdidi "Bilgi Sızıntısı" yani sisteme yerleştirilen keylogger, trojan vb. zararlı yazılımlarla veya donanımsal trojanlarla yapılan, kullanıcı bilgilerini elde etme girişimidir. IoT cihazlardaki algılayıcılara yönelik saldırılarda, Bilgi Sızıntısı saldırısı tuş arabirimi ile gerçekleştirilebilir. Dokunmatik ekran, dokunmatik yüzey veya klavyeye dokunduğunda saldırgan bu veriyi alarak PIN veya şifre bilgisini, sistemin daha önce kaydettiği veritabanındaki önceki bilgilerle birleştirerek çözebilir. Örneğin, "PIN Alma" saldırısı ile ışık ortamındaki veri ve RGBW(kırmızı, yeşil, mavi ve beyaz) algılayıcısı verisi kullanılarak akıllı telefonun PIN girişi elde edilmiştir[70]. Sistemdeki hareket-manyetik-akustik algılayıcılardan, GPS'den, kameradan alınan bilgilerle de bilgi sızıntısı saldırısı yapılabilmektedir[10]. Bu gibi algılayıcıya yönelik saldırıları önlemek amacıyla, Android işletim sistemi için Algılayıcı Yönetim Çatısı olarak Semadroid[71] önerilmiştir. Android işletim sistemine kurulan uygulamaların algılayıcı kullanımlarını kullanıcıya göstererek algılanan bilgilerin sızdırılmasını önlemektedir.

SONUÇ (CONCLUSION)

Bu çalışmada, artık hayatımızın bir parçası olan ve kullanımı giderek artan Nesnelerin İnterneti(IoT) ve kablosuz algılayıcı ağların Fiziksel, Veri, Ağ, Taşıma, Uygulama katmanlarına yapılan saldırılar geçmişten günümüze kadar geniş bir araştırma yapılarak incelenmiştir. IoT sistemlerin farklı ağ yapılarından ve heterojen teknolojilerin birleşiminden oluşması ve internet bağlantısının olması nedeniyle birçok saldırıya açıktır. Gerekli güvenlik önlemlerinin alınması ve kritik noktalardaki veri kaybını, yetkisiz erişimi önlemek amacıyla her saldırının açıklandığı bölümde son paragraf olarak savunma teknikleri önerilmiştir. Bu tekniklerin uygulanabilirliği noktasında, düşük güçlü IoT cihazlar düşünülerek savunma önerileri yapılmıştır. Şimdiye kadar sunulan savunma tekniklerine ilave olarak yeni savunma teknikleri de önerilmiştir.

Gelecek çalışmalarda, IoT cihazların yer alabileceği ağ yapıları ve heterojen teknolojilerin bir arada kullanılabilmesi için yeni güvenlik mekanizmaları üzerine çalışılacaktır. Ayrıca düşük güçlü IoT cihazlara yapılabilecek saldırıları daha erken algılayarak zamanında tespit etmek, gerçekleşmeden önlemek için fazla kaynak tüketen geleneksel güvenlik teknolojilerinden ziyade işlemci, hafıza ve alan kullanımı bakımından daha hafif teknikler geliştirilecektir.

KISALTMALAR (NOMENCLATURE)

AES	Advanced encryption standard(Gelişmiş şifreleme standartı)
CoAP	Constrained application protocol (Kısıtlanmış uygulama protokolü)
DoS	Denial of service(Servis yalanlaması)
DDoS	Distributed denial of service(Dağıtık servis yalanlaması)
DSSS	Direct sequence spread spectrum(Düz sıralı yayılma tayfı)
EDA	Energy deplation attacks (Enerji tüketim saldırıları)
FANET	Flying adhoc networks(Tasarsız hava taşıtı ağları)
FHSS	Frequency-hopping spread spectrum (Frekans atlamalı yayılma tayfı)
GPS	Global positioning system(Global konumlandırma sistemi)
IoT	Internet of things (Nesnelerin interneti)
IIoT	Industrial internet of things (Endüstriyel nesnelerin interneti)
ISR	Instruction set randomization(Komut seti rastgeleleştirme)
LoWPAN	Low-power wireless personal area networks (Düşük güç tüketimli kişisel alan ağı)
LPW	Low-power wireless (Düşük-güçlü ve kablosuz)
M2M	Machine to machine connection (Makineden makineye bağlantı)
MANET	Mobile adhoc networks(Tasarsız mobil ağlar)
MQTT	Message queuing telemetry transport (Mesaj kuyruklamalı ölçüm iletim protokolü)
PAN	Personal Area Network (Kişisel bölge ağı)
QoS	Quality of service (Servis kalitesi)

RFID	Radio frequency identification(Radyo frekansla tanınma)
RSN	RFID sensor networks (RFID algılayıcı ağlar)
SHA	Secure hash algorithm (Güvenli özüt algoritması)
VANET	Vehicular ad-hoc networks(Araçlar arası tasarsız ağlar)
WSN	Wireless sensor networks (KAA-Kablosuz algılayıcı ağlar)

ETİK STANDARTLARIN BEYANI
(DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

KAYNAKLAR (REFERENCES)

[1] Yaqoob I., Ahmed E., Hashem I., Ahmed A., Gani A., Imran M., Guizani M., "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges", ***IEEE Wireless Communications***, 10-16, (2017).

[2] Granjal J., Monteiro E., Silva J.S., "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", ***IEEE Communication Surveys & Tutorials***", 7(3), 1294-1312, (2015).

[3] ***https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends***, Gartner, "Gartner Identifies Top 10 Strategic IoT Technologies and Trends", Erişim Tarihi Ağustos 10, 2019.

[4] ***https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html***, Cisco, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper", Erişim Tarihi Ağustos 10, 2019.

[5] Tomic I., McCann J.A., "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols", ***IEEE Internet of Things Journal***, 1-13, (2017).

[6] Hassija V., Chamola V., Saxena V, Jain D., Goyal P., Sikdar B., "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", ***IEEE Access***, 82721-82740, (2019).

[7] Sikder A.K., Petracca G., Aksu H., Jaeger T.,Uluagac A. S., "A Survey on Sensor-Based Threats to Internet-of-Things (IoT) Devices and Applications", ArXiv Preprint, https://arxiv.org/abs/1802.02041, (2018).

[8] Chelli K., "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", ***Proceedings of the World Congress on Engineering***, (2015).

[9] Bisvas S., Adhikari S., "A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network", ***International Journal of Computer Applications***, (2015).

[10] Korkmaz I., Dagdeviren O., Tekbacak F., Emin Dalkilic M., "A Survey on Security in Wireless Sensor Networks:Attacks and Defense Mechanisms", 223-251, ***Theory and Practice of Cryptography Solutions for Secure Information Systems***, IGI Global, (2013).

[11] Yadav C., Raksha K., Hegde S.S., Anjana N.C, Sandeep K. E, "Security Techniques in Wireless Sensor Networks: A Survey", ***International Journal of Advanced Research in Computer and Communication Engineering***, (2015).

[12] Walters J. P., Liang Z., Shi W., and Chaudhary V., "Wireless Sensor Network Security: A Survey", ***Security in Distributed, Grid and Pervasive Computing***, CRC Press, (2006).

[13] Wang Y., Attebury G., Ramamurthy B., "A Survey of Security Issues In Wireless Sensor Networks", ***IEEE Communications Survey&Tutorials***, (2006).

[14] Chen X., Makki K., Yen K., and Pissinou N., "Sensor Network Security: A Survey", ***IEEE Communication Survey&Tutorials***, (2009).

[15] Xu W., Ma K., Trappe W., ve Zhang Y. "Jamming Sensor Networks:Attack and Defense Strategies", Rutgers University, ***IEEE Network***, (2006).

[16] Mpitziopoulos A., Gavalas D., Pantziou G., Konstantopoulos C., "Defending Wireless Sensor Networks from Jamming Attacks", ***2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications,*** (2007).

[17] Ettouijri Y., Salij-Alj Y.,"Countermeasures against Energy-Efficient Jamming on Wireless Sensor Networks", ***IEEE 2014 International Conference on Multimedia Computing and Systems (ICMCS)***, (2014).

[18] Karlof C., Wagner D., "Security Wireless Sensor Networks Security", ***Ad hoc networks***, (2004).

[19] Babar S., Stango A., Prasad N. R., Sen J., Prasad R., "Proposed Embedded Security Framework for Internet of Things (IoT)", ***2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)***, (2011).

[20] Pacalet R., "Hardware Security: Probing Attacks", ***Telecom ParisTech***, 2019, http://soc.eurecom.fr/HWSec/lectures/probing/main.pdf, Erişim Tarihi: Ağustos 22, 2019.

[21] Hu W., Hider J., Williams D., Filipi A., Davidson J. W., Evans D., Knight J. C., Tuong A. N., Rowanhill J., "Secure and Practical Defense Against Code-injection Attacks using Software Dynamic Translation", ***VEE '06 Proceedings of the 2nd international conference on Virtual Execution Environments***, (2006).

[22] Acıiçmez O., Seifert J.-P., Koç Ç. K., "Predicting Secret Keys via Branch Prediction", ***CT-RSA'07 Proceedings of the 7th Cryptographers' track at the RSA conference on Topics in Cryptology***, pp. 225-242, (2006).

[23] Bhattasali T., Chaki R., Sanyal S., "Sleep Deprivation Attack Detection in Wireless Sensor Network", ***International Journal of Computer Applications*** *40(15):19-25*, (2012).

[24] Nguyen V.-L., Lin P., Hwang R., "Energy Depletion Attacks in Low Power Wireless Networks", ***IEEE Access Journal(Open Access)***, 7, 51915-51932, (2019).

[25] Hosamsoleman A., Payandeh A., Mozayyani N., SaeedSedighianKashi "Detection Collision Attacks In Wireless Sensor Network Usingrule-Based Packet Flow Rate", ***International Journal of Engineering Research and Applications (IJERA)***, (2013).

[26] Chowdhury M., Kader M. F., Asaduzzaman, "Security Issues in Wireless Sensor Networks: A Survey", ***International Journal of Future Generation Communication and Networking***, (2013).

[27] Law Y. W., Hoesel L. V., Doumen J., Hartel P., Havinga P., "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," ***Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks***, Alexandria, VA, USA, (2005).

[28] Abdelzaher T. F., Prabh S., Kiran R., "On Real-time Capacity Limits of Multihop Wireless Sensor Networks", ***IEEE Computer Society***, (2004).

[29] Radosavac S., Crdenas A. A., Baras J. S., Moustakides G.V., "Detecting IEEE 802.11 MAC Layer Misbehavior in Ad Hoc Networks: Robust Strategies against Individual and Colluding Attackers", ***Journal of Computer Security,***

Security of Ad Hoc and Sensor Networks, vol.15, no.1, pp. 103-128, (2007).

[30] Sokullu R., Korkmaz I., Dagdeviren O., "GTS Attack: An IEEE 802.15.4 MAC Layer Attack in Wireless Sensor Networks", ***International Journal On Advances in Internet Technology***, (2009).

[31] Sajjad S. M., Yousaf M., "Security Analysis of IEEE 802.15.4 MAC in the context of Internet of Things (IoT)", ***2014 Conference on Information Assurance and Cyber Security (CIACS)***, (2014).

[32] Xiao Y., Sethi S., Chen H., "Security services and enhancements in the IEEE 802.15.4 wireless sensor networks", ***Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE***, (2005).

[33] Pawar P. M., Nielsen R. H., Prasad N. R., Ohmori S., Prasad R., "Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach", ***Journal of Cyber Security and Mobility***, (2012).

[34] Raymond D. R., "Denial-of-Sleep Vulnerabilities and Defenses in Wireless Sensor Network MAC Protocols", Phd Dissertation, ***Virginia Polytechnic Institute and State University***, (2008).

[35] Manju V. C., Sasikumar, "Mitigation Of Replay Attack In Wireless Sensor Network", ***Int. J. on Information Technology***, (2014).

[36] Kamarei M., Patoogy A., Fazeli M., Salehi M. J., AT2A: Defending Unauthenticated Broadcast Attacks in Mobile Wireless Sensor Networks, ***International Journal of Electronics Communication and Computer Engineering***, (2014).

[37] Perrig A., Szewczyk R., Wen V., Culler D., Tygar J. D., "SPINS: Security Protocols for Sensor Networks", ***Mobile Computing and Networking*** (2001).

[38] Tayebi A., Berber S., Swain A., "Wireless Sensor Network Attacks:An Overview and Critical Analysis", ***Seventh International Conference on Sensing Technolog***y, (2013).

[39] Saghar K., Kendall D., Bouridane A., "RAEED: A solution for HELLO flood attack", ***12th International Bhurban Conference on Applied Sciences & Technology (IBCAST),*** (2015).

[40] Deng J., Han R., Mishra S., "INSENS: Intrusion-tolerant routing for wireless sensor networks", ***Elsevier Journal on Computer Communications, Special Issue on Dependable Wireless Sensor Networks***, v.29, p.216–230, (2005).

[41] Zhu S., Setia S., Sajodia S., "LEAP: Efficient Security Mechanisms for LargeScale Distributed Sensor Networks", ***ACM***, (2004).

[42] Magotra S., Kumar K., "Detection of HELLO flood Attack on LEACH Protocol", ***2014 IEEE International Advance Computing Conference (IACC)***, (2014).

[43] Lakhanpal R., Sharma S., Detection & Prevention of Sybil Attack in Ad hoc Network using Hybrid MAP & MAC Technique, ***2016 International Conference on Computation of Power, Energy Information and Communication***, (2016).

[44] Ngai E. C. H., Liu J., Lyu M. R., "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", ***IEEE,*** (2006).

[45] Kibirige G., Sanga C., "A Survey on Detection of Sinkhole Attack in Wireless Sensor Network", ***International Journal of Computer Science and Information Security***, Vol:13(5),pp:1-9, (2015).

[46] Shila D. M., Anjali T., Defending selective forwarding attacks in WMNs***, Electro/Information Technology***, (2008).

[47] Martins D., Guyennet H., "Wireless Sensor Network Attacks and Security Mechanisms - A short survey", ***2010 13th International Conference on Network-Based Information Systems***, (2010).

[48] Ali S., Khan M.A., Ahmad J., Malik A.W., Rehman A., "Detection and Prevention of Black Hole Attacks in IoT & WSN", ***2018 Third International Conference on Fog and Mobile Edge Computing***, (2018).

[49] Hu Y., Perrig A., Johnson D. B., "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks", ***Proceedings of IEEE INFOCOM***, (2003).

[50] Chiu H., Lui K., "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", ***Proceedings of Wireless Pervasive Computing***, (2006).

[51] Khalil I., Bagchi S., Shroff N.B., "LiteWorp: Detection and Isolation of the Wormhole Attack in Static Multihop Wireless Networks", ***Computer Networks***, Vol.51(13), pp: 3750-3772, (2007).

[52] Khalil I., Bagchi S., Shroff N.B., "MobiWorp: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks", ***Proceedings of International Conference on Security and Privacy in Communication Networks***, (2006).

[53] Seo J., Lee G., "An Effective Wormhole Attack Defence Method for a Smart Meter Mesh Network in an Intelligent Power Grid", ***Sage OpenSource Articles*** 2012, http://journals.sagepub.com/doi/full/10.5772/45995, Erişim Tarihi Eylül 14, 2018.

[54] Parno B., Perrig A., Gligor V., "Distributed detection of node replication attacks in sensor networks", ***26th IEEE Symposium on Security and Privacy***, (2005).

[55] Conti M., Pietro R. Di, Mancini L. V., Mei A., "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks", ***8th ACM International Symposium on Mobile Ad Hoc Networking and Computing***, (2007).

[56] Zhang M., Khanapure V., Chen S., Xiao X., "Memory efficient protocols for detecting node replication attacks inwireless sensor networks," ***17th IEEE International Conference on Network Protocols***, (2009).

[57] Ko L. C., Chen H. Y., Lin G. R., "A neighbor-based detectionscheme for wireless sensor networks against node replication attacks", I***nternational Conference on Ultra Modern Telecommunications and Workshop***s, (2009).

[58] Zhu W. T., "Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme", ***IEEE 2011 International Conference on Network Computing and Information Security***, (2011).

[59] Abbas S., Merabti M., Jones D. L., "Deterring Whitewashing Attacks in Reputation Based Schemes for Mobile Ad hoc Networks", ***IEEE 2010 IFIP Wireless Days Conference***, (2010).

[60] Sun Y. L., Han Z., Yu W., Liu K. J. R., "Attacks on Trust Evaluation in Distributed Networks", ***2006 40th Annual Conference on Information Sciences and Systems IEEE***, (2006).

[61] Samreen S., Jabbar M. A., "Countermeasures for Conflicting Behavior Attack in a Trust Management Framework for a Mobile Ad hoc Network", ***2017 IEEE International Conference on Computational Intelligence and Computing Research***, (2017).

[62] Raymond D. R., Midkiff S. F., "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", ***IEEE CS Pervasive Computing*** pp. 74-79, (2008).

[63] Sathish R., Kumar D.R., "Dynamic Detection of Clone Attack in Wireless Sensor Networks", ***IEEE 2013 International Conference on Communication Systems and Network Technologies***, (2013).

[64] Nasridinov A., Byun J.Y., Park Y.H., "UNWRAP: An Approach on Wrapping-Attack Tolerant SOAP

Messages", ***IEEE Second International Conference on Cloud and Green Computing***, (2012).

[65] Bossi L., Bertino E., Hussain S. R., "A System for Profiling and Monitoring Database Access Patterns by Application Programs for Anomaly Detection", 43(5), ***IEEE Transactions on Software Engineering***, (2017).

[66] Uwagbole S. O., Buchanan W. J., Fan L., "Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention", ***2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)***, (2017).

[67] Sun Y., He D., "Model checking for the defense against cross-site scripting attacks", ***IEEE Proceedings of the Computer Science & Service System (CSSS)***, (2012).

[68] Khalaf B. A., Mostafa S. A., Mohammed M. A., Abduallah W. M., "Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods"**,** ***IEEE Access***, (2019).

[69] Tas O., Kiani F., "A Survey of Attacks on Blockchain Technology", ***International Journal of Informatics Technologies***, 11(4), 369-382, (2018).

[70] Spreitzer R., "Pin skimming: Exploiting the ambient-light sensor in mobile devices," in ***Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices***, (2014).

[71] Xu Z., Zhu S., "SemaDroid: A Privacy-Aware Sensor Management Framework for Smartphones", ***CODASPY*** (2015) http://www.cse.psu.edu/~sxz16/papers/semadroid.pdf, Erişim Tarihi Ağustos 16, 2019