ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

NESNELERİN İNTERNETİNDE GİZLİLİK VE GÜVENLİK YÖNETİMİ

EMRE DENİZ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2019

TEZ ONAYI

Emre DENİZ tarafından hazırlanan "**Nesnelerin İnternetinde Gizlilik ve Güvenlik Yönetimi**" adlı tez çalışması 18/06/2019 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Prof. Dr. Refik Samet
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Jüri Üyeleri:

Başkan: Doç. Dr. Çelebi Uluyol
Gazi Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

Üye : Prof. Dr. Refik Samet
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Üye : Doç. Dr. Gazi Erkan Bostancı
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Yukarıdaki sonucu onaylarım.

Prof. Dr. Özlem YILDIRIM
Enstitü Müdür Vekili

ETİK

Ankara Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

18/06/2019

Emre DENİZ

ÖZET

Yüksek Lisans Tezi

NESNELERİN İNTERNETİNDE GİZLİLİK VE GÜVENLİK YÖNETİMİ

Emre DENİZ

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Ana Bilim Dalı

Danışman: Prof. Dr. Refik Samet

İnternet, günümüzde hayatın içinde çok önemli yere sahip bir teknoloji konumuna gelmiştir. Neredeyse her alanda İnternetle karşı karşıyayız. Sadece bilgisayar, telefon ve tabletler değil, arabalar, bulaşık makineleri ve ilaç kutuları da İnternete bağlıdır. Hayatın her alanında olan bu teknolojiler, Nesnelerin İnterneti olarak tanımlanmaktadır. Nesnelerin İnterneti, haberleşme protokolleri ile iletişimde olan nesneleri içeren, veri toplama ve kontrol yapmaya yarayan bir ağdır. Bu teknoloji, endüstri, tarım, ev, sağlık, çevre, taşımacılık, enerji, su ve şehir gibi alanlarda kullanılmaktadır. Nesnelerin birbiriyle sürekli haberleşme halinde olması ve İnternet bağlantılarının olması siber saldırılara olanak sağlamaktadır. Bu saldırıların başarılı olması halindeki kötü sonuçlarının büyüklüğü nedeniyle Nesnelerin İnternetinde gizlilik ve güvenliğin önemi artmaktadır. Örneğin, İnternet bağlantısı olan nesneler, saldırganların kullanıcıları takip etmesine imkân verebilir ya da bir kimsenin arabasını çalıştırabilir veya kapısını kilitleyebilir. Üreticiler, Nesnelerin İnternetinde çeşitli teknolojiler kullanmaktadırlar. Nesnelerin İnternetinde, bu teknolojilerde bulunan güvenlik açıkları sebebiyle güvenli haberleşme bazı durumlarda sağlanamamaktadır. Güvenli haberleşmenin olması için güvenlik açıklarının belirlenip önlemler alınması gerekmektedir. Bu çalışmada, mevcut çalışmalardan da yararlanılarak güvenlik yönetimi için açıklara karşı olması gereken temel önlemler anlatılmaktadır. Ayrıca üreticilerin ürettiği düğümlerin tek bir noktadan yönetimini sağlamak, bununla birlikte Nesnelerin İnternetinde bilgi güvenliğinde en kritik kısımlardan biri olan mevcut ağlara yeni düğüm katılmasında güvenliği artırmak ve meydana gelebilecek güvenlik açıklarının kapatılmasına katkı yapmak amacıyla yeni bir yöntem önerilmektedir. Yöntem için bir bulut uygulaması geliştirilmiş olup benzetim üzerinde uygulanmakta ve sonuçları değerlendirilmektedir.

Haziran 2019, 51 sayfa

Anahtar Kelimeler: Nesnelerin İnterneti, Tehditler, Saldırılar, Gizlilik, Güvenlik, Güvenlik Yönetimi

ABSTRACT

Master Thesis

INTERNET OF THINGS PRIVACY AND SECURITY MANAGEMENT

Emre DENİZ

Ankara University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Prof. Dr. Refik Samet

Recently, Internet has become an important technology in life. We are facing the Internet in almost every field. We live in a world where not only tablets, smart phones and computers, but also washing machines, medicine bottles and cars are connected to the Internet. These technologies are defined as IoT (Internet of Things). IoT collects data from and controls things that are in a communication with each other. This technology is used in health, household, agriculture, energy, environment, water, city, industry and transportation. Being connected to each other and the Internet causes cyber-attacks to the objects in IoT. IoT information security is important because of the negative results of these attacks. For example, objects that connect to the Internet can allow attackers to track the users, turn on his car or lock his door. In IoT, manufacturers use different technologies. Due to the security vulnerabilities in some of these technologies, secure communication cannot be performed. These vulnerabilities should be identified and precautions should be taken to ensure secure communication. In this study, the basic measures against security vulnerabilities are described. A new method is proposed in order to manage nodes from one point, improve security in network join that is one of most critical issues in IoT and contribute to the closure of vulnerabilities. A cloud application is developed for the method. The method is applied on simulation and results are evaluated.

June 2019, 51 pages

Key Words: Internet of Things, Threats, Attacks, Privacy, Security, Security Mangement

TEŞEKKÜR

Çalışmalarımı yönlendiren, araştırmalarımın ve çalışmalarımın tüm aşamalarında yardım ve desteklerini esirgemeyen danışman hocam sayın Prof. Dr. Refik SAMET'e en içten duygularla teşekkür ederim.

Çalışmalarım süresince fedakârlık gösteren ve beni destekleyip her an yanımda olan aileme de çok teşekkür ederim.

Emre DENİZ
Ankara, Haziran, 2019

İÇİNDEKİLER

KISALTMALAR DİZİNİ

3G	3rd Generation (Üçüncü Nesil)
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks (IPv6 Düşük Güçlü Kablosuz Kişisel Alan Ağları)
AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
DTLS	Datagram Transport Layer Security (Datagram Taşıma Katmanı Güvenliği)
HART	Highway Addressable Remote Transducer Protocol (Veriyolu Adreslenebilir Uzaktan Dönüştürücü)
HTTP	Hyper-Text Transfer Protocol (Metin Transfer Protokolü)
IoT	Internet of Things (Nesnelerin İnterneti)
IP	Internet Protocol (İnternet Protokolü)
M2M	Machine-to-Machine (Makine - Makina)
NFC	Near Field Communication (Yakın Alan İletişimi)
RAM	Random Access Memory (Rastgele Erişimli Bellek)
RFID	Radio Frequency Identification (Radyo Frekanslı Tanımlama)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
Wi-Fi	Wireless Fidelity (Kablosuz Bağlantı)
WiMAX	Worldwide Interoperability for Microwave Access (Mikrodalga Erişim için Dünya Çapında Birlikte Çalışabilirlik)
WSN	Wireless Sensor Network (Kablosuz Algılayıcı Ağları)
XSS	Cross Site Scripting

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

İnternet, günümüzde hayatın içinde çok önemli yere sahip bir teknoloji konumuna gelmiştir. Artık her alanda İnternet kullanmaktayız. Gelişen İnternet ve ağ teknolojileri nedeniyle her yerden ve her zaman İnternete ulaşılabilmektedir. Bu teknolojilere, mobil, kablosuz sensör ağları, uzaktan takip ve kontrol sistemleri ile Nesnelerin İnterneti örnek olarak gösterilebilir.

Ancak gelişen bu teknolojiler her ne kadar yaşamı kolaylaştırsa da bazı güvenlik sorunlarına sebep olmaktadır. Örneğin, yaygın kullanım sayesinde üretilen çok sayıda verinin ihlaller sebebiyle açığa çıkmasının sonuçları ciddi boyutlarda olmaktadır.

Yaygın kullanılan İnternet teknolojilerinden birisi olan Nesnelerin İnterneti, haberleşme protokolleri ile iletişimde olan nesneleri içeren, veri toplama ve kontrol yapmaya yarayan bir ağdır (Gökrem 2016, Arış vd. 2015, Çavdar ve Öztürk 2017). Nesnelerin İnterneti sayesinde günümüzde sadece bilgisayar, telefon ve tabletler değil, arabalar, bulaşık makineleri ve ilaç kutuları da İnternete bağlanabilmektedir. Tüm bu gelişmeler doğrultusunda son yıllarda ortaya çıkan Nesnelerin İnterneti teknolojisinin günlük yaşamdaki rolü git gide artmakta ve 2020 yılında çok sayıda nesnenin birbiriyle bağlı olacağı tahmin edilmektedir (Anonymous 2016). Bu teknoloji, endüstri, tarım, ev, sağlık, çevre, taşımacılık, enerji, su ve şehir alanlarında kullanılmaktadır. (Gökrem 2016, Elbouanani vd. 2015).

Nesnelerin sürekli haberleşme halinde olması ve İnternet bağlantılarının olması siber saldırılara olanak sağlamaktadır (Kumar vd. 2017, Gupta ve Shukla 2016). Ayrıca yapılan çalışmalara göre bu teknoloji, büyük gizlilik ve güvenlik açıklarına sebep olacaktır. Örneğin, İnternet bağlantısı olan nesneler, saldırganların kullanıcıları takip etmesine imkân verebilir ya da bir kimsenin arabasını çalıştırabilir veya kapısını kilitleyebilir. Bunlara ek olarak bağlantılar üzerinden sızılması durumunda bilgiler ele geçirilebilir, sistem etkisiz kılınabilir veya nesneler "zombi" yapılarak başka kaynaklara servis engelleme gibi saldırılar gerçekleştirilebilir.

Üreticiler, Nesnelerin İnternetinde çeşitli teknolojiler kullanmaktadırlar (Sain vd. 2017). Nesnelerin İnternetinde, bu teknolojilerde bulunan güvenlik açıkları sebebiyle güvenli iletişim bazı durumlarda sağlanamamaktadır (Yang vd. 2017, Mosenia ve Jha 2017). Güvenli haberleşmenin olması için açıkların belirlenip önlem alınması gerekmektedir (Chadid vd. 2017).

Nesnelerin İnternetinde güvenlik alanında yeterli çalışma yapılmamasına rağmen ekonomik sebeplerden dolayı şirketlerin bu akıllı nesneleri üretmeye devam etmesi ve herhangi bir ihlal durumundaki kötü sonuçlarının büyüklüğü nedeniyle Nesnelerin İnternetinde gizlilik ve güvenlik yönetiminin önemi artmaktadır.

Tez çalışmasında, öncelikle Nesnelerin İnternetinin tanımı, kullanım alanları, mimarisi ve bu alanda kullanılan kablosuz haberleşme teknolojileri açıklanmaktadır. Ardından mevcut çalışmalar ile Nesnelerin İnternetinde gizlilik ve güvenlik analizi yapılmaktadır. Nesnelere yönelik olabilecek saldırılar; fiziksel, ağ ve yazılım siber saldırıları olarak listelenmektedir. Bu alanda kullanılan haberleşme protokolleri gizlilik ve güvenlik olarak incelenip olası güvenlik açıkları tespit edilmektedir. Güvenlik açıklarına karşı olması gereken temel önlemler anlatılmaktadır. Ayrıca üreticilerin ürettiği düğümlerin tek bir noktadan yönetimini sağlamak, bununla birlikte Nesnelerin İnternetinde bilgi güvenliğinde en kritik kısımlardan birisi olan mevcut ağlara yeni düğüm katılmasında güvenliği artırmak ve meydana gelebilecek güvenlik açıklarının kapatılmasına katkı yapmak amacıyla yeni bir yöntem önerilmektedir. Önerilen yöntem, bulut olarak adlandırılmaktadır. Bu yöntem için öncelikle bir bulut uygulaması geliştirilmekte ve düğümlerin tek bir noktadan yönetimi sağlanmaktadır. Bununla birlikte yeni bir düğüm mevcut bir ağa katılacağı zaman, ağ koordinatörü bulut sistemine bağlanarak katılacak düğüme ait güvenlik bilgilerini almakta ve düğümün kötü amaçlı olup olmadığını doğrulamaktadır. Doğrulamanın başarılı şekilde yapılması durumunda düğüm ağa katılmaktadır. Doğrulama yapılamaması durumunda ise düğüm ağa katılamamaktadır. Ayrıca, önerilen yöntem yaygın olarak kullanılan Nesnelerin İnterneti teknolojilerinden biri olan ZigBee için benzetim üzerinde uygulanmakta ve sonuçları paylaşılmaktadır.

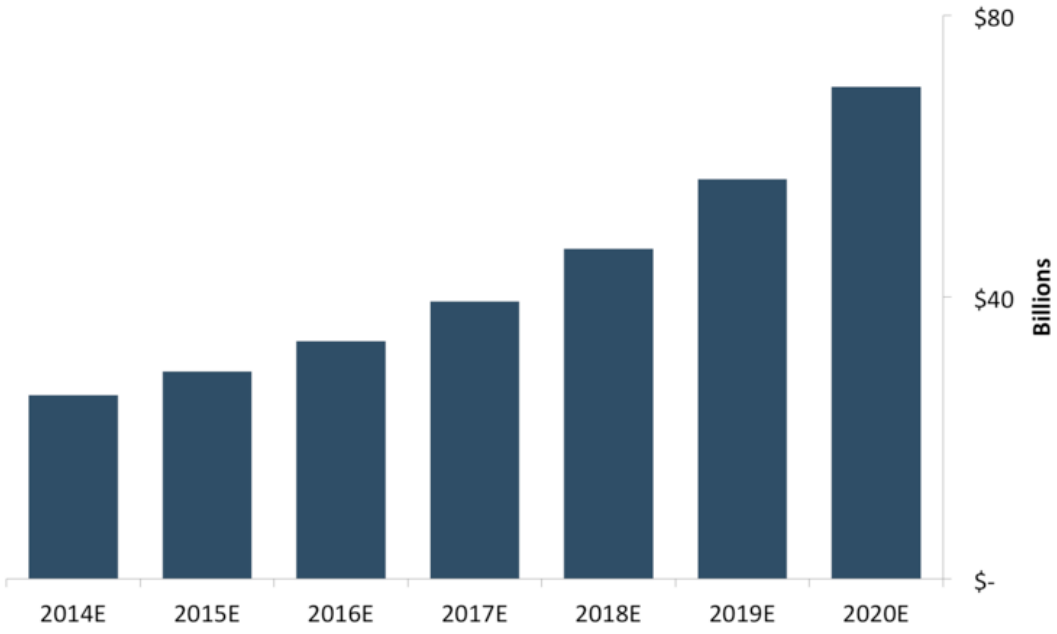
Bu çalışmada, ikinci bölümde Nesnelerin İnterneti hakkında temel bilgiler ve Nesnelerin İnternetinde güvenlik konusunda yapılmış çalışmalardan bahsedilmektedir. Üçüncü bölümde önerilen yöntem detaylı olarak açıklanmaktadır. Dördüncü bölümde önerilen yöntemin uygulanması ve elde edilen sonuçlar sunulmaktadır. Beşinci bölümde ise sonuçlar, yapılan çalışmanın katkıları ve gelecekte yapılabilecek çalışmalar anlatılmaktadır.

2. KURAMSAL TEMELLER ve KAYNAK ÖZETLERİ

Bu bölüm, mevcut çalışmalardan yararlanılarak, Nesnelerin İnternetinin tanımından, kullanım alanlarından, mimarisinden, Nesnelerin İnternetine yönelik saldırı ve tehditler ile bu saldırılara karşı çözüm yöntemleri üzerine yapılmış çalışmaların özetlerinden ve bölüm değerlendirmesinden oluşmaktadır.

2.1 Nesnelerin İnterneti

Nesnelerin İnterneti, haberleşme protokolleri ile iletişimde olan nesneleri içeren, veri toplama ve kontrol yapmaya yarayan bir ağdır. Nesnelerin İnternetinde, fiziksel nesneler birbirleriyle ya da daha büyük sistemlerle bağlantılıdır. Bu teknoloji, yaygınlığını git gide artırmaktadır. Gelecek yıllardaki Nesnelerin İnterneti için tahmini yatırım ve buna bağlı olarak yaygınlıktaki artış şekil 2.1'de gösterilmektedir.



Şekil 2.1 Tahmini Yıllık Nesne Üretimi Yatırım Miktarı (Anonymous 2016)

Şekle göre önümüzdeki yıllarda yatırım miktarlarında artış oranı da artmaktadır.

2.1.1 Tarihçe

1991 yılında Cambridge Üniversitesi'nde bir grup akademisyen kahve makinesinin durumunu görebilmek için makinenin görüntüsünü yakalayan ve akademisyenlerin bilgisayarlarına aktaran bir sistem geliştirmiştir (Kutup 2011). Bu sistemi Nesnelerin İnterneti olarak adlandırmamalarına rağmen bu sistem aslında bir Nesnelerin İnterneti sistemiydi. Geliştirilen bu xcoffee sistemi şekil 2.2'de gösterilmektedir.

Şekil 2.2 Xcoffee Sistemi (Anonymous 2016)

Nesnelerin İnterneti kavramı ise ilk defa 1999 yılında Kevin Ashton tarafından ortaya atılmıştır (Andrea vd. 2015). Kevin Ashton, Procter & Gamble firmasında, RFID (Radio Frequency Identification) teknolojisinden bahsederken Nesnelerin İnterneti kavramını ilk kez kullanmıştır.

2.1.2 Kullanım alanları

Nesnelerin İnterneti aşağıdaki alanlarda kullanılmaktadır;

- Ev
- Sağlık
- Çevre
- Tarım

- Hayvancılık
- Enerji
- Şehir
- Endüstri
- Alışveriş

Örnek bir akıllı enerji sistemi şekil 2.3'te gösterilmektedir.

Şekil 2.3 Akıllı Enerji Sistemi (Anonim 2017)

2.1.3 Mimari

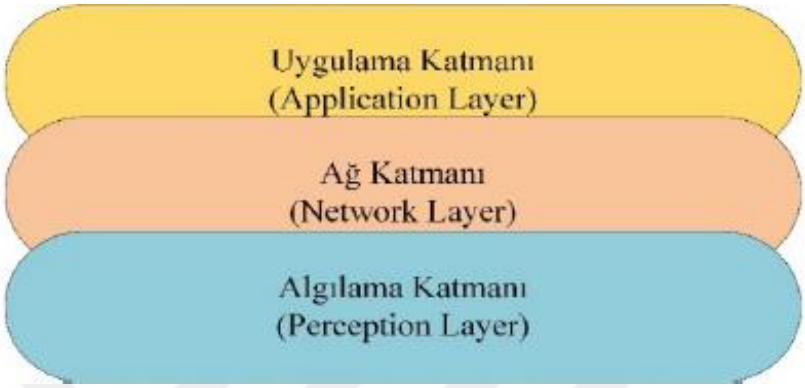
Nesnelerin İnterneti temel mimarisi üç katmandan oluşmaktadır (Çavdar ve Öztürk 2017, Husamuddin ve Qayyum 2017).

Algılama (Fiziksel) Katmanı: Bu katman, verileri toplamaktadır.

Ağ Katmanı: Bu katman, fiziksel katmandan gelen verileri toplayıp işleyerek üst katmana iletmektedir.

Uygulama Katmanı: Bu katman, alt katmanlardan gelen verileri toplayıp kullanıcıya anlamlı sonuçları iletmektedir.

Üç katmanlı temel mimari şekil 2.4'te gösterilmektedir.



Şekil 2.4 Üç Katmanlı Mimari (Çavdar ve Öztürk 2017)

Servis tabanlı Nesnelerin İnterneti mimarisi ise beş katmandan oluşmaktadır (Çavdar ve Öztürk 2017, Kumar vd. 2017).

Nesne Katmanı: Mimarinin ilk katmanıdır. Algılayıcıların verileri topladığı ve fiziksel işlemlerin gerçekleştiği katmandır.

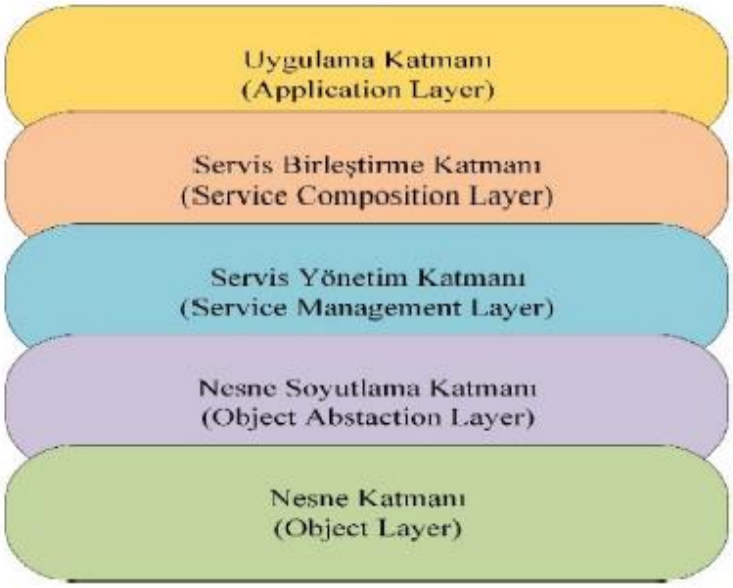
Nesne Soyutlama Katmanı: Veri yönetiminin yapıldığı ve verilerin servis katmanına gönderildiği katmandır.

Servis Yönetim Katmanı: Verilerin alındığı, işlenip karar verilerek bir üst katmana iletildiği katmandır.

Servis Birleştirme Katmanı: Gelen verileri, servisleri birleştirerek hizmete sunan katmandır.

Uygulama Katmanı: En üst katmandır. İşlenmiş hazır veriyi kullanıcıya sunan katmandır.

Beş katmanlı servis tabanlı mimari şekil 2.5'te gösterilmektedir.



Şekil 2.5 Servis Tabanlı Mimari (Çavdar ve Öztürk 2017)

2.1.4 Kablosuz haberleşme teknolojileri

Nesnelerin İnternetinde kullanılan kablosuz haberleşme teknolojileri ve açıklamaları çizelge 2.1'de listelenmektedir (Sain vd. 2017, Giuliano vd. 2017).

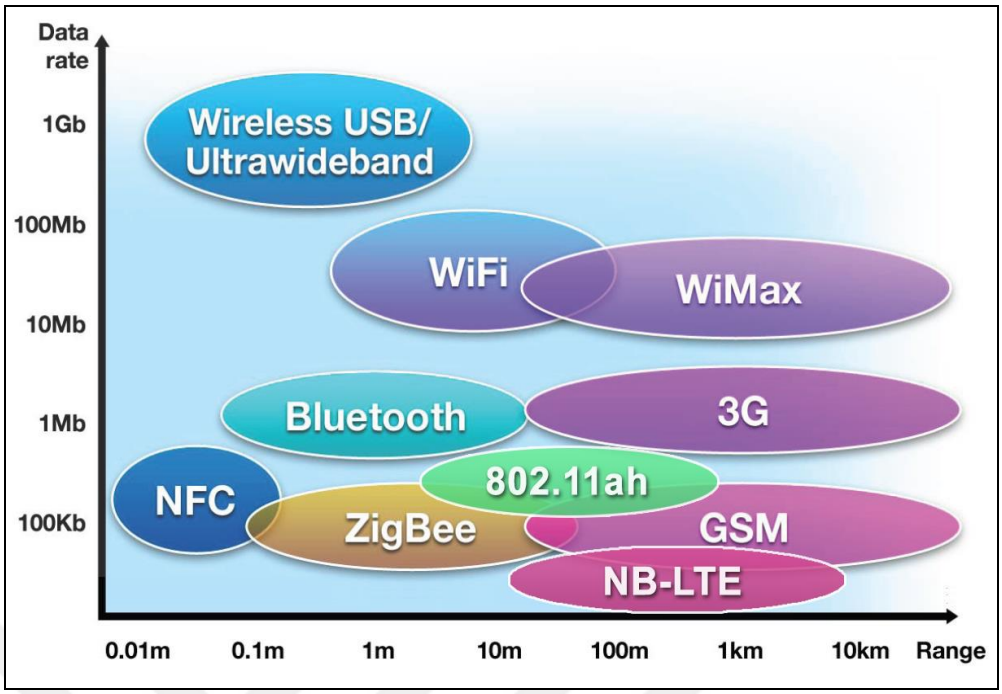
Çizelge 2.1 Kablosuz Haberleşme Teknolojileri

NFC (Near Field Communication)	Yüksek frekanslarda çalışan bir kısa mesafe kablosuz haberleşme teknolojisidir.
RFID	Radyo dalgaları ile iletişimi sağlayan bir kablosuz haberleşme teknolojisidir.
Bluetooth	Kısa mesafelerde iletişim için kullanılan bir radyo frekansı tabanlı kablosuz haberleşme teknolojisidir.
Wi-Fi (Wireless Fidelity)	Yüksek hızda iletişime olanak sağlayan, şifreli veri iletimi yapan ve yüksek enerji tüketimine ihtiyaç duyan bir kablosuz haberleşme teknolojisidir.

Çizelge 2.2 Kablosuz Haberleşme Teknolojileri (devam)

ZigBee	Düşük bant genişliği, düşük güç tüketimi, düşük veri hızı ve düşük maliyet sunan bir kısa mesafe kablosuz haberleşme teknolojisidir.
WirelessHART	HART (Highway Addressable Remote Transducer Protocol) tabanlı bir teknolojidir. Etki alanını genişleterek daha önceden erişim yapılamayan aletlerin ağa dâhil edilmesine olanak sağlar.
6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)	Düşük güç tüketimi, düşük veri hızı ve düşük maliyet sunan bir kısa mesafe kablosuz haberleşme teknolojisidir. IP (Internet Protocol) sürüm 6'ya göre daha düşük güç tüketir.
WiMAX (Worldwide Interoperability for Microwave Access)	Geniş bant hizmeti ve yüksek veri aktarım hızı sunan bir uzun mesafe kablosuz haberleşme teknolojisidir. Wi-Fi teknolojisine benzerdir ancak en önemli farkı daha geniş alanlarda haberleşmeye olanak sağlayabilmesidir.
3G (3rd Generation)	Üçüncü nesil mobil bir kablosuz haberleşme teknolojisidir. Geniş alanlarda kablosuz haberleşmeye olanak sağlar.

Nesnelerin İnternetinde kullanılan haberleşme teknolojilerinin veri aktarım hızı ve mesafe olarak karşılaştırması ise şekil 2.6'da gösterilmektedir.



Şekil 2.6 Haberleşme Teknolojileri Karşılaştırma (Anonymous 2017)

Şekilde görüldüğü üzere WiMAX, 3G ve GSM uzun menzillerde; Bluetooth, ZigBee ve WiFi daha kısa menzillerde; NFC ise en kısa menzillerde çalışmaktadır. Nesnelerin İnternetinin kullanım alanına göre bu karşılaştırma grafiği esas alınarak uygun teknolojiler belirlenebilir.

2.2 Kaynak Özetleri

Bu bölüm iki alt başlıkta incelenecektir. İlk bölümde Nesnelerin İnternetine yönelik saldırı ve tehditler üzerine yapılmış çalışmalardan bahsedilecektir. İkinci bölümde ise saldırı ve tehditlere karşı alınabilecek önlemler üzerine yapılmış çalışmalara değinilecektir.

2.2.1 Saldırı ve tehditler üzerine yapılmış çalışmalar

Arış vd. (2015), yaptıkları çalışmada, Nesnelerin İnternetini hedef alabilecek saldırıları incelemiş ve hedef aldıkları katmanlar açısından sınıflandırmıştır. Ayrıca Nesnelerin İnterneti ortamının özelliklerini göz önüne alan saldırıların tespit sistemleri de

değerlendirilmiştir. Saldırılar fiziksel, veri bağı, ağ, iletim ve uygulama katmanlarına göre sınıflandırılmıştır. Bu çalışma, daha çok servis engelleme saldırıları üzerine yoğunlaşmıştır.

Andrea vd. (2015) ile Husamuddin ve Qayyum (2017), Nesnelerin İnternetine yönelik saldırıları; fiziksel, ağ ve yazılım olmak üzere üç ana kategori altında sınıflandırmıştır. Fiziksel saldırılarda saldırganın, fiziksel bileşenler üzerine yoğunlaştığı belirtilmiştir. Fiziksel saldırılar (ataklar) aşağıdaki gibi gruplandırılmıştır.

- Düğüm Kurcalama Atağı: Bu atakta saldırgan, algılayıcı düğümleri değiştirerek düğüm üzerinde hasara sebep olmaktadır.

- Radyo Frekansı Müdahalesi Atağı: Bu atakta saldırgan, RFID etiketlerine gürültü sinyalleri göndererek haberleşmeye müdahale etmektedir.

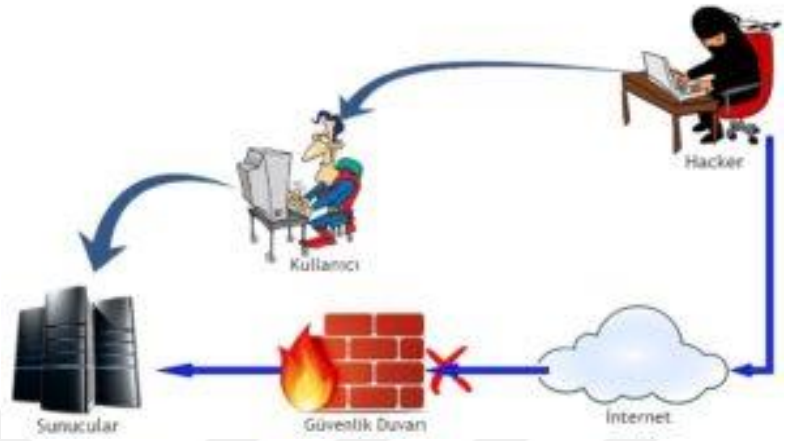
- Düğüm Karıştırma Atağı: Radyo frekansı müdahalesi atağına çok benzerdir. Bu atakta saldırgan, WSN (Wireless Sensor Network) sinyallerini düğümler üzerinden keserek haberleşmeye müdahale etmektedir.

- Kötü Amaçlı Düğüm Atağı: Bu atakta saldırgan, iki düğüm arasında kötü amaçlı düğüm kurulumu yaparak veri akışını ele geçirmektedir.

- Fiziksel Hasar Atağı: Bu atakta saldırgan, fiziksel olarak cihazlara zarar vermektedir.

- Sosyal Mühendislik Atağı: Bu atak günümüzde sıklıkla kullanılmaktadır. Bu atakta saldırgan, doğrudan sistem kullanıcılarının bilgilerini ele geçirerek müdahalede bulunmaktadır. Saldırgan, hedef kişilerin güvenini kazanma yoluyla onların kişisel veya kurumsal bilgilerini ele geçirmektedir. Saldırganın normalde gizli bilgilere erişmesi için internet üzerindeki ve güvenlik duvarlarındaki koruma önlemlerini aşması mümkün olmamaktadır. Ancak sosyal mühendislik

sayesinde kullanıcı bilgilerine ulaşıldığı zaman gizli bilgilere erişmek mümkün olmaktadır. Bu atak şekil 2.7'de gösterilmektedir.



Şekil 2.7 Sosyal Mühendislik (Anonymous 2017)

- Uyku Yoksunluğu Atağı: Nesnelerin İnternetinde kullanılan bataryalar, ömrünü uzatmak için çeşitli uyku rutinlerini takip etmektedir. Bu atakta saldırgan, cihazların uykuya geçmesini engelleyerek kapanmasına sebep olmaktadır.

- Kötü Amaçlı Kod Atağı: Bu atakta saldırgan, cihazlara kötü amaçlı yazılım yükleyerek onları ele geçirmektedir.

Ağ saldırılarında da saldırganın, ağ bileşenleri üzerine yoğunlaştığı belirtilmiştir. Ağ saldırıları aşağıdaki gibi gruplandırılmıştır.

- Trafik Analiz Atağı: Bu atakta saldırgan, kablosuz iletişim üzerinde ağ ve paket bilgilerine erişerek gizli bilgilere ulaşmaktadır.

- RFID Yanıltma Atağı: Bu atakta saldırgan, RFID kimliklerini kullanarak sahte cihazları gerçek cihaz gibi sisteme tanıtarak erişim sağlamaktadır.

- RFID Kopyalama Atağı: Bu atakta saldırgan, RFID etiketlerini kopyalayarak gerçek cihazlar gibi sisteme dâhil olmaktadır.

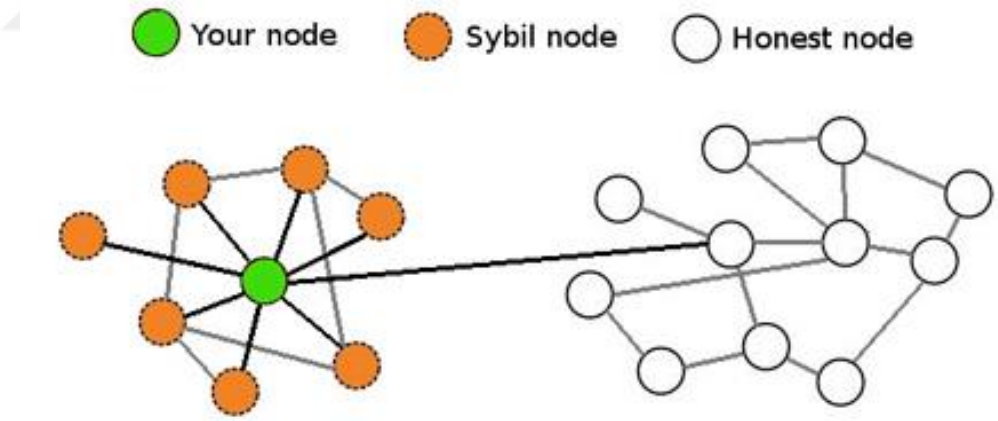
- RFID Yetkisiz Erişim Atağı: Bu atakta saldırgan, kimlik doğrulama eksiklerinden yararlanarak sisteme erişim sağlamaktadır.

- Sinkhole Atağı: Bu atakta saldırgan, tüm ağ trafiğini, oluşturduğu kaynağa yönlendirerek servislerin çalışmasını engellemektedir.

- Ortadaki Adam Atağı: Bu atakta saldırgan, iki nesne arasındaki trafiği fiziksel müdahaleye gerek kalmadan dinleyerek kontrol etmektedir.

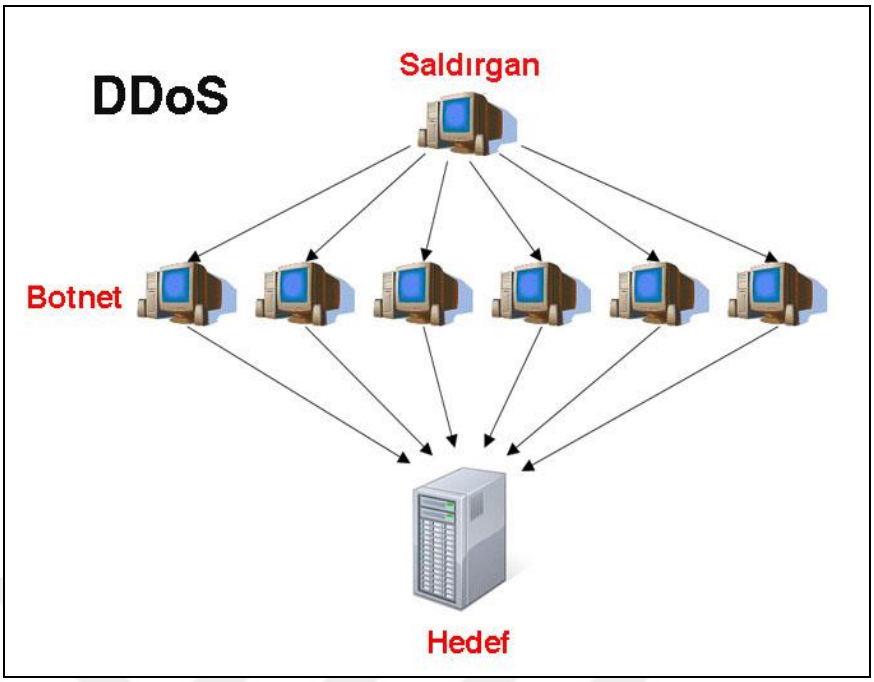
- Yönlendirme Bilgi Atağı: Bu atakta saldırgan, yönlendirme trafiği üzerinde döngü oluşturmaktadır.

- Sybil Atağı: Bu atakta saldırgan, birden fazla cihazı taklit edebilecek kötü amaçlı cihaz ile sisteme dâhil olmaktadır. Bu atağın nasıl işlediği şekil 2.8'de gösterilmektedir.



Şekil 2.8 Sybil Atağı (Agirre vd. 2018)

- Servis Engelleme Atağı: Bu atakta saldırgan, ağ üzerine aşırı trafik göndererek servislerin çalışmasını engellemektedir. Bu atağın şeması şekil 2.9'da gösterilmektedir.



Şekil 2.9 Servis Engelleme Saldırı Şeması (Anonim 2017)

Yazılım saldırılarında da saldırganın, yazılım bileşenleri üzerine yoğunlaştığı belirtilmiştir. Yazılım saldırıları aşağıdaki gibi gruplandırılmıştır.

- Oltalama Atağı: Bu atakta saldırgan, e-posta veya İnternet siteleri sayesinde kullanıcının erişim bilgilerini ele geçirmektedir.

- Virüs, Solucan, Casus Yazılım Atağı: Bu atakta saldırgan, kötü amaçlı yazılımlar sayesinde bilgileri çalmaktadır.

- Kötü Amaçlı Kod Atağı: Bu atakta saldırgan, kullanıcıyı aktif çalışan uygulamalar ile tuzağa düşürerek sisteme müdahale etmektedir.

- Servis Engelleme Atağı: Bu atakta saldırgan, uygulama katmanına servis engelleme saldırıları ile müdahale etmektedir.

Bu çalışmalar, daha çok Nesnelerin İnterneti üzerine yapılabilecek saldırılara yoğunlaşmıştır. Belirtilen saldırılara karşı çözüm yöntemlerinden bahsedilmemiştir.

Zillner (2015), yaptığı çalışmada, Nesnelerin İnternetinde yaygın kullanılan teknolojilerden birisi olan ZigBee'yi incelemiştir. ZigBee Pro sürümünde güvenlik açıkları belirlenmiştir. ZigBee ağları, SecBee programıyla dinlenip saldırılar yapılmış ve düğümler ele geçirilmiştir. Bulunan açıklar son ZigBee sürümünde giderilmiştir. Bu çalışmada bulunan açıklar ZigBee'nin son sürümünde genel olarak kapatıldığı için güncel sürümdeki güvenlik sorunları ele alınmamıştır.

Fan vd. (2017), yaptıkları çalışmada, bir düğümün ağa katılması sırasında güvenlik açıkları olabileceğini ortaya koymuştur. Düğümler ve koordinatör ile bir ZigBee 3.0 ağı hazırlanmıştır. WireShark ve Killerbee adı verilen yazılımlar ile düğümler arasındaki iletişime ulaşılmıştır. Yapılan analiz esnasında iletilen paketlerden birisinin düğüm ekleme hedefiyle gönderildiği ve iletişimde şifrelemeye olanak sağlayan ağ anahtarının, küresel ve bilinen bir bağlantı anahtarıyla şifrelenip gönderildiği anlaşılmıştır. Aynı anahtarla paketin şifresi çözülmüş ve ağ anahtarı elde edilmiştir. Bunun sayesinde tüm iletişimin şifresi çözülüp ağa dışarıdan müdahale edilmiştir. Bu çalışmada, bulunan güvenlik açığını kapatmaya katkı yapmak için kapsamlı ve belirli bir çözüm yöntemi verilmemiştir.

Morgner vd. (2017), yaptıkları çalışma ile ağa katılım metodundaki güvenlik açıklarını analiz etmek için bir ortam hazırlamışlardır. Bilgisayara Z3sec programı yüklenmiş ve bilgisayara radyo alıcılı USB ile bağlanıp 4 markaya ait ZigBee lambalara saldırılar düzenlenmiştir. Bahsedilen bu dört düğümün Touchlink Commissioning yöntemiyle ağa katılması esnasında, ZigBee topluluğu tarafından üreticilere verilen ve 2015 yılında açığa çıkan küresel bağlantı anahtarının kullanılması sebebiyle bir güvenlik açığı oluşmuştur. Ağ anahtarı, ağa katılım paketlerinden elde edilip şifreli iletişim çözülmüş ve diğer düğümlere kapatma ve sıfırlama gibi komutlar gönderilmiştir. Bu çalışmada, ağa katılım esnasındaki güvenlik açığının kapatılmasına katkı yapmak için belirli bir çözüm yöntemi sunulmamıştır.

Deniz ve Samet (2018) yaptıkları çalışma ile öncelikle Nesnelerin İnternetinde ağa katılımdaki güvenlik açıklarını tanımlamışlardır. Düğümlerin yönetimine olanak sağlayan ve bahsedilen güvenlik açıklarını kapatmaya katkı yapmak amacıyla bir bulut

modeli önerilmiştir. Modelin ayrıntıları kavramsal olarak anlatılmıştır. Önerilen modelde mevcut protokole göre yapılan değişiklikler açıklanmıştır. Modelin detayları kavramsal ve teorik olarak açıklanmış ancak model, bir benzetim üzerinde veya gerçek ortamda uygulanmamıştır.

2.2.2 Saldırılara karşı çözüm yöntemleri üzerine yapılmış çalışmalar

Çavdar ve Öztürk (2017), yaptıkları çalışma ile Nesnelerin İnterneti hakkında genel bilgiler vermiştir. Çoklu nesne bağlantılarında veri iletişimi ve nesne tanımayla ilgili sorunların oluşabileceğine değinmiştir. Temel veya referans olabilecek mimari bir modelin olmadığı belirtilip akıllı kontrol ve dinamik bir yapıya sahip, katmanlı bir mimari model önerisinde bulunulmuştur. Diğer modellerden farklı olarak algılama katmanı içinde bulunan karar alt katmanı sayesinde doğrudan kullanılabilecek verinin, trafiğe sebep olmadan direkt olarak aktarım katmanına gönderilebildiği anlatılmıştır. Önerilen modelin sahip olduğu ek özellikler sadece kavramsal olarak verilmiştir.

Kim (2017), yaptığı çalışma ile Nesnelerin İnternetinde genel olarak nesnelerde yetersiz hafıza ve düşük güç kapasitesi olduğundan kriptoloji ve mevcut güvenlik çözümlerinin uygulanamadığını tespit etmiştir. Bu sebeple düşük güç tüketimine ihtiyaç duyan bir yöntem önerilmiştir. Ayrıca özellikle akıllı evler için mevcut güvenlik çözümlerinin daha çok kablosuz bağlantıları temel aldığı belirtilmiştir. Ancak Nesnelerin İnternetinde kablosuz harici teknolojilerin de kullanıldığı belirtilmiştir. Bu teknolojilerde kullanılabilecek kimlik doğrulama ve yetkilendirme üzerine yoğunlaşan bir yöntem, kavramsal olarak önerilmiş ancak benzetim üzerinde veya gerçek ortamda bir doğrulama yapılmamıştır.

Chadid vd. (2017), yaptıkları çalışmada, temel mimariye göre katmanlara ayrı saldırılar olabileceği için her katmana özel farklı güvenlik çözümleri gerektiğini belirtmişlerdir. Ayrıca Nesnelerin İnterneti güvenlik mimarisindeki katmanlar tanımlanmış, her bir katmandaki problemler tespit edilmiş ve mevcut güvenlik çözümleri incelenmiştir. Mevcut güvenlik çözümleri öncelikle gömülü sistemler üzerinde kontrol edilmiş ve güvenlik açığına sebep olabilecek kısımlar için yeni çözümler önerilmiştir.

Mukherjee (2015), yaptığı çalışmada, Nesnelerin İnternetinde kısıtlı kaynak üzerinde şifreleme ve anahtar yönetimine olanak sağlanması gerektiğini belirtmişlerdir. Ayrıca fiziksel katman güvenliği için gizli anahtara ihtiyaç duymayan akıllı tasarım ve açık olarak çalışan gizli anahtar kullanan kablosuz iletişim olmak üzere iki metot önerilmiştir. Bu çalışmada daha çok donanım üzerindeki fiziksel katmanda güvenliğin sağlanması üzerine inceleme yapılmıştır.

Keoh vd. (2014), yaptıkları çalışmada, 6LoWPAN protokolünü kullanan Nesnelerin İnterneti ağlarında erişim için kimlik doğrulama, uçtan uca kanal güvenliği ve anahtar yönetimi içeren bir yöntem kullanmıştır. Performans değerlendirmesi yapılmış ve tüketilen göre RAM (Random Access Memory) miktarı hesaplanmıştır. Ayrıca mevcut bir yöntem olan DTLS (Datagram Transport Layer Security)'ye yeni özellikler eklenerek çözüme katkıda bulunulmuştur.

Giuliano vd. (2017), yaptıkları çalışmada, Capillary ağlarını, IP'li veya IP'siz cihazlardan oluşan M2M (Machine-to-Machine) servislerinin kullanıldığı bir kısa mesafe radyo erişim teknolojisi olarak tanımlamıştır. M2M kısa mesafe haberleşme protokollerine örnek olarak WiFi, Bluetooth, ZigBee, 6LoWPAN gösterilmiştir. Sistemde öncelikle terminaller ile IP'siz nesnelerin iletişim kurduğu ve daha sonra bu terminaller ile geçit arasında haberleşme olduğu belirtilmiştir. Bu haberleşmede güvenliğin sağlanması için bir yöntem önerilmiştir. Önerilen yöntem ile ZigBee ve 6LoWPAN protokollerinin performans ve bilgi güvenliği anlamında karşılaştırması benzetim üzerinde uygulanmıştır. Ayrca bu çalışmada diğer birçok çalışmadan farklı olarak IP'siz cihazları da içeren bir mimaride güvenlik için önerilerde bulunulmuştur.

Agirre vd. (2018), ev içi Nesnelerin İnterneti tabanlı e-sağlık sistemlerinin tanımını yapmışlardır. Bu sistemlerin hangi amaçla ve nasıl kullanılacağından bahsedilmiştir. Ev içi ölçülen değerlerin uzaktaki bir sağlık birimine aktarıldığı ve orada değerlendirildiği söylenmiştir. Ayrıca ölçülen değerlerin, veri tabanlarında olan değerler ile karşılaştırılıp hastalığın gelişinin önceden tahmin edilebileceği anlatılmıştır. E-sağlık sistemleri insan hayatı ile direkt ilişkili olduğu için sistemde haberleşmenin son derece güvenli

olmasının gerekliliği anlatılmış ve güvenlik gereksinimleri açıklanarak bir mimari önerilmiştir.

Judson (2016), yaptığı çalışmada, Nesnelerin İnternetinde güvenlik için gerekli temel bileşenleri belirlemiştir. Ağdaki cihazların güvenliğinden emin olmanın, veriyi şifreleyerek korumanın, cihazlar için yaşam döngüsü yönetimini yapmanın ve çeşitli cihazlarla çalışabilecek güvenlik çözümü uygulamanın bu bileşenler olduğunu tanımlanmıştır. Bileşenler aşağıdaki gibi açıklanmıştır.

- Ağdaki cihazların güvenliğinden emin olmak: Ağda sadece yetkili cihazlar veri transferi veya alımı yapmalıdır. Kimlik doğrulama ve yetkilendirme kullanılmalıdır.

- Veriyi şifreleyerek korumak: Veri gönderimi ve alımı esnasında veri şifrelenmiş olmalıdır.

- Cihazlar için yaşam döngüsü yönetimini yapmak: Uygulanan çözümler veya özellikler, geliştirilebilir ve güncellenebilir olmalıdır. Bunlar merkezi bir yerden kontrol edilmeli ve cihaz ömrü boyunca güncellemeler yapılmalıdır.

- Çeşitli cihazlarla çalışabilecek güvenlik çözümü uygulamak: Geliştirilen çözümler sadece belirli tip cihazlara göre değil, farklı çeşitlerdeki cihazlara da uygulanabilir olmalıdır.

Ayrıca güvenlik alanında Nesnelerin İnternetinde diğer ağlardan nelerin farklı olması gerektiği açıklanmıştır. Bahsedilen çözümler kavramsal olarak açıklanmıştır. Görsel tablolar veya akış diyagramları üzerinde anlatılmamıştır. Önerilen çözümlerin standart mimaride hangi katmanlara yönelik olduğu da söylenmemiştir.

Ning vd. (2013), yaptıkları çalışma ile Nesnelerin İnternetinde kimlik doğrulamanın, kullanıcıların sisteme güvenli giriş yapması için kullanılması gereken bir yöntem olduğunu belirtip kullanıcıların kimliğini doğrulamak ve belirli sistemlere erişime izin verip vermediklerini tespit etmek için kullanıldığını söylemiştir. Yetkilendirme ise kullanıcıların hangi yetkilere sahip olacağını yönetmek için kullanılan bir yöntem olarak tanımlanmıştır. Belirlenen yetkiler ile kullanıcının örneğin, bazı alanlarda sadece izleme, bazı alanlarda ise izleme ve kontrol etme özelliklerine sahip olduğu anlatılmıştır.

Sain vd. (2017), yaptıkları çalışmada farklı haberleşme protokolleri içeren Nesnelerin İnternetinde ortak bir güvenlik çözümüne ihtiyaç olduğunu söylemiştir. Nesnelerin İnternetinde kullanılan kablosuz iletişim protokolleri; NFC, RFID, Bluetooth, Wi-Fi, ZigBee, 6loWPAN, WiMAX ve 3G karşılaştırmalı olarak incelenmiştir. Güvenliğin nasıl sağlanması gerektiği ile ilgili olarak katmanlardaki iletişim güvenliği ve bilgi güvenliğinin gerekliliği belirtilmiştir. Ayrıca kullanıcı girişini daha güvenli hale getirmek için çoklu faktörlü kimlik doğrulama yöntemi kullanılabileceği anlatılmıştır. Bu yöntemde kullanıcının sahip olduğu, bildiği veya kullanıcıya ait olan bilgilerden en az ikisi kullanılarak giriş yapılacağı anlatılmıştır.

Roman vd. (2011), nesne ve servislerin yaşam döngüsünde ve tüm seviyelerinde uygulanabilecek kapsamlı çözüm önerileri sunmayı amaçlamışlardır. Nesneler, günlük hayatımızda çok kolay ulaşılabilir durumda olduğundan ve yaygınlaştığından dolayı geleneksel koruma mekanizmaları artık Nesnelerin İnterneti için yetersiz hale gelmiştir. Riskler ve etkiler analiz edilerek yeni güvenlik politikaları geliştirilmelidir. Obje tanımlamadan servis hizmetine, veri alımından altyapı tanımlarına kadar tüm aşamalarda bu politikalar uygulanmalıdır. Protokol ve ağ güvenliği için kriptoloji ve gizli anahtar yönetimi gereklidir. Veri yönetimi ve gizlilik için araçların geliştirilmesi ve kullanıcıların kendi verilerini yönetebilmesi gereklidir. Kimlik yönetimi için her nesnenin ID'si olmalı ve misafir, ev sahibi gibi kullanıcı tiplerinin tanımlanması gereklidir. Gizliliğin tanımı da, cihazlar arasında ya da cihazlar ile kontrol noktaları arasındaki mesajlara veya kullanıcıların kişisel bilgilerine başka kaynakların erişiminin engellenmesi olarak yapılmıştır. Nesnelerin İnterneti de her yerden, her zaman, her şeye

erişimi kapsadığı için bu teknolojide gizliliğin en hassas konulardan birisi olduğu anlatılmıştır. Nesnelerin İnternetinde kullanıcılar kişisel verileri içeren çok sayıda servise erişim sağladığı için bir ihlal durumunda sonuçların kötü olacağı belirtilmiştir. Bu çalışmada nesnelerin tüm aşamaları için güvenlik gereksinimleri belirlenmiş ancak çözüm önerileri yalnızca teorik olarak sunulmuştur.

Zhou ve Chao (2011), yaptıkları çalışmada, şifrelemenin, açık mesaj metninin bir algoritma ile anlaşılmaz şekle dönüştürülmesi olduğunu tanımlamıştır. İletilen mesajın içeriği saldırgan tarafından ele geçirilse bile şifreleme mekanizması çözülemediği takdirde saldırganın içeriğe ulaşamayacağı belirtilmiştir. Bu çalışma, Nesnelerin İnternetindeki haberleşmedeki şifreleme üzerine genel bir yaklaşım sergilemektedir.

Şengül ve Bostan (2013), yaptıkları çalışmada bulut bilişimi incelemişlerdir. Bulut bilişimin tanımı ve faydalarından bahsedilmiştir. Bulut bilişim sayesinde çalışma verimliliğinin artması, yapılan araştırmalarla desteklenmiştir. Ayrıca bu teknolojide meydana gelebilecek bilgi güvenliği sorunlarından bahsedilmiştir. Bahsedilen sorunların çoğunun çözülmüş olduğu sadece bulut hizmet sağlayıcıları kaynaklı sorunların kaldığı belirtilmiştir. Yapılacak standardizasyon çalışmalarıyla da bu sorunların giderileceği anlatılmıştır.

Anonymous (2016), Nesnelerin İnternetinde haberleşmeyi şifrelemek için kullanılan AES (Advanced Encryption Standard) algoritmasının detaylarını ortaya koymuştur. Günümüzde şifreleme amacıyla kullanılan bu algoritmanın en güvenli metot olduğu ve ilk kez birleşmiş milletler tarafından geliştirilmiş bir standart olduğu anlatılmıştır. Bu algoritmanın hem şifreleme hem de şifreyi çözme işlemini gerçekleştirdiği belirtilmiştir. Şifrelemek ve şifreyi çözmek için tek bir gizli şifreleme anahtarın kullanıldığı simetrik şifreleme ile şifreleme için açık anahtar, şifreyi çözmek için gizli anahtarın kullanıldığı asimetrik şifreleme olmak üzere iki farklı şifreleme yönteminin olduğu söylenmiştir. AES algoritmasının detayları açıklanmıştır. Veriler dizi biçiminde ifade edilmektedir. Veri blokları 128, 192 ve 256 bitlik uzunlukta olabilir. Örneğin, 128 bit uzunluğundaki veride 4x4'lük matrislere ayrılarak hesaplama yapılmaktadır. Veri bloklarına göre kelime uzunlukları ve tur sayısı çizelge 2.2'de listelenmektedir.

Çizelge 3.2 AES Veri Blokları

Veri Blokları	Kelime Uzunluğu	Tur Sayısı
AES-128	4	10
AES-192	6	12
AES-256	8	14

Anahtarın uzunluğuna göre tur sayısı da artmaktadır. Tur, yani döngü sayısı arttıkça veri daha güvenli olmakta ancak buna bağlı olarak bellek ve işlemci kullanımı artmaktadır.

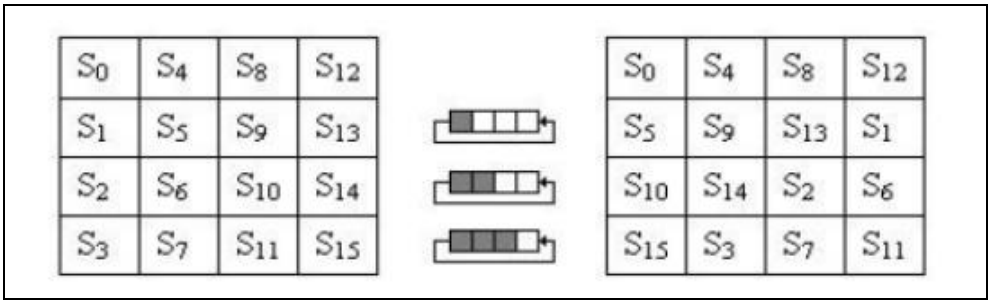
Şifreleme esnasındaki adımlar şöyle devam etmektedir;

- Bayt Değiştirme: Diziden elde edilen matris üzerinde değiştirme işlemi yapılmaktadır. Önceden belirlenmiş S-kutusuna göre durum matrisi değiştirilmektedir. Örneğin, burada ilk eleman 25, S-kutusunda 2. satır ve 5. sütundaki 3F ile değiştirilmektedir. Bayt değiştirme şeması şekil 2.10'da gösterilmektedir.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

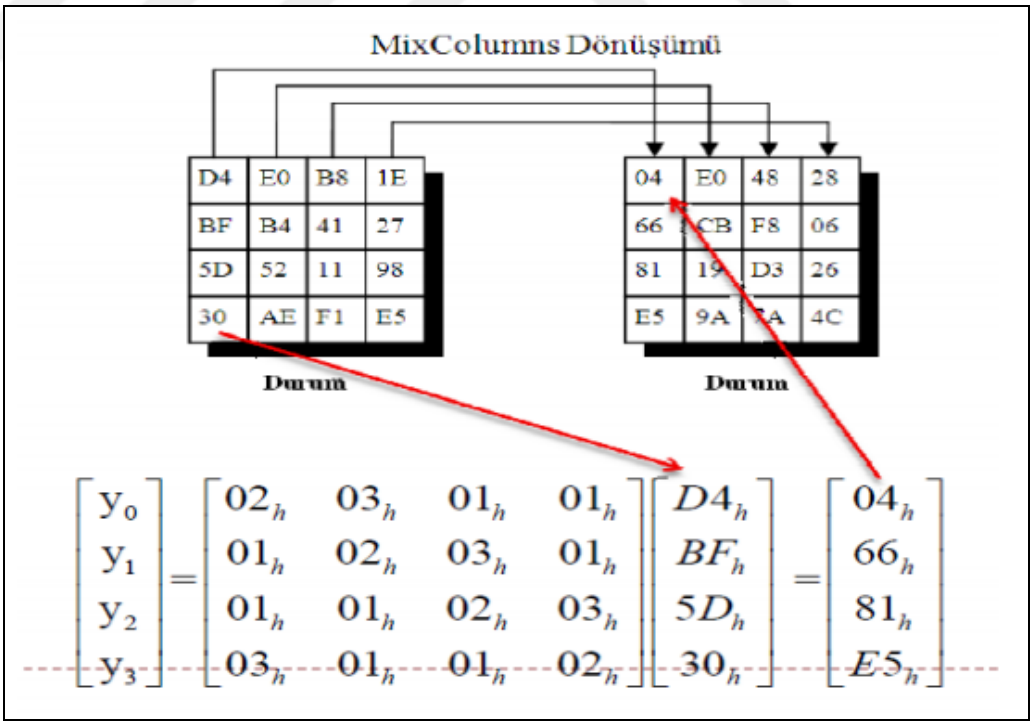
Şekil 2.10 AES Bayt Değiştirme (Anonymous 2016)

- Satır Kaydırma: 4x4'lük durum matrisinde ilk satır aynı kalmaktadır. İkinci satır bir bayt, üçüncü satır iki bayt, üçüncü satır üç bayt kaydırılmaktadır. Satır kaydırma şeması şekil 2.11'de gösterilmektedir.



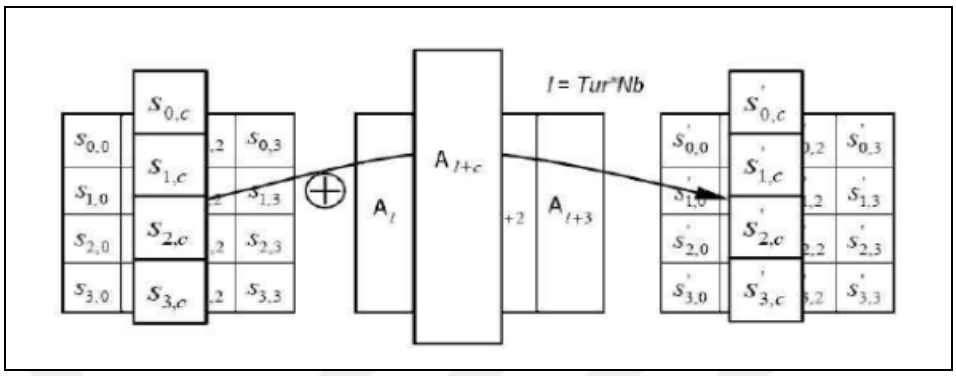
Şekil 2.11 AES Satır Kaydırma (Anonymous 2016)

- Sütun Karıştırma: Her bir sütun a(x) = {03}x^3 +{01}x^2 +{01}x+{02} denklemi ile matris çarpımı yapılarak değiştirilmektedir. Sütun karıştırma şeması şekil 2.12'de gösterilmektedir.



Şekil 2.12 AES Sütun Karıştırma (Anonymous 2016)

- Döngü Anahtarını Ekleme: Her döngünün sonunda anahtar eklenmektedir. Tur ve blok anahtarı XOR işlemine tabii tutularak anahtar oluşturulmaktadır. Döngü anahtarını ekleme şeması şekil 2.13'da gösterilmektedir.



Şekil 2.13 AES Döngü Anahtarını Ekleme (Anonymous 2016)

2.3 Bölüm Değerlendirmesi

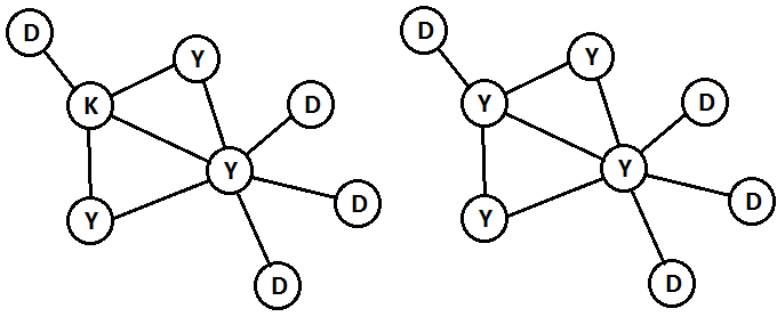
Bu bölümde Nesnelerin İnterneti detaylı olarak tanımlanmış, tarihçesi, kullanım alanları ve mimarisinden bahsedilmiştir. Nesnelerin İnternetine yönelik saldırı ve tehditler üzerine yapılan çalışmaların özetleri verilmiştir. Ardından saldırılara karşı alınacabilecek güvenlik önlemleri üzerine yapılan çalışmaların özetleri de verilmiştir. Yapılan çalışmalara göre Nesnelerin İnternetindeki güvenlik açıklarına temel bir bakış açısıyla çözümler ortaya konmuştur. Bu temel çözümler haricinde üreticilerin ürettikleri düğümlerin tek bir noktadan yönetiminin yapılması, düğümlerin kötü amaçlı olup olmadığının tespit edilmesi ve bununla birlikte mevcut bir ağa yeni katılan düğümlerin doğrulanması üzerine çalışma bulunmadığı görülmektedir. Bu tez çalışmasında da katkı olarak, bahsedilen bu yönetimi yapabilecek ve güvenlik açıklarına çözüm olabilecek yeni bir yöntem önerilmekte olup detayları üçüncü bölümde açıklanmaktadır.

3. MATERYAL ve YÖNTEM

Nesnelerin İnternetinde çeşitli teknolojiler kullanılmaktadır. Bu teknolojilerde genel olarak iletişim, şifreli olarak sağlanmaktadır. Ancak bu şifreleme algoritmalarına ve diğer güvenlik önlemlerine rağmen yine de özellikle güvenlik konusunda en kritik işlemlerden biri olan ağa katılım esnasında bazı güvenli açıkları meydana gelmektedir. Bu teknolojilerde haberleşme güvenliği ve ağa yeni bir düğümün katılımı işlemlerinde benzerlikler bulunmasına rağmen mevcut durumda, tek bir noktadan bütünleşik bir güvenlik yönetimi çözümü olmadığı için her bir teknoloji için gizlilik ve güvenlik yönetiminin ayrı ayrı yapılması gerekmektedir. Bu yönetimin tek bir noktadan yapılmasını ve buna bağlı olarak güvenli ağa katılımın sağlanması için öncelikle mevcut güvenlik yöntemi üzerinde detaylı bir analiz yapılacaktır. Ardından ise buradaki açıklara karşı yeni bir güvenlik yöntemi önerilecektir.

3.1 Güvenlik Analizi

Nesnelerin İnterneti ağı, genel olarak dağıtık ya da merkezi güvenlik modelinde olabilir. Bu modellerde 3 farklı eleman mevcuttur. Bu elemanlar; düğüm (D), koordinatör (K) ve yönlendiricidir (Y). Güvenlik modelleri şekil 3.1'de gösterilmektedir.



(a) (b)

Şekil 3.1 Güvenlik Modelleri (Anonymous 2016)

a. Merkezi, b. Dağıtık

Her eleman bir ya da birden fazla eleman ile iletişim durumunda olabilir. Şekil 3.1 (a)'da görüleceği üzere koordinatör, merkezi güvenlikli ağı yönetir. Koordinatör, yaptığı doğrulamalar neticesinde ağa düğümlerin katılımını kontrol eder. Şekil 3.1 (b)'de görüleceği üzere yönlendiriciler, dağıtık güvenlikli ağı yönetir. Yönlendiriciler, ağa katılacak düğümlerin doğrulamasını yapar (Anonymous 2016).

3.1.1 Güvenlik anahtarları

Güvenlik anahtarları ile tüm iletişim şifrelenerek yapılmaktadır. Ağ Anahtarı ve Bağlantı Anahtarı olmak üzere iki güvenli anahtarı mevcuttur.

a) Ağ Anahtarı: Ağ anahtarı, ağdaki elemanlar tarafından birbirleriyle paylaşılmaktadır. İletişimi şifrelemek ve iletişimin şifresini çözmek amacıyla kullanılmaktadır (Anonymous 2018).

a) Bağlantı Anahtarı: Bağlantı anahtarı kullanılarak ağa yeni katılacak düğüme ağ anahtarı, şifrelenip gönderilmektedir (Anonymous 2018). İki çeşit bağlantı anahtarı bulunmaktadır.

    1) Önceden Yapılandırılmış Küresel Bağlantı Anahtarı: Tüm elemanlarda aynı anahtar vardır. Üreticilerin kendilerine oluşturduğu anahtarı veya üreticilere dağıtılmış küresel bağlantı anahtarı, elemanlar tarafından kullanılmaktadır. Üreticilere dağıtılmış anahtar sayesinde farklı sürüm ve üreticiye ait elemanlar bir ağa katılabilir. Üreticilerin kendine oluşturduğu anahtar ile yalnızca aynı üreticinin ürettiği elemanlar ağa katılabilir.

    2) Önceden Yapılandırılmış Benzersiz Bağlantı Anahtarı: Her düğümde farklı bağlantı anahtarı mevcuttur.

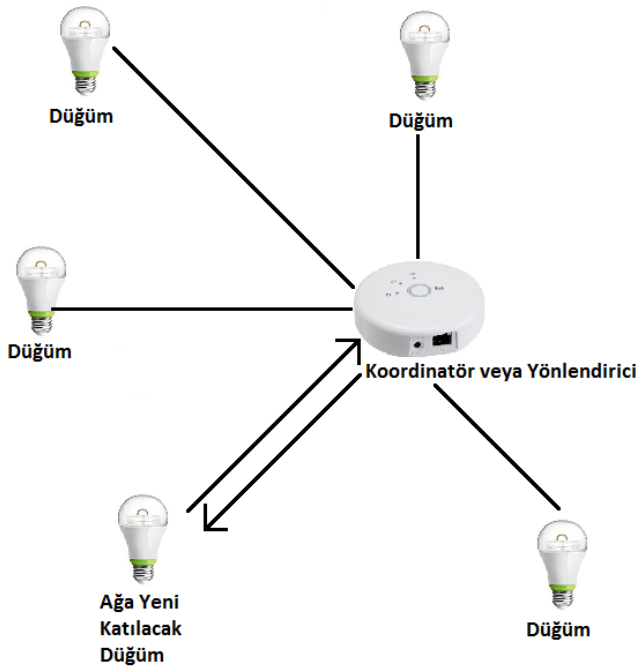
Üreticiler, müşterilerin kolay kurulum yapabilmesi ve yeni üretilen düğümlerin daha eski sürümdeki düğümlerle birlikte çalışabilmesi için ağa katılım esnasında genellikle

küresel bağlantı anahtarının kullanılmasına olanak sağlamaktadırlar. Bu küresel bağlantı anahtarları zaman zaman açığa çıktığından dolayı siber saldırganlardan tarafından da bilinmektedir ve bu durum güvenlik açığına neden olmaktadır. Bu çalışmada, düğümlerin güvenlik yönetiminin yapılması ile birlikte bahsedilen açığı kapatmaya yönelik katkı yapmak için bir yöntem önerilmektedir.

3.1.2 Ağa katılım

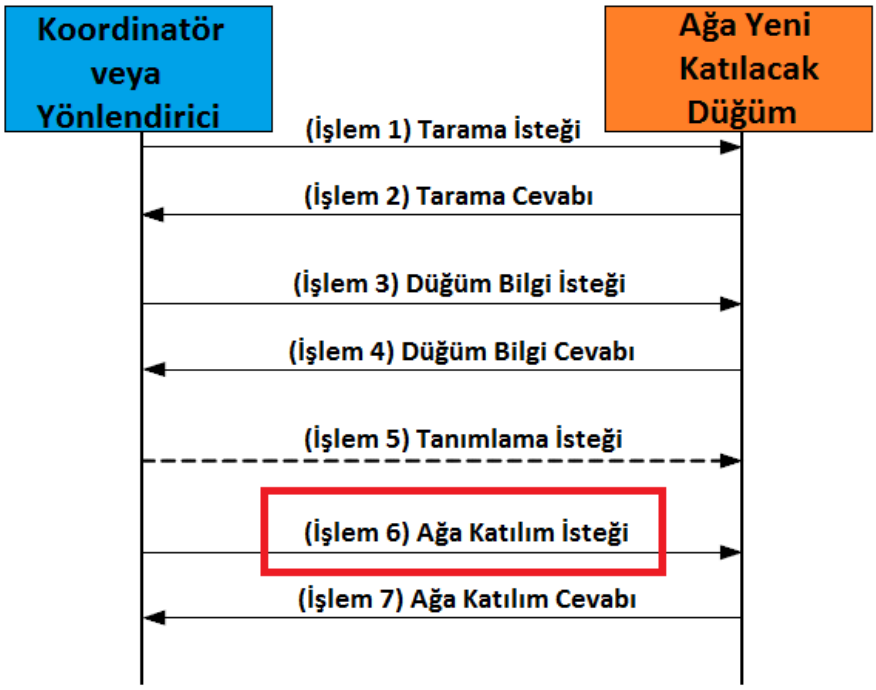
Nesnelerin İnterneti ağlarında kablosuz iletişim, ağ anahtarı kullanılıp şifrelenir. Ağ anahtarı, ağa bir düğüm ekleneceği zaman yeni düğüme gönderilir. Bu gönderim, önceden yapılandırılmış ve dağıtılmış bağlantı anahtarıyla yapılır. Ağ koordinatörü katılım sırasında, ağ anahtarını, bağlantı anahtarıyla şifreleyip katılacak düğüme gönderir. Aynı bağlantı anahtarına sahip olan katılacak düğüm de, şifreli iletiyi çözüp ağ anahtarına ulaşarak ağa katılır (Gislason 2018).

Şekil 3.2 düğümün ağa katılma modelini göstermektedir.



Şekil 3.2 Düğümün Ağa Katılma Modeli

Mevcut durumda, ağa katılım sırasında ağ koordinatörü ve yeni katılacak düğüm arasında bir iletişim olmaktadır. Bu iletişim için koordinatör, öncelikle kapsama alanındaki alanlara tarama isteği göndererek ağa katılacak yeni bir düğüm olup olmadığının sorgulamasını yapmaktadır. Yeni katılacak bir düğüm olması durumunda, bu düğüm gelen isteklere cevaplar vererek bazı adımları tamamlayıp ağa katılım sağlamaktadır. Bu işlemler, Şekil 3.3'te sırasıyla gösterilmektedir.



Şekil 3.3 Düğümün Ağa Katılma Protokolü

Şekil 3.3'te gösterildiği üzere mevcut durumda ağa katılma yedi işlemde gerçekleşmektedir. Bu işlemler sırasıyla şöyledir;

- Tarama İsteği
- Tarama Cevabı
- Düğüm Bilgi İsteği
- Düğüm Bilgi Cevabı
- Tanımlama İsteği
- Ağa Katılım İsteği
- Ağ Katılım Cevabı

3.1.3 Güvenlik açığının tanımlanması

Nesnelerin İnterneti ağlarında iletişim şifrelenerek yapılmaktadır. Ancak saldırganın Şekil 3.3'te gösterilen protokolün altıncı işleminde ağa katılım isteği paketini yakalaması ve önceden yapılandırılmış küresel bağlantı anahtarına sahip olması durumunda, saldırgan iletilen ağ anahtarına ulaşıp ağın kontrolünü ele geçirebilir. Şekil 3.3'te kırmızı renk ile işaretli işlemde, bahsedilen güvenlik açığı oluşmaktadır. Üretilen düğümlerin tek noktadan kontrolü ve bahsedilen güvenlik açığına çözüm olarak önerilen yöntem, sonraki bölümde anlatılacaktır.

3.2 Önerilen Yöntem

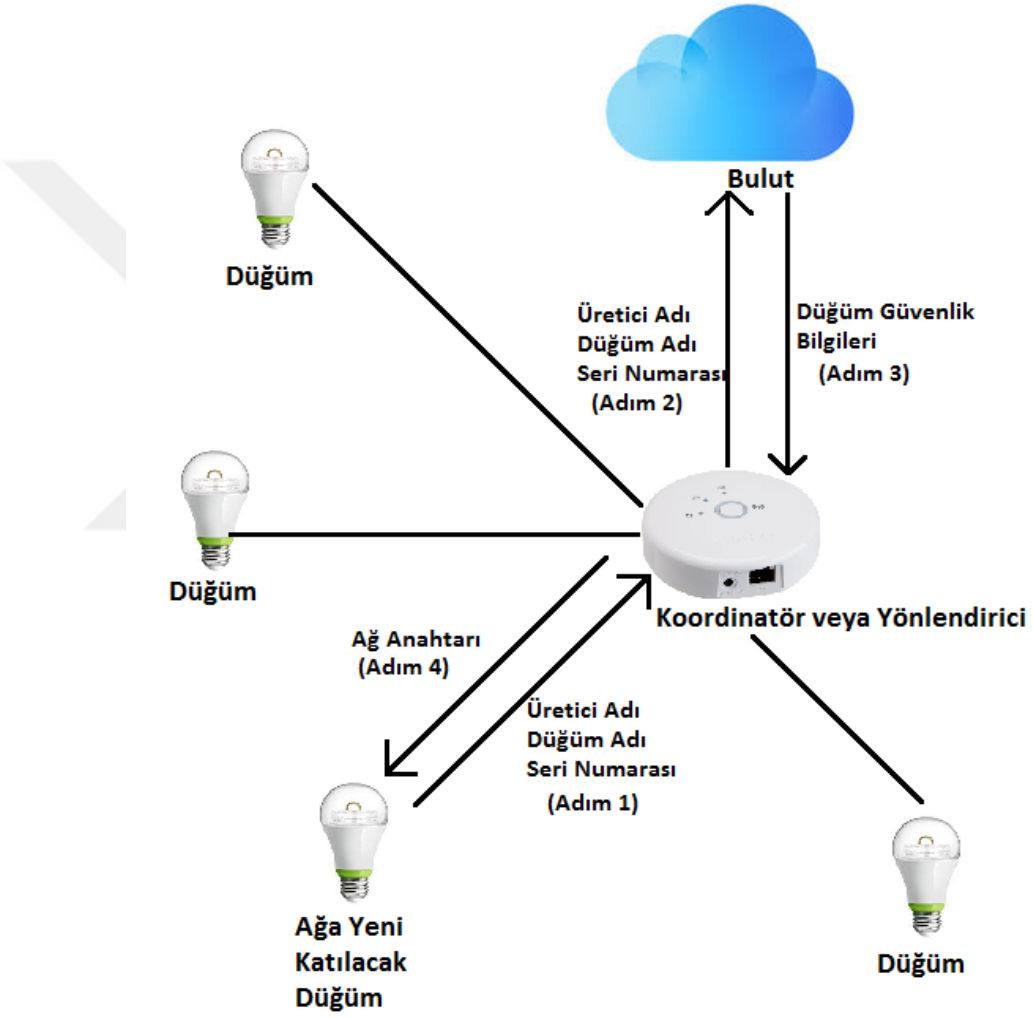
Üretilen düğümleri tek bir noktadan yönetmek ve önceki bölümde bahsedilen güvenlik açığının kapatılmasına katkı olarak Nesnelerin İnterneti ağlarına güvenli katılım için yeni bir yöntem olan bulut yöntemi önerilmektedir. Bu yöntemle düğümlerin üretici adı, ürün adı, seri numarası ve bağlantı anahtarı gibi bilgileri bulutta da tutulmaktadır. Örnek olarak, Çizelge 3.1'de altı adet düğümün bilgileri listelenmektedir.

Çizelge 3.1 Bulut Bilgileri

Üretici Adı	**Ürün Adı**	**Seri Numarası**	**Bağlantı Anahtarı**
Üretici 1	Lamba	L392283	64 53 67 55 6B 58 70 32 73 35 76 38 79 2F 42 3F
Üretici 1	Lamba	L392284	78 21 41 25 44 2A 47 2D 4B 61 50 64 53 67 56 6B
Üretici 2	Işık Sensörü	I245932	34 74 37 77 21 7A 25 43 2A 46 2D 4A 61 4E 64 52
Üretici 2	Işık Sensörü	I245932	6D 5A 71 34 74 36 77 39 7A 24 43 26 46 29 4A 40
Üretici 3	Sıcaklık Sensörü	S201516	5D 4B 61 54 94 65 79 40 6A 24 43 26 46 29 5B 32
Üretici 3	Sıcaklık Sensörü	S201517	6A 32 61 24 64 53 78 42 8A 94 53 46 46 29 4C 45

Ağa yeni bir düğüm ekleneceği durumda, düğümün bilgilerini almak için ağ koordinatörü, buluta bağlanmaktadır. Ağ anahtarını, buluttan aldığı düğüme ait bağlantı anahtarı ile şifreleyerek düğüme iletmektedir. Düğüm de aynı bağlantı anahtarına sahip olduğundan şifreli iletiyi çözerek ağ anahtarına ulaşarak ağa katılım sağlamaktadır.

Şekil 3.4'te, önerilen yönteme göre bir düğümün ağa katılma adımları gösterilmektedir.



Şekil 3.4 Önerilen Yöntemde Düğümün Ağa Katılımı

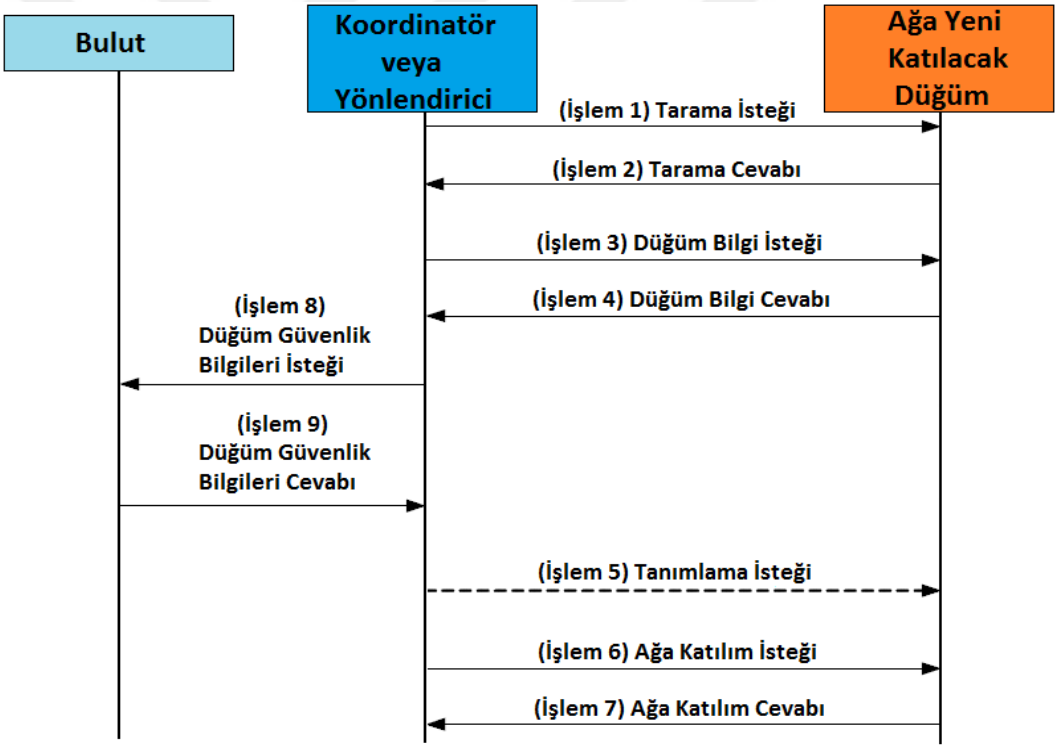
1. Adımda ağa katılım yapacak düğüm, koordinatörün gönderdiği düğüm bilgi isteğinin cevabı olarak; düğüm adı, üretici adı ve seri numarasını koordinatöre iletmektedir.

2. Adımda koordinatör, buluta erişerek 1. adımda elde ettiği bilgilere göre düğüme ait bilgileri istemektedir.

3. Adımda ise bulut, düğümün bilgilerini koordinatöre iletmektedir.

4. Adımda, koordinatör, düğümden aldığı ve buluttan elde ettiği bilgiler örtüşüyorsa, düğümün bağlantı anahtarıyla ağ anahtarını şifreleyerek düğüme iletmektedir. Aynı bağlantı anahtarına sahip olan düğüm de şifreyi çözüp ağ anahtarına ulaşarak ağa katılım yapmaktadır.

Şekil 3.5'te ise önerilen yöntemin protokolü gösterilmektedir.



Şekil 3.5 Önerilen Yöntemde Düğümün Ağa Katılma Protokolü

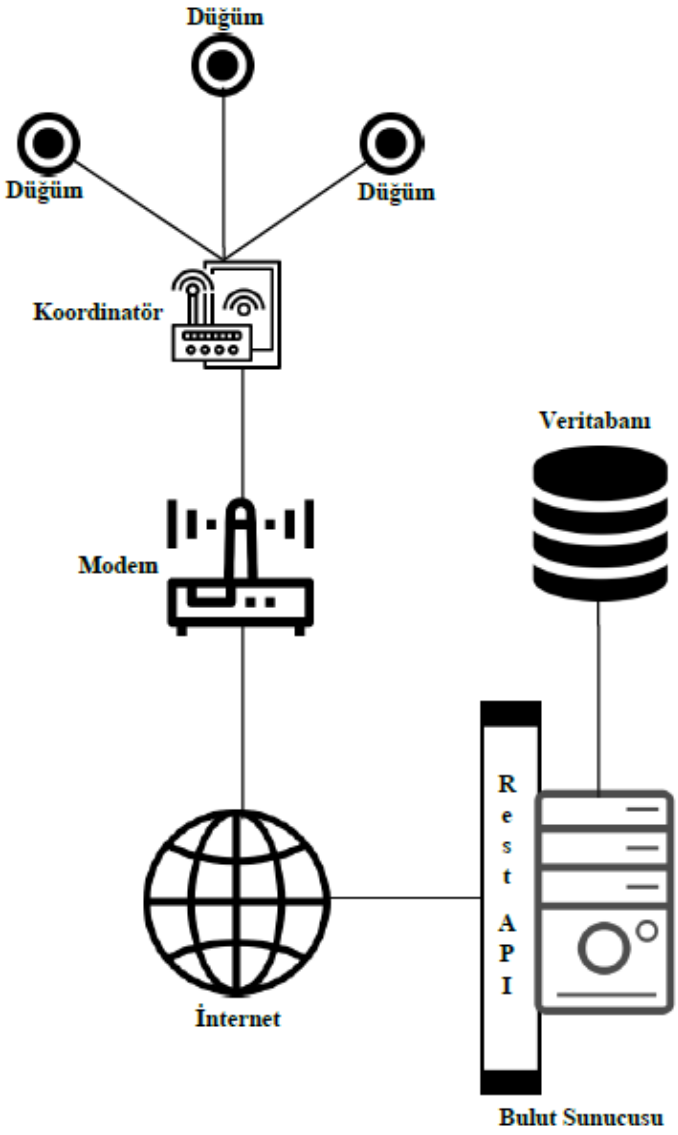
Önerilen yöntemin protokolünde, mevcut protokole sekizinci ve dokuzuncu işlemler ilave edilmiştir. Bu işlemler ile ağa katılım sırasında mevcut protokolde bulunan güvenlik açığının kapatılmasına katkı yapılmaktadır.

Ayrıca Nesnelerin İnternetinde kaynak kısıtı olduğu için bu yöntemde düğümlerin bilgileri, koordinatörde tutulmamaktadır. Bir düğüm ağa katılım yapacağı zaman koordinatör, buluta güvenli erişerek düğümün güvenlik bilgilerini alarak ağa katılımını yapmaktadır.

Yine bu yöntemde bulut sunucularına, sunuculardaalınan standart önlemler uygulanmaktadır. Buluttaki bilgilere kimlik doğrulamayla erişim sağlanmakta ve bilgiler güvenli veri tabanlarında tutulmaktadır. Bu şekilde bulut sunucularında bilgi güvenliği önlemleri alınmaktadır.

3.2.1 Önerilen yöntemin mimarisi

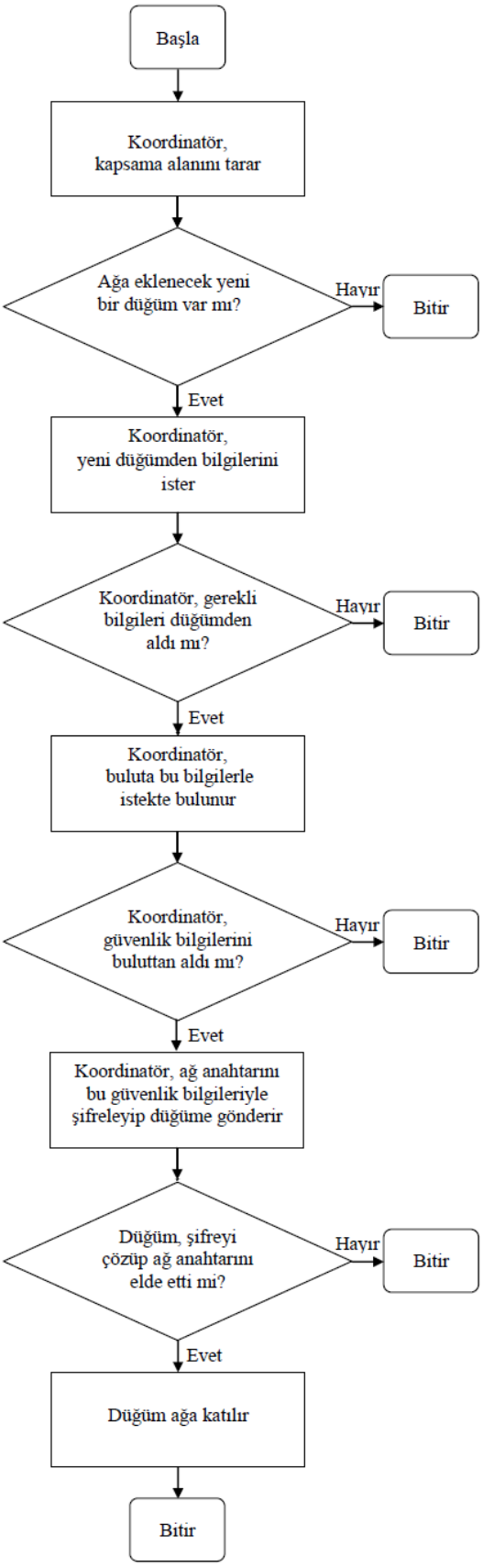
Önerilen yöntemde, koordinatör, modem ile İnternete bağlanmaktadır. İnternet üzerinden bulut sistemine Rest API ile erişim sağlamaktadır. Bu sayede ağa katılmak isteyen düğümlerin bilgilerini bulut sisteminden almaktadır. Şekil 3.6'da önerilen yöntemin mimarisi gösterilmektedir.



Şekil 3.6 Önerilen Yöntemin Mimarisi

3.2.2 Önerilen yöntemin akış şeması

Önerilen yöntemde, bir düğümün ağa katılması için bazı adımların tamamlanması gerekmektedir. Bu adımlar, şekil 3.7'de önerilen yöntemin akış şeması ile gösterilmektedir.



Şekil 3.7 Önerilen Yöntemin Akış Şeması

3.3 Bölüm Değerlendirmesi

Bu bölümde öncelikle Nesnelerin İnternetinde güvenlik analizi yapılmış ve ağa katılım protokolü anlatılmıştır. Düğümlerin tek bir noktadan güvenlik yönetimine olanak sağlayan ve ağa katılım esnasında meydana gelen güvenlik açıklarına çözüm olarak yeni bir yöntem geliştirilmiş, detayları, mimarisi ve akış şeması anlatılmıştır. Ayrıca, önerilen yöntem ile birlikte ağa katılımın kullanıcı dostu olması devam etmektedir. Kullanıcı, bu yöntem ile ağına yeni düğüm eklemek istediğinde yalnızca düğümü çalıştırarak, koordinatörün düğümü ağa eklemesini beklemektedir.

4. ÖNERİLEN YÖNTEMİN UYGULANMASI

Bu bölümde, önerilen yöntemin uygulanması ve gözlemlenen sonuçların değerlendirmesi verilecektir.

4.1 Uygulama Platformu

Tez çalışması kapsamında önerilen yöntemi uygulamak için kullanılan bilgisayarın ve yazılım platformlarının özellikleri aşağıdaki gibidir.

- Intel core i3
- 2.13 GHz CPU
- 3 GB RAM
- Nvidia GeForce
- Windows İşletim Sistemi
- Eclipse IDE
- WAMP Sunucu

WAMP sunucu üzerinde çalışan bulut geliştirilirken kullanılan programlama dilleri ve veri tabanı aşağıdadır.

- PHP
- JavaScript
- MySQL

Benzetim için kullanılan programlama dili ve grafik kütüphanesi aşağıdaki gibidir.

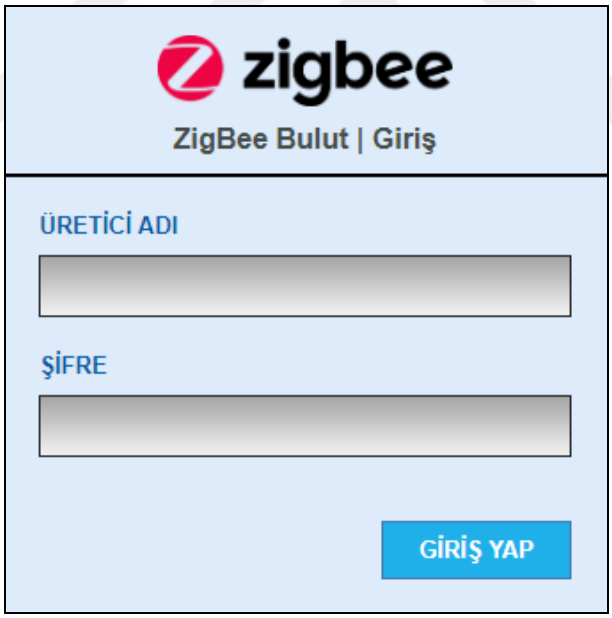
- Java
- Graphics2D

4.2 Veri Seti

Önerilen yöntem, Nesnelerin İnternetinde en çok kullanılan teknolojilerden birisi olan ZigBee düğümleri üzerinde uygulanmıştır. ZigBee düğümlerinin varsayılan özelliklerine göre bilgiler oluşturulmuştur.

4.3 Önerilen Yöntemin Uygulanması

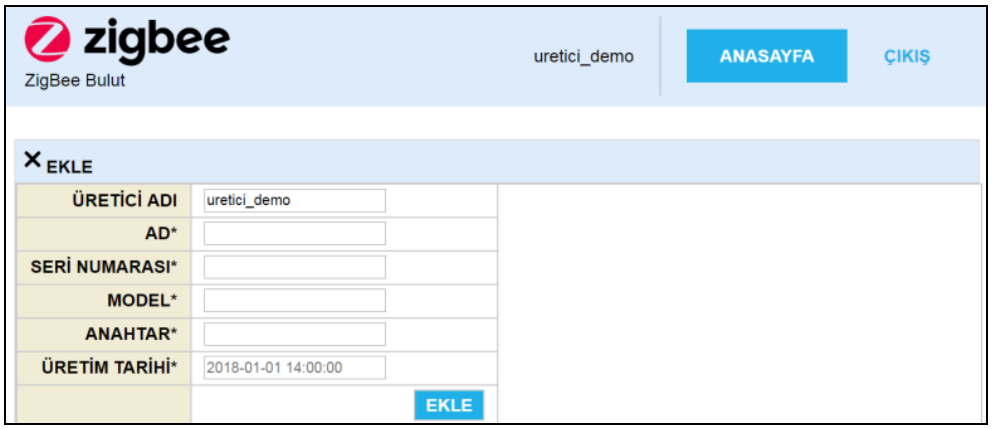
Önerilen yöntem için öncelikle ZigBee Bulut uygulaması geliştirilmiştir. Üreticiler, ürettikleri düğümlerin güvenlik bilgilerini bu sisteme yüklemektedir. Bu sistem ile düğümler tek bir noktadan kontrol edilebilmektedir. Ayrıca bir düğüm ağa katılacağı zaman koordinatör, bu sisteme bağlanıp düğüme ait gerekli bilgileri almaktadır. Şekil 4.1'de uygulamanın giriş ekranı gösterilmektedir.



Şekil 4.1 Uygulama Giriş Ekranı

Üreticilerin uygulamaya giriş yaparken üretici adı ve şifre bilgilerini kullanmaları gerekmektedir.

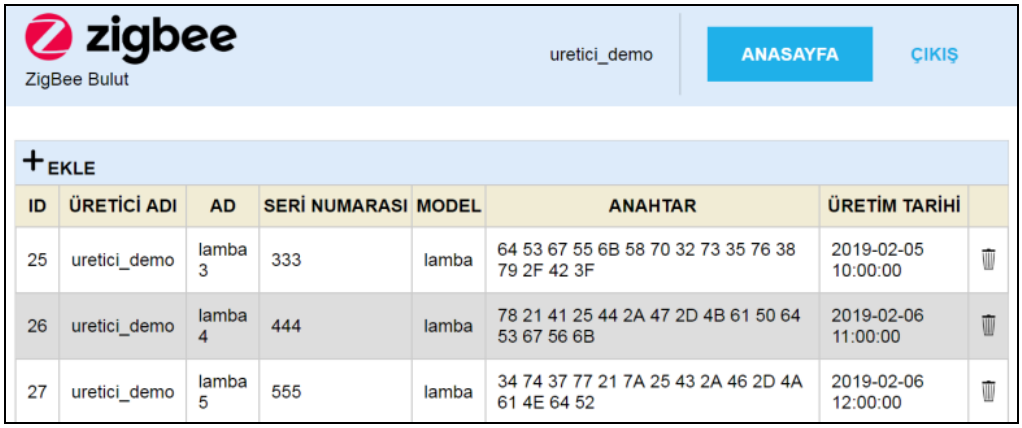
Şekil 4.2'de üreticilerin ürettikleri düğümleri sisteme ekleme ekranı gösterilmektedir.



Şekil 4.2 Düğüm Ekleme Ekranı

Üreticiler düğüm eklerken üretici adı, ad, seri numarası, model, anahtar ve üretim tarihlerini girmeleri gerekmektedir.

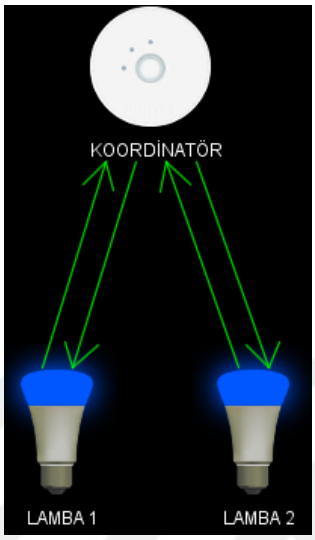
Eklenen düğümler tablo halinde listelenmektedir. Düğüm listesinde eklenen tüm düğümler görüntülenmekte ve bu listeden düğümler silinebilmektedir. Şekil 4.3'te düğüm listesi gösterilmektedir.



Şekil 4.3 Düğüm Listesi

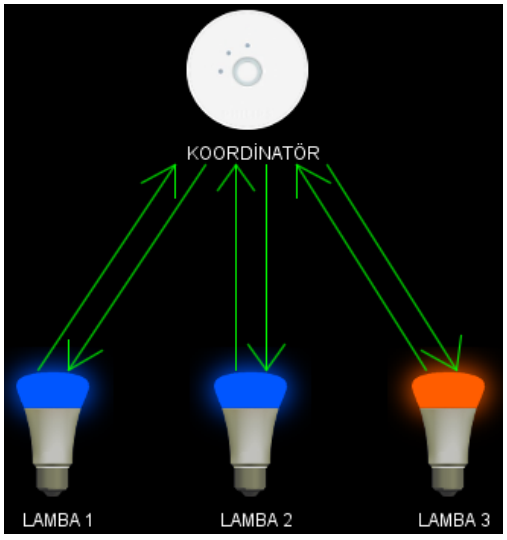
Öncelikle mevcut protokolün benzetimi yapılmıştır. Benzetimde başlangıç durumunda, ZigBee ağında bir koordinatör ve iki akıllı lamba birlikte çalışmaktadır. Benzetimde lamba ve koordinatör arasındaki yeşil renkli oklar bağlantının sağlandığını, kırmızı renkli oklar ise bağlantının kurulmadığını göstermektedir. Ayrıca lamba isimlerinin

kırmızı olması, lambanın kötü amaçlı olduğunu veya atak amacıyla kullanılabileceğini göstermektedir. Şekil 4.4'te ağa yeni bir düğüm katılmadan önceki başlangıç durumu gösterilmektedir.



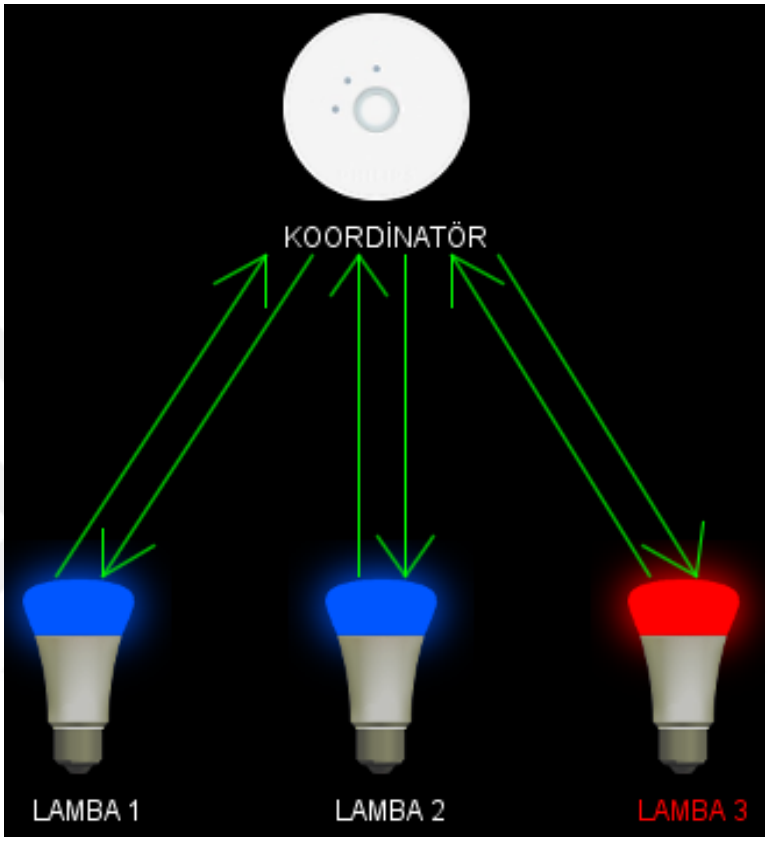
Şekil 4.4 Mevcut Protokolün Benzetimi: Başlangıç Durumu

Ardından kötü amaçlı olmayan lamba 3, küresel bağlantı anahtarını kullanarak ağa katılmaktadır. Şekil 4.5'te görüldüğü gibi koordinatör ve lamba arasında bağlantı sağlanmıştır.



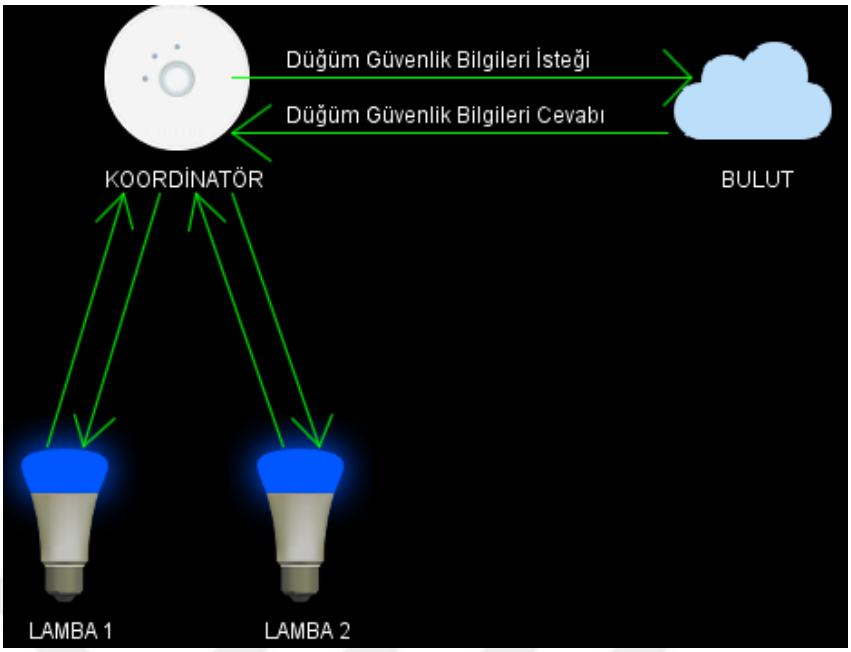
Şekil 4.5 Mevcut Protokolün Benzetimi: Ağa Katılım Durumu

Bir başka durumda ise kötü amaçlı olan lamba 3, küresel bağlantı anahtarını kullanarak ağa katılmaktadır. Bu durumda saldırgan ağdaki güvenlik açığını kullanarak haberleşmeyi çözebilmektedir. Şekil 4.6'da görüldüğü gibi koordinatör ve lamba arasında bağlantı sağlanmıştır.



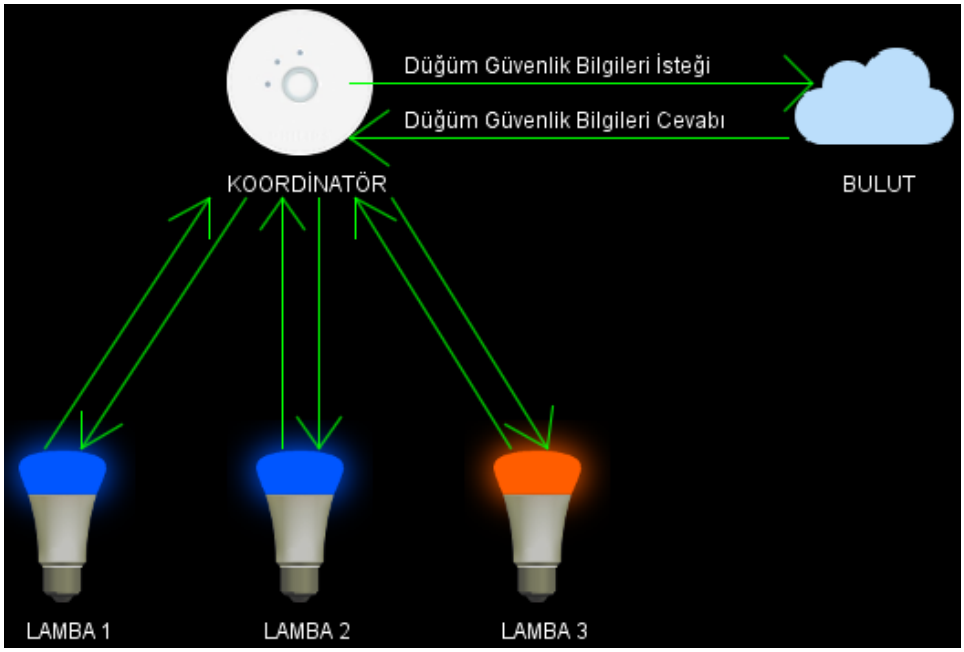
Şekil 4.6 Mevcut Protokolün Benzetimi: Kötü Amaçlı Düğüm Ağa Katılım

Ardından, önerilen bulut yöntemi benzetim ortamında uygulanmıştır. Bu yöntem ile yeni düğüm ağa katılacağı zaman koordinatör bulutla bağlantı kurup gerekli bilgileri almaktadır. Şekil 4.7'de ağa yeni bir düğüm katılmadan önceki başlangıç durumu gösterilmektedir.



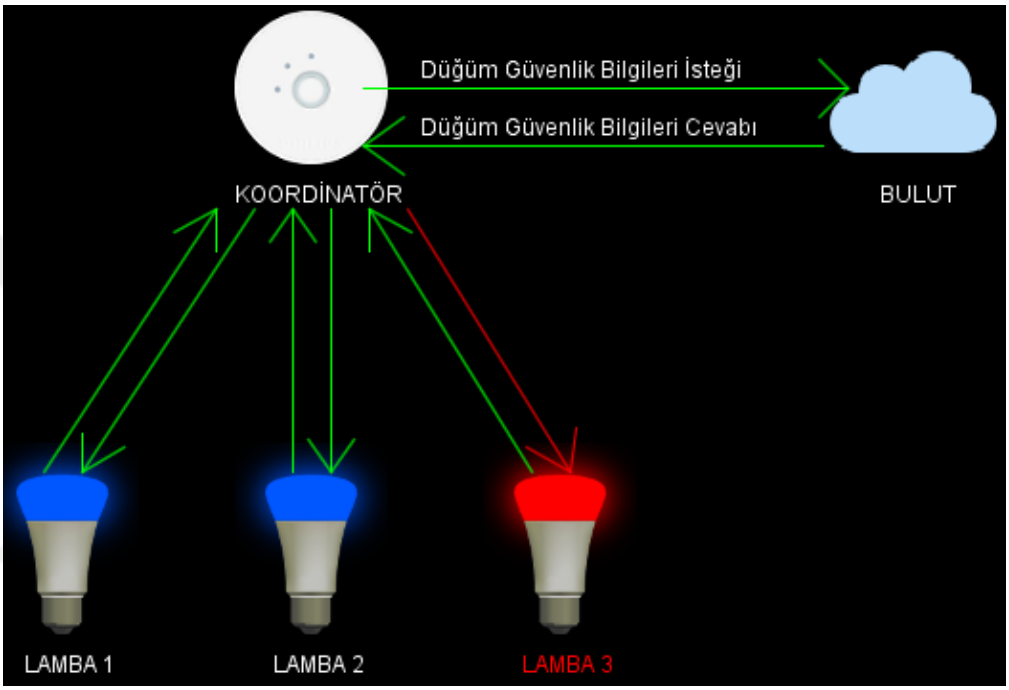
Şekil 4.7 Önerilen Yöntemin Benzetimi: Başlangıç Durumu

Ardından kötü amaçlı olmayan lamba 3, koordinatörün, bulut sistemini kullanmasıyla ağa katılmaktadır. Şekil 4.8'de görüldüğü gibi koordinatör ve lamba arasında bağlantı sağlanmıştır.



Şekil 4.8 Önerilen Yöntemin Benzetimi: Ağa Katılım Durumu

Bir başka durumda ise kötü amaçlı lamba 3, ağa katılım isteği göndermektedir. Ancak bu kötü amaçlı lamba, resmi düğüm üreticileri tarafından üretilmediği için bulut sisteminde bilgileri bulunmamaktadır. Koordinatör de bulut sisteminde bu kötü amaçlı lambaya ait bilgilere ulaşamadığı için lamba ağa katılamamaktadır. Şekil 4.9'da görüleceği üzere koordinatör ve lamba arasında bağlantı kırmızı olmakta ve lambanın ağa katılım isteği reddedilmektedir.



Şekil 4.9 Önerilen Yöntemin Benzetimi: Kötü Amaçlı Düğüm Ağa Katılım

4.4 Sonuçların Değerlendirilmesi

Önerilen yöntem, düğümlerin tek noktadan kontrolüne olanak sağladığı gibi ağa katılım yönteminin kullanıcı dostu olmasını da devam ettirmektedir. Kullanıcı, bu yöntem ile mevcut ağına düğüm eklemek istediğinde yalnızca düğümü çalıştırıp, koordinatörün ağa eklenmesini beklemektedir.

Önerilen yöntemde buluta erişim güvenli bağlantılarla yapılmaktadır. Bu güvenli bağlantı ile birlikte hem ağ koordinatörlerinin hem de üreticilerin buluta erişimi

sırasında bir güvenlik açığı meydana gelmemektedir. Ayrıca bulut, güvenli sunucular üzerinde çalışmakta ve bilgiler bulutta güvenli olarak tutulmaktadır. Bulut sunucularında varsayılan güvenlik önlemleri alınmaktadır. Böylece sunucular çalışmasına güvenli şekilde devam etmektedir.

Yönteme, bulutun düğüm ve koordinatörlerle beraber yerelde çalışması önerisi getirilebilir. Ancak bu durumda uygulama uzakta tek bir noktada çalışmayacağı, tüm koordinatörler ve üreticiler tarafından erişilemeyeceği için öncelikle bulut olmaktan çıkmaktadır. Önerilen yöntem, kullanıcı dostu olma özelliğini taşıdığı ve kullanıcıya ekstra sorumluluklar yüklememeyi amaçladığı ve yeni üretilen düğümlerin bilgilerinin yerellerde çalışan dağıtık sistemlere eklenmesi söz konusu olamayacağı için bu öneri kapsam dışı kalmaktadır. Ayrıca uygulamnın tek noktadan bulut olarak çalışması, bilgi güvenliğini artırmaktadır çünkü bulutta tüm önlemler alınacak ve bulutun yönetiminden sorumlu teknik bilgiye sahip bir birim olacaktır.

Önerilen yöntemdeki bulut sistemine yönelik önceki paragrafta anlatılan güvenlik önlemlerine rağmen bazı dezavantajlı durumlar meydana gelebilir. Örneğin, bulut sistemine yönelik saldırılar başarılı olmaları durumunda, ağa yeni düğümlerin katılmasını engelleyebilir. Bu saldırılardan en yaygın kullanılan ise servis engelleme saldırılarıdır (Masum ve Samet 2018, Aslan ve Samet 2017). Bu saldırının başarılı olması durumunda buluttaki verilerin açığa çıkması durumu olmasa da, buluta erişim kesilecek ve düğümler bu sırada ağa katılım yapamayacaktır. Bulutun güvenlik yönetiminden sorumlu bir birim olması ve saldırı sırasında çözüm üretilmesi, önerilen yöntemdeki ihtiyaçlardan biri olabilir. Ancak önerilen yöntemin, bu dezavantaja rağmen mevcut yöntemden daha güvenli olduğu değerlendirilmektedir.

Önerilen yöntemde, kullanıcının elinde bulunan ancak bilgileri bulutta olmayan güvenilir düğümler ağa katılamayacaktır. Bu durumda kullanıcının, düğümün bilgilerinin buluta eklenmesi amacıyla üreticiyle iletişime geçmesi gerekmektedir.

Bulut uygulamasına yönelik olabilecek siber saldırılar ve alınan önlemler çizelge 4.1'de anlatılmaktadır.

Çizelge 4.1 Siber Saldırılar ve Alınan Önlemler

Siber Saldırılar	**Alınan Önlemler**
SQL (Structured Query Language) Sokuşturma	Kullanıcıdan alınan girdiler filtrelenerek veri tabanına sorguya gönderilmektedir.
XSS (Cross Site Scripting)	Alınan girdiler filtrelenip ekranda kodlanarak gösterilmektedir.
HTTP (Hyper-Text Transfer Protocol) Başlıklarından Bilgi Sızması	HTTP başlık bilgilerinin yollanması engellenmektedir.
Kritik Alanlarda Otomatik Tamamlama	Arayüzde kritik girdileri içeren alanlarda otomatik tamamlama kaldırılmaktadır.

Çizelgeye göre belirtilen siber saldırılara karşı bulut uygulamasında önlemler alınmıştır.

Yapılan çalışmalar incelendiğinde tek noktadan güvenlik yönetimine olanak sağlayan ve ağa katılım esnasında kullanıcıya sorumluluk yüklemeden açıkları kapatmayı amaçlayan bütünleşik bir çözüm bulunmamaktadır. Bu sebeple önerilen yöntemin direkt olarak benzer bir çözüm ile performans karşılaştırması yapılamamaktadır. Ancak önerilen yöntemin performansı kendi içinde değerlendirilecek olursa, mevcut protokoldeki işleyişe ek olarak yalnızca koordinatör, ağa katılacak düğümün bilgilerini almak için buluta bağlanmaktadır. Bu adım, küçük bir gecikmeye neden olmaktadır. Ancak önerilen yöntemin güvenlik açıklarının çözümüne yönelik yaptığı katkıya bakılacak olursa bu küçük gecikme önemsiz kalmaktadır.

5. SONUÇLAR

İnternet, günümüzde hayatı kolaylaştırmayı amaçlaması nedeniyle yaşamda çok önemli bir yer edinmiştir. Gelişen İnternet teknolojileri sayesinde her yerden İnternete erişim sağlanmaktadır. Bu teknolojilere, mobil, kablosuz sensör ağları, uzaktan takip ve kontrol sistemleri ile Nesnelerin İnterneti örnek olarak gösterilebilir.

Ancak gelişen bu teknolojiler yaşamı kolaylaştırsa da bazı güvenlik açıklarına sebep olmaktadır. Örneğin, yaygın kullanım sayesinde üretilen çok sayıda verinin ihlaller sebebiyle açığa çıkmasının sonuçları ciddi boyutlarda olmaktadır.

Yaygın kullanılan İnternet teknolojilerinden birisi olan Nesnelerin İnterneti de artık hayatın içinde çok önemli bir yere sahip olmuştur. Birçok alanda akıllı nesneler kullanılmaya başlanmıştır. Herhangi bir ihlal durumundaki sonuçların büyüklüğü nedeniyle Nesnelerin İnternetinde gizlilik ve güvenlik yönetiminin önemi artmaktadır. Örneğin, İnternete bağlı olan nesneler, saldırganların kullanıcıları takip etmesine imkân verebilir ya da bir kimsenin arabasını çalıştırabilir veya kapısını kilitleyebilir. Bunlara ek olarak kritik sistemlerdeki bir sızmanın sonuçları daha fazla olacaktır. Bütün bu kötü etkiler düşünüldüğünde bu teknolojide gizlilik ve güvenlik yönetimi konusu daha da önem kazanmaktadır.

Tez çalışmasında, öncelikle Nesnelerin İnternetinin tanımı, kullanım alanları, mimarisi ve bu alanda kullanılan kablosuz haberleşme teknolojileri açıklanmaktadır. Ardından mevcut çalışmalar ile Nesnelerin İnternetinde güvenlik analizi yapılmaktadır. Bu alanda kullanılan haberleşme protokolleri incelemekte ve olası güvenlik açıkları tespit edilmektedir. Güvenlik açıklarına karşı olması gereken temel önlemler anlatılmakta ve tek noktadan güvenlik yönetimiyle birlikte özellikle mevcut ağa bir düğüm katılması esnasında meydana gelen güvenlik açıklarının kapatılmasına katkı yapmak amacıyla yeni bir yöntem önerilmektedir. Bu yöntem ile birlikte bir düğüm mevcut bir ağa katılım yapacağı zaman, ağ koordinatörü bulut sistemine bağlanarak katılacak düğüme ait güvenlik bilgilerini almakta ve düğümün kötü amaçlı olmadığını doğrulamaktadır. Doğrulama yapılamaması durumunda ise bu düğüm ağa katılamamaktadır. Ayrıca,

önerilen yöntem için bulut uygulaması geliştirilip yaygın olarak kullanılan Nesnelerin İnterneti teknolojilerinden biri olan ZigBee için benzetim üzerinde uygulanmakta ve sonuçları paylaşılmaktadır. Geliştirilen bulut sistemine yönelik siber saldırılara karşı da bazı önlemler alınmaktadır.

Gelecek çalışmalarda, benzetim üzerinde uygulanan bu yöntem, koordinatör ve düğümlerden oluşan bir ZigBee veya başka bir teknoloji üzerinde uygulanabilir ve gerçeğe daha yakın sonuçlar elde edilebilir.

KAYNAKLAR

Agirre, A., Armentia, A., Estévez, E. and Marcos, M. 2018. A Component-Based Approach for Securing Indoor Home Care Applications. Sensors, 18, 46.

Andrea I., Chrysostomou, C., and Hadjichristofi, G. 2015. Internet of Things: Security vulnerabilities and challenges. 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, pp. 180-187

Anonim. 2017. Web Sitesi: http://www.eie.gov.tr/teknoloji/akilli_sebekeler.aspx, Erişim Tarihi: 06.12.2017.

Anonim. 2017. Web Sitesi: https://www.silawebyazilim.com/ddos-nedir/, Erişim Tarihi: 01.05.2019.

Anonymous 2016. Web Sitesi: http://cryptographicprocessor.weebly.com/uploads/2/4/5/3/24530999/aes.pdf, Erişim Tarihi: 05.12.2017.

Anonymous. 2016. Web Sitesi: http://www.businessinsider.com/how-the-iot-is changing-the-manufacturing-industry-2016-3, Erişim Tarihi: 05.12.2017.

Anonymous. 2016. Web Sitesi: https://www.nxp.com/docs/en/user-guide/JN-UG-3114.pdf, Erişim Tarihi: 15.10.2018.

Anonymous. 2017. Web Sitesi: https://embedur.com/blogsandnews/Is-80211ah-a-contender-for-low-power-IoT.html, Erişim Tarihi: 10.11.2018.

Anonymous. 2017. Web Sitesi: https://teknobolge.com/nedir/sosyal-muhendislik-nedir ve-nasil-korunulur, Erişim Tarihi: 03.05.2018.

Anonymous. 2018. Web Sitesi: https://www.nxp.com/docs/en/user-guide/JN-UG-3113.pdf, Erişim Tarihi: 15.10.2017.

Arış, A., Oktuğ, S. ve Yalçın, S. 2015. Nesnelerin İnterneti Güvenliği: Servis Engelleme Saldırıları. Signal Processing and Communications Applications Conference.

Aslan, O., Samet, R. 2017. Investigation of Possibilities to Detect Malware Using Existing Tools. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), IEEE, pp. 1277-1284.

Chadid, Y., Benabdellah, M., and Azizi, A. 2017. Internet of Things Security in 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems.

Çavdar, T. and Öztürk, E. 2017. Nesnelerin İnterneti için Yeni bir Mimari Tasarımı. Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi.

Deniz, E. and Samet, R. 2018. A New Model for Secure Joining to ZigBee 3.0 Networks in the Internet of Things. 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), ANKARA, Turkey, pp. 102-106.

Elbouanani, A. S., Kiram, M. A. E. and Achbarou, O. 2015. Introduction to the Internet of Things security: Standardization and research challenges. 2015 11th International Conference on Information Assurance and Security (IAS), Marrakech, pp. 32-37.

Fan, X., Susan, F., Long, W. and Li, S. 2017. Security Analysis of Zigbee. MIT.edu

Gislason D. 2008. ZigBee Wireless Networking. p. 1-2.

Giuliano, R., Mazzenga, F., Neri, A. and Vegni, A. M. 2017. Security Access Protocols in IoT Capillary Networks. IEEE Internet of Things Journal, vol. 4, no. 3, pp. 645-657.

Gökrem, L. and Bozoklu, M. 2016. Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum. Gaziosmanpaşa Bilimsel Araştırma Dergisi Sayı:13.

Gupta, K. and Shukla, S. 2016. Internet of Things: Security challenges for next generation Networks. 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, pp. 315-318.

Husamuddin, M. and Qayyum, M. 2017. Internet of Things: A study on security and privacy threats. 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, pp. 93-97.

Judson, B. 2016. How to choose a security solution for the internet of things: A guide for everyone. Device Auuthority.

Keoh, S. L., Kumar, S. S., and Tschofenig, H. 2014. Securing the Internet of Things: A Standardization Perspective. IEEE Internet of Things Journal, vol. 1, no. 3, pp. 265-275.

Kim, J. T. 2017. Analyses of secure authentication scheme for smart home system based on internet on things. 2017 International Conference on Applied System Innovation (ICASI), Sapporo, pp. 335-336.

Kumar, P., Braeken, A., Gurtov, A., Iinatti, J. and Ha, P. H. 2017. Anonymous Secure Framework in Connected Smart Home Environments. IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 968-979.

Kutup, N. 2011. Nesnelerin Interneti; 4H Her yerden, Herkesle, Her zaman, Her nesne ile bağlantı. 16. Türkiye'de İnternet Konferansı.

Masum, E., Samet, R. 2018. Mobil BOTNET İle DDOS Saldırısı. Bilişim Teknolojileri dergisi, Cilt 11, Sayı 2, Sayfalar 111-121.

Morgner, P., Mattejat, S., Benenson, Z., Müller, C. and Armknecht, F. 2017. Insecure to the Touch: Attacking ZigBee 3.0 via Touchlink Commissioning. WiSec '17, Boston, MA, USA.

Mosenia, A. and Jha, N. K. 2017. A Comprehensive Study of Security of Internet of Things. IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602.

Mukherjee, A. 2015. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. Proceedings of the IEEE, vol. 103, no. 10, pp. 1747-1761.

Ning, H., Liu, H. and Yang, L. T. 2013. Cyberentity Security in the Internet of Things. Computer, vol. 46, no. 4, pp. 46-53.

Roman, R., Najera, P. and Lopez, J. 2011. Securing the Internet of Things. Computer, vol.44, no. 9, pp. 51-58.

Sain, M., Kang, Y. J. and Lee, H. J. 2017. Survey on Security in Internet of things: state of the art and challenges.

Şengül, G. and Bostan, A. 2013. Bulut Bilişimde Bilgi Güvenliği ve Standardizasyon Çalışmaları. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, Türkiye, pp. 263-267.

Vasilomanolakis, E., Daubert, J., Luthra, M, Gazis, V., Wiesmaier, A. and Kikiras, P. 2015. On the Security and Privacy of Internet of Things Architectures and Systems. 2015 International Workshop on Secure Internet of Things (SIoT), Vienna, pp. 49-57.

Yang, Y., Peng, H., Li, L. and Niu, X. 2017. General Theory of Security and a Study Case in Internet of Things. IEEE Internet of Things Journal, vol. 4, no. 2, pp. 592-600.

Zhou, L., and Chao, H. C. 2011. Multimedia traffic security architecture for the internet of things. IEEE Network, vol. 25, no. 3, pp. 35-40.

Zillner, T. 2015. ZigBee Exploited: the good, the bad, and the ugly.

ÖZGEÇMİŞ

Adı Soyadı : Emre DENİZ
Doğum Yeri : Balıkesir
Doğum Tarihi: 14.03.1991
Medeni Hali : Evli
Yabancı Dili : İngilizce

Eğitim Durumu:

Lise : Özel Yamanlar Fen Lisesi (2009)
Lisans : Orta Doğu Teknik Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü (2015)
Yüksek Lisans : Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı (Eylül 2016 – Haziran 2019)

Çalıştığı Kurumlar:

Yazılım Geliştirme Personeli, V-Count Teknoloji A.Ş., 2013 – 2015
Yazılım Geliştirme Personeli, Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş., 2015 – (Devam etmekte)

Yayınlar

1. Deniz, E. and Samet, R. 2018. A New Model for Secure Joining to ZigBee 3.0 Networks in the Internet of Things. 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), ANKARA, Turkey, pp. 102-106.

2. Deniz, E. and Samet, R. 2019. Nesnelerin İnternetinde ZigBee 3.0 Ağlarına Güvenli Katılım için Yeni Bir Model Geliştirilmesi. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi.