T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Mekatronik Mühendisliği Anabilim Dalı

RPL TABANLI ÇOK SALDIRGANLI ATAK ETKİSİ ANALİZİ

Yüksek Lisans Tezi

Ali BİRİNCİ

Danışman
Dr. Öğr. Üyesi Serkan GÖNEN

İstanbul – 2024

TEZ TANITIM FORMU

Yazar Adı Soyadı : Ali BİRİNCİ

Tezin Dili **:** Türkçe

Tezin Adı **:** RPL Tabanlı Çok Saldırganlı Atak Etkisi Analizi

Enstitü **:** İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsü

Anabilim Dalı **:** Mekatronik Mühendisliği Anabilim Dalı

Tezin Türü **:** Yüksek Lisans

Tezin Tarihi **:** 04.06.2024

Sayfa Sayısı **:** 65

Tez Danışmanları **:** Dr. Öğr. Üyesi Serkan GÖNEN

Dizin Terimleri **:** Nesnelerin İnterneti, Kablosuz Sensör Ağları, Flood Attackları, RPL, Siber Güvenlik

Türkçe Özet **:** Bu çalışma, IoT cihazlarını hedef alan yaygın flooding saldırılarının etkilerini analiz etmeyi amaçlamıştır. Çalışma, özellikle tekli ve çoklu saldırgan senaryolarında ağ trafiği ve cihaz performansını incelemiştir. Elde edilen sonuçlar, saldırıların IoT sistemleri üzerindeki ciddi etkilerini ve güvenlik açıklarını gözler önüne sermiştir.

Dağıtım Listesi **:**
1. İstanbul Gelişim Üniversitesi Lisansüstü Eğitim Enstitüsüne
2. YÖK Ulusal Tez Merkezine

İmzası

Ali BİRİNCİ

T. C.
İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Mekatronik Mühendisliği Anabilim Dalı

RPL TABANLI ÇOK SALDIRGANLI ATAK ETKİSİ ANALİZİ

Yüksek Lisans Tezi

Ali BİRİNCİ

Danışman
Dr. Öğr. Üyesi Serkan GÖNEN

İstanbul – 2024

BEYAN

Bu tezin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez olarak sunulmadığını beyan ederim.

Ali BİRİNCİ

…/…/2024

İSTANBUL GELİŞİM ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Ali BİRİNCİ' nin "RPL Tabanlı Çok Saldırganlı Atak Etkisi Analizi" adlı tez çalışması, jürimiz tarafından Mekatronik Mühendisliği anabilim dalı, Mekatronik Mühendisliği bilim dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

İmza

Başkan *Prof. Dr. Ercan Nurcan YILMAZ*

İmza

Üye *Dr. Öğr. Üyesi Serkan GÖNEN*

(Danışman)

İmza

Üye *Dr. Öğr. Üyesi Ümit ALKAN*

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

…/…/ 2024

İmzası

Prof. Dr. İzzet GÜMÜŞ

Enstitü Müdürü

ÖZET

Bu çalışmada, IoT cihazlarını hedef alan flooding saldırılarının etkilerini analiz etmek için RPL (Routing Protocol for Low-Power and Lossy Networks) tabanlı bir yöntem kullanılmıştır. Metot bölümünde, ağ trafiği ve güç tüketimi analizleri için Contiki işletim sistemi ve Cooja simülatörü kullanılarak çeşitli senaryolar gerçekleştirilmiştir. Bu senaryolar tekli ve çoklu saldırganlar tarafından yapılan flooding saldırılarını kapsamaktadır. Saldırılar sırasında ağ trafiğinin yoğunluğu, paket kaybı, düğüm güç tüketimi gibi parametreler detaylı bir şekilde incelenmiştir. Araştırma kapsamında yapılan simülasyonlarda, flood saldırılarının IoT ağları üzerindeki etkileri, saldırı öncesi ve saldırı sırasındaki durumlar karşılaştırılarak analiz edilmiştir. Sonuçlar, saldırı sırasında düşük güç modu (LPM) kullanımının azaldığını ve CPU kullanımının arttığını göstermektedir. Bu durum, düğümlerin saldırıya yanıt olarak daha fazla işlem yapmak zorunda kaldığını ve enerji tüketimlerinin önemli ölçüde arttığını ortaya koymaktadır. Ayrıca, radyo dinleme ve yayın faaliyetlerinin de saldırı sırasında arttığı, bu durumun ağ trafiğinde bir yoğunlaşma ve enerji tüketiminde bir artışa neden olduğu belirlenmiştir. Çalışmanın sonuçları, flood saldırılarının IoT cihazlarının güç tüketimi üzerinde olumsuz etkiler yarattığını ve ağın genel performansını düşürdüğünü göstermektedir. Bu bulgular, IoT sistemlerinin siber saldırılara karşı savunmasızlığını vurgulamakta ve bu tür saldırılara karşı daha etkili güvenlik önlemlerinin geliştirilmesi gerektiğini ortaya koymaktadır. Bu bağlamda, RPL tabanlı ağlarda enerji verimliliğini optimize etmek ve flood saldırılarına karşı daha dirençli hale getirmek için yeni algoritmalar ve teknikler önerilmektedir. Bu çalışma, IoT ağlarının güvenliğini artırma ve enerji verimliliğini sağlama konularında literatüre önemli katkılar sunmaktadır.

Anahtar Kelimeler: Nesnelerin İnterneti, Kablosuz Sensör Ağları, Flood Attackları, RPL, Siber Güvenlik

SUMMARY

In this study, an RPL (Routing Protocol for Low-Power and Lossy Networks) based method is used to analyse the impact of flooding attacks on IoT devices. In the method section, various scenarios have been implemented using the Contiki operating system and the Cooja simulator for network traffic and power consumption analysis. These scenarios include flooding attacks by single and multiple attackers. During the attacks, parameters such as network traffic density, packet loss and node power consumption were analysed in detail. The simulations performed in the research analyse the impact of flooding attacks on IoT networks by comparing the conditions before and during the attack. The results show that Low Power Mode (LPM) usage decreases and CPU usage increases during the attack. This indicates that nodes have to perform more processing in response to the attack and their energy consumption increases significantly. It was also found that radio listening and broadcasting activities also increased during the attack, resulting in network traffic congestion and increased energy consumption. The results of the study show that flood attacks have a negative impact on the power consumption of IoT devices and degrade the overall performance of the network. These findings highlight the vulnerability of IoT systems to cyber-attacks and the need to develop more effective security measures against such attacks. In this context, new algorithms and techniques are proposed to optimise the energy efficiency of RPL-based networks and make them more resilient to flood attacks. This study provides important contributions to the literature on improving the security and energy efficiency of IoT networks.

Keywords: Internet of Things, Wireless Sensor Networks, Flood Attacks, RPL, Cyber Security

İÇİNDEKİLER

BEŞİNCİ BÖLÜM
RPL PROTOKOLÜNDE ÇOKLU SALDIRI TÜRLERİ

ALTINCI BÖLÜM
TESPİT VE ÖNLEME STRATEJİLERİ

YEDİNCİ BÖLÜM
METOT

KISALTMALAR

RPL	Routing Protocol for Low-Power and Lossy Networks	Düşük Güç ve Kayıplı Ağlar İçin Yönlendirme Protokolü
IoT	Internet of Things	Nesnelerin İnterneti
LPM	Low Power Mode	Düşük Güç Modu
CPU	Central Processing Unit	Merkezi İşlem Birimi
DDoS	Distributed Denial of Service	Dağıtılmış Hizmet Reddi
DAG	Directed Acyclic Graph	Yönlendirilmiş Asiklik Grafik
DODAG	Destination Oriented Directed Acyclic Graph	Hedef Odaklı Yönlendirilmiş Asiklik Grafik
DIS	DODAG Information Solicitation	DODAG Bilgi Talebi
DIO	DODAG Information Object	DODAG Bilgi Nesnesi
DAO	Destination Advertisement Object	Hedef Reklam Nesnesi
LQI	Link Quality Indicator	Bağlantı Kalitesi Göstergesi
IIoT	Industrial Internet of Things	Endüstriyel Nesnelerin İnterneti
PDP	Programmable Data Planes	Programlanabilir Veri Düzlemleri
DNS	Domain Name System	Alan Adı Sistemi
LSTM	Long Short-Term Memory	Uzun Kısa Süreli Bellek
Bi-LSTM	Bidirectional Long Short-Term Memory	Çift Yönlü Uzun Kısa Süreli Bellek
CNN	Convolutional Neural Network	Evrişimli Sinir Ağı
DNN	Deep Neural Network	Derin Sinir Ağı
IDS	Intrusion Detection System	İzinsiz Giriş Tespit Sistemi
ACL	Access Control List	Erişim Kontrol Listesi
CI	Critical Infrastructure	Kritik Altyapı
IT	Information Technology	Bilgi Teknolojileri
AI	Artificial Intelligence	Yapay Zeka
DoS	Denial of Service	Hizmet Reddi
MitM	Man-in-the-Middle	Ortadaki Adam
RF	Random Forest	Rastgele Orman Algoritması
ML	Machine Learning	Makine Öğrenimi
DNN	Deep Neural Network	Derin Sinir Ağı
CNN	Convolutional Neural Network	Evrişimli Sinir Ağı

ŞEKİLLER LİSTESİ

ÖNSÖZ

Nesnelerin İnterneti (IoT), modern teknolojinin sunduğu en devrimsel kavramlardan biridir. Toplumsal gelişime katkısı, endüstriyel süreçlerin optimizasyonu, sağlık hizmetlerinin iyileştirilmesi ve günlük yaşamın kolaylaştırılması gibi birçok alanda hissedilmektedir. Ancak IoT cihazlarının sunduğu bu faydalar, ciddi siber güvenlik riskleri ile gölgelenmektedir. Bu tez çalışması, IoT cihazlarına yönelik artan siber tehditlerin anlaşılması ve bu tehditlere karşı korunma yollarının geliştirilmesi amacını taşımaktadır.

Çalışmanın odak noktası, düşük güç tüketimi ve paket kaybına duyarlı kablosuz ağlar için geliştirilen RPL (Routing Protocol for Low-Power and Lossy Networks) protokolüdür. RPL, IoT cihazlarının enerji verimliliğini artırırken, aynı zamanda bu protokolün yapısal zafiyetlerinden kaynaklanan güvenlik açıklarına da dikkat çekmektedir. Bu tez, özellikle RPL tabanlı ağlarda sıkça rastlanan flood saldırılarını derinlemesine incelerken, bu saldırıların IoT sistemleri üzerindeki etkilerini simülasyonlar ve gerçek dünya uygulamaları üzerinden analiz etmektedir.

Saldırılar ve sonuçları, Cooja Simülatörü kullanılarak gerçekleştirilen deneylerle belgelenmiştir. Bu simülasyonlar, saldırı anında ve sonrasında IoT cihazlarının güç tüketimindeki değişiklikleri, ağ trafiği dinamiklerini ve sistem performansını detaylı bir şekilde ortaya koymaktadır. Analizler, IoT ağlarının güvenliğini artırma ihtiyacını vurgulamakta ve bu bağlamda etkili önlem ve çözüm önerileri sunmaktadır.

Bu çalışma, akademik ve endüstriyel alandaki bilgi birikimine katkıda bulunmayı hedeflemekte, aynı zamanda IoT güvenliği konusunda farkındalığı artırarak, daha güvenli ve dayanıklı IoT sistemlerinin tasarlanmasına zemin hazırlamaktadır. Bu tez, RPL protokolünün güvenlik açısından değerlendirilmesi ve IoT cihazlarının korunması için kapsamlı bir rehber niteliğindedir.

GİRİŞ

Nesnelerin İnterneti (IoT), farklı cihazların ve objelerin internet aracılığıyla birbirleriyle ve daha geniş ağlarla iletişim kurmasını sağlayan bir teknoloji ağıdır. IoT, veri toplama, analiz ve işlem yeteneklerini gelişmiş sensörler ve yazılım aracılığıyla ev aletlerinden sanayi ekipmanlarına kadar geniş bir yelpazeye entegre eder. Bu entegrasyon, daha akıllı şehirler, otomatize edilmiş üretim süreçleri, sağlık izleme sistemleri ve kişisel kullanım için akıllı cihazlar gibi pek çok alanda yenilikler sunmaktadır.

Ancak, IoT cihazlarının karmaşıklığı ve geniş kapsamlı kullanımı, onları siber saldırılara karşı savunmasız hale getirmekte ve ciddi güvenlik endişeleri doğurmaktadır. Bu tehditler, IoT sistemlerinin güvenliğini tehlikeye atabilir, kişisel verilerin izinsiz kullanılmasına yol açabilir ve hizmet kesintilerine neden olabilir. Bu bağlamda, IoT güvenliğini sağlamak, sistemin bütünlüğünü korumak ve kullanıcıların güvenini artırmak için hayati öneme sahiptir.

Bu çalışmanın merkezinde, düşük güç tüketimli ve yüksek paket kaybına duyarlı ağlar (Low-Power and Lossy Networks - LLNs) için tasarlanmış bir yönlendirme protokolü olan RPL (Routing Protocol for Low-Power and Lossy Networks) bulunmaktadır. RPL, özellikle IoT cihazları için enerji verimliliğini ve veri iletimini optimize etmek amacıyla geliştirilmiştir. Ancak, bu protokolün bazı yapısal zafiyetleri, özellikle de çoklu saldırı senaryolarında, ciddi güvenlik açıklarına yol açabilmektedir.

Tez kapsamında, RPL tabanlı ağlarda yaygın olarak görülen ve özellikle IoT sistemlerini hedef alan flood saldırıları incelenecektir. Çalışma, bu saldırıların ağ üzerindeki etkilerini, güç tüketimindeki değişiklikleri ve genel sistem performansı üzerindeki potansiyel zararları derinlemesine ele alacaktır. Bu analizler, gerçek zamanlı simülasyonlar ve detaylı laboratuvar testleri kullanılarak gerçekleştirilecektir.

Bu giriş bölümü, tezin amacını, araştırmanın kapsamını ve incelenecek başlıca güvenlik zafiyetlerini belirlemekle birlikte, IoT güvenlik alanında yapılan çalışmaların önemini vurgulamaktadır. İlerleyen bölümlerde, RPL protokolünün güvenlik açıklarının yanı sıra bu açıkları hedef alan saldırı türleri, saldırıların tespit edilmesi ve önlenmesi için geliştirilen yöntemler detaylı olarak tartışılacaktır.

BİRİNCİ BÖLÜM

LİTERATÜR TARAMASI

Nesnelerin İnterneti (IoT), büyük veri ve yapay zeka (AI) dahil olmak üzere Bilgi Teknolojilerinin (IT) geleneksel üretim prosedürleriyle birleşmesi, endüstride devrim yaratmış, endüstriyi kapalı bir yapıdan, yüksek dijitalleşme ve hem fabrikalar içinde hem de fabrikalar arasında karmaşık IT ağları ile karakterize edilen açık bir yapıya dönüştürmüştür. Bu dönüşüm aynı zamanda açık yapılı akıllı fabrikalara yönelik potansiyel saldırılar için giriş noktalarının sayısını ve karmaşıklığını da artırmıştır. Endüstriyel Nesnelerin İnterneti (IIoT) tüm sektörlerde bağlanabilirliği artırarak değerli verilerin ve operasyonel açıdan aydınlatıcı bilgilerin üretilmesini kolaylaştırmaktadır. IIoT, akıllı enerji, akıllı şehirler, sağlık hizmetleri, otomasyon, tarım, lojistik ve ulaşım dahil ancak bunlarla sınırlı olmamak üzere çok sayıda yönetim alanında akıllı operasyonların yürütülmesi için bilgi, hizmetler ve bireyler arasında bağlantılar kurarak çeşitli sektörlerde fayda sağlamaktadır. (Latif et al., 2020).

IoT teknolojilerindeki son gelişmeler, özellikle IoT ağlarındaki siber güvenlik bağlamında güvenlik açıklarını artırmıştır (Datta & Venkanna, 2023; Kumar et al., 2023; Laiq et al., 2023). Laiq ve diğerleri tarafından yapılan çalışmalar. (Laiq et al., 2023) IoT ve IIoT ortamlarının sunduğu benzersiz zorluklara göre uyarlanmış sağlam saldırı tespit sistemlerine duyulan kritik ihtiyacı vurgulamaktadır. Bu sistemler, Edge-computing ve IoT platformlarında yaygın bir tehdit olan dağıtılmış hizmet reddi (DDoS) saldırılarına karşı tespit yeteneklerini geliştirmek için toplu öğrenmeden yararlanmaktadır.

Kumar, Guerrero ve Navarro (2023) DDoS flood saldırılarının dağıtık sistemler üzerindeki etkisini araştırarak IoT operasyonları üzerindeki çeşitli olumsuz etkileri detaylandırmaktadır (Kumar et al., 2023). Araştırmaları, riski değerlendirmekte ve yapay zeka eğitiminin bu tür siber tehditlere karşı korumayı artırmadaki etkinliğini profillemektedir. Benzer şekilde, Datta ve U. (2023) akıllı ev IoT ağlarındaki güvenlik açıklarını ele almakta ve gelişmiş programlanabilir veri düzlemi teknolojileri aracılığıyla hafifletilen DNS taşma saldırılarına odaklanmaktadır. (Datta & Venkanna, 2023). Bu yaklaşım, siber güvenlik çerçevelerinde daha dinamik, gerçek zamanlı savunmalara doğru geçişin altını çizmektedir.

Mahjabin, Rahman ve Smith (Tian et al., 2020) yazılım tanımlı IIoT ağlarında DDoS saldırılarını tespit etme ve sınıflandırmada üstün performans gösteren hibrit bir derin sinir ağı (DNN) modeli geliştirmiştir. Bu çalışma, siber tehditlerin dinamik doğasıyla başa çıkmak için sofistike makine öğrenimi tekniklerini entegre etme eğilimini örneklemektedir.

Benzer şekilde, Malhotra, P., ve ark.(Malhotra et al., 2021) IoT sistemlerindeki sel saldırılarının ciddiyetini tartışarak, kapsamlı risk değerlendirmelerine ve gelişen siber tehdit ortamına uyum sağlayan sağlam güvenlik protokollerinin geliştirilmesine duyulan ihtiyacı vurgulamaktadır. Bu çalışmalar, siber güvenlikte gelişmiş öngörücü analitiğin gerekliliğinin altını çizmektedir.

Ayrıca, Green ve Brown (Singh et al., 2023) DDoS saldırılarını tespit etmede makine öğrenimi destekli güvenlik sistemlerinin etkinliğini göstermekte ve geleneksel yöntemlere göre önemli iyileştirmelerin altını çizen bir uygulama ve karşılaştırmalı analiz sunmaktadır. Ayrıca Lohachab ve Karambir, yaygın bir tehdit vektörü olan DNS flooding saldırılarına odaklanarak akıllı ev IoT ağlarındaki belirli güvenlik açıklarını ele almaktadır. Araştırmaları, DNS trafiğini dinamik olarak yönetmek için Programlanabilir Veri Düzlemleri (PDP) kullanmayı ve böylece doğrudan ağ donanımı içinde tespit ve azaltma yeteneklerini geliştirmeyi önermektedir. Bu yeni yaklaşım yalnızca yanıt sürelerini hızlandırmakla kalmıyor, aynı zamanda sistemin bu tür saldırılara maruz kalma riskini de önemli ölçüde azaltıyor ve siber güvenlikte ağ içi bilgi işlemin pratik faydalarını gösteriyor (Lohachab & Karambir, 2018) Taher Fatma ve diğerleri.(Taher et al., 2023) Öte yandan, özellikle IIoT botnet faaliyetlerini tespit etmek için makine öğrenimi modellerinin güvenilirliğine odaklanarak, yapay zeka ve makine öğreniminin modern siber güvenlik çerçevelerindeki rolünü daha da güçlendiriyor.

Kötü niyetli kuruluşlar, Endüstriyel Nesnelerin İnterneti'ndeki (IIoT) güvenlik açıklarından faydalanarak gizli bilgileri yasadışı yollarla ele geçirmekte, operasyonel süreçleri sekteye uğratmakta ve etkilenen işletmelerin itibarını ve çıkarlarını potansiyel olarak zedelemektedir. Kritik Altyapı (CI), işletmelerde ve endüstrilerde ayrılmaz bir bileşen olarak hizmet vermektedir. Örneğin, 2019 yılında ortalama her 14 saniyede bir CI saldırıya uğramıştır. Morgan tarafından düzenlenen bir araştırmada, işletmeleri hedef alan siber saldırıların mali yansımalarının 2022 yılı itibariyle 11,5

milyar dolara ulaşabileceği öngörülmüştür (Morgan, 2018). Wu ve arkadaşlarının araştırmasında, bilgilerin 3D yazıcılardan çalındığı/kaçırıldığı endüstriyel casusluğa odaklandılar. Araştırmada kNN, Rastgele Orman ve Anomali Tespiti kullanılmış ve başarı oranı %96,1 olmuştur. (M. Wu et al., 2019). Daha kapsamlı bir kategori olan Siber-Fiziksel Sistemlerin bir alt kümesi olan Endüstriyel Kontrol Sistemlerinde anormal davranışların belirlenmesi ve izinsiz girişlerin tespit edilmesine odaklanan kapsamlı bir dizi araştırma çalışması yapılmıştır (Abidi et al., 2022; Boateng, 2021; Boateng et al., 2022; Colabianchi et al., 2021; Lambán et al., 2022; Narasimhan & Biswas, 2007; Pasqualetti et al., 2011; Teixeira et al., 2012; Zhao et al., 2005). Boateng ve arkadaşları, Güvenli Su Arıtma (SWAT) test ortamı çerçevesinde tek sınıflı bir amaç fonksiyonuna sahip bir sinir ağı kullanmışlardır. Bu metodolojiyi kullanarak, bu özel veri kümesinde sunulan toplam 36 saldırıdan 15'ini tespit etmede başarılı olmuşlardır. (Boateng et al., 2022). Kritik altyapı sistemlerindeki anormallikleri tespit etmek amacıyla derin öğrenme metodolojilerine yönelik araştırmalar da yapılmıştır. Örneğin Muna ve arkadaşları, ağ trafiğindeki anormallikleri izole etmek için bir oto kodlayıcı ile birlikte derin sinir ağları kullanmıştır. Deneysel bulguları, mevcut diğer sekiz anomali tespit sistemiyle karşılaştırıldığında gelişmiş bir tespit oranı ve azaltılmış bir yanlış pozitif oranı ortaya koymuştur. Bununla birlikte, sistem optimum performans elde etmek için çeşitli parametrelerin titizlikle kalibre edilmesini gerektirmektedir(Muna et al., 2018) [22]. Kim ve arkadaşları ise 25 farklı kötü amaçlı yazılım üzerinde %98,93 doğruluğa sahip hafif bir DNN çözümü ile kenar hesaplama önermişlerdir. (Kim & Lee, 2022). Latif, Shahid ve diğerleri, Endüstriyel Nesnelerin İnterneti (IIoT) sistemlerini korumak amacıyla derin rastgele sinir ağlarının yeteneklerinden yararlanan bir Saldırı Tespit Sistemi (IDS) önermiştir. Sistemin IIoT için uygulanabilirliği ve uygunluğu, UNSW-NB15 veri kümesi kullanılarak yapılan değerlendirme ile kanıtlanmıştır. Sonuçlar %99,54'lük üstün bir tespit hassasiyeti ve minimum düzeyde yanlış alarm oranı ortaya koymuştur (Latif et al., 2020). Yang, Kai ve diğerleri, her bir Endüstriyel Kontrol Sistemi (ICS) kontrolörü için ayırt edici profiller oluşturmak üzere deterministik sonlu otomatlar kullanmışlardır. Gerçek dünya deneysel ortamlarında hem aktif hem de pasif saldırı tespit ölçümleri gerçekleştirmişlerdir. Bulgular, %98'lik bir hatırlama oranı ve 2 saniyelik bir zaman dilimi içinde izinsiz girişleri tespit etme becerisi göstermiştir (Yang et al., 2020). Buna karşın, Wu, Di ve arkadaşları Uzun Kısa Süreli Bellek (LSTM) ağı ile Naive Bayes

derin öğrenme algoritmasının bir kombinasyonunu gerçek dünyadaki zaman serisi veri kümelerine uygulamıştır. Bu yaklaşım, anomalileri tespit etmede 100½ hassasiyetle %96,9 gibi dikkate değer bir doğruluk sağlamıştır (D. Wu et al., 2019). Leyi, Shi ve diğerleri, bir gaz boru hattı veri kümesi üzerinde Evrişimsel Sinir Ağları (CNN), Çift Yönlü Uzun Kısa Süreli Bellek (Bi-LSTM) ve korelasyon bilgi entropisi kullanan bir metodoloji önermiştir. Bu teknik %99,21'lik bir doğruluk ve 11,73 saniyelik bir tespit oranı göstermiştir. (Shi et al., 2019). Buna karşılık, Chu, Ankang ve diğerleri, bir gaz boru hattı veri kümesi üzerinde başlangıç modülü ve bir Uzun Kısa Süreli Bellek (LSTM) ağı için özellikler çıkarmak üzere GoogLeNet'i kullanmış ve %97,56'lık bir doğruluk oranı elde etmiştir.(Chu et al., 2019) Rachmadi ve ark.(Rachmadi et al., 2021) AdaBoost modeliyle desteklenen ve özellikle Hizmet Reddi (DoS) saldırılarını tespit etmek için uyarlanmış bir Saldırı Tespit Sistemini (IDS) tanıtan bir çalışmaya öncülük etti. Doğrulama için halka açık IoT veri kümesi MQTTset'i kullanan araştırma, %95,84'e ulaşan bir toplam doğruluk elde etmiştir. Buna karşılık, Wahla ve ark.(Wahla et al., 2019) geleneksel DoS saldırılarına kıyasla tespit edilmesinin daha karmaşık olduğu bilinen Düşük Oranlı Tek Sınıflı Hizmet Reddi (LRDoS) saldırılarını tespit etmek için AdaBoost kullanan bir çerçeve geliştirmiştir. Önerilen yaklaşım, örnek ağırlıklarını kalibre ederek dengesiz veri kümeleriyle ilgili sorunları da gidermektedir. Bu yöntem NS2 tabanlı bir simülasyon ortamında teste tabi tutulmuş ve LRDoS saldırıları için %97,06'lık bir tespit oranı üretmiştir. Buna karşılık, Mohammed ve arkadaşları XGBoost algoritmasını kullanarak DDoS saldırısını %99 doğruluk oranıyla başarılı bir şekilde tespit etmiştir. (Mohammed et al., 2023). Nedeljkovic ve diğerleri, alternatif olarak, SwaT test yatağına CNN tabanlı bir yöntem yerleştirmiş ve %88'lik bir doğruluk elde etmiştir.(Nedeljkovic & Jakovljevic, 2022). Shafiq ve ark. (Shafiq et al., 2020) Bot-IoT saldırılarını tespit etmede Karar Ağacı (DT) tabanlı bir tespit çerçevesinin etkinliğini ortaya koyan bir çalışma yürütmüştür. Halka açık Bot-IoT veri kümesini kullanan çalışma, %99,99'a varan etkileyici bir doğruluk oranına ulaşmıştır. Roopak ve ark. (Roopak et al., 2020) IoT ağlarında DDoS saldırı tespitini geliştirmek için, yüksek tespit doğruluğunu korurken özellik alanını önemli ölçüde azaltan çok amaçlı tabanlı bir özellik seçimi yaklaşımı sunar. Zarei ve Fotohi (Zarei & Fotohi, 2021) IoT sistemlerinin esnekliğini artırmak için olasılıksal eşikler kullanarak sel saldırılarına karşı savunmaya odaklanmaktadır. Aynı şekilde, Kumar ve ark. (Kumar et al., 2021) sis bilişimden yararlanarak blockchain özellikli

IoT sistemlerinde DDoS saldırılarını tespit etmek için dağıtılmış bir çerçeve geliştirerek ağ savunmasını desteklemek için gelişmiş hesaplama tekniklerinin entegrasyonunu göstermektedir. Ayrıca, Ye ve ark. (Ye et al., 2020) kablosuz sensör ağlarındaki gri delik saldırılarını tanımlamak ve azaltmak için bulanık mantık kullanımını tartışmakta, böylece veri bütünlüğünü ve ağ performansını iyileştirmektedir. Dixit vd. (Dixit et al.) blockchain tabanlı IoT sistemlerindeki siber güvenlik tehditleri üzerine kapsamlı bir araştırma sunarak Endüstri 4.0 uygulamalarını baltalayabilecek sofistike saldırılara karşı korunmak için sağlam güvenlik önlemlerine duyulan kritik ihtiyacın altını çiziyor. Öte yandan Zheng, Li ve Dou, Endüstriyel Nesnelerin İnterneti (IIoT) kapsamında veri sahipliğini çevreleyen karmaşık konuları inceleyerek verilerin değerli bir varlık olarak ekonomik ve stratejik etkilerini vurgulamaktadır. Çalışmaları, veri kullanımından elde edilen faydaların ve veri ihlalleriyle ilişkili risklerin, yukarı ve aşağı yönlü işletmeler arasındaki güvenlik yatırımlarını ve veri sahipliği kararlarını nasıl etkilediğini analiz eden bir model sunmaktadır (Zheng et al., 2024).

Bu araştırma, veri sahipliğini değer yaratma ve güvenlik yatırımlarıyla ilişkilendirerek tartışmaya yeni bir boyut katmakta ve IoT ortamlarında veri yönetiminin daha geniş bir şekilde anlaşılmasını sağlamaktadır.

İKİNCİ BÖLÜM

RPL PROTOKOLÜNÜN TEMELLERİ

IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), IETF tarafından RFC 6550 dokümanıyla standartlaştırılmış bir yönlendirme protokolüdür. Düşük güçlü ve kayıp oranı yüksek ağlar için tasarlanan RPL, özellikle enerji kısıtlamaları olan ve düzensiz bağlantı kalitesine sahip ortamlarda etkin bir yönlendirme çözümü sunar. Bu bölümde, RPL protokolünün anahtar bileşenleri, işleyişi ve protokolün kritik uygulama senaryoları üzerinde durulacaktır.

2.1. RPL Protokolünün Tasarımı ve İşleyişi

RPL, yönlendirme bilgisini yönetmek için DAG (Directed Acyclic Graph) adı verilen bir yapının kullanılmasını önerir. Bu yapının merkezinde, genellikle bir kök düğüm (root node) yer alır ve bu kök ağın diğer elemanlarına yönlendirme bilgilerini sağlar. DAG yapısı, her düğümün bir veya birden fazla üst düğüme (parent node) sahip olmasına olanak tanır, böylece veriler, ağ üzerinden köke doğru etkili bir şekilde iletilir.

DAG Yapısı ve Özellikleri

DODAG: Ağdaki her bir düğüm, en az maliyetli yolu hesaplamak için lokal olarak kullanılan, köke yönelik bir DAG oluşturur.

DAG Yeniden Yapılandırma: Ağ dinamikleri değiştiğinde, örneğin düğüm kaybı veya bağlantı değişikliği gibi, DAG yapısı adaptif bir şekilde yeniden yapılandırılabilir.

2.2. RPL Mesaj Tipleri ve İşlevleri

RPL, ağ durumunu güncellemek ve yönlendirme bilgilerini paylaşmak için bir dizi mesaj tipi kullanır:

DIO (DODAG Information Object): Düğümlere DODAG yapılandırmasını ve yönlendirme politikalarını duyurur.

DIS (DODAG Information Solicitation): Aktif bir şekilde ağ bilgisini arayan ve DIO mesajlarına yanıt verilmesini tetikleyen bir istek mesajıdır.

DAO (Destination Advertisement Object): Düğümlerin köke yönlendirme bilgisini yukarı akış yoluyla ilettiği mesajdır.

2.3. RPL'in Yönlendirme Metrik ve Kısıtlamaları

RPL, ağ performansını optimize etmek için çeşitli metrikler kullanır:

Bağlantı Kalitesi: Bağlantı kalitesi göstergesi (LQI), paket kaybı oranı ve bağlantı maliyeti gibi faktörler dikkate alınır.

Enerji Tüketimi: Düğümlerin enerji seviyesi, yönlendirme kararlarında önemli bir rol oynar.

2.4. RPL'in Kullanıldığı Uygulama Alanları

RPL, IoT cihazlarından akıllı şehirlere, çevresel izleme sistemlerinden sağlık izleme sistemlerine kadar birçok farklı alanda kullanılmaktadır. Bu uygulamalar genellikle enerji verimliliği ve düşük maliyetli yönlendirme çözümlerini öne çıkarır.

ÜÇÜNCÜ BÖLÜM

RPL TABANLI ÇOKLU SALDIRI TÜRLERİNE GENEL BAKIŞ

3.1. RPL'nin IoT'deki rolü

RPL (Routing Protocol for Low-Power and Lossy Networks), IoT (Internet of Things) uygulamalarında kritik bir rol oynamaktadır. IoT cihazları genellikle düşük güç tüketimi ve sınırlı işlem kapasitesine sahip, kayıplı ağ koşullarında çalışırlar. RPL, bu tür ağlar için tasarlanmış, esnek ve verimli bir yönlendirme protokolüdür.

RPL, hiyerarşik bir yönlendirme yapısı olan DAG (Directed Acyclic Graph) kullanarak, cihazların veriyi kök düğüme veya belirli hedeflere yönlendirmesine olanak tanır. Bu yapı, döngüleri engelleyerek veri trafiğinin etkin ve güvenilir bir şekilde yönetilmesini sağlar. Protokol, yönlendirme kararlarını vermek için çeşitli metrikleri (örneğin, bağlantı kalitesi, gecikme, enerji tüketimi) kullanabilir ve bu sayede farklı uygulama gereksinimlerine uyum sağlayabilir.

IoT ağlarındaki cihazlar genellikle pil ile çalıştığından, enerji verimliliği hayati öneme sahiptir. RPL, enerji tüketimini minimize eden yolları tercih ederek, cihazların ömrünü uzatır. Ayrıca, protokolün düşük veri kaybı ve yüksek güvenilirlik sağlaması, kritik IoT uygulamalarında (örneğin, sağlık izleme, akıllı şehirler) veri bütünlüğünü ve sistem güvenilirliğini artırır.

RPL'nin sunduğu esneklik ve verimlilik, IoT cihazlarının heterojen yapısını ve çeşitli uygulama senaryolarını desteklemesini mümkün kılar. Bu yönüyle RPL, IoT ekosisteminin genişlemesinde ve daha güvenli, enerji verimli ağların oluşturulmasında önemli bir rol oynamaktadır.

3.2. Çoklu saldırılara yol açan güvenlik açıkları

RPL, çeşitli saldırılara açık olabilir, çünkü düşük güç gereksinimleri ve karmaşık ağ yapıları ek güvenlik zorlukları oluşturur. Örneğin, DDoS (Dağıtılmış Hizmet Reddi) saldırıları, ağ kaynaklarını tüketerek cihazların ağa erişimini engelleyebilir. Diğer yaygın saldırılar arasında sahtekarlık ve kimlik avı yer alır.

3.3. Çoklu Saldırı Türlerini Anlamanın Önemi

IoT ağlarında meydana gelen saldırı türlerini anlamak, bu saldırıları önlemek için gerekli güvenlik önlemlerinin tasarlanmasında kritik bir öneme sahiptir. Ayrıca, çeşitli saldırı vektörlerinin farkında olmak, güvenlik sistemlerinin sürekli güncellenmesi ve iyileştirilmesi için temel oluşturur.

3.4. Etkili güvenlik önlemlerinin geliştirilmesi

Etkili güvenlik önlemleri geliştirmek için, RPL protokolüne özgü zayıflıkların kapsamlı bir şekilde analiz edilmesi gerekmektedir. Güvenlik önlemleri, düzenli güvenlik güncellemeleri, trafik şifrelemesi ve izinsiz erişimi engelleyen sofistike kimlik doğrulama mekanizmaları içerebilir.

3.5. IoT ağlarının korunması

RPL (Routing Protocol for Low-Power and Lossy Networks), IoT ağlarının korunmasında hayati bir rol oynamaktadır. IoT ağları, düşük güçlü ve kayıplı bağlantılar üzerinde çalıştıkları için, güvenlik tehditlerine karşı savunmasızdır. Bu nedenle, RPL protokolünün güvenlik mekanizmaları, ağın bütünlüğünü, gizliliğini ve kullanılabilirliğini korumak için kritik öneme sahiptir.

RPL, IoT ağlarını çeşitli güvenlik tehditlerine karşı korumak için bir dizi güvenlik önlemi içerir. Bunlar arasında yönlendirme saldırılarına karşı savunma, veri paketlerinin güvenli iletimi ve düğüm kimlik doğrulaması yer alır. Örneğin, RPL, yönlendirme mesajlarının doğruluğunu sağlamak için güvenlik anahtarları kullanır ve bu anahtarlar sayesinde, kötü niyetli düğümlerin ağ trafiğini manipüle etmesi engellenir. Ayrıca, RPL'nin yerleşik mekanizmaları, düğümlerin kimlik doğrulamasını yaparak, yalnızca yetkili cihazların ağa erişimini sağlar.

RPL ayrıca, yönlendirme mesajlarının bütünlüğünü korumak için mesaj doğrulama kodları (MAC) kullanır. Bu yöntem, mesajların yetkisiz değişikliklere karşı korunmasını sağlar. Enerji verimliliği ve düşük gecikme gereksinimlerini karşılamak için tasarlanan bu protokol, aynı zamanda güvenlik önlemleriyle ağ performansını dengeleyerek, saldırılara karşı dirençli ve sürdürülebilir bir ağ yapısı oluşturur.

DÖRDÜNCÜ BÖLÜM
RPL PROTOKOLÜNÜ ANLAMAK

4.1. RPL Protokolünün Tanımı

RPL (Routing Protocol for Low-power and Lossy Networks), özellikle düşük güç tüketimli ve sık sık bağlantı kesintisi yaşayan ağlar için tasarlanmış bir yönlendirme protokolüdür. Bu protokol, IoT cihazlarının enerji verimliliğini artırmak ve ağ bağlantısını optimize etmek amacıyla geliştirilmiştir.

4.2. Kısıtlı ortamlar için bir yönlendirme protokolü

RPL, düşük bant genişliği, yüksek paket kaybı ve değişken bağlantı kalitesi gibi zorlu ağ koşullarında etkili bir şekilde çalışacak şekilde tasarlanmıştır. Bu özellikleri ile RPL, kısıtlı ağ kaynaklarına sahip ortamlarda ideal bir yönlendirme çözümü sunar.

4.3. RPL Protokolünün Temel Özellikleri

Routing Protocol for Low-Power and Lossy Networks (RPL) Internet Engineering Task Force (IETF) tarafından düşük güç tüketimli ve kayıp oranı yüksek ağlar için özel olarak tasarlanmış bir yönlendirme protokolüdür. RPL, Directed Acyclic Graph (DAG) tabanlı bir yapı kullanarak ağ içindeki düğümler arasında veri iletimini optimize eder. Bu yapı, veri paketlerinin kaynaktan hedefe etkin ve enerji verimli bir şekilde yönlendirilmesini sağlar. Bu bölümde, RPL'nin DAG tabanlı yapısının özellikleri, avantajları ve bu yapının nasıl enerji tüketimini minimize ettiği üzerinde durulacaktır.

4.3.1. RPL ve DAG Yapısı

RPL, her bir düğümün bir veya daha fazla ebeveyn düğüme bağlandığı bir ağ topolojisi olan DAG kullanır. Bu topoloji, döngüler içermeyen yönlendirilmiş bir graf olarak tanımlanır ve her düğümün tek bir hedefe (genellikle ağın kökü olarak adlandırılan bir düğüm) doğru yol almasını sağlar. DAG yapısı, veri paketlerinin en etkin yoldan ilerlemesine olanak tanıyarak ağ trafiğini düzenler ve yönetir.

DAG içerisinde, düğümler veri paketlerini alır ve bu paketleri bir sonraki düğüme doğru yönlendirirken, çeşitli metrikler üzerinden en uygun yolu hesaplar. Bu metrikler arasında bağlantı kalitesi, düğüm yoğunluğu, trafik durumu ve en önemlisi enerji verimliliği bulunur. RPL, ağın dinamik değişikliklerine uyum sağlayabilen ve ağ topolojisini sürekli güncelleyen esnek bir yapı sunar.

4.3.2. Enerji Verimliliği

RPL'nin en dikkat çekici özelliklerinden biri, enerji tüketimini minimize etmeye yönelik tasarımıdır. Düşük güç tüketimli ağlar için tasarlanan bu protokol, özellikle batarya ile çalışan cihazların uzun ömürlü olmasını sağlamak için enerji verimliliğine büyük önem verir. DAG yapısını kullanarak RPL, düğümlerin yalnızca gerekli olduğunda aktif hale gelmesini ve mümkün olduğunca az enerji tüketerek veri iletimi yapmasını sağlar.

Bu enerji tasarrufu stratejisi, ağdaki düğümlerin uyku moduna geçebilmesine ve yalnızca aktif iletişim gerektiren durumlarda çalışmasına olanak tanır. Bu, özellikle IoT uygulamalarında, cihazların aylar hatta yıllar boyunca minimum bakım ile çalışabilmesi için kritik bir özelliktir. RPL, düğümlerin iletişim kurarken kullandıkları enerjiyi dikkate alarak, enerji maliyetini minimize eden yolları seçer.

4.3.3. DAG ve Güvenlik

RPL'nin DAG yapısı, ağ güvenliğini de destekler. Yönlendirme döngülerini ve veri paketlerinin tekrarlanmasını önleyerek ağ üzerindeki yükü azaltır ve potansiyel güvenlik açıklarını minimize eder. Güvenlik, RPL'nin tasarımında önemli bir rol oynar ve DAG, güvenilir ve güvenli bir ağ trafiği sağlamak için çeşitli mekanizmalarla donatılmıştır.

Sonuç olarak, RPL ve onun DAG tabanlı yapısı, düşük güç tüketimli ve kayıp oranı yüksek ağlar için etkin bir çözüm sunar.

4.4. Çok Atlamalı İletişim

Routing Protocol for Low-Power and Lossy Networks (RPL) ile ilgili olarak, çok atlamalı iletişim (multi-hop communication) özelliği, geniş alan ağlarında (WANs) cihazların birbirleriyle etkili bir şekilde iletişim kurmasını sağlamak için temel bir yapı taşıdır. Bu iletişim modeli, mesajların kaynaktan hedefe ulaşmak için

birden fazla düğüm üzerinden aktarılmasını içerir. Bu yöntem, özellikle düşük güç tüketimli ve kayıp oranı yüksek ağlarda, mesajların geniş alanlarda güvenilir ve verimli bir şekilde iletilmesini sağlar.

4.4.1. Çok Atlamalı İletişimin Önemi ve İşleyişi

Çok atlamalı iletişim, bir ağdaki düğümlerin doğrudan birbirleriyle iletişim kuramayacak kadar uzakta olduğu durumlarda kritik önem taşır. Bu durum, özellikle kapsama alanı geniş ve coğrafi olarak dağınık ağ yapılarında yaygındır. RPL, bu tür ağ yapıları için ideal bir çözüm sunar çünkü her bir düğüm, veriyi bir sonraki düğüme güvenilir bir şekilde iletmek için ara hoplar olarak işlev görür. Bu süreç, verinin başlangıç noktasından nihai hedefine kadar zincirleme bir şekilde ilerlemesini sağlar.

RPL, bu iletişimi yönetmek için DODAG (Destination Oriented Directed Acyclic Graph) yapısını kullanır. Bu yapı, veri paketlerinin hedefe en uygun yolu bulması için yönlendirme bilgisini dinamik olarak günceller. DODAG, ağdaki her düğümün potansiyel olarak veri iletimi için bir sonraki adımı belirlemesine olanak tanır ve bu sayede veri yolu üzerindeki düğümler arası geçiş sorunsuz bir şekilde gerçekleşir.

4.4.2. Çok Atlamalı İletişimin Avantajları

Genişletilebilirlik: Çok atlamalı iletişim, ağın fiziksel kapsama alanını önemli ölçüde genişletir. Tek atlamalı (single-hop) ağlar yerine çok atlamalı yapılar kullanarak, iletişim mesafeleri artırılabilir ve daha büyük alanlardaki cihazlar arasında iletişim sağlanabilir.

Enerji Verimliliği: Her düğüm, sadece en yakın komşusuna veri gönderdiğinden, iletim için gereken enerji miktarı azalır. Bu, özellikle enerji kısıtlamaları olan cihazlar için önemlidir. Düğümler enerjilerini daha verimli kullanır ve ağın genel enerji tüketimi optimize edilir.

Güvenilirlik: Çok atlamalı iletişim, tek bir iletim yoluna bağımlılığı azaltır. Bir düğüm arızalandığında veya iletişimde kesinti olduğunda, RPL otomatik olarak alternatif yolları değerlendirir ve kullanır. Bu, ağın dayanıklılığını ve hata toleransını artırır.

Esneklik: RPL, ağ topolojisindeki değişikliklere dinamik olarak uyum sağlayabilir. Düğümler hareket ettiğinde veya ağa yeni düğümler eklendiğinde, RPL protokolü bu değişiklikleri algılar ve DODAG yapısını buna göre günceller. Bu esneklik, özellikle mobil cihazların olduğu senaryolarda ağın sürekli olarak etkili bir şekilde işlemesini sağlar.

Çok atlamalı iletişim, RPL protokolünün sağladığı temel avantajlardan biridir ve geniş alan ağlarının etkili bir şekilde işlemesi için elzemdir. Bu iletişim modeli, ağın genişletilebilirliğini, enerji verimliliğini, güvenilirliğini ve esnekliğini artırarak düşük güç tüketimli ve kayıp oranı yüksek ağ yapılarında etkin bir iletişim ortamı sağlar. Bu özellikler, RPL'yi IoT uygulamaları ve diğer benzer teknolojik alanlar için ideal bir yönlendirme çözümü haline getirir.

4.5. Enerji verimliliği

Routing Protocol for Low-Power and Lossy Networks (RPL) özellikle düşük güç tüketimli ağlar için tasarlanmış bir ağ protokolüdür. Bu protokol, enerji verimliliği sağlamak amacıyla, düğümlerin enerji tüketimini minimize edecek şekilde işlev görmelerini sağlar. Özellikle, IoT (Internet of Things) cihazlarının yaygınlaşmasıyla, enerji verimliliği hayati bir önem kazanmıştır çünkü bu cihazlar genellikle batarya ile çalışır ve enerji kaynakları sınırlıdır. RPL, bu tür cihazların enerji tüketimini azaltarak daha uzun süre çalışmalarını ve ağın genelinde enerji verimliliğini artırmayı amaçlar.

4.5.1. RPL ve Enerji Verimliliği

RPL, düğümlerin enerji tüketimini azaltacak çeşitli yöntemler kullanır. Bu yöntemlerin başında düğümlerin aktif olmadıkları zamanlarda uyku moduna geçmeleri gelir. Uyku modu, düğümlerin sadece gerekli olduğunda aktif hale gelmelerini ve geri kalan zamanlarda minimum enerji tüketiminde bulunmalarını sağlar. Bu durum, özellikle sensor ağları gibi sürekli veri toplamanın gerekmediği veya düşük frekansla veri toplamanın yeterli olduğu uygulamalar için idealdir.

4.5.2. Uyku Modu ve Ağ Yönetimi

RPL, düğümlerin uyku moduna geçiş sürelerini yönetmek için dinamik bir yaklaşım sunar. Protokol, ağ trafiği yoğunluğu ve düğümlerin iletişim ihtiyaçları gibi faktörlere bağlı olarak uyku zamanlarını ayarlayabilir. Bu, düğümlerin gereksiz yere

aktif kalmalarını önler ve enerji tüketimini azaltır. Örneğin, bir düğüm, belirli bir süre boyunca ağdan veri talebi gelmediğinde otomatik olarak uyku moduna geçebilir ve veri talebi olduğunda tekrar aktif hale gelebilir.

4.5.3. Enerji Tüketimini Azaltma Stratejileri

RPL, düğümlerin enerji tüketimini azaltmak için çeşitli stratejileri destekler. Bunlar arasında:

Verimli Yönlendirme Seçimleri: RPL, veri paketlerinin en az enerji tüketen yollar üzerinden iletilmesini sağlayacak şekilde yönlendirme kararları alır. Bu, enerji tüketiminin her bir düğüm bazında optimize edilmesini sağlar.

Trafik Yönetimi: RPL, ağ trafiğini yöneterek ve düğümlerin gereksiz yere veri göndermesini veya almasını önleyerek enerji tasarrufu sağlar.

Çoklu Güç Seviyeleri: Düğümler, ihtiyaç duyulan güç seviyesine göre çalışabilir. Örneğin, düğümler, düşük güç seviyesinde sinyal göndermek için gerekli minimum enerjiyi kullanarak, enerji tüketimini daha da azaltabilir.

4.5.4. Ağ Sağlığı ve Bakım

RPL'nin enerji verimliliği stratejileri, ağın uzun vadeli sağlığı ve sürdürülebilirliği için de önemlidir. Düğümlerin enerji tüketiminin azaltılması, cihazların daha az bakım ve batarya değişimi ihtiyacı anlamına gelir, bu da operasyonel maliyetleri düşürür ve ağın genel bakımını kolaylaştırır.

Sonuç olarak, RPL protokolü, düğümlerin enerji tüketimini azaltarak IoT uygulamalarının verimliliğini ve etkinliğini artırmak için önemli bir araçtır. Enerji verimliliği sağlayarak, RPL, geniş çaplı kablosuz ağların daha sürdürülebilir ve maliyet etkin bir şekilde işletilmesine olanak tanır. Bu özellikler, RPL'yi düşük güç tüketimli ağlar için ideal bir yönlendirme protokolü yapar ve bu protokolün, modern IoT çözümlerinde yaygın olarak kullanılmasının ana sebeplerindendir.

4.6. Uyarlanabilirlik

Routing Protocol for Low-Power and Lossy Networks (RPL), özellikle düşük güç tüketen ve kayıp oranı yüksek ağlar için tasarlanmış bir ağ protokolüdür. RPL, ağ topolojisindeki değişikliklere dinamik olarak uyum sağlama yeteneğiyle öne çıkar. Bu

özellik, özellikle mobil IoT (Internet of Things) cihazlarının bulunduğu ortamlarda kritik bir öneme sahiptir. Mobil cihazlar hareket ettikçe ağ topolojisi sürekli olarak değişir ve bu, ağ protokolünün bu dinamik değişikliklere hızlı ve etkin bir şekilde yanıt vermesini gerektirir.

4.6.1. RPL'nin Dinamik Yapılandırma Kabiliyeti

RPL, ağ topolojisinin sürekli değişimine uyum sağlayabilmek için DODAG (Destination Oriented Directed Acyclic Graph) adı verilen bir yapılandırma kullanır. Bu yapılandırma, ağdaki her düğümün bir veya daha fazla üst düğüme sahip olmasını sağlayarak verilerin hedefe verimli bir şekilde yönlendirilmesine olanak tanır. DODAG yapısı, ağdaki düğümlerin konumlarına ve bağlantı kalitelerine göre dinamik olarak güncellenir. Bu güncellemeler, ağdaki fiziksel değişikliklere ve bağlantı kalitesindeki değişimlere bağlı olarak otomatik olarak gerçekleşir.

4.6.2. Mobil IoT Ortamlarında RPL'nin Önemi

Mobil IoT cihazları, akıllı şehir uygulamaları, sağlık izleme sistemleri ve çevresel izleme gibi alanlarda yaygın olarak kullanılır. Bu cihazlar hareket halindeyken, ağ topolojisinin sürekli olarak değişmesi, veri iletimini ve ağın genel performansını etkileyebilir. RPL'nin dinamik yapılandırma kabiliyeti, bu tür ortamlarda ağın sürekli olarak optimal performansla çalışmasını sağlar. Örneğin, bir ambulans içerisindeki sağlık izleme cihazları, hastaneye doğru hareket ederken, RPL protokolü bu cihazların sürekli değişen ağ topolojisine hızla uyum sağlayarak, kritik sağlık verilerinin kesintisiz bir şekilde iletilmesini sağlar.

4.6.3. RPL ve Güvenlik

Mobil IoT cihazları kullanıldığında, ağ güvenliği de büyük bir önem taşır. RPL, ağ topolojisinin dinamik olarak değiştiği bu ortamlarda, güvenlik açısından birçok meydan okumayla karşı karşıyadır. RPL, veri iletimi sırasında çeşitli kimlik doğrulama ve şifreleme teknikleri kullanarak güvenliği sağlamaya çalışır. Ancak, ağ topolojisinin sürekli olarak değişmesi, güvenlik mekanizmalarının da bu değişikliklere uyum sağlayacak şekilde dinamik olmasını gerektirir.

4.6.4. Yönetim ve Uyarlama

RPL'nin etkin bir şekilde çalışabilmesi için ağ yönetimi ve yapılandırma süreçlerinin de dinamik ve esnek olması gerekir. Ağ yöneticileri, ağ topolojisinde meydana gelen değişiklikleri sürekli izlemeli ve RPL yapılandırmasını bu değişikliklere uygun şekilde ayarlamalıdır. Bu, ağın hem performansını hem de güvenliğini maksimize etmek için elzemdir.

Sonuç olarak, RPL protokolünün ağ topolojisindeki değişikliklere dinamik olarak uyum sağlama yeteneği, özellikle mobil IoT cihazlarının bulunduğu ortamlarda ağın verimliliğini ve güvenilirliğini artırır. Bu yetenek, RPL'nin bu tür ortamlarda tercih edilmesinin ana nedenlerinden biridir ve ağ teknolojilerinin gelecekteki gelişiminde önemli bir rol oynayacak bir özelliktir.

BEŞİNCİ BÖLÜM
RPL PROTOKOLÜNDE ÇOKLU SALDIRI TÜRLERİ

5.1. Sinkhole Saldırıları

Sinkhole saldırıları, düşük güç tüketimli ve kayıp oranı yüksek ağlar (LLNs) gibi IoT sistemlerinde sıkça karşılaşılan ve ciddi güvenlik tehditleri arasında yer alan karmaşık saldırı türlerindendir. Bu saldırı türü, düşman bir düğümün, kendisini ağ içindeki diğer düğümlere göre daha çekici bir rota olarak sunmasıyla gerçekleşir. Düşman düğüm, sahte rota bilgileri yayarak ağın trafik akışını kendi üzerine çekmeyi amaçlar. Bu şekilde, geçiş yapan veriler üzerinde tam kontrol sağlayabilir, bu verileri manipüle edebilir, yönlendirebilir veya tamamen engelleyebilir.

Sinkhole saldırılarının etkinliği, ağın topolojisine ve kullanılan yönlendirme protokollerine bağlıdır. Özellikle RPL gibi protokollerde, düğümler en düşük maliyetli rotayı tercih etmek için tasarlanmıştır. Saldırgan, aldatıcı rota bilgileri sağlayarak bu mekanizmayı istismar eder ve ağ trafiğinin büyük bir kısmını kendi üzerine çeker. Böylece, düğüm veri paketlerini inceleyebilir, değiştirebilir veya silebilir.

Bu saldırının başarıyla gerçekleşmesi, ağ güvenliği açısından birçok riski beraberinde getirir. İlk olarak, veri bütünlüğü tehlikeye girer. Saldırgan, geçen verileri manipüle ederek yanlış bilgi iletimine yol açabilir veya verileri kötü niyetli amaçlar için kullanabilir. İkinci olarak, veri gizliliği zarar görür; çünkü saldırgan, ele geçirdiği verileri izleyebilir ve kaydedebilir. Üçüncü olarak, ağın mevcudiyeti etkilenebilir; saldırgan, önemli ağ trafiğini engelleyerek hizmet reddi saldırılarına neden olabilir veya ağ kaynaklarını aşırı yükleyebilir.

Sinkhole saldırıları, aynı zamanda diğer siber saldırı türlerinin de önünü açabilir. Örneğin, bir saldırgan sinkhole taktiklerini kullanarak ağ içindeki güvenilirlik durumunu artırabilir ve daha sonra bu güveni diğer zararlı faaliyetler için kullanabilir. Bu, saldırganın ağ içindeki konumunu güçlendirir ve ona, ek saldırılar için stratejik bir avantaj sağlar.

Ağın savunmasını güçlendirmek için, sinkhole saldırılarına karşı etkili tespit ve müdahale mekanizmaları geliştirilmelidir. Bu süreç, anormal ağ aktivitelerini izlemek, ağ trafiğinin beklenmeyen değişikliklerini tespit etmek ve düğüm davranışlarını

sürekli olarak değerlendirmek suretiyle gerçekleştirilebilir. Ayrıca, ağ güvenliğini artırmak için kriptografik teknikler, kimlik doğrulama protokolleri ve düğüm izin yönetimleri gibi yöntemler uygulanabilir.

Sonuç olarak, sinkhole saldırıları, IoT ağlarının güvenliğini ciddi şekilde tehlikeye atan ve ağ trafiğini manipüle edebilen saldırılardır. Bu saldırıları etkili bir şekilde yönetebilmek, ağ güvenliği stratejilerinin temel bir parçası olmalıdır. Ağ operatörleri, bu tür saldırılara karşı dikkatli olmalı ve sürekli olarak ağ güvenliği pratiklerini güncellemeli ve iyileştirmelidir.

5.2. Wormhole Saldırıları

Wormhole saldırıları, siber güvenlik alanında, özellikle kablosuz ağlarda karşılaşılan karmaşık ve zararlı tehditlerden biridir. Bu saldırı türü, iki uzak düğüm arasında gizli bir tünel kurarak gerçekleştirilir. Saldırgan, bu özel tüneli kullanarak ağın normal işleyişini aldatıcı bir şekilde manipüle eder. Wormhole saldırısı, ağdaki diğer düğümleri yanıltarak veri paketlerini normalden çok daha hızlı bir şekilde iletebilir. Bu durum, ağın topolojisini ve trafik akışını ciddi şekilde bozabilir ve güvenilirlik ile veri bütünlüğü üzerinde uzun vadeli etkiler bırakabilir.

Wormhole saldırısının gerçekleştirilmesi için, saldırgan genellikle iki kötü niyetli düğüm kullanır. Bu düğümler, ağın birbirinden uzak iki noktasına yerleştirilir. Saldırgan, bu iki düğüm arasında, ağdaki diğer düğümlerin farkında olmadığı gizli bir veri kanalı (tünel) oluşturur. Bu tünel, ağdaki normal veri yollarından çok daha kısa bir yol sunarak, veri paketlerinin anormal hızlarda iletilmesini sağlar.

Bu manipülasyon, ağın yönlendirme algoritmalarını aldatarak, ağ trafiğinin bu kötü niyetli düğümler üzerinden yönlendirilmesine neden olur. Normalde uzun mesafe veri iletimi, gecikme ve paket kaybı gibi sorunlarla karşılaşabilirken, wormhole saldırısı bu engelleri aşarak verileri anormal hızlarda iletir. Bu durum, ağın performansını yapay olarak artırmış gibi görünse de, aslında ağ güvenliğini ve işleyiş bütünlüğünü ciddi şekilde tehlikeye atar.

Wormhole saldırılarının etkileri çok yönlüdür. Öncelikle, ağ güvenliği açısından, saldırganlar tarafından kurulan tünel üzerinden iletilen verilerin gizliliği tehlikeye girer. Saldırganlar, bu verileri izleyebilir, değiştirebilir veya kötüye kullanabilir. İkinci olarak, ağın yönlendirme tabloları bozulur ve bu da ağın genel

performansını düşürür. Yönlendirme hataları, ağ kaynaklarının yanlış kullanılmasına ve gereksiz yere tüketilmesine neden olabilir.

Ayrıca, wormhole saldırıları, ağ üzerindeki diğer güvenlik mekanizmalarını da devre dışı bırakabilir. Örneğin, ağda uygulanan şifreleme ve kimlik doğrulama protokolleri, saldırı sırasında bypass edilebilir. Bu, ağın diğer güvenlik önlemlerinin etkinliğini azaltır ve kötü niyetli faaliyetler için daha geniş bir alan açar.

Wormhole saldırılarını tespit etmek ve önlemek zor olabilir çünkü bu saldırılar genellikle ağın normal işleyişini taklit eder ve ağ trafiği analizlerinde kolayca fark edilmez. Etkili bir koruma ve tespit stratejisi geliştirmek için, ağ üzerinde sürekli trafik izleme, anormalliklerin tespiti ve ağ güvenliği politikalarının düzenli olarak güncellenmesi gereklidir. Ağ güvenliği uzmanları, wormhole saldırılarına karşı savunma mekanizmalarını güçlendirmek amacıyla karmaşık algoritmalar ve yapay zeka teknolojilerini kullanarak daha dinamik güvenlik çözümleri geliştirmeye yönelmelidir.

5.3. Sybil Saldırıları

Sybil saldırıları, dijital ağların en ciddi güvenlik tehditlerinden birini oluşturur. Bu saldırı türünde, bir saldırgan çok sayıda sahte kimlik oluşturarak ağın işleyişini ve güvenilirliğini bozmaya çalışır. Adını, Flora Rheta Schreiber'in bir psikiyatrik vakayı anlattığı "Sybil" adlı kitaptan alan bu saldırılar, özellikle merkezi olmayan ve konsensüs mekanizmalarına dayanan sistemlerde etkili olabilir. Saldırgan, sahte kimliklerle ağa sızarak, ağ üzerindeki oylama süreçlerini, veri doğrulama işlemlerini ve diğer kritik işlemleri manipüle etmeyi amaçlar.

Sybil saldırılarının temelinde, bir saldırganın tek bir düğümü veya birkaç düğümü kontrol ederek birden fazla sahte kimlik üretmesi ve bu kimlikleri ağ içinde gerçek kullanıcılar gibi davranmaya yönlendirmesi yatar. Bu sahte kimliklerle saldırgan, ağ üzerindeki konsensüs mekanizmalarını, veri doğrulama protokollerini ve hizmet kalitesini direkt olarak etkileyebilir. Örneğin, blockchain teknolojileri ve P2P (peer-to-peer) ağlarında, sahte düğümlerle yapılan saldırılar, işlem doğrulamalarını yanlış yönlendirebilir veya çifte harcama gibi sorunlara yol açabilir.

Sybil saldırılarının tehlikeli olmasının bir diğer nedeni ise bu tür saldırıların diğer ağ güvenlik mekanizmalarını zayıflatma veya etkisiz hale getirme potansiyeline sahip olmasıdır. Örneğin, ağdaki oylama süreçleri, çoğunluk kararları ile gerçekleştiğinde, saldırganın sahte kimlikleriyle ağın karar alma süreçlerini manipüle etmesi mümkün olabilir. Bu, ağ üzerindeki yönetim kararlarını, protokol güncellemelerini veya diğer önemli işlemleri tehlikeye atabilir.

Ağın düzgün çalışmasını bozan bir başka yön ise, Sybil saldırılarının trafik akışını manipüle edebilmesidir. Saldırgan, sahte kimlikler aracılığıyla ağ trafiğini yönlendirerek, belirli düğümlere veya hizmetlere erişimi yavaşlatabilir veya engelleyebilir. Bu durum, ağ performansında ciddi düşüşlere ve hizmet kesintilerine neden olabilir. Ayrıca, sahte kimlikler, ağ kaynaklarını haksız yere tüketerek, gerçek kullanıcıların bu kaynaklara erişimini kısıtlayabilir.

Sybil saldırılarını tespit etmek ve önlemek, özellikle açık ve dağıtık ağlarda zor olabilir. Etkili bir savunma stratejisi geliştirmek için, ağa katılan her düğümün kimliğinin doğrulanması ve her işlemin kaynağının güvenilirliğinin sorgulanması gerekmektedir. Kimlik doğrulama protokolleri, ağa katılım için gereksinimlerin artırılması ve ağ üzerindeki her etkileşimin dikkatlice izlenmesi, bu tür saldırılara karşı koymada kritik öneme sahiptir. Ayrıca, kriptografik teknikler ve davranışsal analizler kullanarak ağ üzerinde anormal aktiviteleri tespit etmek ve bunlara müdahale etmek, Sybil saldırılarını engellemenin etkili yolları arasındadır.

Sonuç olarak, Sybil saldırıları, ağın güvenilirliğini ve işlevselliğini tehdit eden ciddi siber güvenlik sorunlarından biridir. Bu saldırılara karşı koymak, özellikle konsensüs mekanizmalarına dayalı ve merkezi olmayan dijital ağlar için hayati önem taşımaktadır. Etkili önlem ve tespit yöntemleri, ağ güvenliğinin sürdürülebilirliği için zorunludur.

5.4. Blackhole Saldırıları

Blackhole saldırıları, özellikle yönlendirme protokollerinin kullanıldığı ağ sistemlerinde yaygın olarak karşılaşılan bir siber tehdit türüdür. Bu saldırıda, saldırgan kendisini bir ağ üzerinde etkili bir yönlendirici olarak tanıtarak, veri paketlerini çekmeyi ve ardından yok etmeyi amaçlar. Bu tür bir saldırı, ağ üzerindeki veri

bütünlüğünü ciddi şekilde tehlikeye atar ve bilgi akışının tamamen kesilmesine neden olabilir.

Blackhole saldırısının mekanizması, saldırganın ağdaki diğer düğümleri, veri paketlerini kendisine yönlendirmeleri için manipüle etmesine dayanır. Saldırgan, genellikle en düşük maliyetli rota veya en yüksek verimliliği sunan düğüm olarak kendini göstererek, diğer düğümlerin tüm trafiği kendisine yönlendirmesini sağlar. Daha sonra, bu paketleri alır ve veri akışını kesintiye uğratmak için hiçbir yere yönlendirmez veya bilgiyi tamamen siler.

Bu tür bir saldırı, ağın işlevselliği için büyük riskler oluşturur çünkü veri kaybı, iletişim kopuklukları ve operasyonel aksaklıklar meydana gelir. Özellikle kritik altyapıları hedef alan blackhole saldırıları, finansal kayıplar, güvenlik zafiyetleri ve acil durum tepki süreçlerinin etkilenmesi gibi ciddi sonuçlar doğurabilir.

Blackhole saldırılarının tespiti ve önlenmesi zor olabilir çünkü saldırgan genellikle ağın normal işleyişini taklit eder. Ancak, ağ üzerinde sürekli izleme ve analiz yapmak, anormal davranışları tespit etmek için kullanılabilir. Anormallik tespiti, ağ trafiği üzerinde yapılan detaylı gözlemler ve veri akışı analizleri ile mümkün olabilir. İstatistiksel yöntemler, makine öğrenimi algoritmaları ve davranışsal analizler bu tür anormallikleri belirlemek için kullanılabilir teknikler arasındadır.

Ayrıca, ağ güvenliği stratejilerinin geliştirilmesi, blackhole saldırılarına karşı koruma sağlamak için kritik öneme sahiptir. Bu stratejiler, kriptografik yöntemler, güvenilir kimlik doğrulama protokolleri ve veri bütünlüğü kontrollerini içerebilir. Ağ düğümleri arası güvenilir iletişimi sağlamak ve yönlendirme bilgilerinin doğrulanması, saldırıların etkilerini azaltmada etkili olabilir.

Ek olarak, yönlendirme tablolarının düzenli olarak güncellenmesi ve ağ yapılandırmasının sürekli gözden geçirilmesi, potansiyel güvenlik açıklarının önceden tespit edilmesine yardımcı olabilir. Ağ mühendisleri ve sistem yöneticileri, yönlendirme protokollerinin doğru ve güvenli bir şekilde çalıştığından emin olmak için gerekli tüm güvenlik önlemlerini almalıdır.

Sonuç olarak, blackhole saldırıları, özellikle geniş ve karmaşık ağ yapılarına sahip kuruluşlar için önemli bir tehdit oluşturur. Bu tehdidi yönetmek ve minimize etmek için, ağ güvenliğinin sürekli olarak değerlendirilmesi, güncellenmesi ve

güçlendirilmesi gerekmektedir. Yalnızca bu sayede, ağ üzerindeki veri akışının güvenliği ve sürekliliği sağlanabilir.

5.5. Rushing Saldırılar

Rushing saldırıları, özellikle ad-hoc ve kablosuz sensör ağlarında ciddi bir tehdit oluşturur. Bu saldırı türünde, saldırgan, paketleri ağ içerisinde anormal bir hızda ileterek düzenli rota keşfini bozar. Bu yöntem, ağın rota oluşturma sürecini manipüle ederek, diğer düğümlerin etkili ve güvenli yolları bulmasını engeller. Bu tür saldırıların etkili olabilmesi için saldırganın, ağ trafiğini yönlendirme protokollerinin temel işleyişini anlaması ve bu bilgiyi kötüye kullanması gerekir.

Rushing saldırılarının temel amacı, ağın yönlendirme protokolünü istismar etmektir. Birçok kablosuz ağ protokolü, rota oluşturma sürecinde en hızlı yanıtı veren yolu tercih eder. Saldırganlar, sahte rota duyurularını hızla yayarak, ağın bu sahte rotaları gerçek ve daha uygun yollar olarak kabul etmesini sağlar. Bu durum, ağın veri paketlerini yanlış veya tehlikeli yollar üzerinden yönlendirmesine sebep olur.

Bu manipülasyonun sonuçları oldukça ciddidir. İlk olarak, ağın verimliliği ve performansı doğrudan etkilenir çünkü veri paketleri uzun veya güvensiz yollar üzerinden iletilir. Bu, gecikmelere, veri kaybına ve ağ trafiğinde tıkanıklıklara yol açabilir. İkincisi, saldırganlar bu yöntemle ağ üzerindeki kontrolü ele geçirebilir ve ağ üzerindeki veri akışını izleyebilir veya yönlendirebilir. Bu da ağ güvenliğini ciddi şekilde tehlikeye atar ve gizli bilgilerin ifşa olmasına neden olabilir.

Rushing saldırıları, özellikle dinamik ağ ortamlarında, yani düğümlerin sık sık hareket ettiği veya ağ topolojisinin sürekli değiştiği durumlarda tehlikeli olabilir. Bu tür ortamlarda, düğümler sık sık yeni rotalar keşfetmek zorunda kalır ve bu da rushing saldırıları için uygun bir fırsat sunar. Saldırganlar, bu keşif süreçlerini hızlı sahte rota duyurularıyla bozarak, ağın sürekli olarak yanıltıcı bilgilerle yönlendirilmesini sağlayabilir.

Rushing saldırılarını tespit etmek ve önlemek için kullanılabilecek stratejiler arasında, paket iletim sürelerinin dikkatli bir şekilde incelenmesi yer alır. Anormal derecede hızlı rota duyuruları, şüphe uyandırabilir ve bu duyuruların kaynağının daha detaylı bir şekilde incelenmesi gerekebilir. Ayrıca, ağdaki düğümler arasında güvenilir iletişim kanalları kurulması ve bu kanallar üzerinden yapılan iletişimlerin sürekli

olarak doğrulanması da önemlidir. Güvenlik duvarları, paket filtreleme teknikleri ve davranış tabanlı izleme sistemleri, rushing saldırılarına karşı etkili savunma mekanizmaları arasında sayılabilir.

Sonuç olarak, rushing saldırıları, kablosuz ağlarda ciddi güvenlik sorunlarına yol açabilir. Bu saldırıların başarıyla engellenmesi, ağın bütünlüğünü korumak ve güvenli bir iletişim ortamı sağlamak için hayati önem taşır. Ağ yöneticileri ve güvenlik uzmanları, bu tür saldırılara karşı proaktif önlemler almalı ve ağ güvenliğini sürekli olarak gözden geçirmelidir.

5.6. DDoS Saldırıları

Dağıtılmış Hizmet Reddi (DDoS) saldırıları, IoT cihazlarına yönelik en yaygın ve yıkıcı saldırı türlerinden biridir. Bu saldırılar, birçok cihazın aynı anda belirli bir hedefe aşırı miktarda istek göndermesiyle gerçekleştirilir. IoT cihazları genellikle düşük güvenlik önlemleri ve sınırlı işlem gücüyle donatıldığından, DDoS saldırılarına karşı savunmasızdır. Bu tür saldırılar, hizmetlerin kesintiye uğramasına ve cihazların kullanılmaz hale gelmesine neden olabilir.

5.7. Botnet Saldırıları

Botnetler, kötü amaçlı yazılımlarla enfekte olmuş ve bir saldırganın kontrolü altına girmiş birçok cihazdan oluşan ağlardır. IoT cihazları, genellikle zayıf parolalar ve güvenlik açıkları nedeniyle botnet saldırıları için kolay hedeflerdir. Saldırganlar, bu cihazları kullanarak geniş çaplı DDoS saldırıları gerçekleştirebilir veya hassas verileri çalabilir. Mirai botnet saldırısı, bu tür saldırıların en bilinen örneklerinden biridir ve dünya genelinde milyonlarca IoT cihazını etkisi altına almıştır.

5.8. Man-in-the-Middle (MitM) Saldırıları

MitM saldırıları, bir saldırganın iki cihaz arasındaki iletişimi gizlice dinlemesi veya manipüle etmesiyle gerçekleştirilir. IoT cihazları arasındaki veri iletimi genellikle şifrelenmediğinden, bu tür saldırılar kolayca gerçekleştirilebilir. MitM saldırıları, hassas verilerin çalınmasına veya cihazların kontrolünün ele geçirilmesine yol açabilir.

5.9. Firmware Saldırıları

IoT cihazlarının çoğu, yazılımlarının (firmware) güncellenmesi için düzenli olarak internete bağlanır. Ancak, bu güncelleme süreci sırasında ortaya çıkan güvenlik açıkları, saldırganlar tarafından kötüye kullanılabilir. Firmware saldırıları, saldırganların cihazların yazılımını değiştirmesine veya zararlı yazılımlar yüklemesine olanak tanır. Bu da cihazların işlevselliğini bozabilir veya onları saldırganların kontrolüne geçirebilir.

5.10. Kimlik Avı (Phishing) Saldırıları

Kimlik avı saldırıları, kullanıcıların hassas bilgilerini (parolalar, kredi kartı bilgileri vb.) çalmak amacıyla sahte e-postalar veya web siteleri kullanılarak gerçekleştirilir. IoT cihazlarının yönetimi genellikle kullanıcıların bu tür bilgilerle oturum açmasını gerektirdiğinden, kimlik avı saldırıları IoT cihazlarına yönelik ciddi bir tehdit oluşturur. Kullanıcıların bu tür saldırılara karşı bilinçlendirilmesi ve güvenlik önlemlerinin alınması önemlidir.

5.11. Fiziksel Saldırılar

IoT cihazları, fiziksel olarak erişilebilen yerlerde kullanıldığında, fiziksel saldırılara karşı da savunmasızdır. Saldırganlar, cihazların fiziksel bileşenlerine erişerek veri çalabilir, cihazları manipüle edebilir veya işlevsiz hale getirebilir. Bu tür saldırılar, özellikle kritik altyapılarda kullanılan IoT cihazları için büyük bir tehdit oluşturur.

5.12. Zayıf Parolalar ve Kimlik Doğrulama Açıkları

IoT cihazlarının büyük bir kısmı, varsayılan veya zayıf parolalarla korunur. Bu durum, saldırganların cihazlara kolayca erişmesine olanak tanır. Güçlü parolalar kullanılması ve çok faktörlü kimlik doğrulama yöntemlerinin uygulanması, bu tür saldırılara karşı etkili bir savunma sağlayabilir.

5.13. Ransomware Saldırıları

Ransomware, cihazlardaki verilere erişimi engelleyerek veya verileri şifreleyerek, kullanıcıdan fidye talep eden kötü amaçlı yazılımlardır. IoT cihazları, bu tür saldırılar için potansiyel hedefler arasında yer alır. Özellikle sağlık sektöründe

kullanılan IoT cihazları, ransomware saldırılarının hedefi haline gelebilir, çünkü bu cihazların kesintisiz çalışması hayati önem taşır.

5.14. Güvenlik Açıkları ve Güncellemeler

IoT cihazlarının yazılımlarında bulunan güvenlik açıkları, saldırganlar tarafından sıklıkla hedef alınır. Bu açıklar, cihazların işlevselliğini bozabilir veya saldırganların cihazları kontrol etmesine olanak tanır. Güvenlik açıklarının düzenli olarak yamalanması ve cihazların yazılımlarının güncel tutulması, bu tür saldırılara karşı etkili bir önlem olabilir.

ALTINCI BÖLÜM
TESPİT VE ÖNLEME STRATEJİLERİ

6.1. İzinsiz Giriş Tespit Sistemleri

İzinsiz Giriş Tespit Sistemleri (Intrusion Detection Systems - IDS), ağ güvenliği için kritik öneme sahip araçlardır. Bu sistemler, RPL (Routing Protocol for Low-Power and Lossy Networks) gibi özellikle düşük güç tüketimli ve kayıp oranı yüksek ağlar için tasarlanmış ağlarda, potansiyel tehditleri ve anormal davranışları izleyerek önemli bir savunma hattı oluşturur. RPL ağları, genellikle çevresel izleme, sağlık uygulamaları ve akıllı şehirler gibi kritik uygulamalar için kullanıldığından, bu tür ağların güvenliğini sağlamak büyük önem taşır.

IDS'ler, ağ trafiğini sürekli olarak analiz eder ve ağdaki olağandışı veya şüpheli davranışları saptadığında uyarı verir. Bu sistemler, hem bilinen tehdit imzalarını hem de davranışsal anomalileri tespit edebilen çeşitli teknikler kullanır. Bilinen tehdit imzaları, daha önce tanımlanmış ve veritabanında saklanan saldırı kalıplarına dayanır. Davranışsal tespit ise, ağın normal işleyişinden sapmaları analiz ederek, herhangi bir olağandışı aktiviteyi algılamaya çalışır.

RPL ağlarında IDS kullanımı, birkaç sebepten dolayı kritik önem taşır:

Veri Bütünlüğü ve Gizlilik: RPL ağları genellikle hassas verileri işler. Bu verilerin bütünlüğünün ve gizliliğinin korunması gerekir. IDS, bu veriler üzerinde gerçekleşebilecek herhangi bir izinsiz erişim veya manipülasyon girişimini tespit edebilir.

Ağ Performansı: RPL ağları düşük güç ve kapasite ile çalıştığı için, ağ performansını düşürebilecek herhangi bir saldırı veya anormal davranış, sistem üzerinde ciddi etkilere sahip olabilir. IDS, bu tür davranışları erkenden tespit ederek, sistem kaynaklarının korunmasına yardımcı olur.

Ağ Sağlamlığı: RPL ağları, genellikle zorlu çevresel koşullarda çalışır. Bu ağlar üzerindeki saldırılar, ağın sağlamlığını tehlikeye atabilir. IDS, ağ sağlamlığını tehdit edebilecek saldırıları ve ağ yapılandırmasını bozabilecek her türlü girişimi tespit etme kapasitesine sahiptir.

IDS'lerin etkinliği, kullanılan algılama yöntemlerine ve sistemin sürekli güncellenmesine bağlıdır. Saldırı vektörleri sürekli evrildiği için, IDS sistemlerinin tehdit imzaları düzenli olarak güncellenmelidir. Ayrıca, yanlış pozitifleri (yanlış alarmlar) minimize etmek ve gerçek tehditleri doğru bir şekilde ayırt edebilmek için sistemlerin doğruluğunu artırmak önemlidir.

Etkili bir IDS kurulumu, ağın ihtiyaçlarına ve tehdit modeline uygun olarak tasarlanmalıdır. Örneğin, bir sağlık izleme sisteminde veri gizliliği, bir çevresel izleme sisteminde ise veri bütünlüğü daha fazla önem taşıyabilir. Bu nedenle, her iki durum için de IDS ayarlarının ve politikalarının özelleştirilmesi gerekir.

Sonuç olarak, RPL gibi özel ağlarda IDS kullanımı, ağ güvenliğini sağlamanın yanı sıra, ağın etkin ve verimli bir şekilde çalışmasını da destekler. Bu sistemler, ağ üzerindeki olağandışı davranışları sürekli izleyerek, olası siber tehditlere karşı proaktif bir savunma sunar. Bu savunma, ağın ve üzerinde taşınan verilerin korunması için hayati önem taşır.

6.2. Gerçek zamanlı anomali tespiti

Gerçek zamanlı anomali tespit sistemleri, ağ güvenliği alanında giderek daha fazla önem kazanmaktadır. Bu sistemler, ağ trafiğinin sürekli izlenmesi ve herhangi bir anormalliğin hızla tespit edilmesi prensibine dayanır. Anomali tespit sistemleri, özellikle büyük ve karmaşık ağ yapılarında, güvenlik ihlallerini ve diğer zararlı faaliyetleri erken aşamada saptayarak, olası zararların önüne geçmek için kritik bir role sahiptir.

Bu sistemler, ağ üzerindeki trafik akışını analiz ederek, normal operasyonlardan sapma gösteren davranışları belirlemek için gelişmiş algoritmalar ve makine öğrenimi tekniklerini kullanır. Anomali tespit süreci, genellikle iki ana kategori altında incelenebilir: istatistiksel anomaliler ve davranışsal anomaliler.

6.2.1. İstatistiksel Anomaliler:

İstatistiksel anomali tespiti, ağ trafiğindeki istatistiksel örüntülerin sürekli olarak analiz edilmesiyle gerçekleşir. Bu yaklaşım, normal durumda gözlemlenen trafik örüntülerinin matematiksel bir modelini oluşturur ve gerçek zamanlı trafik verilerini bu modelle karşılaştırır. Ölçümler arasındaki önemli sapmalar, potansiyel bir anomali

olarak değerlendirilir. Bu tür sapmalar, DDoS saldırıları gibi aşırı trafik yüklenmesi veya ağ üzerindeki beklenmedik sessizlikler gibi durumları içerebilir.

6.2.2. Davranışsal Anomaliler:

Davranışsal anomali tespiti, ağ üzerindeki cihazların veya kullanıcıların davranışlarını analiz eder. Bu yaklaşım, her bir ağ elemanının davranışını öğrenir ve bu davranışlara dayalı bir profil oluşturur. Herhangi bir cihazın veya kullanıcının davranışı, oluşturulan bu profilin dışına çıktığında, sistem bir anomali olduğunu algılar. Örneğin, bir kullanıcının normalde erişmediği hassas verilere birden fazla erişim denemesi yapması, bir davranışsal anomali olarak kabul edilebilir.

Gerçek zamanlı anomali tespit sistemlerinin etkinliği, kullanılan algoritmalara ve veri işleme kapasitesine bağlıdır. Makine öğrenimi, bu sistemlerin temel taşıdır ve genellikle iki yöntem kullanılır:

6.2.2.1. Gözetimli Öğrenme:

Gözetimli öğrenme modelleri, önceden etiketlenmiş veri setleri kullanarak eğitilir. Bu modeller, normal ve anormal trafik arasındaki farkları öğrenir ve yeni verileri bu kategorilere göre sınıflandırır. Gözetimli öğrenme, bilinen saldırı türlerini tespit etmede oldukça etkilidir, ancak daha önce karşılaşılmamış saldırı türlerini tespit etmede sınırlı olabilir.

6.2.2.2. Gözetsiz Öğrenme:

Gözetsiz öğrenme, etiketlenmemiş veri setleri üzerinde çalışır ve verilerdeki doğal kümelenmeleri veya örüntüleri keşfetmeye çalışır. Bu yöntem, bilinmeyen veya değişen saldırı vektörlerini tespit etme potansiyeline sahiptir çünkü spesifik önceden tanımlanmış kategorilere dayanmaz.

Gerçek zamanlı anomali tespit sistemleri, sürekli veri akışı içinde hızlı ve etkin bir şekilde çalışacak şekilde tasarlanmıştır. Bu sistemler, ağ güvenliği için proaktif bir savunma hattı sağlar ve potansiyel tehditlere karşı hızla müdahale edilmesine olanak tanır. Ancak, yanlış pozitiflerin (yanlış alarmlar) ve yanlış negatiflerin (tehditlerin gözden kaçması) minimizasyonu, bu sistemlerin etkinliği için kritik öneme sahiptir. Bu nedenle, algoritmaların sürekli olarak güncellenmesi ve iyileştirilmesi gerekmektedir.

6.3. Güvenli Yönlendirme Protokolleri

Güvenli yönlendirme protokolleri, ağların hem yapısal hem de işlevsel güvenliğini artırmak için kritik öneme sahiptir. Özellikle RPL (Routing Protocol for Low-Power and Lossy Networks) gibi düşük güç tüketimli ve yüksek paket kaybı riski taşıyan ağlar için tasarlanmış protokollerde, güvenlik mekanizmalarının entegrasyonu, ağın sağlamlığını ve verimliliğini doğrudan etkiler. Bu tür güvenli yönlendirme protokolleri, ağ trafiğinin şifrelenmesi, güvenilir düğümler arasında güvenli iletişim kanallarının oluşturulması ve potansiyel olarak zararlı olan sahtekar düğümlerin izolasyonu gibi çeşitli güvenlik önlemlerini içerir.

6.3.1. Ağ Trafiğinin Şifrelenmesi

Ağ trafiğinin şifrelenmesi, verilerin izinsiz erişim ve manipülasyona karşı korunmasında temel bir yöntemdir. Veriler, kaynak düğümden hedef düğüme iletilirken, çeşitli şifreleme algoritmaları kullanılarak güvenli bir şekilde kodlanır. Bu işlem, verilerin üçüncü taraflar tarafından okunmasını veya değiştirilmesini önemli ölçüde zorlaştırır. Özellikle, açık ağlarda veri iletimi sırasında, şifreleme, veri bütünlüğü ve gizliliğin korunmasında kritik bir rol oynar.

6.3.2. Güvenilir Düğümler Arasında Güvenli Kanalların Oluşturulması

Güvenli yönlendirme protokolleri, ağ içindeki güvenilir düğümler arasında özel iletişim kanalları kurarak, bu düğümlerin birbirleriyle güvenli bir şekilde iletişim kurmalarını sağlar. Bu kanallar genellikle, ileri düzey kimlik doğrulama mekanizmaları ve şifreleme protokolleri ile desteklenir. Bu yaklaşım, ağ içindeki güvenilir düğümlerin kimliklerinin doğrulanmasını ve veri iletimi sırasında güvenliğin sağlanmasını mümkün kılar.

6.3.3. Sahtekâr Düğümlerin İzolasyonu

Ağa sızma girişiminde bulunan veya ağ operasyonlarını bozmak için tasarlanmış zararlı düğümlerin tespit edilmesi ve izole edilmesi, ağın bütünlüğünü korumak için önemlidir. Güvenli yönlendirme protokolleri, davranış analizi, itibar sistemleri ve sürekli izleme gibi teknikler kullanarak, bu tür sahtekar düğümleri etkili bir şekilde tespit edebilir. Tespit edilen sahtekar düğümler, ağdan izole edilerek, diğer düğümlerin güvenliğinin ve ağın genel performansının korunması sağlanır.

6.3.4. Uygulama ve Zorluklar

Güvenli yönlendirme protokollerinin uygulanması, teknik ve operasyonel bazı zorlukları beraberinde getirir. Öncelikle, güvenlik önlemlerinin ağın performansı üzerinde bir yük oluşturmaması gerekmektedir, özellikle düşük güç ve kaynak kısıtlamalarına sahip ağlar için bu kritik bir konudur. Ayrıca, güvenlik önlemlerinin sürekli olarak güncellenmesi ve yeni tehditlere karşı adaptasyonunun sağlanması gerekir.

Sonuç olarak, güvenli yönlendirme protokolleri, ağın bütünlüğünü, veri gizliliğini ve işlevsel güvenliğini sağlamada hayati rol oynar. Bu protokoller, karmaşık ağ yapılarını ve değerli veri akışlarını korumak için tasarlanmış olup, sürekli evrilen siber tehditlere karşı etkin bir savunma sunar. Ağ mühendisleri ve sistem yöneticileri için, bu protokollerin etkin bir şekilde uygulanması ve yönetilmesi, ağ güvenliğinin sürdürülebilirliği açısından büyük önem taşır.

6.4. Kimlik doğrulama ile geliştirilmiş esneklik

Kimlik doğrulama mekanizmaları, Routing Protocol for Low-Power and Lossy Networks (RPL) gibi ağların temel güvenlik altyapısını oluşturur. Bu mekanizmalar, düğümlerin birbirleriyle güvenli bir şekilde iletişim kurmasını sağlar, yetkisiz erişimi engeller ve veri bütünlüğünü korur. RPL ağlarının esnekliğini ve güvenilirliğini artırmak için kimlik doğrulama, özellikle düşük güç tüketen ve yüksek veri kaybı riski taşıyan ağlarda kritik bir öneme sahiptir.

6.4.1. Kimlik Doğrulama Mekanizmalarının Önemi

RPL, genellikle çevresel izleme, akıllı şehir uygulamaları, sağlık izleme sistemleri gibi kritik alanlarda kullanılır. Bu uygulamalar, doğru ve zamanında veri toplamanın yanı sıra veri güvenliğinin de korunmasını gerektirir. Kimlik doğrulama mekanizmaları, ağa katılmak isteyen düğümlerin öncelikle güvenilir olduklarını kanıtlamalarını gerektirir. Bu süreç, her düğümün ağdaki diğer düğümler tarafından tanınmasını ve kabul edilmesini sağlar. Böylece, yetkisiz cihazların ağa erişimi ve zararlı faaliyetleri önlenmiş olur.

6.4.2. Kimlik Doğrulama Yöntemleri

RPL ağlarında kullanılan kimlik doğrulama yöntemleri genellikle şunları içerir:

Güçlü Şifreleme Protokolleri: Veri iletimi sırasında kullanılan şifreleme protokolleri, iletişim sırasında verilerin güvenliğini sağlar. Bu protokoller, verilerin şifrelenmesi ve şifresinin çözülmesi için karmaşık anahtarlar kullanır.

Dijital İmzalar: Dijital imzalar, bir düğümün verileri göndermeden önce bu verilere eklediği, doğrulama amacı taşıyan özel kodlardır. Bu imzalar, verilerin değiştirilmeden ulaştığını garantiler ve veri bütünlüğünü sağlar.

İki Faktörlü Kimlik Doğrulama: Bazı RPL uygulamaları, özellikle hassas verilerin işlendiği durumlarda, iki faktörlü kimlik doğrulama sistemlerini kullanabilir. Bu sistemler, fiziksel bir cihazın yanı sıra bir şifre veya biyometrik veri gibi ikinci bir doğrulama katmanı gerektirir.

Sertifikalar ve Anahtar Yönetimi: Güvenli iletişim kanalları kurulurken, sertifikalar ve anahtar yönetim sistemleri büyük rol oynar. Bu sistemler, düğümlerin birbirlerini güvenilir bir şekilde tanımasını ve iletişim kurmasını sağlar.

6.4.3. Güvenlik ve Esneklik

Kimlik doğrulama mekanizmaları, RPL ağlarının esnekliğini artırır çünkü ağa katılan her düğümün güvenilirliğini garantiler. Bu, ağın genel güvenlik düzeyini yükseltir ve olası güvenlik zafiyetlerini azaltır. Ayrıca, güvenilir kimlik doğrulama süreçleri, ağın genişletilmesi ve yeni düğümlerin entegrasyonu sırasında da önemli bir rol oynar. Yeni düğümlerin güvenli bir şekilde ağa dahil edilmesi, ağın büyümesini ve gelişimini desteklerken, güvenlik standartlarının korunmasını da sağlar.

RPL gibi düşük güç tüketimli ve kayıp oranı yüksek ağlarda kimlik doğrulama mekanizmalarının uygulanması, sadece veri güvenliğini ve bütünlüğünü korumakla kalmaz, aynı zamanda ağın genel işleyişini ve esnekliğini de artırır. Bu mekanizmalar, ağın sağlam bir şekilde genişlemesine olanak tanırken, potansiyel güvenlik tehditlerine karşı koruma sağlar ve ağın uzun vadeli sürdürülebilirliğini destekler.

6.5. Güvenli Komşu Keşfi

Güvenli komşu keşfi, ağın sağlıklı ve güvenilir işleyişi için kritik bir süreçtir, özellikle kablosuz ağlar ve düşük güç tüketimli ağlar (LLNs) gibi dinamik ortamlarda bu süreç büyük önem taşır. Bu mekanizma, ağdaki düğümlerin birbirlerini güvenilir bir şekilde tanımasını ve keşfetmesini sağlayarak, düğümlerin kimliklerini doğrulamak ve sahte ya da kötü niyetli düğümleri ağdan uzak tutmak amacı taşır.

6.5.1. Güvenli Komşu Keşfinin Temel Prensipleri

Güvenli komşu keşfi, ağın her bir düğümünün diğer düğümlerle etkileşime girebilmesi için güvenilir bir yöntem sunar. Bu süreç, ağdaki her düğümün kimlik bilgilerinin doğrulanması, ağa yeni katılan düğümlerin güvenli bir şekilde tanıtılması ve ağın genel güvenlik durumunun korunmasını içerir. Güvenli keşif süreci, genellikle şu adımları takip eder:

Kimlik Doğrulama: Düğümler arasındaki ilk iletişimde, her iki tarafın kimlikleri karşılıklı olarak doğrulanır. Bu, genellikle dijital sertifikalar, kriptografik anahtarlar veya iki faktörlü doğrulama mekanizmaları kullanılarak gerçekleştirilir.

Kimlik Bilgilerinin Değişimi: Güvenilir bir bağlantı kurulduktan sonra, düğümler birbirlerine kimlik bilgilerini ve diğer güvenlikle ilgili bilgileri paylaşır. Bu bilgiler, ağın diğer düğümleri tarafından daha sonraki iletişimlerde referans olarak kullanılabilir.

İzleme ve Güncelleme: Düğümlerin ağdaki davranışları sürekli olarak izlenir ve herhangi bir anormallik veya güvensiz davranış belirlendiğinde, ilgili düğüm izole edilebilir veya ağdan çıkarılabilir. Bu, ağın bütünlüğünü korumak için elzemdir.

6.5.2. Güvenli Komşu Keşfinin Önemi

Güvenli komşu keşfi, ağ güvenliğini birkaç yönüyle destekler:

Güvenlik Zafiyetlerini Azaltma: Sahte ve zararlı düğümlerin ağa erişiminin önlenmesi, ağdaki güvenlik zafiyetlerini önemli ölçüde azaltır.

Veri Bütünlüğü ve Gizliliğinin Korunması: Güvenilir düğümler arasında sağlam kimlik doğrulama ve güvenli iletişim kanallarının kurulması, veri bütünlüğünü ve gizliliğini sağlar.

Ağın Dayanıklılığını Artırma: Ağdaki düğümlerin güvenilirliğinin sürekli olarak sağlanması, ağın genel dayanıklılığını ve esnekliğini artırır. Güvenilir düğümler üzerinden yapılan iletişim, ağın performansını ve kararlılığını olumlu yönde etkiler.

6.5.3. Uygulama Zorlukları

Güvenli komşu keşfinin uygulanması bazı zorluklar içerir. Özellikle dinamik ve geniş ağlarda, düğümlerin sürekli olarak eklenip çıkarılması, güvenlik protokollerinin uygulanmasını karmaşıklaştırabilir. Ayrıca, yüksek düzeyde güvenlik sağlamak amacıyla kullanılan şifreleme ve doğrulama teknikleri, düşük güç tüketimli ağlarda kaynak kullanımını artırabilir. Bu nedenle, güvenlik ve performans arasında dengeli bir yaklaşım benimsemek önemlidir.

Sonuç olarak, güvenli komşu keşfi, RPL gibi ağ protokollerinin güvenliğini ve işlevselliğini artıran hayati bir süreçtir. Bu süreç, ağın güvenilirliğini artırarak, ağ üzerinden yapılan iletişimin güvenliğini ve verimliliğini maksimize etmeye yardımcı olur.

6.6. Yetkisiz erişimin azaltılması

Yetkisiz erişimin azaltılması, ağ güvenliğinin temel taşlarından biridir ve bu amaçla çeşitli stratejiler ve teknikler geliştirilmiştir. Ağ güvenliği politikaları, erişim kontrol listeleri (ACL), fiziksel güvenlik önlemleri ve daha birçok yöntem, yetkisiz kullanıcıların ağ kaynaklarına erişimini engelleyerek veri ihlallerini önlemek için kullanılır. Bu yöntemlerin her biri, ağın bütünlüğünü korumak, veri sızıntılarını önlemek ve ağ üzerindeki güvenliği sağlamak için önemlidir.

6.6.1. Ağ Güvenliği Politikaları

Ağ güvenliği politikaları, organizasyonların ağ üzerinde hangi davranışların kabul edilebilir olduğunu ve hangi davranışların yasaklandığını belirleyen kurallar bütünüdür. Bu politikalar, kullanıcıların ağa erişimini, kullanıcı hesap yönetimini, veri koruma standartlarını ve ağ üzerinde izin verilen hizmetleri içerir. Etkili bir ağ güvenliği politikası, yetkisiz erişimi azaltmak için net kurallar ve prosedürler sağlar. Politikalar, ağ güvenliğinin sürekli olarak gözden geçirilmesini ve güncellenmesini de gerektirir, böylece yeni tehditlere ve teknoloji değişikliklerine karşı adapte olabilir.

6.6.2. Erişim Kontrol Listeleri (ACL)

Erişim kontrol listeleri, ağ cihazlarındaki belirli kaynaklara kimlerin erişebileceğini belirlemek için kullanılır. ACL'ler, ağ trafiğini filtreleyerek sadece yetkili kullanıcıların ve sistemlerin belirli ağ kaynaklarına erişmesine izin verir. Her giriş noktasında, paketler belirlenen kurallar setine göre kontrol edilir ve sadece uygun şartları karşılayan trafiğe izin verilir. Bu, ağın belli bölümlerine erişimi sınırlar ve yetkisiz kullanıcıların hassas bilgilere erişimini engeller.

6.6.3. Fiziksel Güvenlik Önlemleri

Fiziksel güvenlik önlemleri, ağ kaynaklarına fiziksel erişimi kısıtlamak için kritik öneme sahiptir. Bu önlemler, ağ donanımlarının kilitleme sistemleri, güvenlik kameraları, alarm sistemleri ve güvenlik personeli gibi koruyucu tedbirleri içerir. Ağ sunucuları, yönlendiriciler ve diğer kritik donanımlar genellikle kilitli ve güvenli odalarda saklanır. Ayrıca, veri merkezlerine girişler sıkı bir şekilde kontrol edilir ve yalnızca yetkili personelin erişimine izin verilir. Fiziksel güvenlik, siber güvenlikle birlikte ele alındığında, ağ kaynaklarına yetkisiz erişimin önüne geçmek için daha etkili bir koruma sağlar.

6.6.4. Kapsamlı Güvenlik Stratejisi

Yetkisiz erişimin azaltılması için kapsamlı bir güvenlik stratejisi uygulamak, ağ güvenliğini çok yönlü bir şekilde güçlendirir. Bu strateji, teknolojik önlemlerle birlikte, kullanıcı eğitimi ve bilinçlendirme programlarını da içermelidir. Kullanıcıların güvenlik politikaları, tehlikeler ve korunma yöntemleri hakkında bilgilendirilmesi, insan kaynaklı hataları azaltabilir ve güvenlik kültürünü güçlendirebilir.

Sonuç olarak, yetkisiz erişimin azaltılması, ağ güvenliği için çok yönlü bir yaklaşım gerektirir. Bu, sadece teknolojik çözümlerle değil, aynı zamanda etkili politikalar, fiziksel önlemler ve sürekli kullanıcı eğitimi ile mümkündür. Bu yöntemler birlikte uygulandığında, ağ kaynaklarına yetkisiz erişimi önemli ölçüde azaltabilir ve veri ihlallerini engelleyebilir. Bu stratejilerin sürekli olarak değerlendirilmesi ve güncellenmesi, ağın güvenliğini uzun vadede sağlamak için elzemdir.

YEDİNCİ BÖLÜM

METOT

Flood saldırıları, bir hedef sistemin hizmet vermesini engellemek amacıyla büyük miktarda veri veya istek göndermeyi içeren siber saldırı türleridir. Bu tür saldırılar, özellikle IoT (Internet of Things) cihazları ve ağları üzerinde ciddi etkiler yaratabilir. Flood saldırılarının neden diğer saldırı türlerine göre daha tehlikeli olduğu ve sistem üzerindeki etkileri, bu yazıda detaylı bir şekilde ele alınacaktır.

7.1. Flood Saldırılarının Seçilme Nedenleri

Flood saldırıları, birçok siber saldırı türü arasında seçilmesinin birkaç ana nedeni vardır. Savunma bakış açısıyla bu nedenler aşağıda belirtilmiştir:

1. Kolay Erişilebilirlik ve Uygulama Basitliği: Flood saldırıları, genellikle düşük teknik bilgi gerektiren ve basit araçlarla gerçekleştirilebilen saldırı türleridir. İnternette bu tür saldırıları gerçekleştirmek için birçok ücretsiz ve ücretli araç bulunmaktadır. Bu durum, saldırganların flood saldırılarını tercih etmelerini kolaylaştırır ve sık sık kullanılmasına neden olur.

2. Etkili ve Geniş Kapsamlı Sonuçlar: Flood saldırıları, hedef sistemin kapasitesini aşarak hizmet dışı kalmasına neden olur. Bu tür saldırılar, kısa sürede büyük etki yaratma potansiyeline sahiptir ve hedeflenen sistemlerin performansını ciddi şekilde düşürebilir. Özellikle kritik altyapılar veya yoğun trafikli web siteleri gibi yüksek değere sahip hedefler üzerinde büyük etki yaratırlar.

3. Zayıf Güvenlik Önlemleri: Birçok IoT cihazı ve ağı, yeterli güvenlik önlemlerine sahip değildir. Bu durum, flood saldırılarının başarı oranını artırır. Özellikle varsayılan şifreler ve güncellenmeyen yazılımlar, saldırganların bu tür saldırıları gerçekleştirmelerini kolaylaştırır.

4. Tespit ve Müdahale Zorlukları: Flood saldırıları sırasında gönderilen veri veya istekler, genellikle normal trafik olarak algılanabilir. Bu durum, saldırıların tespit edilmesini ve saldırılara müdahale edilmesini zorlaştırır. Özellikle gelişmiş saldırılar, sahte IP adresleri kullanarak izlerini gizleyebilir ve saldırının kaynağını tespit etmek zorlaşır.

5. Karmaşıklık ve Kaynak Gereksinimi: Flood saldırıları, yüksek bant genişliği ve işlem gücü gerektirir. Saldırganlar, ele geçirdikleri botnetler aracılığıyla bu tür saldırıları gerçekleştirebilirler. Botnetler, birçok cihazın aynı anda koordineli bir şekilde saldırı gerçekleştirmesini sağlar, bu da saldırının etkisini artırır.

7.2. Flood Saldırılarının Tehlikesi

Flood saldırılarının diğer siber saldırı türlerine göre daha tehlikeli olmasının birkaç ana nedeni vardır:

1. Ağ Tıkanıklığı: Flood saldırıları, ağ trafiğini aşırı derecede artırarak ağın tıkanmasına neden olur. Bu durum, hizmetlerin yavaşlamasına veya tamamen durmasına yol açar. Özellikle kritik hizmetler veren sistemler için bu durum kabul edilemez sonuçlar doğurur.

2. Hizmet Kesintileri: Hedef sistemin aşırı yüklenmesi sonucu, hizmetlerde kesintiler yaşanır. Bu kesintiler, kullanıcı memnuniyetsizliğine ve iş kayıplarına neden olabilir. Özellikle e-ticaret siteleri veya bankacılık sistemleri gibi kesintisiz hizmet vermesi gereken sistemler için bu durum büyük bir risk oluşturur.

3. Veri Kaybı ve Bütünlük Sorunları: Flood saldırıları sırasında iletilen veri paketleri kaybolabilir veya bozulabilir. Bu durum, veri bütünlüğünün bozulmasına ve önemli bilgilerin kaybolmasına neden olabilir. Ayrıca, bu tür saldırılar sırasında yapılan veri yedeklemeleri de başarısız olabilir.

4. Güvenlik Zafiyetlerinin Ortaya Çıkması: Flood saldırıları, hedef sistemin mevcut güvenlik açıklarını ortaya çıkarabilir. Saldırı sırasında sistemin aşırı yüklenmesi, güvenlik mekanizmalarının yetersiz kalmasına ve saldırganların sistemde daha fazla açık bulmasına yol açabilir.

5. Maliyet Artışı: Flood saldırıları, hedef sistemin kaynaklarını tüketerek maliyetlerin artmasına neden olur. Özellikle bulut tabanlı hizmetlerde, aşırı trafik ve kaynak kullanımı ek maliyetler doğurabilir. Bu durum, hem işletmelerin hem de bireysel kullanıcıların bütçesini zorlayabilir.

7.3. Flood Saldırılarının Sistem Üzerindeki Etkileri

Flood saldırılarının hedef sistem üzerindeki etkileri geniş kapsamlı ve ciddi olabilir. Bu etkiler aşağıdaki gibi özetlenebilir:

1. Performans Düşüşü: Flood saldırıları, sistem kaynaklarını tüketerek performansın düşmesine neden olur. Bu durum, sistemin normal işlemlerini gerçekleştirmesini zorlaştırır ve kullanıcı deneyimini olumsuz etkiler.

2. Hizmet Kesintisi: Hedef sistemin aşırı yüklenmesi sonucu hizmetlerde kesintiler yaşanabilir. Bu kesintiler, kullanıcıların hizmetlere erişimini engeller ve iş sürekliliğini tehdit eder.

3. Veri Bütünlüğünün Bozulması: Saldırı sırasında iletilen veri paketlerinin kaybolması veya bozulması, veri bütünlüğünün bozulmasına yol açar. Bu durum, sistemin güvenilirliğini ve veri doğruluğunu tehlikeye atar.

4. Ağ Trafiğinin Artması: Flood saldırıları, ağ trafiğini aşırı derecede artırarak ağın tıkanmasına neden olur. Bu durum, diğer sistemlerin ve hizmetlerin de etkilenmesine yol açar.

5. Kaynak Tüketimi ve Maliyet Artışı: Flood saldırıları, hedef sistemin kaynaklarını tüketerek maliyetlerin artmasına neden olur. Bu durum, hem işletmelerin hem de bireysel kullanıcıların bütçesini zorlayabilir.

Flood saldırıları, özellikle IoT cihazları ve ağları için ciddi bir tehdit oluşturan siber saldırı türleridir. Bu saldırıların kolay uygulanabilir olması, geniş kapsamlı etkiler yaratması ve tespit edilmesinin zor olması, onları diğer saldırı türlerine göre daha tehlikeli hale getirir. Flood saldırılarının etkilerini minimize etmek ve bu tür saldırılara karşı savunma sağlamak için güçlü güvenlik önlemlerinin alınması gerekmektedir. Bu önlemler arasında ağ trafiğinin izlenmesi, güçlü kimlik doğrulama yöntemlerinin kullanılması ve düzenli güvenlik güncellemelerinin yapılması yer almaktadır. Bu şekilde, flood saldırılarının hedef sistemler üzerindeki olumsuz etkileri azaltılabilir ve sistemlerin güvenliği artırılabilir.

Bu projede, IoT teknolojilerini hedef alan siber saldırıların saldırgan sayılarına göre aldıkları etkilerin değişimleri kıyaslanmıştır.

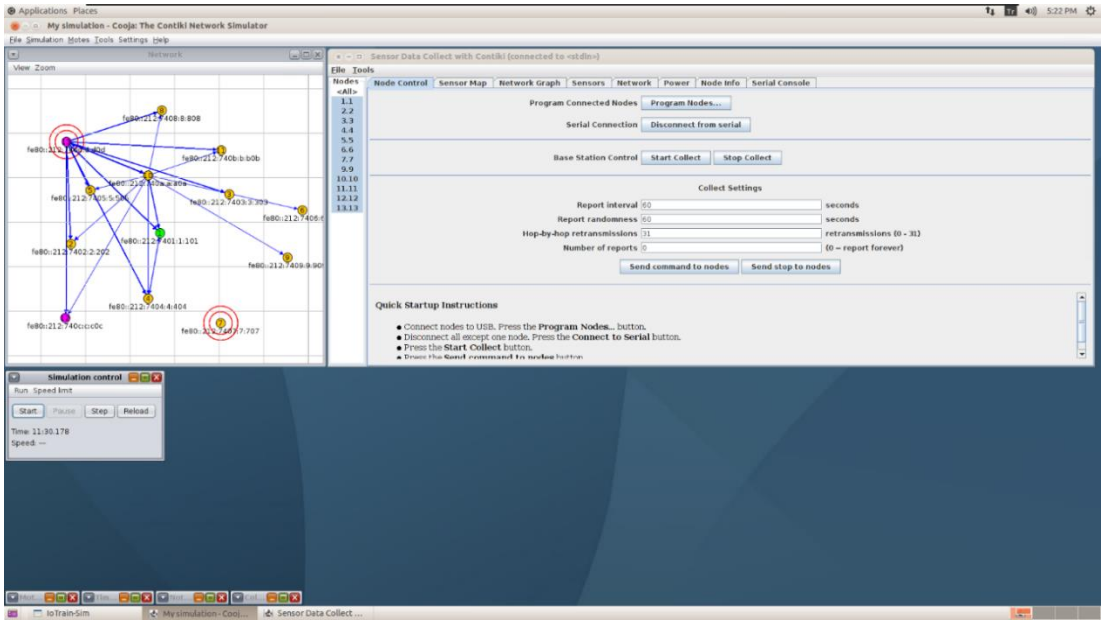
Sürekli olarak ağdaki değişiklikler incelenmiştir. Saldırılar ve analizler yapılırken Contiki işletim sistemi üzerinde çalışan Cooja Simülatörü kullanılmıştır.

7.4. Contiki İşletim Sistemi

Contiki OS, Adam Dunkels tarafından 2002 yılında Linux tabanlı olarak geliştirilmiş açık kaynak kodlu bir işletim sistemidir. (Dunkels et al., 2004) Düşük güç ve düşük maliyetli mikro denetleyicilerin (skymote, wismote) internete açılmasını sağlamaktadır. Nesnelerin interneti ise dünya çapında tanımlanabilen fiziksel objelerin ve bunların internet ile birleşiminin bir ağıdır. Nesnelerin interneti ağını oluşturabilmek için birçok teknoloji altyapısı kullanılmaktadır (Wi-Fi, Bluetooth, ZigBee, RFID, Hücresel Veri, Ethernet)(Padmaja et al., 2017).

Bu teknolojiler ise fiziksel bir dünya üzerinde makineden makineye (M2M) ya da makineden insana (H2M) iletişime olanak sağlayan sanal bir dünya oluşturur. Kablosuz sensör ağları (WSN) ise düğümlerin birbirleriyle otonom şekilde iletişim kurduğu, fiziksel ve sanal dünyaya bağlanabildiği akıllı sistemlerdir.

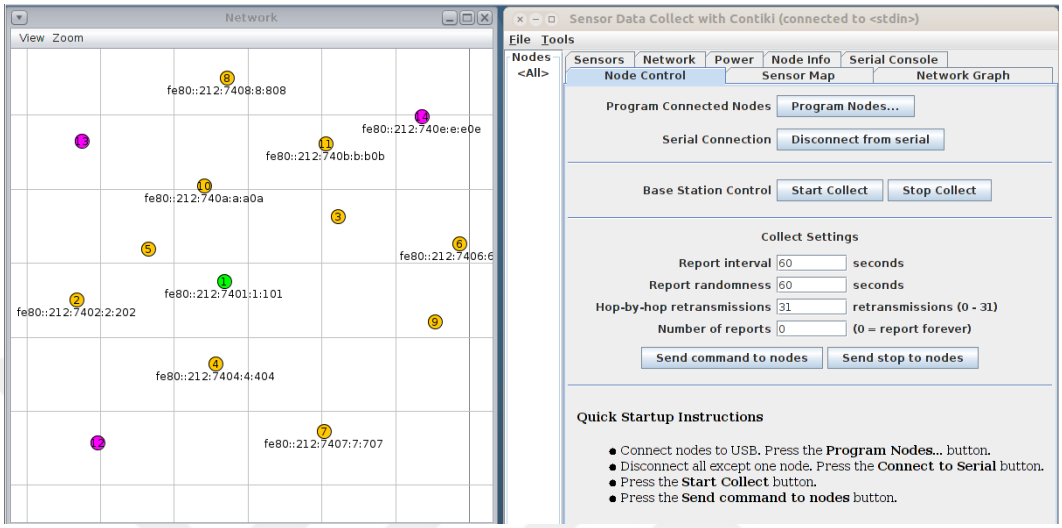
7.4.1. Yetkisiz erişimin azaltılması



Şekil 1 Contiki OS üzerinde çalışan Cooja Simülatörü

Contiki ile dağıtılan çapraz katman java tabanlı kablosuz sensör ağı simülatörü olarak tanımlanabilir. Fizikselden uygulama katmanına kadar farklı seviyelerin

simülasyonuna izin verir ve ayrıca bir dizi sensör düğümünün donanımının öykünmesine izin verir. Cooja simülatörü sayesinde contiki işletim sisteminde geliştirilen bir uygulamanın simülasyonu yapılabilir, test edilebilir.



Şekil 2 Cooja Simülatör Menüleri

7.5. Saldırı Aşamaları

Bu bölümde IoT cihazlarına karşı düzenlenen saldırılardan biri olan Flood Attack gerçekleştirilmiş olup sistem üzerindeki etkisi analizlerle tartışılmıştır.

7.5.1. IOT Saldırısı Adımları IOT

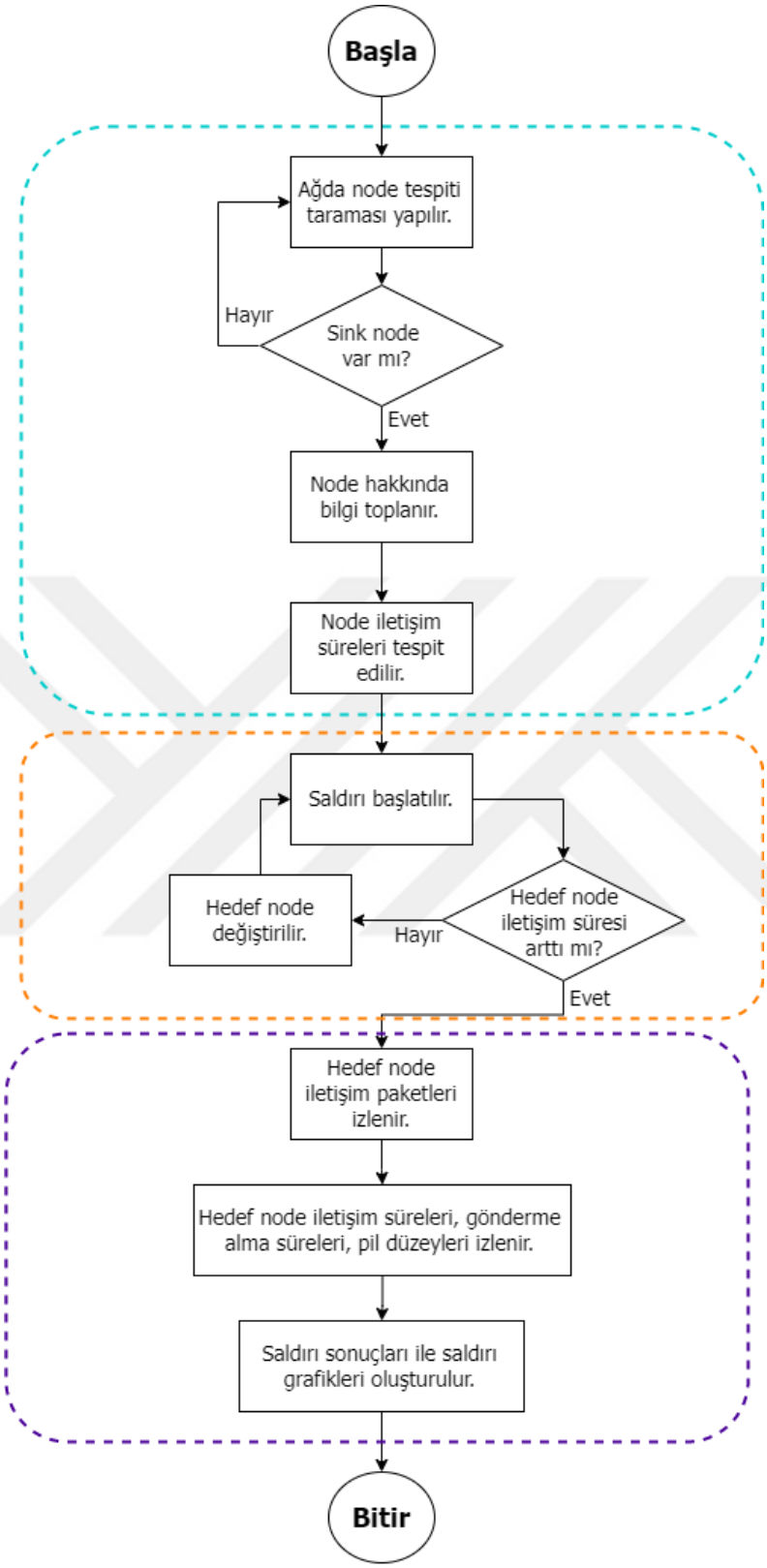
IoT saldırısı aşağıdaki aşamalar ile gerçekleştirilmiştir. Bu saldırı RPL tabanlı saldırıların analizini incelemek için tasarlanmıştır.

• Contiki OS üzerinde Cooja simülatör aracılığıyla nesnelerin interneti (IoT) cihazlarının ağ trafiğinin oluşturulması.

• Oluşturulan topolojilerde toplamda 12, 13 ve 14 node kullanılmıştır. Saldırgan sayıları 1, 2 ve 3 olarak değiştirilmiş olup saldırı altında olan 1 node kullanılmıştır. Geriye kalanlar ise standart node olarak tasarlanmıştır.

• Flood Attack saldırısıyla RPL tabanlı bir saldırı simüle edilmiştir.

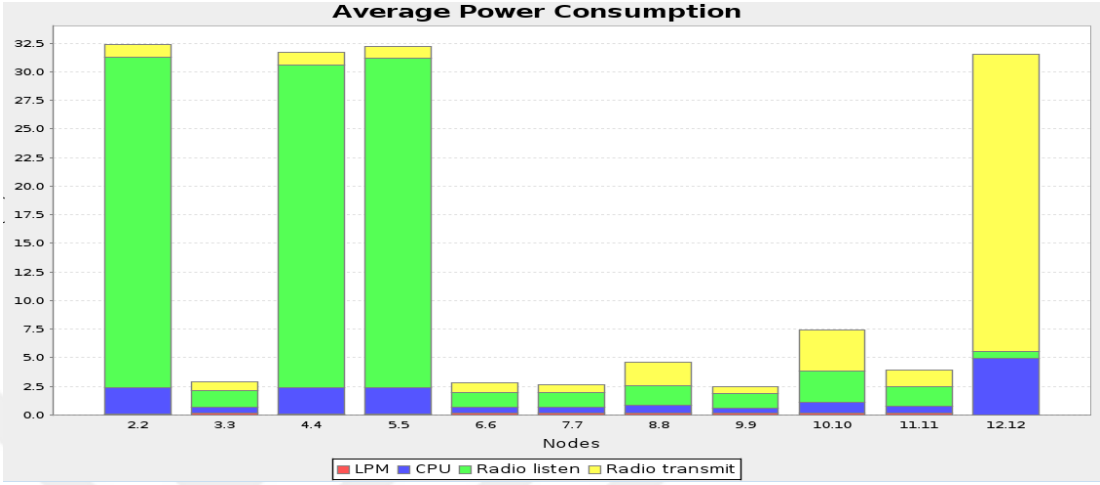
• Test Anything Protocol (TAP) tekniklerini kullanarak ağ trafiğini yakalanmıştır.



Şekil 3 Uygulama algoritması

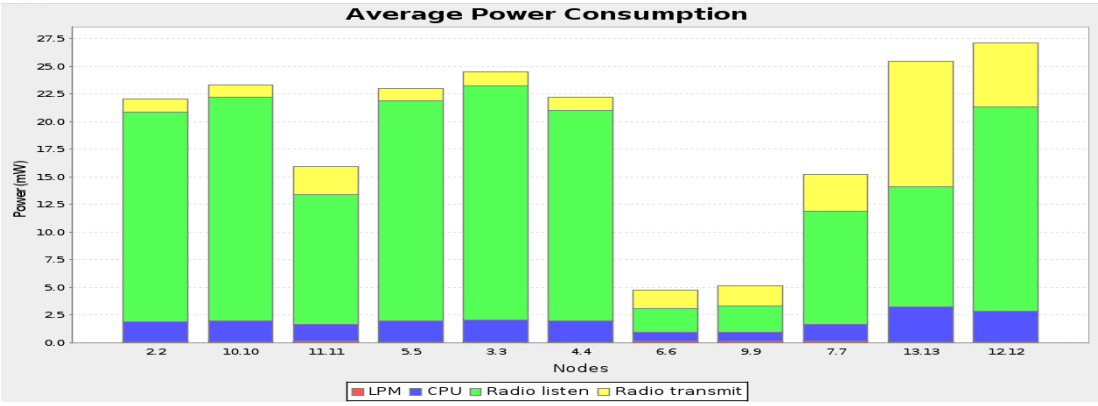
7.6. IOT Saldırısı Analizi

IOT ağlarının çalışması tamamen güç tüketimi ile bağlantılıdır. Bu bağlamda ağın sürekliliğini sağlamakta ki temel etken güç tüketimini uygun seviyede tutmak olacaktır.



Şekil 4 Saldırı Öncesi Durum

Saldırıdan önceki değerlere kıyasla Flood saldırısı sırasındaki güç tüketim değerleri yükseltilir. Ayrıca, yeşil alanda gösterildiği üzere dinleme trafiği de saldırı altındaki makinelerde daha yüksektir. Mavi alanda CPU tüketimi saldırgan makinede daha fazla olmaktadır.



Şekil 5 Saldırı Sırasındaki Durum

Saldırgan sayısının arttırılması durumunda saldırıya maruz kalan makinelerdeki dinleme trafiği saldırganlara göre yüksektir. Saldırganların ise iletme trafikleri

dinleme trafiklerine göre daha yüksektir. Aynı şekilde saldırganlar daha fazla CPU güç tüketimine sahiptir.

Şekil 4 ve 5 bir IoT sistemine yapılan saldırının cihazlar üzerindeki güç tüketimine etkilerini göstermektedir. İlk grafik saldırı olmadan önceki durumu, ikinci grafik ise saldırı sırasındaki durumu temsil etmektedir. Analizim aşağıdaki gibi:

LPM (Low Power Mode): İki grafikte de, çoğu düğümün (node) büyük bir çoğunluğunda güç tüketiminin büyük oranda düşük güç modundan (LPM) kaynaklandığı görülüyor. Ancak, saldırı durumunda bazı düğümlerde LPM tüketimi azalırken, bazılarında artmış. Bu, saldırının düğümlerin uyku moduna geçişini etkileyebileceğini gösteriyor.

CPU Kullanımı: CPU tüketimi, çoğu düğümde saldırı durumunda artmıştır. Bu, saldırı sırasında düğümlerin daha fazla işlem yapmak zorunda kaldığını ve bu nedenle daha fazla enerji tükettiğini gösterir. Özellikle, 12.12 ve 13.13 düğümlerinde CPU kullanımı önemli ölçüde artmıştır.

Radyo Dinleme ve Yayın: Radyo dinleme ve yayın tüketimi, saldırı sırasında çoğu düğümde artmıştır. Bu, saldırının ağ trafiğini artırdığını ve dolayısıyla düğümlerin daha fazla radyo işlemi yapmak zorunda kaldığını gösterir. 10.10 ve 12.12 düğümleri, bu artışın en belirgin olduğu yerlerden bazılarıdır.

Toplam Güç Tüketimi: Saldırı durumunda, düğümlerin toplam güç tüketimi genellikle artmıştır. Özellikle, düğüm 12.12'deki toplam güç tüketimi önemli ölçüde yükselmiş, bu da bu düğümün saldırıdan en fazla etkilenen düğüm olduğunu gösteriyor.

Sonuç olarak, saldırının IoT cihazlarının güç tüketimini artırdığı ve cihazların performansını olumsuz yönde etkilediği görülmektedir. Bu, IoT güvenlik önlemlerinin önemini ve cihazların siber saldırılara karşı daha dayanıklı hale getirilmesi gerektiğini vurgulamaktadır.

SONUÇLAR VE ÖNERİLER

Bu çalışma, IoT cihazlarına karşı gerçekleştirilen flood saldırılarının etkilerini azaltmak konusunda literatüre önemli katkılar sağlamaktadır. IoT cihazlarının güvenlik açıkları ve sınırlı enerji kaynakları, bu sistemlerin sürdürülebilir ve güvenilir bir şekilde çalışmasını zorlaştırmaktadır. Çalışmada, RPL tabanlı ağlarda flood saldırılarının enerji tüketimi üzerindeki etkileri detaylı bir şekilde analiz edilmiştir. Flood saldırıları, ağ üzerindeki veri trafiğini artırarak cihazların enerji tüketimini önemli ölçüde artırmaktadır. Bu durum, özellikle batarya ile çalışan IoT cihazlarının ömrünü kısaltmakta ve ağın genel performansını olumsuz yönde etkilemektedir.

Araştırma, tekli ve çoklu saldırgan senaryolarında yapılan simülasyonlar ve gerçek zamanlı analizlerle, flood saldırılarının IoT cihazlarının enerji tüketimi üzerindeki spesifik etkilerini ortaya koymaktadır. Çalışmada, saldırı sırasında cihazların düşük güç modunda geçirdiği sürenin azaldığı, CPU kullanımının ve radyo dinleme yayın faaliyetlerinin arttığı gözlemlenmiştir. Bu bulgular, flood saldırılarının cihazların enerji verimliliğini ciddi şekilde düşürdüğünü ve sistem performansını olumsuz etkilediğini göstermektedir.

Literatüre yapılan bu katkılar, IoT ağlarının enerji verimliliğini optimize etmek ve flood saldırılarına karşı daha dirençli hale getirmek için yeni stratejilerin geliştirilmesine olanak tanımaktadır. Çalışma, enerji verimliliğini artıran uyku modu ve ağ yönetimi stratejilerinin yanı sıra, saldırı tespiti ve önleme mekanizmalarının etkinliğini vurgulamaktadır. Bu bağlamda, IoT cihazlarının güvenliğini sağlamak ve enerji tüketimini minimize etmek için geliştirilen yeni algoritmalar ve teknikler, IoT sistemlerinin sürdürülebilirliğini ve güvenilirliğini artırmakta önemli rol oynamaktadır. Böylece, IoT teknolojilerinin daha geniş uygulama alanlarında güvenli ve verimli bir şekilde kullanılmasına katkıda bulunulmaktadır.

Bu çalışma, IoT cihazlarını hedef alan yaygın flooding saldırılarının etkilerini analiz etmeyi amaçlamıştır. Çalışma, özellikle tekli ve çoklu saldırgan senaryolarında ağ trafiği ve cihaz performansını incelemiştir. Elde edilen sonuçlar, saldırıların IoT sistemleri üzerindeki ciddi etkilerini ve güvenlik açıklarını gözler önüne sermiştir.

Saldırı sırasında IoT cihazlarının çoğunda düşük güç modu kullanımı önemli ölçüde azalmış, buna karşın CPU kullanımı artmıştır. Bu durum, cihazların saldırıya yanıt olarak daha fazla işlem yapmak zorunda kaldığını göstermektedir.

Flooding saldırıları, radyo dinleme ve yayın faaliyetlerinde belirgin bir artışa neden olmuştur. Bu artış, ağ trafiğinin yoğunlaştığını ve cihazların daha fazla enerji harcadığını ortaya koymaktadır.

Saldırı sırasında düğümlerin toplam güç tüketimi artmıştır. Özellikle bazı düğümlerde bu artış daha belirgin olmuştur. Bu bulgu, saldırıların enerji verimliliği üzerinde olumsuz etkileri olduğunu ve cihazların batarya ömrünü kısalttığını göstermektedir.

Flooding saldırıları, ağın genel performansını düşürmüş ve paket kaybı oranlarını artırmıştır. Bu durum, IoT sistemlerinin güvenilirliğini ve verimliliğini tehlikeye atmaktadır.

RPL protokolünün yapısal zafiyetlerinden kaynaklanan güvenlik açıkları, saldırganların ağ trafiğini manipüle etmesine ve cihazların normal işleyişini bozmasına olanak tanımıştır. Bu, RPL tabanlı ağların siber saldırılara karşı savunmasız olduğunu göstermektedir.

Çalışmanın bulgularına dayanarak, IoT sistemlerinin güvenliğini artırmak ve saldırılara karşı daha dirençli hale getirmek için aşağıdaki önerilerde bulunulmuştur:

Gelişmiş Güvenlik Protokolleri: IoT cihazları ve ağları için daha gelişmiş ve güçlü güvenlik protokolleri geliştirilmelidir. Özellikle, RPL protokolüne yönelik güvenlik iyileştirmeleri yapılmalı ve potansiyel saldırı vektörlerine karşı koruma sağlayacak ek mekanizmalar entegre edilmelidir.

Gerçek Zamanlı Anomali Tespiti: Ağ trafiğini sürekli izleyen ve anormal davranışları tespit eden gerçek zamanlı anomali tespit sistemleri kullanılmalıdır. Bu sistemler, olası saldırıları erken aşamada tespit ederek müdahale edilmesini sağlayacaktır.

Enerji Verimliliği Optimizasyonu: IoT cihazlarının enerji verimliliğini artırmak için uyarlanabilir güç yönetimi stratejileri geliştirilmelidir. Cihazların düşük güç

modunda daha uzun süre kalmasını sağlayacak algoritmalar ve teknikler uygulanmalıdır.

Ağ Trafiğinin Şifrelenmesi: IoT ağlarında veri güvenliğini sağlamak için tüm ağ trafiği şifrelenmelidir. Bu, veri iletimini güvenli hale getirerek, izinsiz erişim ve veri manipülasyonunu önleyecektir.

Kimlik Doğrulama ve Yetkilendirme: Cihazların ve kullanıcıların kimlik doğrulama süreçleri sıkılaştırılmalıdır. Güvenilir kimlik doğrulama mekanizmaları ve yetkilendirme protokolleri, yalnızca yetkili cihaz ve kullanıcıların ağa erişimini sağlayacaktır.

Eğitim ve Farkındalık: IoT sistemlerinin kullanımı ve yönetimi konusunda, kullanıcılar ve ağ yöneticileri için eğitim programları düzenlenmelidir. Kullanıcı farkındalığı, güvenlik açıklarının azaltılmasına ve siber saldırılara karşı daha hazırlıklı olunmasına katkı sağlayacaktır.

Bu öneriler, IoT sistemlerinin güvenliğini artırmak ve RPL tabanlı ağların saldırılara karşı daha dirençli hale gelmesini sağlamak amacıyla önemli adımlar olarak değerlendirilmektedir. Uygulanan güvenlik önlemleri, IoT cihazlarının ve ağlarının uzun vadeli sürdürülebilirliğini ve güvenilirliğini sağlayacaktır.

KAYNAKÇA

Abidi, M. H., Alkhalefah, H., & Umer, U. (2022). Fuzzy harmony search based optimal control strategy for wireless cyber physical system with industry 4.0. *Journal of intelligent manufacturing*, 1-18.

Boateng, E. A. (2021). Anomaly detection for industrial control systems based on neural networks with one-class objective function. *Proceedings of Student Research and Creative Inquiry Day*, *5*.

Boateng, E. A., Bruce, J., & Talbert, D. A. (2022). Anomaly detection for a water treatment system based on one-class neural network. *Ieee access*, *10*, 115179-115191.

Chu, A., Lai, Y., & Liu, J. (2019). Industrial control intrusion detection approach based on multiclassification GoogLeNet-LSTM model. *Security and Communication Networks*, *2019*, 1-11.

Colabianchi, S., Costantino, F., Di Gravio, G., Nonino, F., & Patriarca, R. (2021). Discussing resilience in the context of cyber physical systems. *Computers & Industrial Engineering*, *160*, 107534.

Datta, S., & Venkanna, U. (2023). Securing Smart Home IoT Network Against DNS Flooding Attack using P4. 2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS),

Dixit, A., Trivedi, A., & Godfrey, W. W. A survey of cyber attacks on blockchain based IoT systems for industry 4.0. *IET Blockchain*, *n/a*(n/a). https://doi.org/https://doi.org/10.1049/blc2.12017

Dunkels, A., Gronvall, B., & Voigt, T. (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors. 29th annual IEEE international conference on local computer networks,

Kim, H.-m., & Lee, K.-h. (2022). IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories. *Applied Sciences*, *12*(15), 7679.

Kumar, P., Kumar, R., Gupta, G. P., & Tripathi, R. (2021). A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. *Transactions on Emerging Telecommunications Technologies*, *32*(6), e4112. https://doi.org/https://doi.org/10.1002/ett.4112

Kumar, S., Guerrero, A., & Navarro, C. (2023). Cyber Security Flood Attacks and Risk Assessment for Internet of Things (IoT) Distributed Systems. 2023 IEEE World AI IoT Congress (AIIoT),

Laiq, F., Al-Obeidat, F., Amin, A., & Moreira, F. (2023). DDoS Attack Detection in Edge-IIoT using Ensemble Learning. 2023 7th Cyber Security in Networking Conference (CSNet),

Lambán, M. P., Morella, P., Royo, J., & Sánchez, J. C. (2022). Using industry 4.0 to face the challenges of predictive maintenance: A key performance indicators development in a cyber physical system. *Computers & Industrial Engineering*, *171*, 108400.

Latif, S., Idrees, Z., Zou, Z., & Ahmad, J. (2020). DRaNN: A deep random neural network model for intrusion detection in industrial IoT. 2020 international conference on UK-China emerging technologies (UCET),

Lohachab, A., & Karambir, B. (2018). Critical analysis of DDoS—An emerging security threat over IoT networks. *Journal of Communications and Information Networks*, *3*, 57-78.

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W.-C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors*, *21*(5), 1809.

Mohammed, A. S., Anthi, E., Rana, O., Saxena, N., & Burnap, P. (2023). Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication. *Computers & Security*, *124*, 103007.

Morgan, S. (2018). *Global ransomware damage costs predicted to hit $11.5 billion by 2019*. Retrieved Feb 11th from https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/

Muna, A.-H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of information security and applications*, *41*, 1-11.

Narasimhan, S., & Biswas, G. (2007). Model-based diagnosis of hybrid systems. *IEEE Transactions on systems, man, and cybernetics-Part A: Systems and humans*, *37*(3), 348-361.

Nedeljkovic, D., & Jakovljevic, Z. (2022). CNN based method for the development of cyber-attacks detection algorithms in industrial control systems. *Computers & Security*, *114*, 102585.

Padmaja, P. L., Ramanjaneyulu, T., Narayana, I. L., & Srikanth, K. (2017). Role of COOJA simulator in IoT. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *6*(2), 139-143.

Pasqualetti, F., Dörfler, F., & Bullo, F. (2011). Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. 2011 50th IEEE Conference on Decision and Control and European Control Conference,

Rachmadi, S., Mandala, S., & Oktaria, D. (2021). Detection of DoS attack using AdaBoost algorithm on IoT system. 2021 International Conference on Data Science and Its Applications (ICoDSA),

Roopak, M., Tian, G. Y., & Chambers, J. (2020). Multi-objective-based feature selection for DDoS attack detection in IoT networks. *IET Networks*, *9*(3), 120-127. https://doi.org/https://doi.org/10.1049/iet-net.2018.5206

Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future generation computer systems*, *107*, 433-442.

Shi, L., Zhu, H., Liu, Y., & Liu, J. (2019). Intrusion detection of industrial control system based on correlation information entropy and CNN-BiLSTM. *Journal of Computer Research and Development*, *56*(11), 2330-2338.

Singh, H., Bhatta, N. P., Jawad, K. T., Singh, H., Amsaad, F., & Hopkinson, K. (2023). ML-Assisted Security for the Detection of DDoS Attacks in Connected IIoT Environment: Implementation and Comparative Analysis. NAECON 2023-IEEE National Aerospace and Electronics Conference,

Taher, F., Abdel-Salam, M., Elhoseny, M., & El-Hasnony, I. M. (2023). Reliable machine learning model for IIoT botnet detection. *Ieee access*.

Teixeira, A., Pérez, D., Sandberg, H., & Johansson, K. H. (2012). Attack models and scenarios for networked control systems. Proceedings of the 1st international conference on High Confidence Networked Systems,

Tian, Y., Huang, B., Jia, B., & Zhao, L. (2020). Optimizing AP and Beacon Placement in WiFi and BLE hybrid localization. *Journal of Network and Computer Applications*, *164*, 102673.

Wahla, A. H., Chen, L., Wang, Y., Chen, R., & Wu, F. (2019). Automatic wireless signal classification in multimedia Internet of Things: An adaptive boosting enabled approach. *Ieee access*, *7*, 160334-160344.

Wu, D., Jiang, Z., Xie, X., Wei, X., Yu, W., & Li, R. (2019). LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT. *IEEE Transactions on Industrial Informatics*, *16*(8), 5244-5253.

Wu, M., Song, Z., & Moon, Y. B. (2019). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *Journal of intelligent manufacturing*, *30*(3), 1111-1123.

Yang, K., Li, Q., Lin, X., Chen, X., & Sun, L. (2020). iFinger: Intrusion detection in industrial control systems via register-based fingerprinting. *IEEE Journal on Selected Areas in Communications*, *38*(5), 955-967.

Ye, Q., Wang, Y., Xi, M., & Tang, Y. (2020). Recognition of grey hole attacks in wireless sensor networks using fuzzy logic in IoT. *Transactions on Emerging Telecommunications Technologies*, *31*(12), e3873. https://doi.org/https://doi.org/10.1002/ett.3873

Zarei, S. M., & Fotohi, R. (2021). Defense against flooding attacks using probabilistic thresholds in the internet of things ecosystem. *SECURITY AND PRIVACY*, *4*(3), e152. https://doi.org/https://doi.org/10.1002/spy2.152

Zhao, F., Koutsoukos, X., Haussecker, H., Reich, J., & Cheung, P. (2005). Monitoring and fault diagnosis of hybrid systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *35*(6), 1225-1240.

Zheng, C., Li, Y., & Dou, R. (2024). Who should own the data? The impact of data value creation on data ownership. *Computers & Industrial Engineering*, *190*, 110093.