NESNELERİN İNTERNETİNDE ZIGBEE 3.0 AĞLARINA GÜVENLİ KATILIM İÇİN YENİ BİR MODEL ÖNERİSİ

Emre DENİZ ve Refik SAMET
Ankara Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ankara, Türkiye
denize@ankara.edu.tr, samet@eng.ankara.edu.tr

ÖZET

Günümüzde İnternet, günlük yaşamda çok önemli bir yere sahiptir. Nesnelerin İnterneti de özellikle modern İnternet dünyasında en çok kullanılan teknolojilerden birisi olmuştur. Nesnelerin İnterneti teknolojisi, iletişim ve haberleşme protokolleri sayesinde nesnelere ait verileri toplayıp analizini yaparak nesneleri kontrol etmektedir. Ancak yaygınlaşan akıllı nesnelerin birbiriyle iletişim halinde olması ve İnternete bağlı olması çeşitli siber saldırılara olanak sağlamaktadır. Herhangi bir ihlal durumundaki olumsuz sonuçlar nedeniyle Nesnelerin İnternetinde güvenlik konusu önem taşımaktadır. Bu makalede, Nesnelerin İnternetinde en çok kullanılan teknolojilerden biri olan ZigBee ele alınmıştır. ZigBee protokolündeki güvenlik açıklarına çözüm olarak yeni bir model önerilmiş, benzetim üzerinde uygulanmış ve sonuçları değerlendirilmiştir.

Anahtar Kelimeler— Nesnelerin İnterneti, ZigBee, Gizlilik, Güvenlik, Ağa Katılım

A New Model for Secure Joining to ZigBee 3.0 Networks in the Internet of Things

ABSTRACT

Recently, Internet has an important role in the life. Internet of Things (IoT), especially in the modern Internet world, is one of the most used technologies. IoT collects data from and controls the objects that communicate with each other via protocols. Being connected to each other and the Internet causes cyber-attacks to the smart objects in IoT. Information security of IoT becomes important because of the negative consequences of these attacks. In this paper, ZigBee, that is one of the most common IoT technologies, is analyzed. A new model and its simulation implementation are proposed as a solution to vulnerabilities in ZigBee. Also the results of this model are evaluated.

***Keywords*—** Internet of Things, ZigBee, Privacy, Security, Network Join

I. GİRİŞ (INTRODUCTION)

Nesnelerin İnterneti, çeşitli iletişim ve haberleşme protokolleri sayesinde birbiri ile iletişim kuran nesnelere ait verileri toplayıp analizini yaparak nesneleri kontrol eden bir ağdır [1], [2], [3].

Günümüzde artık her alanda İnternet karşımıza çıkmaktadır. Gelişen teknolojiler sayesinde neredeyse her zaman ve her yerden İnternete erişim sağlanmaktadır [4]. Yalnızca tabletler, akıllı telefonlar ve bilgisayarlar değil, artık elektrik prizleri, çamaşır makineleri, ilaç şişeleri ve arabalar da İnternete bağlanmaktadır. Tüm bu gelişmeler doğrultusunda son yıllarda ortaya çıkan Nesnelerin İnterneti teknolojisinin günlük yaşamdaki rolü git gide artmaktadır. Bu teknoloji, sağlık, ev, tarım, enerji, çevre, su, şehir, endüstri ve taşımacılık gibi alanlarda kullanılmaktadır [1], [5].

Yaygınlaşan akıllı nesneler, bunların birbiriyle iletişim kurabilmesi ve İnternete bağlı olması çeşitli siber saldırıları da beraberinde getirmektedir [6], [7]. Her hangi bir ihlal durumundaki olumsuz sonuçlar sebebiyle bu alanda bilgi güvenliği oldukça önem taşımaktadır. Örneğin, İnternete bağlanan nesneler, siber saldırganların kurbanlarını takip etmesine imkân sağlayabilir veya uzaktan bağlantı ile bir saldırgan, herhangi bir kimsenin

elektriğini kapatabilir, arabasını çalıştırabilir veya kapısının kilidini açabilir duruma gelecektir.

Nesnelerin İnternetinde üreticiler, farklı teknolojiler kullanmaktadır [8]. Bu teknolojilerden bazılarında bulunan güvenlik açıkları [9] nedeniyle Nesnelerin İnternetinde uçtan uca güvenli haberleşme sağlanamamaktadır [10]. Uçtan uca güvenli haberleşmenin sağlanması için söz konusu güvenlik açıklarının tespit edilip önlemler alınması gerekmektedir [11].

Nesnelerin İnternetinde yaygın olarak kullanılan teknolojilerden biri olan ZigBee protokolünde bazı güvenlik açıkları bulunmaktadır [12], [13], [14]. Örnek olarak, Touchlink Commissioning metodu gösterilebilir [15]. Bu metodun en önemli özelliği kullanıcı dostu kurulumu esas almasıdır. Bu metot ile özellikle ev sistemlerinde kullanıcılar sadece düğümü çalıştırarak kolay bir kurulum yapmaktadır. Fakat metodun sunduğu bu kolaylığa rağmen, ağa katılım sırasında küresel bağlantı anahtarı kullanılması sebebiyle güvenlik açıkları meydana gelmektedir.

Bu makalede, yukarıda bahsedilen ZigBee teknolojisindeki güvenlik açığının kapatılmasına katkı yapmak için yeni bir ZigBee Bulut modeli önerilmektedir. Bu model ile ZigBee ağlarına katılımın daha güvenli hale geldiği değerlendirilmektedir.

Bu makalede, ikinci bölümde ilgili çalışmalar, üçüncü bölümde ZigBee güvenlik analizi, dördüncü bölümde önerilen model ve beşinci bölümde sonuçlar anlatılacaktır.

II. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

Nesnelerin İnternetini hedef alabilecek saldırıların incelenmesi ve hedef aldıkları katmanlar açısından sınıflandırması [2] numaralı çalışmada anlatılmıştır. Bu çalışmada saldırılar, fiziksel, veri bağı, ağ, iletim ve uygulama katmanlarına göre sınıflandırılmıştır. Ayrıca Nesnelerin İnternetine yönelik saldırıların tespit sistemleri de değerlendirilmiştir. Çalışma, daha çok servis engelleme saldırıları üzerine yoğunlaşmıştır.

Farklı iletişim protokolleri içeren Nesnelerin İnternetinde ortak bir güvenlik çözümüne ihtiyaç olduğu [8] numaralı çalışmada belirtilmiştir. Bu çalışmada Nesnelerin İnternetinde kullanılan kablosuz iletişim protokolleri; Bluetooth, Wi-Fi, ZigBee, NFC (Yakın Alan İletişimi), RFID (Radyo Frekanslı Tanımlama), 6LoWPAN (IPv6 Düşük Güçlü Kablosuz Kişisel Alan Ağları) ve 3G (Üçüncü Nesil) karşılaştırmalı olarak incelenmiştir. Güvenliğin nasıl sağlanması gerektiği ile ilgili olarak katmanlardaki iletişim güvenliği ve bilgi güvenliğinin gerekliliği belirtilmiştir. Ayrıca Nesnelerin İnternetinde kullanılan kontrol veya izleme uygulamalarına kullanıcı girişini daha güvenli hale getirmek için çoklu faktörlü kimlik doğrulama yönteminin kullanılabileceği belirtilmiştir. Bu yöntem ile kullanıcının sahip olduğu, bildiği veya kullanıcıya ait olan bilgilerden en az ikisi kullanılarak giriş yapılacağı anlatılmıştır.

ZigBee Pro sürümü üzerinde, [16] numaralı çalışmada güvenli analizi yapılmış ve bazı açıklar bulunmuştur. ZigBee Pro sürümü, 2016 yılında yayınlanan ve son sürüm olan ZigBee 3.0 sürümünden önceki sürümdür. Bu çalışmada SecBee adı verilen program ile ZigBee Pro ağları dinlenerek ataklar yapılmış ve düğümlerin kontrolü ele geçirilmiştir. Çalışmada tespit edilen açıklar, ZigBee 3.0 sürümünde kapatılmıştır.

ZigBee 3.0 sürümünde önceki paragrafta bahsedilen geliştirmelere rağmen bazı güvenlik açıkları hala bulunmaktadır. Örneğin, bir düğümün ağa katılması esnasında güvenlik açıkları meydana gelebilir. [17] numaralı çalışmada bu güvenlik açığından bahsedilmiştir. Bu çalışmada koordinatör ve düğümler kullanılarak deneysel bir ZigBee 3.0 ağı oluşturulmuştur. Killerbee, WireShark gibi yazılımlarla düğümler arasındaki haberleşme analiz edilmiştir. Analiz sırasında paketlerden birinin yeni düğüm eklenmesi amacıyla gönderildiği ve ağ anahtarının Zigbee09 bağlantı anahtarıyla şifrelendiği tespit edilmiştir. Aynı anahtar kullanılarak şifreli paket çözülmüş ve ağ anahtarı ele geçirilmiştir. Bu sayede tüm haberleşmenin şifresi çözülüp ağın kontrolü ele geçirilmiştir. Söz konusu çalışmada bu güvenlik açığını kapatmak için belirli ve kapsamlı bir çözüm modeli önerilmemiştir.

Ağa katılım metodunun incelenmesi amacıyla ZigBee 3.0 sürümü üzerinde yapılan bir diğer çalışmada da güvenlik açığı bulunmuştur [18]. Bu çalışmada güvenlik açığının tespiti için

deneysel bir ortam kurulmuştur. Z3sec programı yüklü dizüstü bilgisayara, yazılım tabanlı radyo alıcısı USB ile bağlanarak 4 farklı markaya ait ZigBee akıllı lambalara ataklar yapılmıştır. Bu dört düğümün, Touchlink Commissioning metodu ile ağa katılım için ZigBee grubu tarafından üreticilere anlaşma ile dağıtılan ve 2015 yılında sızan bağlantı anahtarını kullandıklarından dolayı ağa katılım esnasında güvenlik açığı meydana geldiği tespit edilmiştir. Ağa katılım paketlerinden ağ anahtarı ele geçirilip şifreli haberleşme çözülmüş ve ardından diğer düğümlere sıfırlama, fabrika ayarlarına döndürme veya kapatma gibi komutlar yollanmıştır. Bu çalışmada da ağa katılım sırasında meydana gelen açığın kapatılması için belirli bir çözüm modeli önerilmemiştir.

Ağa katılımdaki güvenlik açıkları ile ilgili bir diğer çalışmada ise yapılan güvenlik analiziyle açıklar tanımlanmıştır [19]. Bu çalışmada ardından açıklara çözüm olarak ZigBee Bulut modeli önerilmiştir Modelin ayrıntıları kavramsal olarak anlatılmıştır. Önerilen modelde mevcut protokole göre yapılan değişiklikler açıklanmıştır. Ancak önerilen model, bir benzetimde veya gerçek ortamda uygulanmamıştır.

Mevcut çalışmalar incelendiğinde ZigBee 3.0 sürümü güvenliğiyle ilgili az sayıda çalışma olduğu görülmüştür. Özellikle ağa katılımdaki güvenlik açıkları konusunda sadece birkaç çalışma olduğu ve açıklara yönelik bir çözüm önerilmediği gözlenmiştir. Bu makalede ağa katılımdaki bahsedilen güvenlik açıklarının kapatılması amacıyla ZigBee Bulut modeli önerilmektedir.

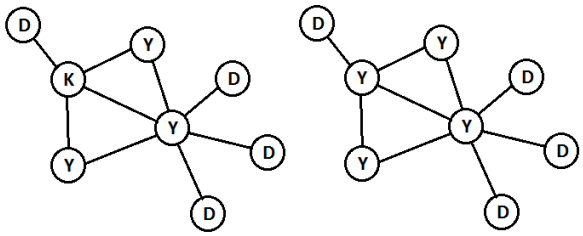
III. ZIGBEE GÜVENLİK ANALİZİ (ZIGBEE SECURITY ANALYSIS)

ZigBee standardında tüm kablosuz haberleşme şifreli olarak yapılmaktadır. Şifreleme algoritması olarak AES-128 algoritması kullanılmaktadır [20]. Algoritmada anahtar olarak ağ ve bağlantı anahtarları kullanılmaktadır.

3.1 Güvenlik Modeli

Bir ZigBee 3.0 ağı, merkezi veya dağıtık güvenlik modeline sahip olabilir. Bu modellerde üç çeşit eleman vardır. Bunlar, Şekil 1'de görüleceği üzere koordinatör (K), yönlendirici (Y) ve düğümdür (D).

Her eleman bir veya birden fazla eleman ile iletişim halinde olabilir. Şekil 1 (a)'da gösterilen merkezi güvenlikli ağ, koordinatör tarafından yönetilir. Koordinatör, doğrulama sonucu ağa yeni düğümlerin katılmasını kontrol eder. Şekil 1 (b)'de gösterilen dağıtık güvenlikli ağı ise yönlendiriciler yönetir. Ağa yeni katılacak düğümlerin doğrulamasını yönlendiriciler yapar [15].



(a) Merkezi (b) Dağıtık

Şekil 1. Güvenlik Modelleri [15]

3.2 Güvenlik Anahtarları

Güvenlik anahtarları sayesinde tüm kablosuz haberleşme şifreli olarak yapılmaktadır. Ağ Anahtarı ve Bağlantı Anahtarı olmak üzere iki güvenli anahtarı mevcuttur.

a) *Ağ Anahtarı:* Ağ anahtarı, haberleşmeyi şifrelemek ve haberleşmenin şifresini çözmek için kullanılmaktadır. Ağdaki tüm elemanlar tarafından birbirleriyle paylaşılmaktadır [21].
b) *Bağlantı Anahtarı:* Ağa yeni katılacak düğüme ağ anahtarı, bağlantı anahtarı ile şifrelenerek gönderilmektedir [21]. İki çeşit bağlantı anahtarı bulunmaktadır.

- *Önceden Yapılandırılmış Küresel Bağlantı Anahtarı:* Ağdaki tüm elemanlar için aynıdır. Elemanlar, ZigBee grubu tarafından üreticilere dağıtılmış olan anahtarı (ZigBee09) veya üreticilerin kendine özel oluşturduğu anahtarı kullanmaktadır. ZigBee grubunun dağıttığı anahtar ile farklı üretici ve sürüme sahip elemanlar mevcut ağa katılabilir. Üreticiye özel anahtar kullanılarak ise sadece aynı üreticiye ait elemanlar ağa katılabilir.

- *Önceden Yapılandırılmış Benzersiz Bağlantı Anahtarı:* Her bir düğüm farklı bağlantı anahtarına sahiptir.

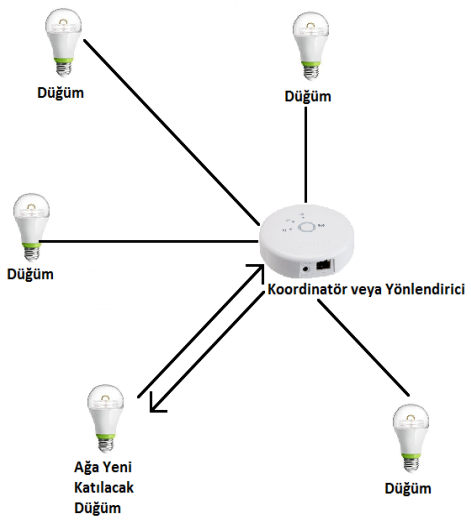
Ağa katılım esnasında sadece ZigBee09 açık anahtarı kullanıldığında güvenlik açığı meydana gelmektedir. Bu makalede bahsedilen açığı kapatmaya katkı yapmak için bir model önerilmektedir.

3.3 Ağa Katılım

ZigBee 3.0 sürümünde ağa katılım Touchlink Commissioning metoduyla gerçekleştirilmektedir [22]. Bu metot sayesinde farklı üreticilere ve sürümlere sahip düğümler aynı ağa katılabilir.

ZigBee 3.0 ağlarında kablosuz haberleşme, ağ anahtarı ile şifrelenmiş olarak yapılır. Ağa yeni bir düğüm katılacağı zaman ağ anahtarı, yeni düğüme aktarılır. Bu aktarım, yukarıda bahsedilen metotta önceden yapılandırılmış bağlantı anahtarıyla (ZigBee09) yapılır. Katılım esnasında ağ koordinatörü, ağ anahtarını bu bağlantı anahtarıyla şifreleyerek yeni düğüme gönderir. Yeni düğüm de aynı bağlantı anahtarına sahip olduğundan, gelen şifreli metni çözerek ağ anahtarına ulaşıp ağa katılır [22], [23].

Şekil 2, yeni düğümün mevcut bir ZigBee 3.0 ağına katılım modelini göstermektedir.



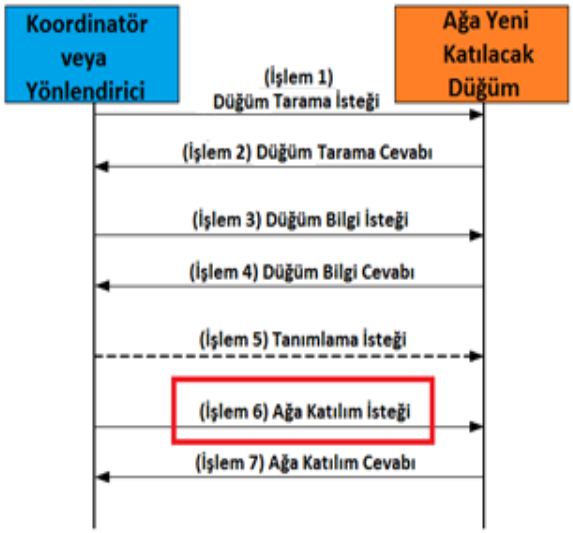
Şekil 2. Yeni Düğümün Ağa Katılım Modeli

Şekil 3'te görüldüğü gibi mevcut durumda ağa katılım yedi işlemde gerçekleşmektedir.

3.4 Güvenlik Açığının Tanımlanması

ZigBee 3.0 ağlarında haberleşme şifreli olarak yapılır. Ancak saldırgan Şekil 3'te anlatılan protokolün 6. işleminde koordinatörün düğüme ilettiği "ağa katılım isteği" paketini yakalar ve bağlantı anahtarına (ZigBee09) sahipse, aynı paketle iletilen ağ anahtarına ulaşıp ağın kontrolünü ele geçirebilir. Bu güvenlik açığının oluştuğu işlem Şekil 3'te çerçeve ile işaretli kısımda gösterilmiştir. Bu güvenlik açığına çözüm olarak önerilen model dördüncü bölümde anlatılacaktır.

Mevcut durumda, ZigBee 3.0 ağına katılım Şekil 3'te gösterilen protokolle yapılmaktadır.



Şekil 3. Yeni Düğümün Ağa Katılım Protokolü

IV. ÖNERİLEN MODEL (PROPOSED MODEL)

Önceki bölümde bahsedilen güvenlik açığına çözüm olarak ZigBee 3.0 ağlarına güvenli katılım için yeni bir model olan ZigBee Bulut önerilmektedir. Bu modelle düğümlere ait üretici adı, ürün adı, seri numarası ve bağlantı anahtarı gibi bilgiler bulutta saklanmaktadır. Tablo 1'de örnek olarak 4 adet düğüme ait bilgiler gösterilmektedir.

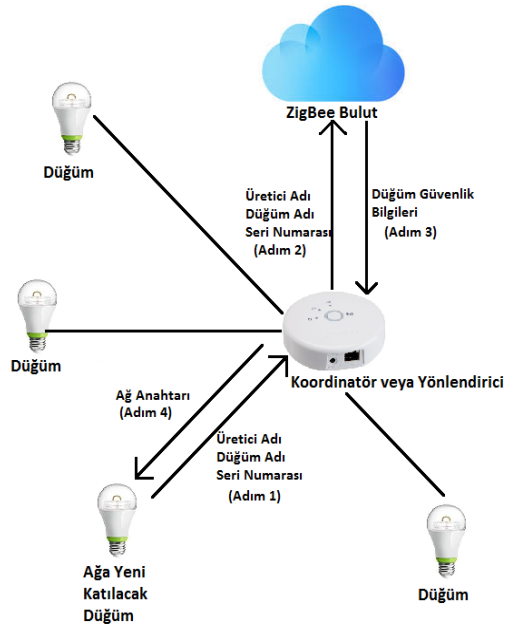
ZigBee 3.0 ağına yeni bir düğüm katılacağı zaman, ağ koordinatörü buluta bağlanıp düğümün bilgilerini almaktadır. Bu bilgilerden biri olan düğüme ait bağlantı anahtarı ile ağ anahtarını şifreleyip düğüme bunu göndermektedir. Düğüm de şifreli metni sahip olduğu aynı bağlantı anahtarı ile çözerek ağ anahtarına ulaşıp ağa katılmaktadır.

4.1 ZigBee Bulut Güvenlik Modeli

Şekil 4'te, önerilen modele uygun olarak yeni bir düğümün ağa katılım adımları anlatılmaktadır.

Tablo 1. ZigBee Bulut Bilgileri

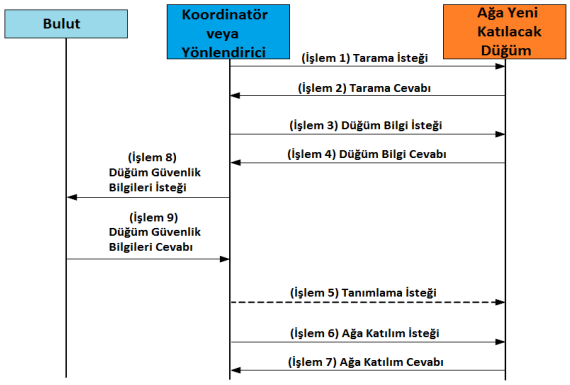
Üretici Adı	Ürün Adı	Seri Numarası	Bağlantı Anahtarı
Üretici 1	Akıllı Lamba	A271145	4D 6A 45 21
Üretici 1	Akıllı Lamba	A281146	AB 54 14 E6
Üretici 2	Nem Sensörü	N151620	2E CD 4C 2D
Üretici 2	Nem Sensörü	N151621	5D BD 1C 2A



Şekil 4. Önerilen Modelde Yeni Düğümün Ağa Katılımı

1. Adımda ağa yeni katılacak düğüm, koordinatörün düğüm bilgi isteğine cevap olarak düğümün üretici adı, düğümün adı ve seri numarasını koordinatöre göndermektedir.
2. Adımda koordinatör buluta ulaşıp 1. adımda temin ettiği bilgilere uygun düğüme ait güvenlik bilgilerini talep etmektedir.
3. Adımda ise bulut, koordinatöre düğüme ait güvenlik bilgilerini göndermektedir.
4. Adımda, koordinatör, eğer düğümün temin ettiği ve buluttan temin edilen bilgiler uyuşuyorsa, düğüme ait bağlantı anahtarını kullanarak ağ anahtarını şifreleyip düğüme göndermektedir. Düğüm de aynı bağlantı anahtarıyla şifreyi çözerek ağ anahtarına ulaşıp ağa katılmaktadır.

Şekil 5'te ise önerilen modelin protokolü anlatılmaktadır. Önerilen protokolde, mevcut protokole 8. ve 9. işlemler eklenmiştir. Bu işlemler sayesinde mevcut protokolde bulunan ağa katılım esnasındaki güvenlik açığı kapatılmaktadır.



Şekil 5. Önerilen Modelde Yeni Düğümün Ağa Katılım Protokolü

Ayrıca ZigBee kısıtlı kaynaklar üzerinde çalıştığı için bu modelde koordinatör üzerinde düğümlere ait bilgiler saklanmamaktadır. Bir düğüm ağa katılacağı zaman koordinatör, buluta güvenli erişim yapıp düğümün bilgilerini alıp ağa katılmasını sağlamaktadır.

Yine bu modelde bulut sunucularında, standart web sunucularında alınan önlemler alınmaktadır. Bulutta düğümlere ait bilgilere kimlik doğrulama sistemiyle erişim sağlanıp bilgiler şifreli olarak veri tabanlarında saklanmaktadır. Böylece bulut sunucularında da güvenlik sağlanmaktadır.

4.2 Önerilen Modelin Mimarisi

Önerilen modelde, koordinatör, modem ile İnternete bağlanmaktadır. İnternet üzerinden ZigBee Bulut sistemine Rest API ile erişim sağlamaktadır. Bu sayede ağa katılmak isteyen düğümlerin bilgilerini bulut sisteminden almaktadır. Şekil 6'da önerilen modelin mimarisi gösterilmektedir.

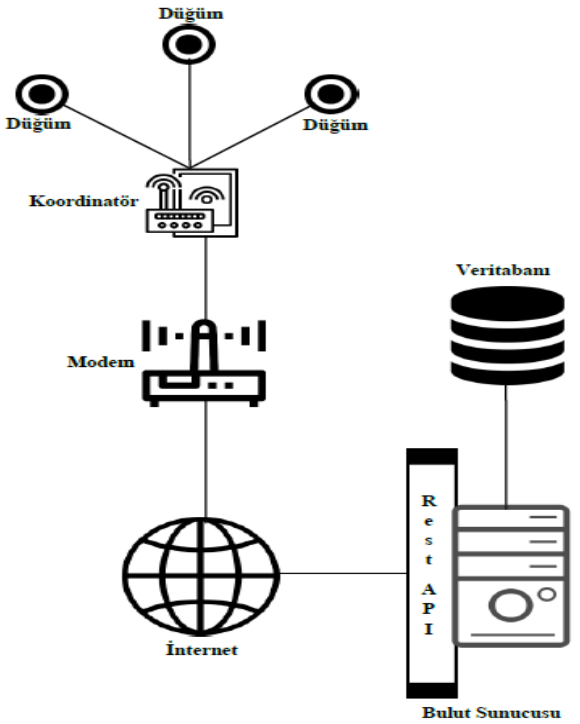
4.3 Önerilen Modelin Akış Şeması

Önerilen modelde, bir düğümün ağa katılması için bazı adımların tamamlanması gerekmektedir. Bu adımlar, Şekil 7'de önerilen modelin akış şeması ile gösterilmektedir.

4.4 ZigBee Bulut Uygulaması

Önerilen model için öncelikle ZigBee Bulut uygulaması geliştirilmiştir. Üreticiler, ürettikleri düğümlerin güvenlik bilgilerini bu sisteme

yüklemektedir. Bir düğüm ağa katılacağı zaman koordinatör, bu sisteme bağlanıp düğüme ait gerekli bilgileri almaktadır. Şekil 8'de uygulamanın giriş ekranı gösterilmektedir. Şekil 9'da üreticilerin ürettikleri düğümleri sisteme ekleme ekranı gösterilmektedir. Eklenen düğümler tablo halinde listelenmektedir. Şekil 10'da düğüm listesi gösterilmektedir.

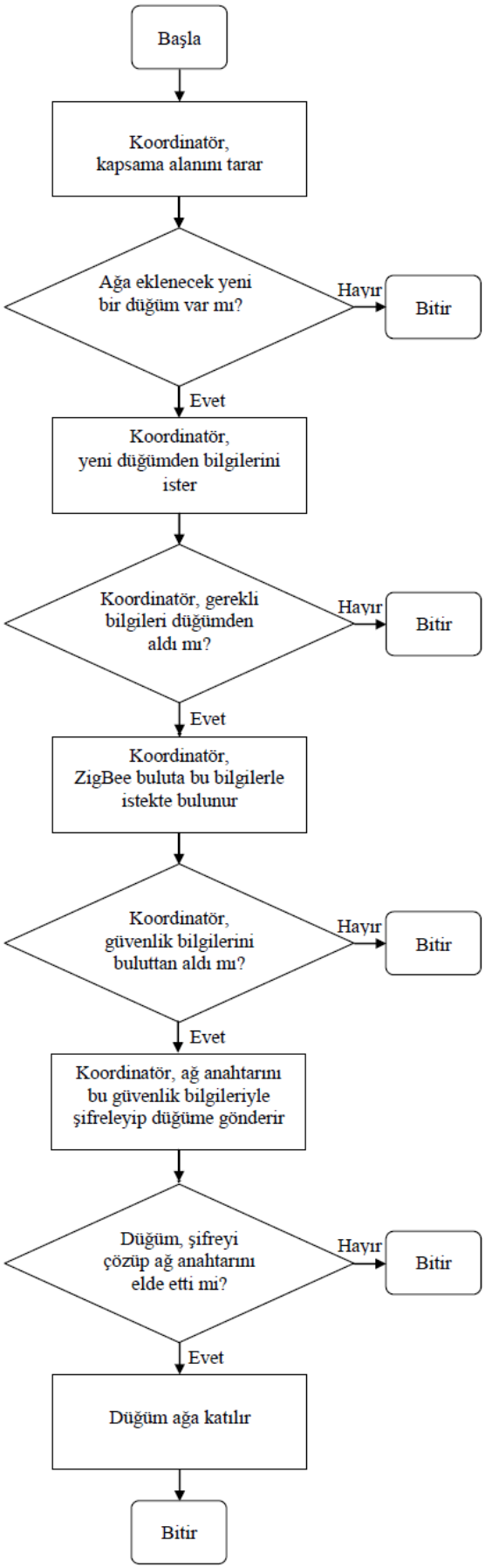


Şekil 6. Önerilen Modelin Mimarisi

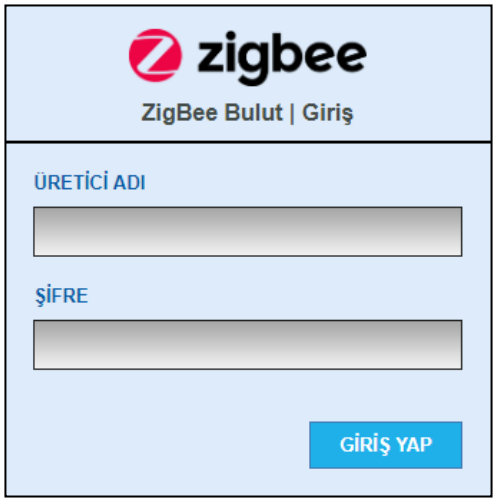
4.5 Önerilen Modelin Benzetimi

Benzetim, Java programlama dili ve Eclipse IDE ortamı kullanılarak geliştirilmiştir. Grafik kütüphanesi olarak Java Graphics2D kullanılmıştır. Benzetim, Intel Core i3, 3GB RAM ve Nvidia GeForce ekran kartına sahip kişisel bilgisayar üzerinde uygulanmıştır. Benzetimde başlangıçta koordinatör ve düğümler çalışmakta olup ardından yeni düğümler katılmaktadır.

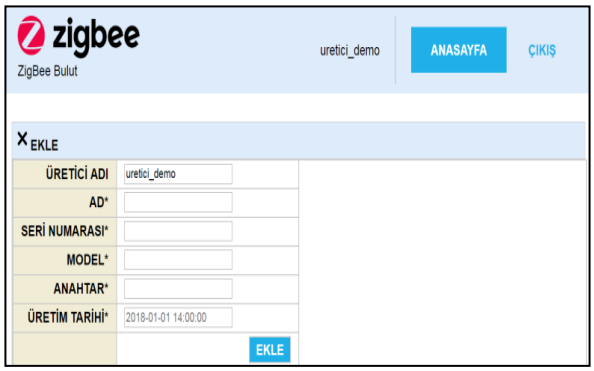
Öncelikle mevcut protokolün benzetimi yapılmıştır. Benzetimde başlangıç durumunda, ZigBee ağında bir koordinatör ve iki akıllı lamba birlikte çalışmaktadır. Benzetimde lamba ve koordinatör arasındaki yeşil renkli oklar bağlantının sağlandığını, kırmızı renkli oklar ise bağlantının kurulmadığını göstermektedir. Ayrıca lamba isimlerini kırmızı olması, lambanın zararlı veya atak amacıyla kullanılabileceğini göstermektedir. Şekil 11'de ağa yeni bir düğüm katılmadan önceki başlangıç durumu gösterilmektedir.



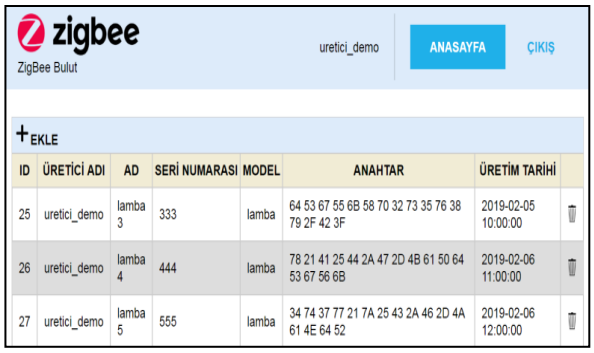
Şekil 7. Önerilen Modelin Akış Şeması



Şekil 8. Uygulama Giriş Ekranı



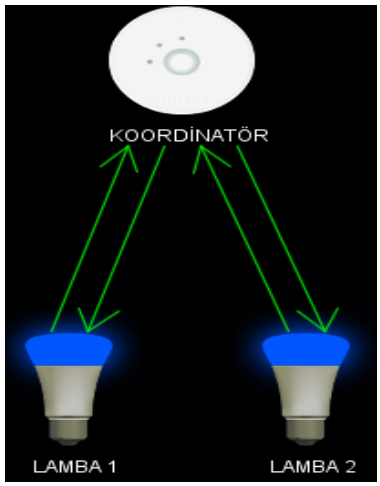
Şekil 9. Düğüm Ekleme Ekranı



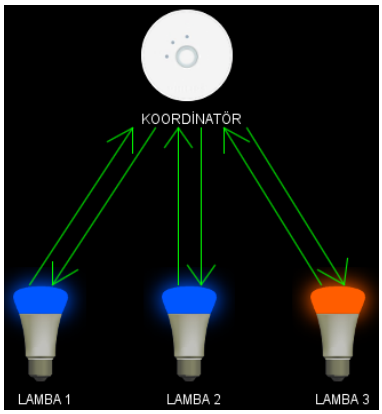
Şekil 10. Düğüm Listesi

Ardından zararlı olmayan lamba 3, küresel bağlantı anahtarını kullanarak ağa katılmaktadır. Şekil 12'de görüldüğü gibi koordinatör ve lamba arasında bağlantı sağlanmıştır.

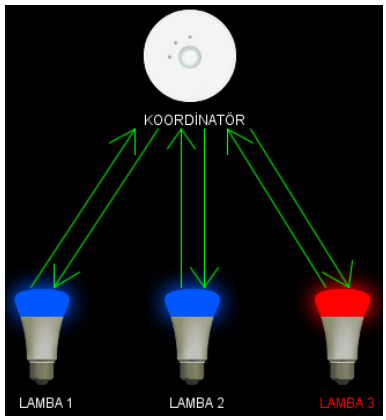
Bir başka durumda ise zararlı olan lamba 3, küresel bağlantı anahtarını kullanarak ağa katılmaktadır. Bu durumda saldırgan ağdaki güvenlik açığını kullanarak haberleşmeyi çözebilmektedir. Şekil 13'de görüldüğü gibi koordinatör ve lamba arasında bağlantı sağlanmıştır.



Şekil 11. Mevcut Protokolün Benzetimi: Başlangıç Durumu

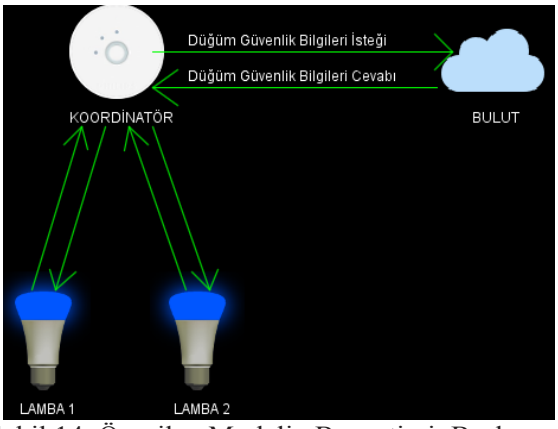


Şekil 12. Mevcut Protokolün Benzetimi: Ağa Katılım Durumu



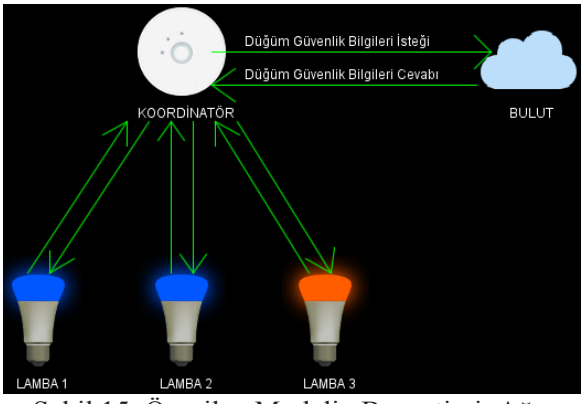
Şekil 13. Mevcut Protokolün Benzetimi: Zararlı Düğüm Ağa Katılım

Ardından, önerilen ZigBee Bulut modelindeki yöntemler benzetim ortamında uygulanmıştır. Bu model ile yeni düğüm ağa katılacağı zaman koordinatör, bulut ile bağlantı kurup gerekli bilgileri almaktadır. Şekil 14'de ağa yeni bir düğüm katılmadan önceki başlangıç durumu gösterilmektedir.



Şekil 14. Önerilen Modelin Benzetimi: Başlangıç Durumu

Ardından zararlı olmayan lamba 3, koordinatörün, bulut sistemini kullanmasıyla ağa katılmaktadır. Şekil 15'de görüldüğü gibi koordinatör ve lamba arasında bağlantı sağlanmıştır.

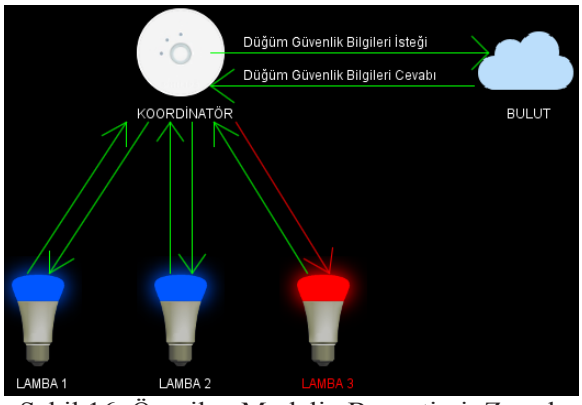


Şekil 15. Önerilen Modelin Benzetimi: Ağa Katılım Durumu

Bir başka durumda ise zararlı olan lamba 3, ağa katılım isteği göndermektedir. Ancak bu zararlı lamba, resmi düğüm üreticileri tarafından üretilmediği için bulut isteminde bilgileri bulunmamaktadır. Koordinatör de bulut sisteminde bu zararlı lambaya ait bilgilere ulaşamadığı için lamba ağa katılamamaktadır. Şekil 16'da görüleceği üzere koordinatör ve lamba arasında bağlantı kırmızı olmakta ve lambanın ağa katılım isteği reddedilmektedir.

4.6 Önerilen Modelin Değerlendirmesi

Önerilen model, ağa katılımın kolay ve kullanıcı dostu olma özelliğini devam ettirmektedir. Bu modelle kullanıcı, mevcut ağına yeni düğüm ekleyeceğinde her zamanki gibi sadece düğümü çalıştırıp, koordinatör tarafından ağa eklenmesini beklemektedir.



Şekil 16. Önerilen Modelin Benzetimi: Zararlı Düğüm Ağa Katılım

Önerilen modelde buluta erişim güvenli bağlantı üzerindendir. Bu sayede hem üreticilerin hem de ağ koordinatörlerinin erişimi sırasında bir güvenlik problemi oluşmamaktadır. Ayrıca bulut, güvenli sunucular üzerinde çalışmakta ve bilgiler bulutta şifreli olarak saklanmaktadır. Bulut sunucularına standart güvenlik önlemleri uygulanmaktadır. Böylece sunucular güvenli şekilde çalışmasına devam etmektedir.

Mevcut modelde ağa katılım sırasında yapılıp başarılı olabilecek ortadaki adam ve trafik analiz saldırılarından, önerilen model, sunduğu bulut sistemi sayesinde ağa katılımda şifresiz haberleşme olmayacağı için etkilenmeyecektir. Ancak önerilen modeldeki bulut sistemine yönelik önceki paragrafta bahsedilen güvenlik önlemlerine rağmen saldırılara karşı bazı dezavantajlar ortaya çıkabilir. Örneğin, bulut sistemine yönelik olası siber saldırılar, başarılı olması durumunda ZigBee ağlarına yeni düğümlerin katılmasını engelleyebilir. Bu saldırılardan en çok karşılaşılabilecek olan ve en yaygın kullanılan ise servis engelleme saldırılarıdır [24], [25]. Bu saldırıların başarılı olması durumunda bulut sisteminde herhangi bir veri kaybı meydana gelmemesine rağmen buluta erişim kesilebilir ve bu esnada yeni düğümler ağa katılamayabilir. Bahsedilen saldırılara karşı bulut sisteminin güvenliğinden sorumlu bir birim olması ve saldırı esnasında hızlı çözüm üretilmesi, önerilen modelin gereksinimlerinden birisi olabilir. Ancak önerilen modelde ortaya çıkabilecek bu dezavantaja rağmen önerilen modelin, mevcut modelden daha güvenli olduğu değerlendirilmektedir.

Alternatif çözümler düşünüldüğü zaman, bahsedilen güvenlik açığına çözüm olarak ağa

katılım için gerekli, düğüme ait bağlantı anahtarı gibi bilgiler, düğüm üzerinde barkot etiketleri ile saklanabilir. Ağa katılım esnasında kullanıcı, barkot okuyucular ile bu bilgileri koordinatöre okutur ve işlem tamamlanır. Bu çözüm üreticilere her bir düğüm için barkot etiketi ve koordinatöre okuyucu maliyeti gerektirdiği gibi barkotların başka okuyucular tarafından okunmasına ve güvenlik bilgilerin ele geçirilmesine de sebep olabilir. Bunlara ek olarak kullanıcıya bazı ekstra sorumluluklar yüklediği için kolay kurulum özelliğine de aykırı olacaktır. Bu nedenlerden dolayı ZigBee Bulut çözümünün, bu muhtemel ve benzer çözümlere göre daha güvenli olduğu değerlendirilmektedir.

Ayrıca önerilen modelin performansı değerlendirilecek olursa, mevcut protokole ek olarak sadece yeni düğümün güvenlik bilgilerini almak için koordinatör, buluta bağlanmaktadır. Bu durum küçük bir gecikmeye sebep olmaktadır. Ancak önerilen modelin güvenlik açıklarına getirdiği çözümler düşünüldüğünde bu küçük gecikme göz ardı edilmektedir.

V. SONUÇLAR (CONCLUSIONS)

Modern İnternet dünyasında en çok kullanılan teknolojilerden biri olan Nesnelerin İnterneti, artık hayatın çok önemli bir parçası haline gelmiştir. Evlerde, iş yerlerinde, sanayide, sağlıkta ve birçok alanda akıllı nesneler kullanılmaya başlanmış ve daha da yaygınlaşacağı düşünülmektedir. Kullanılan nesnelerin çoğu, insan hayatıyla direkt olarak ilişkili olduğundan herhangi bir güvenlik ihlali durumunda sonuçları kötü olmaktadır. Örneğin, bir siber saldırgan uzaktan evinizdeki akıllı kapı kilidini açabilir veya üzerinizdeki sağlık değerlerini ölçen düğümden kişisel bilgilerinizi ele geçirebilir. Ayrıca kritik sistemlerdeki bir ihlalin etkileri daha da fazla olacaktır. Tüm bu olumsuz etkiler düşünüldüğünde bu teknolojide bilgi güvenliği konusu önem kazanmaktadır.

Bu makalede, Nesnelerin İnterneti alanında en çok kullanılan teknolojilerden biri olan ZigBee üzerinde bilgi güvenliği analizi yapılmıştır. Ardından ZigBee 3.0 sürümü üzerinde güvenlik değerlendirmeleri ve çözüm önerileri yapılmıştır. Bunun sonucunda ZigBee 3.0 ağlarına katılım sırasındaki güvenlik açıklarını ortaya çıkaran mevcut çalışmalardan da yola çıkarak açıkları kapatmaya katkı yapmak amacıyla bir çözüm modeli önerilmiştir. Modelin işleyiş ve protokolü anlatılıp model için bir bulut sistemi geliştirilmiştir. Bulutta düğümlere ait hangi bilgilerin tutulacağı ve sistemin işleyişi anlatılmıştır. Ardından ağa katılımdaki mevcut model ve önerilen model benzetim üzerinde uygulanmıştır. Her iki durum için de benzetimde elde edilen sonuçlar paylaşılmıştır. Ayrıca önerilen model, muhtemel başka çözümlerle karşılaştırılmış ve güvenliği artırmasına ek olarak hem maliyet hem de kullanım kolaylığı açısından diğer çözümlerden avantajlı olduğu değerlendirilmiştir. Bunların sonucunda önerilen modelin, yeni bir düğümün ağa katılımını, mevcut durumdan daha güvenli hale getirdiği tespit edilmiştir.

Gelecek çalışmalarda, benzetim üzerinde uygulanan bu model, koordinatör ve düğümlerden oluşan bir ZigBee ağı üzerinde uygulanabilir ve gerçeğe daha yakın sonuçlar elde edilebilir.

KAYNAKLAR (REFERENCES)

[1]. L. Gökrem, M. Bozoklu "Nesnelerin İnterneti: Yapılan Çalışmalar ve Ülkemizdeki Mevcut Durum" in Gaziosmanpaşa Bilimsel Araştırma Dergisi Sayı:13, Aralık 2016

[2]. A. Arış, S. Oktuğ, S. Yalçın "Nesnelerin İnterneti Güvenliği: Servis Engelleme Saldırıları" in Signal Processing and Communications Applications Conference, May 2015

[3]. T. Çavdar, E. Öztürk "Nesnelerin İnterneti için Yeni bir Mimari Tasarımı" in Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 2017

[4]. J. Zhou, Z. Cao, X. Dong and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," in IEEE Communications Magazine, vol. 55, no. 1, pp. 26-33, January 2017

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

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

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

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

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

[10]. A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," in IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 1 Oct.-Dec. 2017

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

[12]. ZigBee Alliance. 2016. zigbee alliance Accelerates IoT Unification with 20 zigbee 3.0 Platform Certifications. (December 2016). http://www.zigbee.org/zigbee-alliance-accelerates-iot-unification-with-20-zigbee-3-0-platform-certifications/

[13]. N. Vidgren, K. Haataja, J. L. Patiño-Andres, J. J. Ramírez-Sanchis and P. Toivanen, "Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned," 2013 46th Hawaii International Conference on System Sciences, Wailea, Maui, HI, 2013, pp. 5132-5138

[14]. X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 816-829, Oct. 201

[15]. ZigBee 3.0 Devices User Guide, 2016. https://www.nxp.com/docs/en/user-guide/JN-UG-3114.pdf

[16]. T. Zillner, "ZigBee Exploited: the good, the bad, and the ugly" (August 16 2015).

[17]. X. Fan, F. Susan, W. Long, S. Li, "Security Analysis of Zigbee", MIT.edu, 2017

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

[19]. E. Deniz and R. Samet, "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, 2018, pp. 102-106

[20]. ZigBee Specification, 2012. http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf

[21]. ZigBee Alliance, ZigBee 3.0 Stack User Guide, 2018. https://www.nxp.com/docs/en/user-guide/JN-UG-3113.pdf

[22]. D. Gislason, "ZigBee Wireless Networking", p. 1-2, 2008

[23]. ZigBee Cluster Library (for ZigBee 3.0) User Guide, 2018. https://www.nxp.com/docs/en/user-guide/JN-UG-3115.pdf

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

[25]. O. Aslan, R. Samet "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, 2017.