Journal of the Faculty of Engineering and Architecture of Gazi University 33:4 (2018) 1247-1272

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Security for the internet of things: a survey of existing mechanisms, protocols and open research issues

Sedat Görmüş[1], Hakan Aydın[2*], Güzin Ulutaş[1]

[1]Department of Computer Engineering, Karadeniz Technical University, Trabzon, 61080, Turkey
[2]Department of Software Engineering, Of Technology Faculty, Karadeniz Technical University, Trabzon, 61080, Turkey

Highlights:

- Security in internet of things
- Research challenges in internet of things protocols
- Introduction of security features of state of the art 6TiSCH and 6LoWPAN protocols

Keywords:

- Wireless sensor networks
- Internet of things
- Embedded devices
- The Institute of Electrical and Electronics Engineers
- Internet Engineering Task Force
- IPv6 over Low-Power Wireless Personal Area Networks
- Protocol for Carrying Authentication for Network Access
- IPv6 over the TSCH mode of IEEE 802.15.4e

Article Info:

Review Article
Received: 26.01.2017
Accepted: 10.10.2017

DOI:

10.17341/gazimmfd.416406

Acknowledgement:

Correspondence:

Author: Hakan Aydın
e-mail: hakanaydin@ktu.edu.tr
phone: +90 462 3772968

Graphical/Tabular Abstract

As small devices are being integrated to the Internet, there is a growing interest toward technologies enabling this integration. Internet Engineering Task Force (IETF) has been developing technologies such as 6LoWPAN, 6TiSCH to reliably include small devices into the Internet. The goal of these efforts is to create the next generation Internet where the small devices can communicate with each other over the Internet without complex network gateways. This new concept, which will be connecting billion of devices to each other over the Internet, is called the Internet of Things (IoT). As a result, the new Internet will be not only a network of personal computers, mobile devices and servers, but also it will include vehicles, house appliances, factories and wearable devices. As the small devices increasingly becomes the part of the Internet, billions of small devices will be the source and the destination of a large portion of the Internet traffic. A large portion of the Internet enabled embedded devices will have to face the security challenges put forward by Internet with limited resources. In this study, the protocols and mechanisms for securing IoT networks will be analyzed at each layer of the protocol stack.

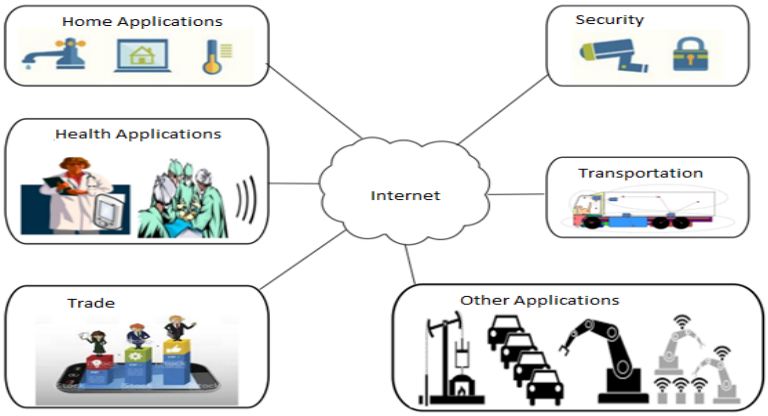


Figure A: Internet of Things usage areas

Purpose: In this study, the protocols used for secure communication in the Internet technology of things are examined by considering the architectural structure of small devices.

Theory and Methods:
At each layer of the protocol stack, the challenges and possible solutions will be presented. Furthermore, the steps necessary for enabling a secure and dependable IoT will be outlined from the perspective of new protocols such as 6LoWPAN, 6TiSCH. experimental method or theory of the study should be given briefly.

Results:
As can be understood from the work done, the Internet of things should be considered an integral part of the security of the next generation Internet, and in this context solutions with low complexity and high reliability must be configured for the Internet networks of Things.

Conclusion:
Current asymmetric cryptographic techniques should be optimized to be usable in restricted devices and made compatible with IoT technology.

Journal of the Faculty of Engineering and Architecture of Gazi University 33:4 (2018) 1247-1272

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Nesnelerin interneti teknolojisi için güvenlik: var olan mekanizmalar, protokoller ve yaşanılan zorlukların araştırılması

Sedat Görmüş[1], Hakan Aydın[2]*, Güzin Ulutaş[1]

[1]Karadeniz Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Trabzon, 61080, Türkiye
[2]Karadeniz Teknik Üniversitesi, Of Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Trabzon, 61080, Türkiye

Ö N E Ç I K A N L A R

- Nesnelerin interneti için var olan güvenlik mekanizmalarının araştırılması
- 6LoWPAN ve 6TiSCH protokollerinin güvenlikteki önemi
- Kablosuz duyarga ağlar için güvenlik gereksinimlerinin incelenmesi

Makale Bilgileri

Tarama Makalesi
Geliş: 26.01.2017
Kabul: 10.10.2017

DOI:
10.17341/gazimmfd.416406

Anahtar Kelimeler:
Kablosuz duyarga ağlar, nesnelerin interneti, gömülü cihazlar

ÖZET

Küçük cihazların İnternet'e dahil olmasıyla yeni araştırma alanları ortaya çıkmaktadır. Internet Engineering Task Force (IETF) 6LoWPAN, 6TiSCH gibi protokol eklentileriyle, uyumlu ve kararlı bir şekilde küçük cihazların İnternet'e dahil edilmesi için çalışmalar yürütmektedir. Bu çalışmaların nihai hedefi, birbirleriyle İnternet üzerinden haberleşebilecek nesnelerin oluşturacağı yeni nesil İnternet'i mümkün kılmaktır. Milyarlarca cihazı birbirine global olarak bağlayacak olan bu yeni nesil ağ kavramına Nesnelerin İnternet'i (Internet of Things) adı verilmektedir. IoT ağlarının yaygınlaşması ile birlikte bu tür ağların üzerinde milyarlarca cihaz aktif olarak veri üretecek ve bu verileri tüketeceklerdir. Yeni nesil İnternet'i oluşturacak küçük ve gömülü cihazların büyük bölümü, kısıtlı kaynaklarla global İnternet'in ortaya koyduğu birçok güvenlik tehdidiyle başa çıkmak zorunda kalacaklardır. Bu çalışmada Nesnelerin İnterneti teknolojisindeki güvenli haberleşme için kullanılan protokoller küçük cihazların mimari yapısı göz önüne alınarak katman katman incelenecektir. Bu katmanlardaki güvenlik mekanizmalarından ve karşılaşılan zorluklardan bahsedilip; güvenli bir Nesnelerin İnterneti için atılması gereken adımlar hakkında öneriler ortaya konulacaktır. Bu bağlamda 6TiSCH ve 6LoWPAN gibi yeni nesil Nesnelerin İnterneti protokolleri tanıtılarak; bu protokollerde yaşanılan zorluklar için muhtemel güvenlik mekanizmaları ele alınacaktır.

Security for the internet of things: a survey of existing mechanisms, protocols and open research issues

H I G H L I G H T S

- Security in internet of things
- Research challenges in internet of things protocols
- Introduction of security features of state of the art 6TiSCH and 6LoWPAN protocols

Article Info

Review Article
Received: 26.01.2017
Accepted: 10.10.2017

DOI:
10.17341/gazimmfd.416406

Keywords:
Wireless sensor networks, internet of things, embedded devices

ABSTRACT

As small devices are being integrated to the Internet, there is a growing interest toward technologies enabling this integration. Internet Engineering Task Force (IETF) has been developing technologies such as 6LoWPAN, 6TiSCH to reliably include small devices into the Internet. The goal of these efforts is to create the next generation Internet where the small devices can communicate with each other over the Internet without complex network gateways. This new concept, which is expected to connect billions of small devices to each other over the Internet, is called the Internet of Things (IoT). In this new global network, billions of small devices will be the source and the destination of a large portion of the Internet traffic. The Internet enabled embedded devices will have to face the security challenges of this new global network with limited resources. In this study, the protocols and mechanisms for securing IoT networks is analaysed at each layer of the protocol stack outlining challenges and possible solutions. Furthermore, the steps necessary for enabling a secure and dependable IoT is presented from the perspective of new protocols such as IETF 6LoWPAN and 6TiSCH.

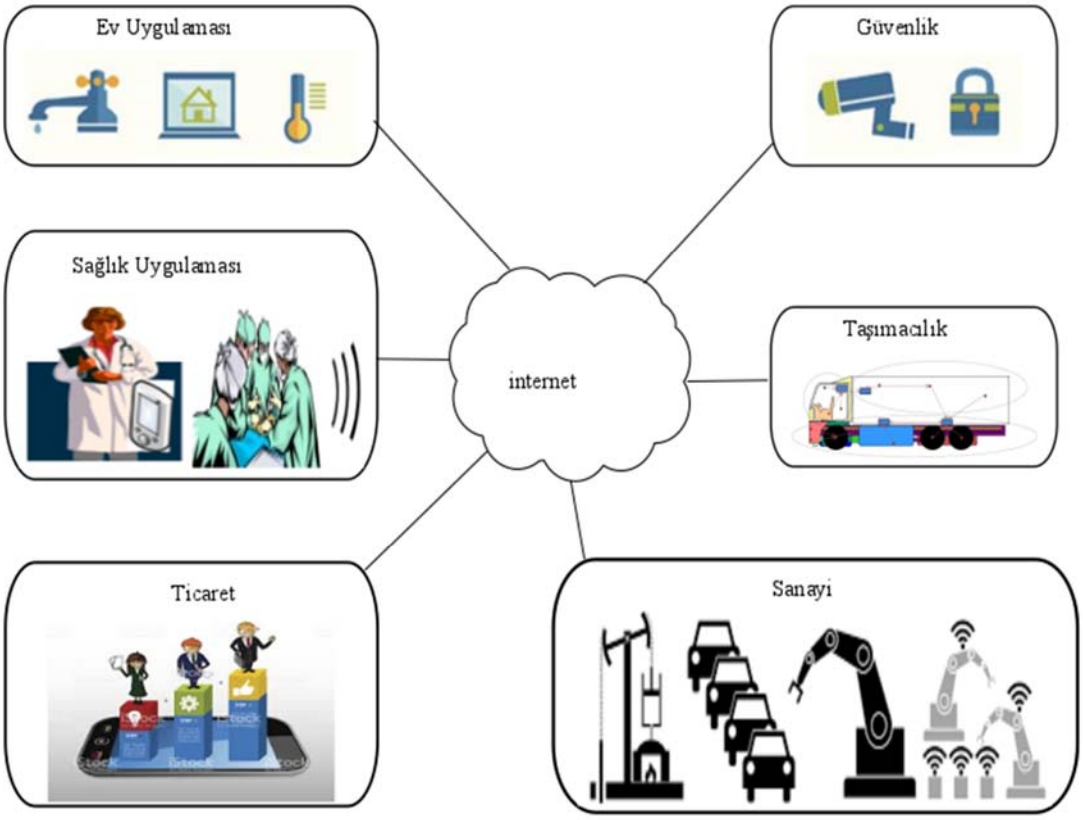
*Sorumlu Yazar/Corresponding Author: hakanaydin@ktu.edu.tr / Tel: +90 462 3772968

1. GİRİŞ (INTRODUCTION)

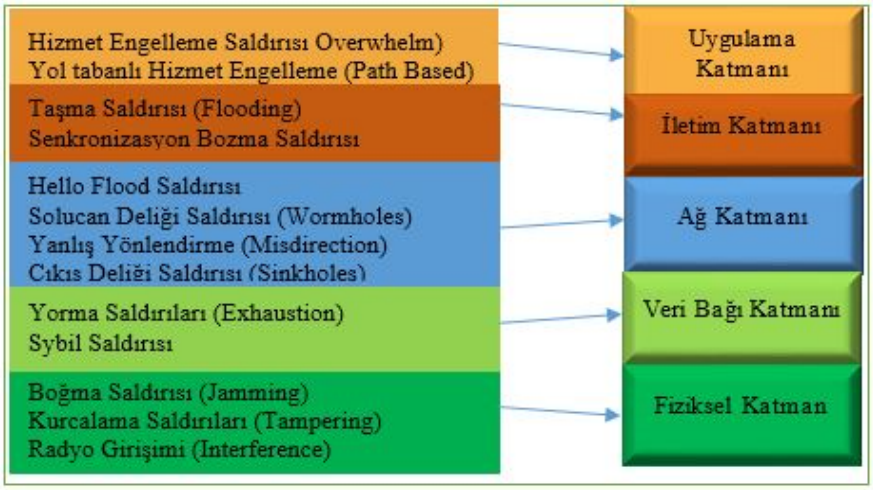
Kablosuz duyarga ağları (KDA), çok sayıda küçük boyutlu, düşük maliyetli ve kısa mesafede kablosuz ortam üzerinden haberleşebilen duyarga düğümlerinden meydana gelen ağlardır. Bu ağlarda, düğümler rastgele olarak ortama bırakılabilmekte ve geliştirilen protokoller sayesinde kablosuz ortam üzerinden birbirleri ile haberleşerek kendi kendilerine organize olabilmektedirler. Kablosuz duyarga ağlarının normal şartlarda erişimin imkânsız olduğu bölgelere kolaylıkla yerleştirilebilmeleri ve uzun süreler boyunca bakım istemeden çalışabilmeleri, bu ağların çok çeşitli alanlarda kullanılabilmelerini mümkün kılmaktadır.

Bugün kablosuz duyarga ağları sağlıktan inşaat sektörüne, kimyadan çevre izlemeye, savaş alanlarının gözetim altında tutulmasına, fabrika otomasyonundan evleri uzaktan kontrol etmeye kadar geniş bir yelpazede kullanılmaktadırlar [1]. Şekil 1'de İnternete bağlanmış kablosuz duyarga ağlarına ait bazı örnekler verilmiştir. Bu şekilde İnternete bağlı küçük cihazların oluşturacağı yeni İnternete "Nesnelerin İnterneti" adı verilmektedir. Hayatımızın önemli bir parçası olacağı düşünülen bu teknoloji akıllı şehirler, akıllı şebekeler ve akıllı toplum (smart community) kavramlarıyla karşımıza çıkmaktadır [2]. Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılan tanımıyla Nesnelerin İnterneti, herhangi bir zamanda herhangi bir yerde her nesnenin birbirine bağlanabileceği bir teknolojidir. Var olan tanımlardan yola çıkılarak Nesnelerin İnterneti, tüm nesnelerin çeşitli haberleşme protokolleri ve algılama yöntemleri aracılığıyla tanımlanarak birbirleri ile iletişime geçebileceği, İnternet ortamına çıkabilecekleri akıllı ağlardan oluşan bir teknoloji olarak tanımlanabilir [3].

Cisco [4] tarafından yapılan bir araştırmaya göre Nesnelerin İnterneti kapsamında İnternete bağlanacak cihazların sayısının 2020 yılında 50 milyara ulaşacağı tahmin edilmektedir. Nesnelerin İnterneti ağlarındaki cihazların İnternete dâhil olması ile birlikte bu cihazların İnternetin maruz kaldığı güvenlik sorunları ile başa çıkması gerekecektir. Nesnelerin İnterneti ağlarındaki cihazların kısıtlı bant genişliği, hafıza ve hesaplama yeteneğine sahip olmaları, onları bu tür tehditlere karşı daha savunmasız bırakmaktadır. Bundan dolayı, bu cihazların geleneksel güvenlik tekniklerini kullanarak İnternetin ortaya koyduğu güvenlik sorunlarıyla başa çıkmaları mümkün görülmemektedir. Yapılan çalışmalarda kablosuz duyarga ağ mimarisini oluşturan fiziksel [5], veri bağı, ağ, iletim ve uygulama katmanlarının farklı özellikteki saldırılara karşı savunmasız olduğu görülmektedir [6-8]. Şekil 2'de farklı katmanlar için literatürde ortaya konulan saldırı türleri özetlenmektedir.



Şekil 1. Nesnelerin İnterneti kullanım alanları (Internet of Things usage areas)



Şekil 2. Kablosuz duyarga ağ katmanlarını etkileyen saldırı türleri
(Attack types affecting wireless sensor networks)

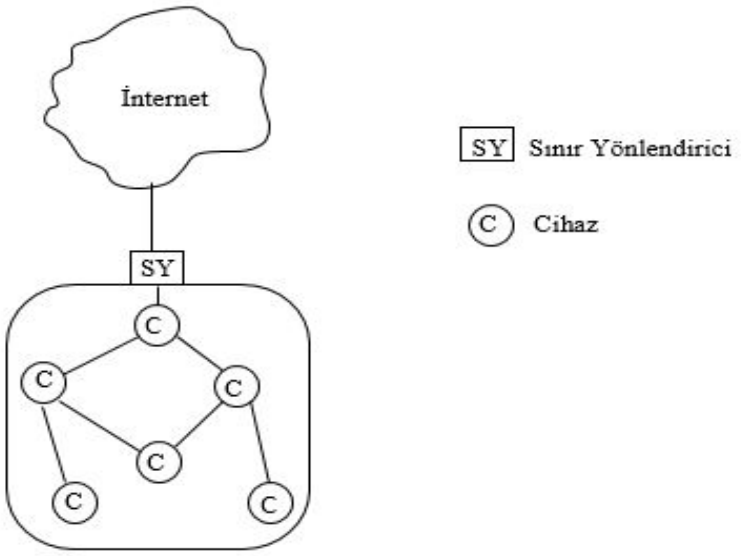
Bu tarama makalesinde literatürde kablosuz duyarga ağları için ortaya konan güvenli haberleşme mekanizmaları özetlenerek bu mekanizmaların Nesnelerin İnterneti uygulamalarına nasıl uyarlanacağı irdelenecektir. Katmanlardaki güvenlik mekanizmalarından ve karşılaşılan zorluklardan bahsedilecek ve güvenli bir Nesnelerin İnterneti için atılması gereken adımlar hakkında öneriler ortaya konulacaktır. Bu bağlamda Bölüm 2'de Nesnelerin İnterneti için protokol yığını, Bölüm 3'te Nesnelerin İnterneti için güvenlik gereksinimleri anlatılacaktır. Bölüm 4'te Nesnelerin İnterneti güvenliği için yapılan çalışmalar ele alınacaktır. Bölüm 5'te protokol yığını katmanlarındaki var olan güvenlik mekanizmaları ele alınacak ve özetlenecektir. Bölüm 6'da protokol yığını katmanlarında güvenlik sağlanırken karşılaşılan zorluklardan ve bu zorluklara karşı alınacak tedbirlerden bahsedilecektir. Son bölümde ise bu çalışma baz alınarak Nesnelerin İnterneti ağlarındaki güvenlik için çeşitli yöntemler önerilmiştir.

2. NESNELERİN İNTERNETİ İÇİN PROTOKOL YIĞINI
(INTERNET OF THINGS PROTOCOL STACK)

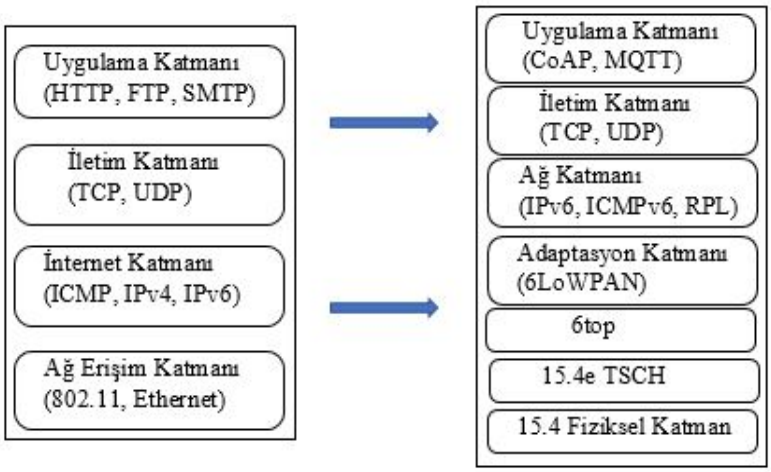
Bu bölümde Nesnelerin İnterneti teknolojisindeki cihazların kullanmış olduğu yığın yapısı incelenecektir. Şekil 3'te örnek bir Nesnelerin İnterneti ağı gösterilmiştir. Bu ağda cihazlar (C) birbirleriyle ve sınır yönlendiricisiyle (SY) haberleşebilmektedirler [9]. Nesnelerin İnterneti teknolojisindeki cihazlar kabiliyetlerine göre veri üretebilirler veya hem veri üretip hem de bu verileri işleyerek sınır yönlendiriciye iletirler. Sınır yönlendirici de cihazlardan toplamış olduğu bu verileri "İnternet" ortamına aktarır. Bu işlemleri gerçekleştirmek için TCP/IP protokol yığınının var olan katmanlarına bazı eklemeler/değişiklikler yapılması gerekmektedir. IEEE ve IETF tarafından Nesnelerin İnternetini gerçeklemeye yönelik önerilen bazı protokol eklentileri Şekil 4'te verilmiştir. Şekil 4'te 6LoWPAN [10], 6Top [11], IEEE 802.15.4-e TSCH [12], CoAP (Constrained Application Protocol) [13], MQTT (Message Queuing Telemetry Transport) [14] gibi protokol eklentilerinin protokol yığınındaki konumları verilmiştir. Her bir protokol parçası, öncelikle düşük güç tüketimi için uyarlanmıştır. Ortam erişim katmanında yer alan IEEE 802.15.4-e TSCH protokolünün temel hedefi yüksek kararlılık ve düşük enerji ile veri paketlerini iletmektir. 6Top katmanı ise IEEE 802.15.4-e TSCH kullanan düğümlerin kaynak ihtiyaçlarını dağıtık olarak karşılamayı hedefler. 6LoWPAN katmanı IPv6 ile IEEE 802.15.4 arasında bir uyum katmanı olarak karşımıza çıkar. RPL (IPv6 Routing Protocol for Low Power and Lossy Networks) protokolü düşük kontrol trafiği gerektiren bir yönlendirme protokolüdür [15]. CoAP ve MQTT ise farklı senaryolar için uygulama protokolü ihtiyacını karşılamak amacıyla tasarlanmıştır. Bütün bu eklentiler sayesinde düşük güçlü ve kayıplı düğümlerin kararlı bir şekilde İnternet'e bağlanması hedeflenmektedir. Nesnelerin İnterneti teknolojisini kullanan cihazlar iletişim için "IP" adreslerine ihtiyaç duyarlar. Önümüzdeki 10 yılda Nesnelerin İnterneti cihazlarının 50 milyar adede ulaşması beklenmektedir. Bunun sonucu olarak var olan IPv4 IP havuzu yeterli olmayacaktır. Bu nedenle 128 bit adresleme sağlayan IPv6, Nesnelerin İnterneti için uygun bir adresleme havuzu sunan bir protokoldür. IPv6 protokolüne geçiş ile IP çakışmalarının önüne geçilmesi adına önemli bir engelin ortadan kalkacağı düşünülmektedir. IEEE 802.15.4 fiziksel katmanının gönderebileceği maksimum paket boyutunun 127 Byte olması ve IPv6 protokolünün minimum parçalamadan göndermesi gereken paket uzunluğunun 1280 Byte olması bir adaptasyon katmanı gereksinimini ortaya çıkarmıştır [16, 17]. Bu katman IPv6 paketlerini çok daha küçük 802.15.4 parçalarına sığdırabilmek için "IP" paketlerini küçük parçalara ayırmakta ve paket başlık bölümlerini sıkıştırmaktadır. 6LoWPAN protokolü bu gereksinimleri karşılamak için geliştirilmiştir.

2.1. 6LoWPAN
(IPv6 over Low-Power Wireless Personal Area Networks)

6LoWPAN standardı IEEE 802.15.4 fiziksel katmanına sahip cihazların IPv6 adresleme standardına uyumlu olarak



Şekil 3. Nesnelerin İnterneti ağı (Architecture of an ınternet of things network)



Şekil 4. Standart TCP/IP modeli ve 6LoWPAN tabanlı protokol yığını (Standard TCP / IP model and 6LoWPAN based protocol stack)

İnternete dahil olmasını sağlamak amacıyla oluşturulmuştur. 6LoWPAN protokolü, "İnternet Protokolü, küçük cihazlara bile uygulanabilir olmalıdır" fikrinden doğmuştur [16-18]. Geleneksel olarak duyarga düğümleri İnternet'e uygulama katmanı ağ geçidi(gateway) üzerinden dâhil edilmektedir. Uygulama katmanı ağ geçidi protokol çevrimi yapacağı için birçok protokolü anlayacak şekilde tasarlanmalıdır ve bu durum birçok zorluğu beraberinde getirmektedir. Bu nedenle IETF, IEEE 802.15.4 fiziksel katmanı üzerinden IPv6 paketlerinin taşınabilmesi için gerekli olan protokol ihtiyaçlarını belirlemek amacıyla çalışma grupları başlatmıştır. 6LoWPAN çalışma grubunun ortaya koyduğu protokol eklentileri sayesinde IP paketleri düşük güçlü ağlarda sorunsuzca taşınabilmektedir. 6LoWPAN'ın özellikleri aşağıdaki gibi özetlenebilir:

- 16 ve 64 bitlik 802.15.4 adreslemeyi destekler.
- Verimli IP ve TCP/UDP başlık (header) sıkıştırma.
- Komşu bulma yardımıyla otomatik ağ konfigürasyonu.
- Unicast, multicast ve broadcast desteği.
- Paketleri bölme-birleştirme (1280 byte'lık IPv6 maksimum iletim birimini 127 byte'lık IEEE 802.15.4 çerçeveleri şeklinde parçalama).

6LoWPAN başlık sıkıştırma (header compression), çerçeveleme (framing), adresleme (addressing), komşu bulma (neighbor discovery) ve IPv6 paketlerini parçalama-birleştirme (fragmentation-defragmentation) işlemleri için gerekli protokol eklentilerini tanımlar. Parçalama ve başlık sıkıştırma işlemleri aşağıda detaylı bir şekilde incelenmiştir.

Parçalama(Fragmentation): 6LoWPAN adaptasyon katmanının birincil görevi parçalama ve birleştirme işlemleridir. 6LoWPAN, IP katmanından aldığı parçalama eşiğinden büyük paketleri öncelikle küçük parçacıklara böler. 6LoWPAN'ın bir IPv6 paketini iki düğüm arasında

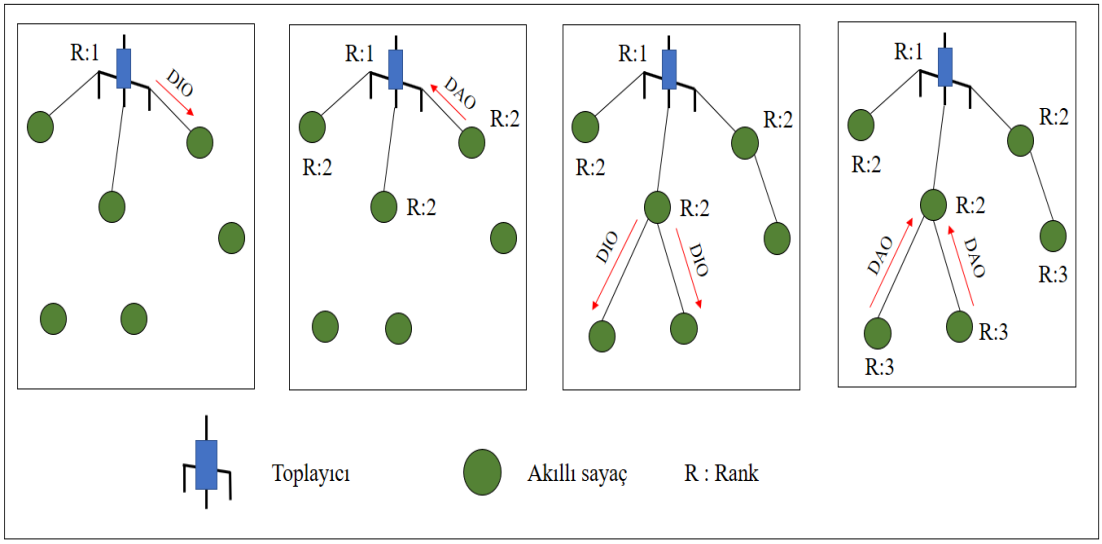
iletmek için 60 saniyeye ihtiyacı vardır. Bu süreye parçalama, iletim ve birleştirme adımları dâhildir. Bu işlem sırasında ilk parçacığa paket başlığını koyar ve hedef düğüme gönderilmek üzere ortam erişim katmanına yönlendirir. Geri kalan parçacıklar ise parçacık başlığı ve sıra numarası bilgisiyle hedef düğüme yönlendirilir. Hedef düğüm parçacıkları alıp sıraya koyar ve bütünleştirilmiş IP paketini IP katmanına yönlendirir. IP katmanı perspektifinden parçalama birleştirme söz konusu değildir.

Başlık Sıkıştırma (Header Compression): IPv6'nın küçük cihazlara getirilmesinin önündeki en büyük engellerden biri de bu protokolün gerektirdiği başlık uzunluğunun oldukça büyük olmasıdır. Zira 802.15.4 gibi küçük paket boyutlarına sahip protokollerin bu durumda verimlilikleri ciddi şekilde düşecektir. Bunu engellemek için 6LoWPAN katmanı IP başlık sıkıştırma ve açma işlemlerini gerçekleştirir. 6LoWPAN bu özellikleriyle IP paketlerinin düşük güçlü ağlarda sorunsuzca iletilmesini sağlar. Düşük güçlü ağların geniş kapsama alanlarında kullanılabilmeleri için çok sekmeli yapılara ihtiyaç vardır. Bu da 6LoWPAN katmanına ek olarak bir yönlendirme katmanı ihtiyacını ortaya çıkarır. Bundan dolayı IETF, ROLL (Routing over Low Power and Lossy Links /Düşük Güç ve Kayıplı Ağlar Üzerinde Yönlendirme) ismini verdiği başka bir çalışma grubu ile RPL [19] (IPv6 Routing Protocol for Low-Power and Lossy Networks / DüşükGüç ve Kayıplı Ağları için IPv6 Yönlendirme Protokolü) standartlarını Nesnelerin İnterneti sistemleri için geliştirmiştir. RPL protokolünün temel işlevi kablosuz duyarga düğümü ile İnternet bulutu arasındaki veri trafiğinin yönlendirilmesidir. RPL yönlendirme için gerekli yolları oluştururken kablosuz duyargaların düşük güç tüketim ihtiyaçlarını, iletim kanalının kayıplı olmasını ve bant genişliğinin düşük olmasını dikkate almalıdır.

RPL, IPv6 tarafından oluşturulan yerel bağlantıları kullanarak ağaç tabanlı bir topoloji oluşturur. Bu topolojide veri akışı bir kök cihazdan uç cihaza ve tersi yönde olur. En uygun veri akış yolunun belirlenmesi için "Rank" adı verilen ve cihazların ağdaki konumunu belirten bir parametre kullanılır. Rank hesaplanmasında ise amaç fonksiyonu (objective function) ismi verilen ve seçilen bir parametreye göre yolun kalitesini hesaplayan algoritmalar kullanılır. Örneğin, hattın paket düşürme olasılığını gösteren bir metrik yardımıyla Rank hesabı yapılabilir. Şekil 5'te RPL protokolünün çalışma adımları kısaca özetlenmektedir.

RPL protokolü öncelikle, kök düğüm olarak belirlenmiş düğümün DODAG (Destination Oriented Directed Acyclic Graph-Hedef tabanlı yönlü döngüsüz graf) Information Object (DIO) ismi verilen kontrol paketlerini ağa yaymasıyla başlar. Bu adımı takiben, DIO mesajını alan düğümler (çocuk düğümler) kendi rank bilgilerini bir amaç fonksiyonu kullanarak hesaplarlar. Burada tipik olarak amaç fonksiyonu DIO mesajının geldiği düğümün (ata düğümün) rank değerine kanalın kalitesini ifade eden bir değer (link metric) ekler ve bu hesaplanan değer çocuk düğümün rank değeri olarak belirlenir. Çocuk düğüm yayınlayacağı DIO mesajlarına hesaplanan rank değerini ekler. DIO mesajları Trickle [20] adı verilen bir algoritmayla değişken periyotlarla gönderilir. Ağın kararlı olduğu durumda Trickle algoritması DIO yayın periyodunu maksimum değere çeker. Ağ yapılandırması başladığında ya da ağ topolojisinde bir değişiklik olduğunda DIO yayın periyodu minimum değerine çekilir. Böylece, ağda değişiklik olmadığı sürece, kontrol trafiği azaltılmış olur. Bu karakteristik özellik, RPL'in düşük güç gerektiren ağlar için uygun bir yönlendirme protokolü olmasını sağlar.

Her düğüm DIO mesajını aldıktan sonra en uygun Rank'a sahip düğümü (Rank'ı küçük olan tercih edilir) atası olarak belirler ve yönlendirme tablosuna bu düğümün IPv6 lokal adresini varsayılan yönlendirici olarak ekler. Düğüm, varsayılan yönlendirici dışında farklı düğümleri yedek yönlendirici olarak bir tabloya ekler. Tipik olarak, iki ya da üç yedek yönlendirici tutulur. Varsayılan yönlendirici



Şekil 5. RPL protokolü (RPL protocol)

düğümünün bağlantı(link) kalitesi düştüğünde ya da ulaşılamaz olduğu durumlarda, aday yönlendirici düğümlerden biri Rank değerine göre varsayılan yönlendirici olarak seçilir. Bu şekilde, DIO mesajını alan düğüm kök düğüme doğru yönlendirme yolunu belirlemiş olur. Bu adımı takiben, düğüm Destination Advertisement Object (DAO) adı verilen bir mesaj oluşturur ve bu mesajı varsayılan yönlendirici düğüme gönderir. Çocuk düğümden DAO mesajını alan düğüm iki farklı şekilde bu mesajı işleyebilir. İlk durumda, düğüm mesajın içerisindeki yol bilgisini lokal yönlendirme tablosuna ekler ve bu yöntem depolama modu (storing mode) olarak adlandırılır. İkinci durumda DAO mesajındaki yönlendirme bilgileri, ara düğümler tarafından depolanmaz. Kök düğüm, DAO içerisindeki farklı düğümlere ait birleştirilmiş yol bilgisini lokal yönlendirme tablosuna ekler. İlk yöntem yönlendirme bilgisini lokalde sakladığı için sekme sayısını ağ içerisindeki noktadan noktaya (P2P) haberleşme durumlarında azaltacaktır. Fakat, bu lokal düğümlerin daha fazla bellek ihtiyacını ortaya çıkarır. Diğer taraftan, eğer yönlendirme tablosu sadece kök düğümde tutulursa, P2P haberleşme için veriler kök düğümü üzerinden yönlendirilmek zorunda kalacaktır. Bu yaklaşımın avantajı ise kök düğüm dışındaki düğümlerin bellek ihtiyacını azaltmasıdır.

RPL belirtilen mesajları kullanarak ağaç tabanlı bir ağ yapılandırması ortaya koyar. DIO ve DAO mesajları dışında, RPL ağa dâhil olma adımlarını kısaltmak için DODAG Information Solicitation (DIS) adı verilen bir mesajdan yararlanır. DIS mesajını alan düğümler, DIO mesajıyla bu mesaja cevap verirler. Böylece ağa katılmak isteyen düğümler DIO periyodunu beklemeden hızlıca ağa katılabilirler. RPL Instance (Oluşum) adı verilen ve aynı ağ üzerinde farklı amaç fonksiyonları kullanarak farklı topolojiler oluşturan yapıları da destekler [19, 21].

RPL bu sayılan özelikleriyle düşük güçlü ve kayıplı ağlar için ideal bir yönlendirme protokolü ortaya koyar. Ayrıca IPv6 ile uyumlu şekilde çalışması, düğümlerin bellek ihtiyaçlarını belli ölçüde azaltır. Bu sayede, birçok Nesnelerin İnterneti uygulaması için varsayılan yönlendirme protokolü olarak karşımıza çıkar.

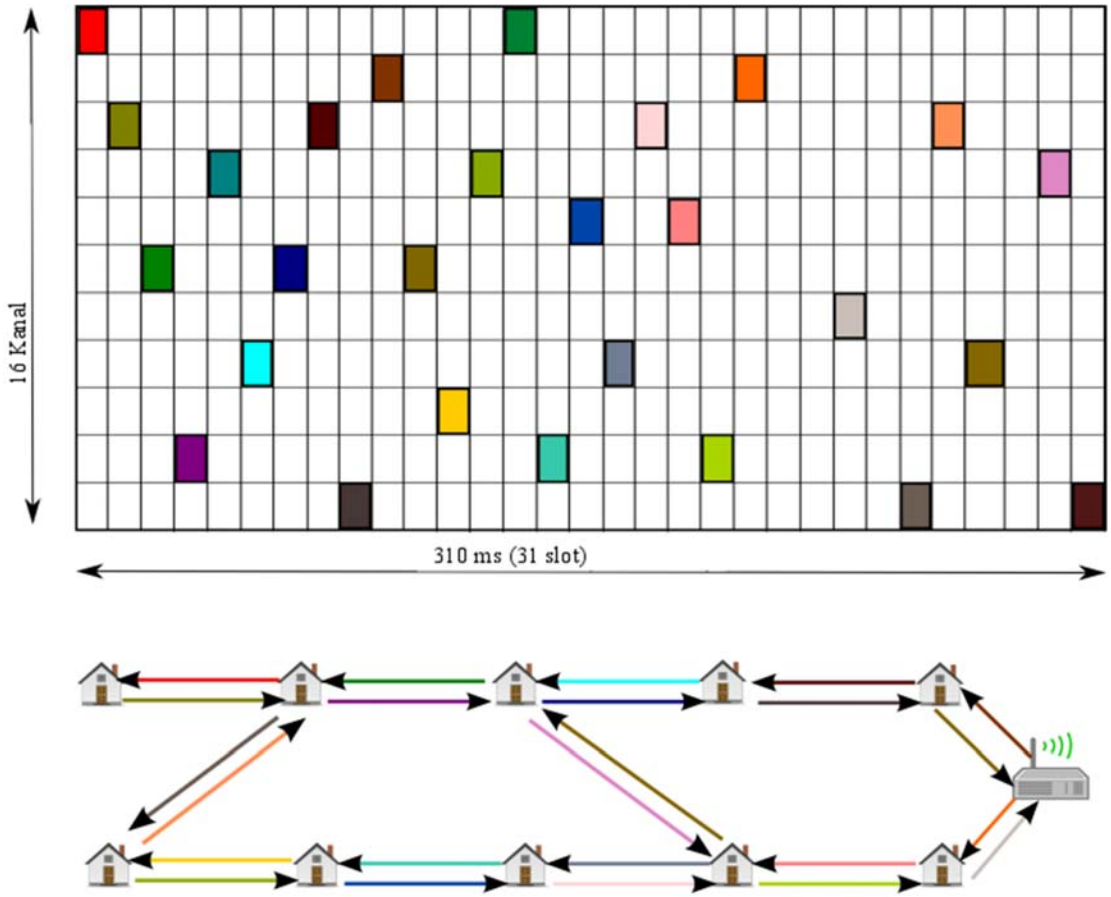
2.2. 6TİSCH (IPv6 over the TSCH mode of IEEE 802.15.4e)

İnternete bağlı sistemleri endüstriyel süreçlere dâhil ederek verimliliğin arttırılmasını hedefleyen Endüstri 4.0 ve Endüstriyel İnternet kavramları yakın zamanda sıkça karşımıza çıkmaktadır [22]. Bu kavramları hayata geçirecek önemli yapı taşlarından birinin Nesnelerin İnterneti teknolojileri olduğu düşünülmektedir. Bu anlamda, Endüstriyel İnternet uygulamaları geleneksel duyarga ağlarından beklenen performans hedeflerine ek olarak düşük ve öngörülebilir ağ gecikmesini öncelikli bir gereksinim olarak karşımıza çıkarmaktadır. Bundan dolayı, bu uygulama alanında kullanılacak İnternete bağlı kablosuz duyarga modülleri, yeni gereksinimlere göre tasarlanmış yazılımsal ve donanımsal parçaları içermelidirler. 2012 yılında IEEE endüstriyel gereksinimleri karşılamak amacıyla, 802.15.4 protokolüne zaman paylaşımlı (Time Slotted) ve kanal atlamalı(Channel-Hopping) ortam erişim yöntemini ekledi [12]. 802.15.4-e TSCH olarak adlandırılan ortam erişim protokolünün ana hedefi kablo seviyesinde kararlılığa ek olarak düşük gecikmeye sahip kablosuz duyarga ağlarını endüstriyel uygulamalar için hayata geçirmektir. Bu yöntemde, düğümler iletim ortamına önceden kestirilebilir bir gecikmeyle kendilerine ayrılmış zaman diliminde erişirler. Böylece uygulamanın gerektirdiği gecikme kriterlerini sağlayacak şekilde ağ trafiği şekillendirilebilir, kontrol ve otomasyon için kritik olan performans hedefleri yakalanabilir. Ayrıca, bu yöntemi kullanan düğümler kendilerine tahsis edilmiş frekans kanalları arasında atlayarak sistemin maruz kalabileceği girişim sorunlarının üstesinden gelmeye çalışırlar. Kanal atlama yöntemi özellikle girişimin yüksek olabileceği endüstriyel alanlar için üstün bir kararlılık performansı sağlar. IEEE 802.15.4-e TSCH protokolünde düğümler arasındaki senkronizasyon kanala gönderilen işaretçiler sayesinde sağlanabileceği gibi, düğümler arasındaki haberleşme sırasında gönderilen geri bildirim (ACK) paketlerine koyulabilecek zaman damgalarıyla da sağlanabilir [12].

IEEE 802.15.4-e TSCH protokolü kestirilebilir gecikmeyle sağlıklı haberleşmeyi iki komşu düğüm arasında gerçekleştirmek için yeterlidir. Fakat birçok uygulama için çoklu sekme içeren (multi hop routing) bir ağ yapısı kaçınılmazdır. Bu nedenle, 802.15.4-e ortam erişim protokolünü Nesnelerin İnternetine dâhil edecek ve Endüstriyel İnternet'in parçası haline getirecek standart çözümler gereklidir. Bu standart çözümler sayesinde kestirilebilir ve yüksek güvenilirlik sağlayan duyarga ağların gerçeklenmesi mümkün olacaktır. 6Tisch (IPv6 routing over time slotted channel hopping MAC) [11] belirttiğimiz bu eksikliği gidermek üzere IETF (Internet Engineering Task Force) tarafından standartlaştırma sürecindedir. IETF'in öncelikli hedefi IPv6 tabanlı bir yönlendirme protokolünün zaman paylaşımlı ve kanal atlamalı bir ortam erişim protokolü ile uyumlu çalışmasını sağlamak için gerekli olan sistem parçalarını tanımlamaktır. Bu parçalardan en önemlisi kaynak dağıtmayı sağlayan yazılım parçasıdır.

2.2.1. 6Tisch ağlarından kaynak yönetimi (Resource management on 6Tisch networks)

6Tisch protokolünü gerçeklemek için, 6loWPAN protokolü tarafından sunulan uyarlama katmanına ek uyum sağlayıcı öğelerin gerçeklenmesi gerekir. Bunlardan en önemlisi zaman ayrışımlı erişimi sağlayacak çizelgeleri oluşturacak öğedir. Bu öğe iki düğüm arasındaki haberleşme ve ağdaki yönlendirme içerikleri için gerekli olan çizelgeleri oluşturmakla yükümlüdür. Bu öğe ayrıca kendi içinde paket anahtarlama yaparak yönlendirme ve trafik biçimlendirme işlemlerini yapabilir. Şekil 6 örnek bir 6Tisch çizelgesini göstermektedir. Şekilden de anlaşılacağı gibi çizelge çerçevesi 31 zaman dilimine sahip olacak şekilde tasarlanmıştır ve her zaman dilimi 10 milisaniye sürmektedir. Bu çizelgede ayrılan kaynaklar 310 milisaniye

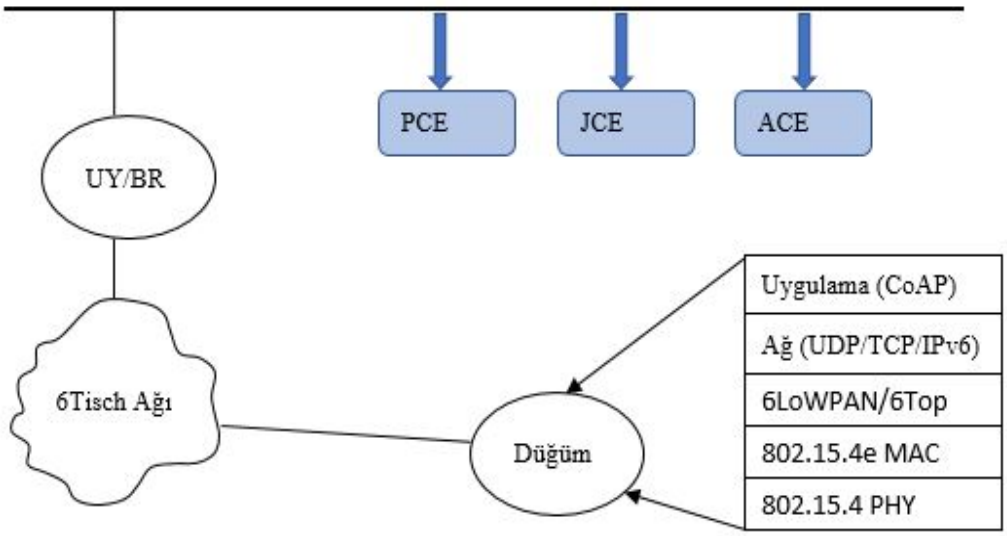


Şekil 6. Örnek 6Tisch çizelgesi (An example 6Tisch schedule) [23]

sonra kendini tekrar eder. Doğal olarak, uygulama gereksinimine göre çizelge çerçevesinin boyutu ve zaman dilimi uzunluğu değiştirilebilir. Her ardışık çerçeve çizelge için düğümler farklı bir kanalda ortama erişirler. Bu sayede bir çerçeve çizelgede girişime uğrayan çizelge öğeleri, bir sonraki çerçeve çizelge sırasında farklı bir kanalda yer alacaklarından, haberleşmenin girişime maruz kalma ihtimali minimize edilmiş olacaktır. Bu da verilerin yüksek güvenilirlikle ağ içinde taşınmasına yardımcı olacaktır [24]. Ağdaki düğümler haberleşme için çizelgede ortak haberleşme için belirlenen zaman dilimleri haricindeki bütün zaman dilimlerini kullanılabilirler. Zaman dilimleri Gönderim(Transmit)), Alım (Receive) ya da Ortak(Shared) olarak işaretlenebilir. Ancak, çizelgede sürekli olarak düşük performans gösteren kanal çizelgeden çıkartılabilir. Bu işaretleme ve çıkarma işlemini yapacak öğe dağıtık olarak gerçeklenebileceği gibi merkezi olarak da gerçeklenebilir. Merkezi olarak çizelgelerin belirlendiği durumda, bütün düğümler kendilerine gerekli olan kaynakları ağda bulunan merkezi öğeden talep ederler. Kaynak ayırımı işlemleri güvenli CoAP protokolü üzerinden gerçeklenebilir. Merkezi çizelgelemenin pratik olmadığı geniş ağlarda, dağıtık bir çizelge belirleme yöntemi tercih edilmelidir. Bu da düğümlerin aralarındaki haberleşme için gerekli kaynakları merkezi bir kontrolden bağımsız olarak belirlemesiyle çözülebilir [12]. 6Tisch protokolünde düğümler arasındaki çizelge belirleme işlemi çoğu zaman dağıtık olarak gerçekleştirilir. Ancak, ağın oluşturulması, güvenlik, kimliklendirme ve zamanlama gibi işlemler için gerekli olan mekanizmalar merkezi olarak gerçeklenebilir. Bu öğelerin ağ içindeki konumu Şekil 7'de gösterilmiştir. Yol Hesaplama Öğesi (Path Computation Element) ağın yapılandırılması için gerekli kaynakların ayrılmasını sağlar. Bağlanma Kordinasyon Öğesi (Join Coordination Element) ağa bağlanacak düğümün kimliklendirilmesi işlemini koordine eder. Kısıtlı Ortamlar için Kimliklendirme Öğesi (Authentication Coordination Element) düğümün ağa dâhil edilmesi sırasında kimliklendirilmesi ve yetkilendirilmesi işlevlerini yerine getirir. Bütün bu öğeler Şekil 7'de görüldüğü gibi Uç Yönlendiricisinin bulunduğu ağda gerçeklenebileceği gibi, farklı ağların parçası olarak da gerçeklenebilirler. Merkezi yönetim öğeleri kendi aralarında ve ağdaki düğümlerle CoAP protokolü [13] kullanarak haberleşirler.

2.3. İletim ve Uygulama Katmanları
(Transport and Application Layers)

İletim katmanı için ise Nesnelerin İnterneti uygulamalarının ihtiyaçlarına göre TCP veya UDP protokollerinden biri tercih edilebilir. Protokol yığınının en üst katmanı olan uygulama katmanında ise Kısıtlı Uygulama Protokolü (CoAP) ve MQTT gibi protokoller bulunmaktadır. CoAP kaynak kısıtlı cihazların uygulama katmanı için



Şekil 7. 6Tisch merkezi kontrol öğeleri (6Tisch centralized control items) [23]

özelleştirilmiş bir protokoldür ve temel olarak HTTP protokolünün UDP üzerinden çalışan versiyonu olarak görülebilir. CoAP tasarım anlamında HTTP protokolüne büyük oranda benzerlik gösterir ve iki protokol arasında dönüşüm yapmak oldukça kolaydır. CoAP İnternet üzerinden duyarga cihazlarına erişim için kullanılabileceği gibi duyargaların İnternet'le haberleşmesi için de kullanılabilir. CoAP ile gerçekleştirilen veri transferinin güvenliği DTLS (Datagram Transport Layer Protocol) yardımıyla sağlanabilir. Nesnelerin İnterneti uygulamaları için geliştirilmekte olan iletim ve uygulama katmanı güvenlik yöntemleri ileriki bölümlerde detaylı bir şekilde ele alınacaktır.

3. NESNELERİN İNTERNETİ İÇİN GÜVENLİK GEREKSİNİMLERİ (INTERNET OF THINGS SECURITY REQUIREMENTS)

Nesnelerin İnternetinde güvenli haberleşme için çeşitli gereksinimler sağlanmalıdır. Bu gereksinimler gizlilik, bütünlük, kimlik doğrulama, veri güncelliği, hizmet bütünlüğü, heterojenlik ve anahtar yönetim sistemleri gibi güvenliğin ana unsurlarıdır. Nesnelerin İnternetinde güvenli haberleşme gereksinimleri bu bölümde başlıklar halinde incelenmiştir [25, 26].

3.1. Gizlilik (Privacy)

Duyargalar üye oldukları ağda haberleşirken, ağda iletilen mesajlara ağa dâhil olmayan düğümlerin erişmeleri engellenmelidir [27]. Bu hedefi gerçekleyecek şekilde ağdaki düğümler güvenli bir haberleşme kanalını kendi aralarında tesis etmelidirler. Güvenli haberleşmeyi gerçeklemek ve mesajın yetkili olmayan tüzel kişiler tarafından dinlenmesini engellemek için iletilen mesajların şifrelenmesi gerekir [28, 29]. Ağın mesaj trafiği seçilen protokol katmanında farklı yöntemler kullanılarak şifrelenir. Şifreleme teknikleri Bölüm 5'te detaylı bir şekilde incelenecektir.

3.2. Veri Bütünlüğü (Message Integrity)

Veri bütünlüğü kaynak tarafından iletilen mesajın ağda ilerlerken değiştirilmeden hedefe ulaşması olarak tanımlanabilir [29]. Ağda iletilen mesajın herhangi bir ağ öğesi tarafından değiştirildiği algılanmalıdır ve değiştirilmiş mesaj reddedilmelidir. Bir mesajın iletim sırasında değiştirilip değiştirilmediği Mesaj Asıllama Kodu (MAK) gibi bir mekanizmayla bulunabilir.

3.3. Kaynak Doğrulama (Authorization)

Kaynak doğrulama, iletişim halinde olan düğümlerin karşılıklı olarak kimliklerini doğrulaması olarak tanımlanabilir. Bu durumda, saldırgan düğüm, kaynak doğrulama olmadan haberleşmeye dâhil olamaz [29].

3.4. Veri Güncelliği (Data Freshness)

Ağda iletilen mesajların taze(yeni) olması veya eski mesajların tekrarlarının olmaması olarak tanımlanabilir [29]. Ağda herhangi bir mesaj daha önceki bir mesajın tekrar iletilmiş haliyse, bu veri ağdaki düğümler tarafından değerlendirilmemelidir. Ağdaki veri güncelliğinin sağlanması için standart yaklaşım, iletilen her bir mesajın içerisine mesajın geçerli olduğu süreyi gösteren bir zaman damgasının eklenmesidir.

3.5. Hizmet Bütünlüğü (Service Integrity)

Hizmet bütünlüğü düğümlerden alınan verilerin bozulmadan güvenli bir şekilde toplanabilmesidir [27]. Veri toplama işleminde düğümler komşu düğümlerden aldıkları veriyi ya ağ geçidine ya da veriyi işleyecek düğümler varsa o

düğümlere iletirler. Güvenli veri toplama gerçek dünya verilerinin ölçümünün doğru hesaplanmasını ve bozulmuş düğümlerden elde edilen verilerin tespit edilmesi hizmet bütünlüğü açısından önemlidir.

3.6. Heterojenlik (Heterogenicity)

Nesnelerin İnterneti teknolojisinde üreticiler tarafından geliştirilen farklı özelliklere (bit oranı, kapasite, versiyon, fonksiyon) sahip cihazlar birbirleriyle haberleşebilmelidir. Belirtilen özelliklere sahip cihazların kendi aralarında sorunsuz bir şekilde haberleşebilmesi için donanımın kabiliyetlerine göre otomatik olarak ayarlanabilen güvenlik protokolleri geliştirilmelidir [30].

3.7. Anahtar Yönetimi (Key Management)

Nesnelerin İnternetini oluşturan cihazlar, verilerin güvenliğini sağlamak için bazı güvenlik parametrelerini kendi aralarında değiş-tokuş yapmalıdırlar [31-33]. Bu amaçla, cihazlar arasında karşılıklı güveni sağlayan güvenlik mekanizmaları için basitleştirilmiş anahtar yönetimi ve minimum enerji harcayan anahtar dağıtım yöntemleri kullanılmalıdır.

4. DÜŞÜK GÜÇLÜ AĞLAR İÇİN YAPILAN ÇALIŞMALAR (STUDIES FOR LOW POWER AND LOSSY NETWORKS)

IEEE 802.15.4 standardı düşük güç tüketimi, düşük maliyeti nedeniyle çoğu KDA uygulaması için seçilen yegâne fiziksel katman olarak karşımıza çıkmaktadır. Bu nedenle fiziksel katman ve ortam erişim katmalarının güvenliği 802.15.4 standardı baz alınarak irdelenecektir.

Mevcut anahtarlama yöntemleri, enerji gereksinimi ve işlem maliyeti açısından IEEE 802.15.4 standardına uygun değildir. [34] numaralı çalışmada IEEE 802.15.4 standardı için üretilmiş bir grup anahtar yönetimi algoritması olan Hibrid Topoloji Grup Anahtar Yönetimi Algoritması (HT-GKMA) önerilmiş ve var olan anahtarlama yöntemleriyle (Iolus, Hydra, Kronos, Octopus, CKA (Conference Key Agreement), Burmester Ve Desmedt Protokolü, Diffie-Hellman Anahtar Değişimi) karşılaştırılmıştır. Sonuçlar, önerilen yöntemin enerji tüketim performansı açısından var olan yöntemlere göre daha iyi olduğunu göstermiştir. IEEE 802.15.4 tabanlı Ad Hoc kablosuz ağlar için bir güvenlik tasarımı [35]'te ele alınmıştır. Geliştirilen güvenlik tasarımı yaklaşımı Ortam Erişim, Ağ ve Uygulama katmanları için ayrıntılı olarak ele alınmış ve mesaj bütünlüğü, şifreleme servisleri, anahtar kurulum protokolleri açısından değerlendirilmiştir.

Perrig vd. [29] kablosuz haberleşme ve sınırlı kaynaklara sahip ortamlar için SPINS güvenlik protokolünü sunmuşlardır. Bu protokol iki güvenlik bloğundan oluşmaktadır: SNEP ve µTESLA. SNEP (Secure Network Encryption Protocol), veri gizliliği, mesaj asıllaması/bütünlüğü ve veri tazeliği sağlamaktadır. Veri gizliliği, bir blok şifreleme algoritması olan RC5 ve bir blok şifreleme yaklaşımı olan CTR (Counter Mode) kullanılarak gerçekleştirilmektedir. Veri tazeliğinin sağlanması ve tekrar gönderme saldırılarının önlenmesi için sayaç olarak başlangıç vektörü (IV) kullanılmaktadır. Veri bütünlüğü için ise Mesaj Asıllama Kodu (MAK) üreten CBC–MAC (Cipher Block Chaining Message Authentication Code) kullanılmaktadır. Diğer yandan, µTESLA (Micro Timed Efficient Stream Loss–tolerant Authentication) sınırlı kaynaklara sahip ortamlar için asıllanmış yayın (broadcast) sağlayan bir protokoldür. Bu protokolde, toplayıcı/ağ geçidi gizli anahtarıyla her paket için bir asıllama kodu üretmektedir. Ağ geçidinden paketi alan düğüm, SNEP protokolüyle paketi onaylamakta ve anahtar baz istasyonu tarafından açıklanıncaya kadar aldığı paketi tamponunda saklamaktadır. Anahtar açıklandığı zaman ise düğüm, tamponundaki paketleri bu anahtarla onaylamaktadır. Burada anahtarın yayınlanma sıklığı tamponlanan verinin tazeliğiyle ilgili sorunlara yol açabilir. Karlof vd. [36] mevcut güvenlik protokollerinin duyarga ağ güvenliği için yeterli olmamasından yola çıkarak TinySEC isimli bir veri bağı katmanı güvenlik mimarisi geliştirmişlerdir. TinySEC, güvenlik için sadece bütünlük TinySEC–Auth (Authentication Only TinySEC) ve bütünlük ve şifreleme (TinySEC–AE, Authenticated Encryption TinySEC) olmak üzere iki farklı kullanım seçeneği sunmaktadır. Sadece bütünlük seçeneği, bir MAK ile tüm paketi doğrularken, veriyi şifrelememektedir. Bütünlük ve şifreleme seçeneğinde ise hem veri şifrelenirken hem de paket (başlık+veri) bir MAK ile doğrulanmaktadır. TinySEC'de şifreleme algoritması olarak SKIPJACK blok şifreleme algoritması, simetrik şifreleme blok modu olarak ise CBC kullanılmaktadır. KDA'ların sınırlı enerji kaynakları düşünülerek enerji etkin bir veri bağı katmanı güvenlik protokolü olan LLSP (Link Layer Security Protocol) Lighfoot vd. tarafından gerçekleştirilmiştir [37]. LLSP'de veri gizliliği, simetrik blok şifreleme algoritmalarından AES ve blok şifreleme yaklaşımlarından CBC'nin bir arada kullanılması ile sağlanmaktadır. TinySEC'e benzer şekilde, bu protokolde veri güvenliğini arttırmak için bir başlangıç vektörü kullanılmaktadır. Mesaj bütünlüğü için ise MAK üzerinden sağlanmıştır. LLSP, tekrarlama ataklarına karşı kullanılan sayaç değerinin, paket başlığına eklenmesi yerine gönderici ve alıcı arasında bir kaymalı kaydedici kullanarak protokol yükünü azaltmıştır.

Luk vd. [38] düşük enerji tüketimi ve yüksek güvenlik sağlayan güvenli bir ağ katmanı protokolü MiniSec'i (A Secure Sensor Network Communication) geliştirmişlerdir. MiniSec, MiniSec–U olarak adlandırılan tek–kaynak haberleşme ve MiniSec–B olarak adlandırılan çok–kaynak yayım haberleşme olmak üzere iki farklı yaklaşıma sahiptir. Her ikisinde de başlangıç vektörü olarak bir sayaç kullanılırken, veri gizliliği ve bütünlüğünü sağlamak için OCB (Offset Codebook Mode) şifreleme kullanılmıştır [39]. OCB yöntemi CBC ile aynı fonksiyonu yerine getirirken yaklaşık olarak %50 daha düşük işlem gerektirmektedir. MiniSec–U'da her gönderici için yerel ayrı bir sayaç tutan alıcının bulunmasını gerektiren senkronize olmuş

algoritmalar çalışırken, MiniSec–B'de her gönderici için öyle bir gereksinim bulunmamaktadır. Ancak MiniSec–B'de, tekrarlama saldırılarını önlemek için, veri bir Bloom filtrenin içinde depolanmaktadır. MiniSec, önceki yaklaşımlarla karşılaştırıldığında çok daha az enerji gerektiren yüksek seviyeli bir güvenlik sunmaktadır. Yüksek Lisans Tezinde Soylu literatürde yer alan grup anahtar yönetimi protokollerinden TGDH (Ağaç Tabanlı Diffie Hellman Grup Anahtar Yönetimi) yöntemi üzerinde iyileştirme yapmıştır [40]. Çalışmada, TGDH yöntemindeki Diffie Hellman anahtarlama yerine işlem ve bellek gereksinimini azaltan Eliptik Eğri Diffie Hellman anahtarlama yöntemi kullanılmıştır. Eliptik Eğri Diffie Hellman yöntemi sayesinde daha küçük boyutlu anahtarla hem işlem maliyeti ve hem de bellek gereksinimi düşürülmüş ve bu yöntem düşük güçlü duyarga ağları için uygun bir çözüm olarak ortaya konulmuştur. Szczechowiak vd. [41] kablosuz duyarga ağlarında eliptik eğri kriptolojisinin kullanımı ile ilgili yaptıkları çalışmayı sunmuşlardır. Yapılan bu çalışmada kısıtlı kaynaklara sahip cihazlar için kullanılan simetrik şifreleme yöntemlerinin yanı sıra eliptik eğri tabanlı şifrelemenin de kullanılabileceği gösterilmiştir. Bu cihazlarda simetrik anahtar ve açık anahtar şifrelemesini desteklemek için MIRACL [42] kütüphanesi kullanılmıştır. Eliptik eğri kriptolojisi için geliştirilen bu yöntem NanoECC adlandırılmış ve Tmote Sky [43] ile MICA2 [44] cihazları üzerinde test edilmiştir. TinyECC protokolü [45]'te ortaya konmuştur. Bu protokol sayesinde, duyarga ağ uygulamalarına kolaylıkla ayarlanabilen ve bütünleşik eliptik eğri tabanlı açık anahtar kriptoloji işlemleri için açık kaynak kodlu bir yazılım geliştirilmiştir. TinyECC bellek kullanımı, çalışma zamanı ve kaynak tüketimi gibi gereksinimlere göre farklı karmaşıklığa sahip yazılım parçalarıyla konfigüre edilebilen bir yapıda tasarlanmıştır.

Raza vd. [46] Nesnelerin İnternetinde güvenlik gereksinimlerini karşılamak için kullanılan IEEE 802.15.4 bağlantı katmanı güvenliği ile IPSec'i karşılaştırmışlardır. Uçtan uca güvenlik sağlamayan bağlantı katmanın (Link Layer) aksine klasik ağlarda uçtan uca güvenlik sağlayan IPSec protokolü gerekli düzenlemeler yapılarak Nesnelerin İnterneti ağları için uygun hale getirilmiştir. Performans analizleri sonucunda veri boyutunun küçük olduğu haberleşme durumunda bağlantı katmanı güvenliğinin daha etkili olduğu (ortalama cevaplama süresi); veri boyutunun arttığı durumlarda ise IPSec'in daha kullanışlı olduğu gözlemlenmiştir. Aynı şekilde uç düğümlerde bağlantı katmanı güvenliğinin; çok atlamalı düğümlerde ise IPSec protokolünün daha etkili olduğu vurgulanmıştır. Paket boyutu ve düğüm sayısı arttığında ihtiyaç duyulan ölçeklenebilirliği IEEE 802.15.4 bağlantı katmanına göre IPSec daha iyi sağlayabilmektedir. Zhao vd. [47] yaptıkları çalışmada Nesnelerin İnternetinde kullanılan protokol katmanlarındaki güvenlik problemlerini ve bu problemlerin çözümlerini araştırmışlardır. Nesnelerin İnterneti teknolojisini kullanan cihazların kısıtlı kaynaklara sahip olmasından dolayı sade ve etkili güvenlik mekanizmalarıyla sorunların üstesinden gelinmeye çalışılmıştır. Simetrik ve asimetrik şifreleme teknikleri, kullanılan cihaz ve ihtiyaca göre seçilerek güvenlik problemleri engellenmeye çalışılmıştır. Güvenlik problemlerinin herhangi bir katmana ait olmadığı ve tüm katmanların dikkate alınarak çözümler üretilmesi gerektiği ifade edilmiştir.

RPL'deki güvenlik sorunlarıyla ilgili olarak, güvenliğin nasıl ele alınacağı konusunda öneriler ve ROLL yönlendirme mekanizmalarına karşı ataklar çalışma [48]'de ele alınmıştır. Bu çalışma gizlilik, bütünlük, inkâr edememe ve kaynak doğrulamayı içeren güvenlik referans modeli tarafından kullanan güvenlik tehditlerini tanımlamaktadır. Bu modelde güvenlik gereksinimlerine karşı yapılan ataklar sınıflandırılmış ve ROLL yönlendirme protokolleri için güvenlik mekanizması önerilmiştir. Bu çalışmadaki varsayımlar ROLL yönlendirme protokolleri için temel güvenlik önerileri olarak gelecekte kullanılabilir. RPL dışarıdan gelen ataklara ([49, 50]) karşı önlem alırken içerden gelen ataklara karşı herhangi bir mekanizma sunmamaktadır. Anhtuan vd. protokol tarafından kullanılan rank konseptini ve içeriden gelen atakları incelemişlerdir [51]. Rank özelliklerini karşı yapılan saldırılar ve bunun sonucu olarak ağın performans analizini değerlendirmişlerdir.

Jing vd. [52] Nesnelerin İnterneti ağlarında kullanılan WSN, RFID, 3G vs. gibi teknolojilerin getirmiş olduğu güvenlik zaafiyetlerini ve ihtiyaç duyulan güvenlik mekanizmalarını güncel çalışmalara atıf yaparak özetlemişlerdir. Makalede ağ teknolojisinin üç katman içerdiği varsayılarak bu katmanlar için güvenlik problemleri analiz edilmiştir. Ayrıca farklı protokollerin(WSN-RFID) kullanılması durumunda ortaya çıkabilecek güvenlik sorunları incelenmiştir ve bu sorunlara yönelik çözüm önerileri sunulmuştur. Nesnelerin İnterneti teknolojisinde gerçekleştirilen teknolojilerin ve öngörülen uygulamaların anlatıldığı bir diğer çalışma [53]'tür. Yazarlar mimari, iletişim, adresleme, keşif, veri işleme, veri yönetimi, güvenlik ve gizlilik gibi farklı araştırma alanlarını incelemişlerdir. Büyük miktarda birbirine bağlı cihazlar ve bu cihazların üretmiş olduğu önemli miktarda verilerin topluma, ekonomiye ve bireylere sağladığı yeni fırsatlar araştırılmıştır. Nesnelerin İnterneti ağlarında olması gereken güvenlik gereksinimleri yapılan çalışmalar da dikkate alınarak araştırılmıştır. Günümüzde bu teknoloji üzerine yapılan standartlaştırma çalışmalarından bahsedilip teknolojinin gelişmesiyle birlikte yeni araştırma konularının ortaya çıkabileceği söylenmektedir.

Al-Fuqaha vd. [54] Nesnelerin İnterneti konseptine öncülük eden teknolojileri, protokolleri, uygulamaları ve IoT'nin farklı yönlerini ele alan araştırmaları sunmaktadırlar. Çalışmanın IoT'yi oluşturan farklı bileşenlerin ve protokollerin genel mimarisini anlamak için IoT teknolojileri hakkında fikir edinmek isteyen araştırmacılar ve uygulayıcılar için etkili bir kaynak olabileceği düşünülmektedir. Ayrıca literatürde sunulan IoT zorluklarının bir kısmı incelenirken; günümüzde standart olarak kabul edilebilecek protokoller detaylı bir şekilde ele alınmıştır. Büyük veri analizi de dahil olmak üzere ortaya

çıkan diğer teknolojiler ile IoT arasındaki ilişkiyi araştırılmıştır. İstenilen hizmetin sağlanabilmesi için IoT'nin geliştirilmesi aşamasında karşılaşılan başlıca sorunlar literatürde yapılan çalışmalar dikkate alınarak çözüm önerileri sunulmaktadır. Alaba vd. [55] IoT teknolojisindeki güvenlik senaryolarını tartışarak olası saldırıların ve tehditlerin analizini yapmışlardır. Yazarlar IoT ağlarındaki güvenlik mekanizmalarının iyileştirilmesi için olası çözüm önerileri sunmuşlardır. Ayrıca geleneksel ağ ile IoT ağları arasındaki farklar katman bazında detaylı şekilde incelenmiştir. Her iki ağdaki güvenlik sorunu ele alınırken farklı yaklaşımlar ve tekniklerin kullanılması gerektiği belirtilmiştir.

IoT ağlarında kullanılan cihazlar kendi aralarında veri alışverişi yapabilmek için birbirlerini doğrulamaları gerekmektedir. Var olan yöntemler genelde bağlantı ve ağ katmanında karşılıklı doğrulamayı sağlarken; daha etkili bir yöntem üzerinde durulmamıştır. Tablo 1'de güncel yetkilendirme çalışmaları verilmiştir. Wong [56] hash tabanlı kullanıcı yetkilendirme şemasını ilk sunan kişidir. Bu yöntem daha az karmaşık, sade ve dinamik olmasına rağmen tekrar, sahtecilik ve şifre değiştirme gibi işlemleri eksik olduğundan etkin bir şekilde kullanılamaz. Das şifre tabanlı kullanıcı doğrulama alanında günümüze kadar en fazla atıf alan çalışmayı gerçekleştirmiştir [57]. Gerçekleştirilen şemaya göre ağ geçidi şifre tabanlı bir doğrulama mekanizması sunar. Das şeması simetrik ve asimetrik şifreleme içermediğinden tüm işlemler hash ve XOR işlemleri ile gerçekleştirilir. Bu da kısıtlı kaynaklara sahip cihazlar için etkili bir yöntem olabileceğini gösterebilmektedir. Fakat yapılan çalışmalar sonucunda bazı güvenlik açıklığı, karşılıklı doğrulama ve anahtar yönetimi içermemektedir. He vd. [58] Das protokolüne benzer bir çalışma gerçekleştirmişlerdir. Geliştirilen yöntem gelişmiş şifre güvenliği sağlamasına rağmen güvenlik kusurlarını telafi edememektedir. Khan vd. [59] Das protokolünü iyileştirmek için bazı önemli değişiklikler yapmışlardır. İlk olarak şifre saklamada direkt düz metin yerine hash değeri saklanmaktadır. İkinci olarak sisteme şifre güncelleme özelliği kazandırmışlardır. Chen vd. yapmış oldukları çalışmada kullanıcı ve ağ geçidi arasında karşılıklı doğrulamayı sağlamışlardır fakat çalışmaları tekrar, sahtecilik ve bypass gibi saldırılara karşı savunmasızdır [60]. Yeh vd. [60] eliptik eğri tabanlı kullanıcı doğrulama ve anahtar yönetimi sunmuşlardır. Kullanıcı ve sensor düğümleri arasında Deffie-Hellman anahtar tabanlı karşılıklı doğrulama şeması için [62, 63] çalışmaları önerilmiştir. Yapılan çalışmalarda açık anahtar şifreleme kullanıldığı için işlem karmaşıklığının ve depolama alanı ihtiyacının artması bu çalışmaları sorunlu hala getirmektedir. Tablo 1'de yapılan çalışmaların avantaj/dezavantajları gösterilmektedir.

5. NESNELERİN İNTERNETİ PROTOKOL YIĞINI KATMANLARINDA VAR OLAN GÜVENLİK MEKANİZMALARI (SECURİTY MECHANISMS IN PROTOCOL STACK)

5.1. Fiziksel Katmanda Güvenlik (Physical Layer Security)

Frekans seçimi, taşıyıcı frekansının oluşumu, sinyal algılama, modülasyon, gönderim ve alım işlemlerinin yürütüldüğü katmandır. Fiziksel katman, güç tüketimini doğrudan etkilediği için kablosuz duyarga düğüm tasarımında ayrı bir öneme sahiptir. Seçilen modülasyon tekniği, iletim hızı, gönderme gücü ve görev çevrim süresi gibi güç tüketimini etkileyen faktörler fiziksel katman tasarımı ile ilgili parametrelerdir.

Düğümler çoğu durumda zor doğa koşulları altında çalışmak zorunda oldukları için fiziksel saldırılara karşı hassastırlar [64, 65] ve seçilen modülasyon tekniğinin bu saldırılara (gürültüye, girişime, boğma(jamming)) karşı dayanıklı olması gerekmektedir. Frekans atlamalı yayılım spektrumu (Frequency-Hopping Spread Spectrum-FHSS) ve doğrudan sıralı yayılım spektrumu (Direct-Squence Spread Spectrum-DSSS) kablosuz ağlarda ve KDA'da kullanılan modülasyon tekniklerindendir. Her iki teknik de girişime dayanıklı olmasına karşın DSSS tekniği dar bant girişimlerine FHSS'ye oranla daha dayanıklıdır. Ayrıca ultra geniş bant, darbe radyo ve darbe konum modülasyon teknolojilerinin kullanımı KDA'larda enerji tüketiminin azalmasına ve daha

Tablo 1. Güncel güvenlik şemalarının karşılaştırılması (Comparing current security schemes)

Öğeler	[56]	[57]	[58]	[59]	[60]	[61]	[62]	[63]
Kullanıcı, GWN ve sensör düğümünün her ikisi arasındaki karşılıklı kimlik doğrulama	H	H	H	E	E	E	E	E
Şifre Koruması	H	H	E	E	H	E	E	H
Kimlik Koruması	H	E	E	E	E	H	H	H
Anahtar Kabulü	H	H	H	H	H	E	E	E
Tekrar Saldırılarına Karşı Dayanıklılık	H	E	E	E	E	H	E	E
Şifre güncelleme / değiştirme	H	H	E	E	H	H	E	E
Sahtecilik Ataklarına Karşı Dayanıklılık	E	H	H	E	H	E	H	H

E: Evet, H: Hayır

güvenilir iletişimin gerçekleşmesine olanak sağlayacaktır [66]. Düşük Hız-Kablosuz Kişisel Alan Ağlarında, iki farklı tür aygıt çeşidi mevcuttur. Bunlar; Tam Fonksiyonlu Cihazlar (FFD-Full-Function Device) ve Düşük Fonksiyonlu Cihazlar (RFD-Reduced-Function Device)'dır [67, 68]. Tam fonksiyonlu cihazlar, herhangi bir topolojide bulunabilir, ağ koordinatörlüğü yapabilir ve herhangi bir cihazla haberleşebilir. Düşük fonksiyonlu cihazlar, sadece yıldız topolojide bulunabilir, ağ koordinatörlüğü yapabilme özelliği yoktur ve yalnızca ağ koordinatörü ile haberleşebilir. Bu cihazlar çok sekmeli topolojilerde yaprak(leaf) düğüm olarak yer alabilirler.

Saldırgan fiziksel katmanda karıştırıcı RF sinyalleri yollayarak düğümlerin haberleşmesini engelleyebilir. Sinyal karıştırıcı saldırılarına karşı alınacak tedbir frekans sıçratma ve iletişim spektrumunun yayılmasıdır. Bu teknikler saldırganın iletişimin frekansını bozabilmesi için daha fazla enerji harcamasını zorunlu kılar. Bu saldırı sonucunda ağdaki düğüm devre dışı kalabilir ve ağın yaşam süresi kısalabilir. IEEE 802.15.4 standardı böyle sorunlara çözüm üretmemekle birlikte fiziksel katmanda herhangi bir güvenlik mekanizması sunmamaktadır.

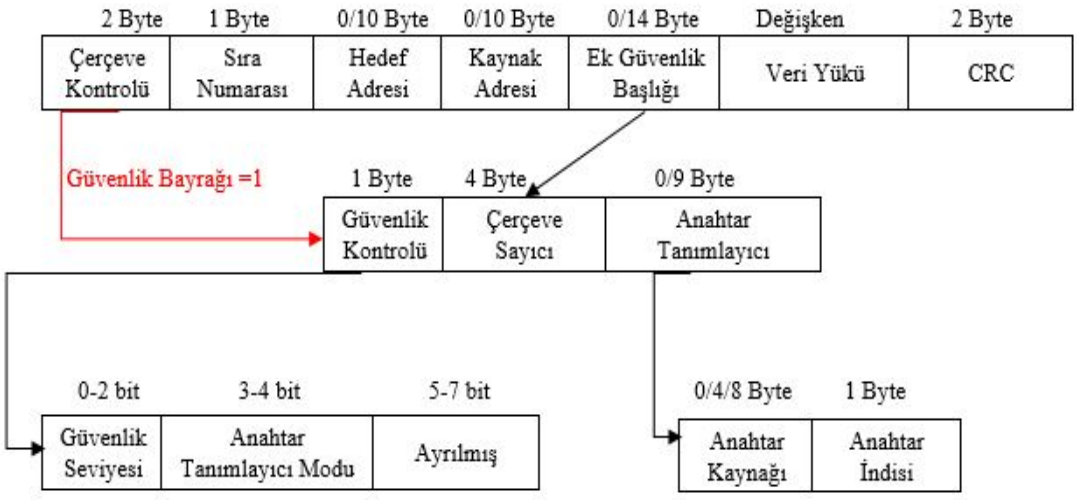
5.2. Ortam Erişim Protokolünde Güvenlik (Medium Access Control Security)

Ortam erişim kontrolü (Medium Access Control (MAC)), kablosuz iletim ortamının düğümler arasında etkin bir şekilde paylaştırılmasını sağlayan bir mekanizmadır. MAC katmanı, veri paketlerinin parçalanması, hata düzeltme, hareket yönetimi, güç koruma ve şifreleme gibi işlemleri kapsamaktadır. IEEE 802.15.4-2011 standardı, bağlantı katmanındaki haberleşmenin güvenliğini sağlamak için ortam erişim katmanında güvenlik hizmeti sunmaktadır ve bu güvenlik hizmeti Şekil 4'te gösterilen protokol yığınında kullanılan diğer güvenlik mekanizmalarına yardımcı olmaktadır. cc2538 [69] ve cc2420 [70] gibi cihazların donanımsal olarak simetrik şifrelemeyi ve IEEE 802.15.4 güvenlik mekanizmasını desteklemesi buna örnek olarak verilebilir. Bu cihazlar, protokol yığını içindeki uygun kontrol parametrelerini ayarlayarak güvenlik gereksinimlerini belirleyebilir. Eğer güvenlik modu belirlenmezse, cihazlardaki güvenlik modu varsayılan olarak NULL olmaktadır. Cihazlar ortam erişim katmanında güvenliği sağlamak için Şekil 8'deki Ek Güvenlik Başlığı alanını kullanmalıdır. Belirtilen alan Çerçeve Kontrol içindeki güvenlik bayrağı 1'e setlenerek aktif edilir. Eğer belirtilen bayrak değeri herhangi bir değere setlenmez veya 0'a setlenirse Ek Güvenlik Başlığı altındaki güvenlik mekanizmaları kullanılamaz [71].

Cihaz güvenlik seviyesini belirlemek için farklı seçeneklere sahiptir. Güvenlik seviyesi iletilen veri paketinin başlık kısmında tutulan Güvenlik Seviyesi alanı ile sağlanır. Her güvenlik seviyesi, farklı bir güvenlik özelliği ve farklı paket formatı sunar. 802.15.4 tanımlamasında Tablo 2'de görülen 8 farklı güvenlik durumu mevcuttur. Güvenlik modu aktif olduğunda IEEE 802.15.4 bağlantı katmanı veri paketi Şekil 8'deki gibidir. Ek Güvenlik Başlığı'ndaki ilgili alanlar doldurularak tablodaki sekiz güvenlik modundan biri kullanılmaktadır.

Tablo 2. IEEE 802.15.4 tarafından desteklenen güvenlik modları (Security modes in the IEEE 802.15.4 standard)

Güvenlik Modu	Tanımlama
NULL	Güvenlik yok
AES-CTR ([70])	Sadece şifreleme, CTR Modu
AES-CBC-MAC-128 ([71])	128 bit MAC
AES-CBC-MAC-64	64 bit MAC
AES-CBC-MAC-32	32 bit MAC
AES-CCM-128 ([72])	Şifreleme ve 128 bit MAC
AES-CCM-64	Şifreleme ve 64 bit MAC
AES-CCM-32	Şifreleme ve 32 bit MAC



Şekil 8. IEEE 802.15.4 veri ve kontrol alanları (Security data and control fields in IEEE 802.15.4.)

5.3. Ağ Katmanında Güvenlik (Network Layer Security)

6LoWPAN tabanlı mimaride, Ağ katmanı güvenliğinin sağlanmasında, IPv4 için tanımlı olan IPSec protokolünün IPv6 ağları için adapte edilmiş bir formu olan "6LoWPAN için IPSec" protokolünden faydalanılmaktadır. IP katmanında tanımlanmış bir güvenlik protokolü olan IPSec ile: Uçtan uca kimlik doğrulama, bütünlük kontrolü, veri gizliliğin sağlanması ve tekrar ataklarına karşı koruma gibi çeşitli güvenlik gereksinimleri karşılanabilmektedir. İşletim sistemi düzeyinde gerçekleştirilen IPSec protokolü, herhangi bir iletim katmanı protokolü ile beraber kullanılabilmektedir. 6LoWPAN teknolojileri için adapte edilen IPSec protokolünün yaygın olarak kullanılmamasının en önemli sebepleri, beraberinde getirmiş olduğu işlem yükü ve iletim katmanından gelen verinin güvenlik gerektirip / gerektirmemesine bakmaksızın şifreleyerek iletmesi olarak söylenebilir. IPSec protokolünün işlem yaptığı iki farklı mod mevcuttur: İletim modu ve Tünel modu. Yönlendiriciler arası trafikte IPSec kullanılması durumunda tercih edilen tünel modu, IP paketini ve başlıklarını beraber şifreler ve yeni bir IP başlığı üreterek güvenliği sağlanmış paketi oluşturur. Bilgisayarlar arası güvenliği sağlamak için kullanılan iletim modunda ise IPSec, orjinal IP başlığını değiştirmediği gibi yeni bir IP başlığı da oluşturmayacaktır.

İki farklı modda kullanılabilen ve uçtan uca güvenliği ağ katmanında sağlayan IPSec üç alt protokolden oluşmaktadır. AH (Authentication Header) protokolü IP paketinin kaynağını doğrulamada ve bütünlüğünü kontrol etmede kullanılır. ESP (Encapsulating Security Payload) protokolü ise gizliliğin sağlanmasında, veri kaynağının doğrulanmasında, tekrarlama ataklarına karşı olarak kullanılır. SA (Security Assocication) IP seviyesinde güvenliğin sağlanmasında kullanılacak olan algoritmalar ve parametre bilgilerinin genel adıdır. Alt protokollere ilişkin kısa detaylar aşağıdaki şekilde verilebilir.

AH protokolü paketin bütünlüğünü sağlaması ve asıllanması(doğrulanması) amacıyla kullanılmaktadır. AH protokolü IP paketinin tamamı üzerinde işlem yapar yani dış IP başlığını da bütünlük ve asıllama işlemlerine dâhil eder. Yalnızca IP paketinin yolda değişen TTL (time to live) gibi değerlerini bu işlemlerin dışında tutar. AH protokolü veri gizliliğini sağlamamaktadır ve IPSec mimarisini gerçekleyen cihazlar için şart koşulmamıştır. AH protokolü ağ üzerinde daha çok yönlendiriciler arasında asıllama amacıyla kullanılmaktadır. IP başlığının asıllanması yönlendiricilerin birbirlerinin IP adreslerini kimlik bilgisi olarak kullanması durumunda önemli bir gereksinimdir.

ESP protokolü paketin bütünlüğünün yanı sıra gizliliğinin de sağlanmasını destekler. ESP protokolü AH'den farklı olarak dış IP başlığı üzerinde herhangi bir güvenlik servisi işlemi yürütmez. ESP'de, AH gibi asıllama işlemlerinde kriptolojik özüt fonksiyonlarını kullanır. Şifreleme işlemlerinde ise ağ performansında düşüşe sebebiyet vermemek için genellikle simetrik şifreleme algoritmalarından faydalanmaktadır. IP paketinin veri kısmı iki uç arasında paylaşılan ortak anahtarlar ile şifrelenmekte ve asıllanmaktadır. Gerek AH gerekse ESP protokolleri, IPv6 paketlerinin güvenliğinin sağlanmasında kullanılabilmektedir. Hangi protokolün kullanılacağı tamamen uygulama ihtiyaçlarına bağlı olarak belirlenmektedir. Fakat her iki protokol için de tanımlanmış bir sıkıştırma standardı yoktur. 2011 yılında Raza vd. [75] gerçekleştirmiş oldukları çalışmada AH ve ESP başlıkları için kodlama yöntemi önermişlerdir. Çalışmada IPSec protokolünün tünel modu göz ardı edilmiş ve IPSec'in doğrudan 6LoWPAN ağlarında kullanımının veri paketi boyutlarındaki artışa sebebiyet vereceğine vurgu yapılmıştır. Sıkıştırılmış IPSec olarak da adlandırılabilecek olan çatı, ESP ve AH başlıkları için Next Header Compression tanımlamalarını yapmıştır.

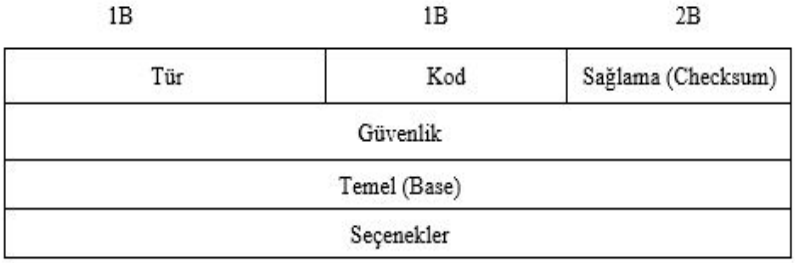
SA protokolü Security Association, IP seviyesinde güvenliğin sağlanmasında kullanılacak olan algoritmalar ve bu algoritmaların kullanmış olduğu parametrelere ilişkin bilgilerin geneline verilen addır ve tek yönlü trafik için tutulur. Eğer iki yönlü güvenlik gerektiren bir haberleşme mevcut ise, iki yönlü ilişkilendirmenin tutulması gerekmektedir. SA'ların oluşturulması esnasında IPSec protokolü IKEv2'den faydalanmaktadır. 6LoWPAN ağları için IPSec düşünüldüğünde, IKEv2 çok fazla iletişim gerektirmesi sebebi ile kullanılamamaktadır. Raza vd. gerçekleştirmiş oldukları çalışmada "Sıkıştırılmış IPSec" için "Hafif IKEv2" tanımlamışlardır. Hafif IKEv2'nin en önemli farklı asimetrik algoritma olarak işlem yükü daha hafif olan eliptik eğri şifreleme yönteminden faydalanıyor olmasıdır. Anahtar değişimi esnasında ise Diffie-Hellman protokolü hem IKEv2 de hem de "Hafif IKEv2"'de kullanılan bir standarttır. Diffie-Hellman protokolünden oturum anahtarlarının paylaştırılması esnasında faydalanılmaktadır.

5.3.1. RPL protokolünde güvenlik (RPL security)

Ağ katmanı protokolü olarak da bilinen RPL, düşük güçlü ağların yönlendirme ihtiyacını karşılamak için geliştirilen, düşük kontrol trafiği gerektiren bir protokoldür. RPL protokolünü kullanan cihazlar, hedef tabanlı yönlü döngüsüz graf (DODAG) kullandıkları için ağa dâhil olurken döngü içermezler [76].

RPL, cihazlar arasında yönlendirme mesajlarının değişimini güvenli bir şekilde gerçekleştirmek için üç farklı güvenlik profili tanımlar. Şekil 9'da 4 Byte ICMPv6 mesaj başlığından sonra iletilen güvenli RPL kontrol mesajının formatı gösterilmiştir. RPL kontrol mesajındaki "Kod" alanının anlamlı biti verilen RPL mesajına (DIS, DIO, DAO) güvenli olup olmadığını belirtir. Güvenlik mekanizmasının formatı Şekil 10'daki gibidir. "Güvenlik" alanındaki bilgi, mesajın güvenlik sürecinde kullanılan kriptolama algoritmalarını ve güvenlik seviyesini belirtir.

Şekil 9'da görülen algoritma alanı RPL mesajının farklı yöntemlerle şifrelenmesini sağlar. Algoritma alanının 0 olarak setlendiği duruma karşılık gelen yöntemde mesaj bütünlük desteği için 128 bitlik AES-CCM ve mesajı



Şekil 9. Güvenli RPL kontrol mesajı (Secure RPL control message)

Şekil 10. RPL kontrol mesajının güvenlik bölümü (Security section of a secure RPL control message)

doğrulamada ise mesajın özüt değerinin (SHA256) özel anahtar (RSA) kullanarak şifrelenmesiyle elde edilen sayısal imza kullanılır. Seviye alanı desteklenen paket güvenliğini gösterir; veri doğrulama ve isteğe bağlı olarak veri gizliliği seviyelerini oluşturmaya izin verir. RFC 6550 [77] aynı zamanda, 2048 ve 3072 bitlik RSA kullanan imzaların yanında MAC-32 ve MAC-64 doğrulama kodlarıyla gizliğinin, bütünlüğün ve veri doğrulamanın yapısını belirtmek için çeşitli değerler tanımlar. Bayraklar alanı ilerde ortaya çıkacak gereksinimler için ayrılmıştır. RPL kontrol mesajlarının çeşitli güvenlik versiyonları gizlilik ve gecikmeye karşı koruma sağlayabilirler. RPL'deki kriptolama algoritmalarının kullanımı ile ilgili olarak, AES-CCM güvenliği sağlamada temel olarak kabul edilir ve birçok protokol gerçeklemesi tarafından desteklenirler [78]. Standardın önerdiği minimum güvenliğe ek olarak gelecekte RPL'in güvenliği için farklı algoritmalar kullanılabilir. RPL protokolüne ait mesaj doğrulama kodları ve imzalar güvensiz IPv6 paketleri üzerinden hesaplanmaktadır. RPL ICMPv6 mesajı şifrelendiğinde şifreleme güvenlik alanından sonraki ilk byte ile başlar ve paketin son byte'na kadar devam eder. Şekil 10'da gösterilen "ATM (anahtar tanımlama modu)" alanı mesaj güvenliğinin sağlanma sürecinde kripto anahtarın gerekli olup olmadığını belirtir. RFC 6550 [77] şu anda bu alan için farklı değerler tanımlamıştır ve dijital imzalar ve grup anahtarlama gibi farklı anahtar yönetim biçimlerini desteklemektedir. Bu alan paket korumasını çeşitli seviyelerde destekler ve anahtar kaynağı, anahtar indeksi olarak iki alt bölüme ayrılır.

RPL DIO, DIS, DAO, DAO-ACK mesajlarına ek olarak tekrarlama saldırılarına karşı olarak kullanılmak üzere Uygunluk Kontrolü (Consistency Check-CC) mesajı tanımlar. Bu mesajla gönderici düğüm alıcı düğümün RPL mesajları için kullandığı sayaç değerini göndermesini ister. Bu şekilde gönderici ve alıcı arasında oluşabilecek bir tekrar atağının önüne mesaj içine gömülen bir sayıcı ve CC mesajıyla sağlanan sayıcı senkronizasyonuyla geçilmiş olur.

RPL mesaj gizliliğini ve bütünlüğünü destekler ve ihtiyaç durumunda bağlantı katmanı güvenlik araçlarını kullanabilir. Eğer bağlantı katmanında güvenlik mekanizması tanımlanmamışsa, RPL güvenliğini kendi tanımladığı bir güvenlik profili aracılığıyla sağlayabilir. RPL unsecured, pre-installed ve authentication olmak üzere 3 farklı güvenlik profili tanımlar.

Unsecured: Bu yöntem RPL protokolündeki varsayılan güvenlik seviyesidir ve RPL kontrol mesajları gönderilirken herhangi bir güvenlik mekanizması uygulanmaz. Pre-installed: Cihazlar önceden yapılandırılmış simetrik anahtarları kullanarak RPL topolojisine dâhil olabilirler. Kullanılan simetrik anahtarlar bütünlük, kimlik doğrulama ve gizlilik gibi güvenlik gereksinimlerini sağlar.

Authenticated: Bu güvenlik modu yönlendiriciler gibi çalışan cihazlar için uygundur. Önceden belirlenen anahtarlar kullanılarak cihazların ağa katılması söz konusu ise; anahtar mekanizması ağa katılmak isteyen bu cihazları kimlik doğrulama ve yetkilendirme işlemine tabi tutacaktır [78]. RPL standardı asimetrik şifreleme kullanıldığında düğümlerin nasıl anahtar alımı yapacağını şu an için net olarak belirlemez. RPL standardının gelecek versiyonları bu mekanizmaları nasıl destekleyeceklerini açıkça ortaya koymalıdır. Ek güvenlik mekanizmaları tanıtılmasa da RPL ile ilgili diğer kaynaklar güvenlik konusundaki analizleri içermektedirler [79]. Çeşitli uygulama alanları için RFC dokümanlarında tartışılan yönlendirme gereksinimleri bu analizleri oluşturmaktadır [80-82]. Böyle dökümanlar yönlendirme kontrol mesajlarının gizlilik, bütünlük ve doğrulama gibi güvenlik gereksinimlerinin önemini tartışmaktadırlar.

5.3.2. 6TiSCH güvenliği (6TiSCH security)

6TiSCH protokolünün güvenliği diğer katmanlardaki güvenlikle bir arada düşünülmelidir. IETF 6TiSCH grubu düğümlerin 6Top protokolü üzerinden güvenli olarak ağa dâhil olması için çalışmalar yürütmektedir [83]. Bu çalışmalarda ele alınan güvenlik mekanizmalarının ana hedefi yeni ağa dâhil olacak düğümlerin kimliklendirmesinin en düşük kaynak tüketimiyle gerçeklemektir.

Düğümün ağa dâhil edilmesi işlemi Şekil 7'de verilen PCE (Path Computation Element), JCE (Join Coordination Element) ve ACE (Authentication Coordination Element) öğelerinin görev aldığı bir yetkilendirme protokolüyle gerçekleştirilir. Bu protokolde ağa dâhil olmak isteyen düğüm öncelikle ağa işaretçi paketleri vasıtasıyla senkronize olur. Senkronizasyon sağlandıktan sonra, düğüm ağa ait bir şifre/sertifika yardımıyla geçici olarak uç düğüm olarak kimliklendirilir. Bu durumda düğüm başka düğümlerin kendine bağlanmasına izin veremez ve RPL ağının parçası olamaz. Geçici olarak ağa dâhil olan düğüm, öncelikle JCE öğesine DTLS ile şifrelenmiş CoAP paketi ile kimliklendirme isteği gönderir. JCE bu isteği aldıktan ve kimlik doğrulama yaptıktan sonra düğüme kendisine ait sertifika bilgileri güvenli olarak gönderir. Böylece düğüm doğru ağa ve doğru JCE öğesine bağlandığını tasdik etmiş olur. JCE doğrulama işlemi sırasında PCE öğesinden düğüm için gerekli haberleşme kaynaklarını (bant genişliği, ortak hücreler, vb.) alır ve bu bilgileri düğüme iletir. Düğüm kendisini JCE'ye tanıttıktan sonra, ağa dâhil olmak için JCE'den aldığı sertifika ve ağa ait bilgilerle ACE öğesine bağlanır ve bu öğeden kendisini belli süre boyunca ağ genelinde kimliklendirecek şifreleri ve sertifikaları alır. ACE öğesi düğümlere ait erişim izinlerini tutarak düşük güçlü düğümlerin hafıza gereksinimi yüksek olan bu tür işlerden kurtulmasını sağlar. Sayılan adımlarla kimliklendirilen düğümler ağa dâhil olurlar ve RPL DIO paketlerini ağa yaymaya başlarlar.

Burada bağlanan düğümün JCE öğesine trafiği varsayılan yönlendiriciler üzerinden yapılır. Zira, daha önce belirtildiği gibi düğümün ağdaki yönlendirme bilgilerine erişmesine ilk aşamada güvenlik nedeniyle izin verilmez. Ancak tersi yönde olan yönlendirme bu durumda bir sorun teşkil edecektir. Bunun nedeni, düğümün ağa tam dahil edilmemesi sonucu, düğüme ait yönlendirme bilgilerinin ağdaki düğümlerde bulunmamasıdır. Bu sorunu çözmek için, ağa bağlanma isteği yapan düğümün ilk istek gönderdiği ağa öncede dahil olmuş düğüm yardımcı düğüm olarak belirlenir. JCE kendisine ait sertifikaları ve ağ parametrelerini bu yardımcı düğüme gönderir ve yardımcı düğüm ağa katılma isteği gönderen düğüme bu bilgiler JCE adına iletir. Bu şekilde ters yönde adresleme işlemi yardımcı düğüm üzerinden gerçeklenmiş olur.

6TiSCH ağları farklı saldırılara maruz kalabilir. Bunlardan en öngörülebilir olanı hizmet engelleme ataklarıdır. Burada ağa dâhil olmak isteyen düğüm senkronize olduktan sonra sürekli olarak ağa bağlanma ve yönlendirici bulma istekleri gönderebilir ve diğer düğümlerin kaynaklarını tüketebilir. Bu tür saldırıları engellemek için bağlanan düğümün gönderebileceği veri miktarı sınırlanabilir ya da agresif bir trafik üreten bağlanma aşamasındaki düğümler engellenebilir. Diğer bir saldırı şekli ise bağlanma hakkı olan ve kötü niyetli olmayan bir düğümün kötü niyetli bir ağ tarafından kandırılmaya çalışılmasıdır. Bu saldırı da düğüme gömülecek ağa ait bir sertifika üzerinden gerçekleştirilebilir. Bu ve buna benzer saldırıları engelleyecek çözümler hali hazırda standarda dâhil edilmektedir. Orjinal çözümler ve kararlı güvenlik algoritmaları araştırılarak 6TiSCH protokolüne dâhil edilmelidir.

5.4. İletim Katmanında Güvenlik (Transport Layer Security)

6LoWPAN mimarisindeki iletim katmanı uç birimlerde çalışan uygulamalar arasındaki iletişim oturumlarını (communication sessions) üretmekten ve yönetmekten sorumludur. Bir aygıt üzerinde aynı anda birden fazla uygulamanın kendi iletişim kanallarını kullanmasına izin veren iletim katmanında kullanılan en yaygın protokol Transmission Control Protocol (TCP)'dir. Bağlantı uyumlu olarak çalışan TCP protokolü, düşük güç gerektiren cihazlardan oluşan 6LoWPAN ağı için işlem yükü getiren bir iletim katmanı protokolüdür. Bu nedenle 6LoWPAN ağlarında daha düşük yük getiren ve bağlantısız olan User Datagram Protocol (UDP) daha iyi bir alternatif olacaktır. Genel amaçlı ağlarda, uygulama katmanındaki protokollerin güvenliği TCP üzerinde çalışan ve iletim katmanında yer alan Transport Layer Security (TLS) protokolü ile gerçekleştirilmektedir. UDP protokolünün kullanılması durumunda ise iletim katmanındaki güvenlik Datagram Transport Layer Security (DTLS) ile gerçekleştirilmektedir. DTLS, UDP'den kaynaklı paket kayıplarını yöneten, alıcı tarafta paket yeniden düzenlemesini gerçekleştiren ve daha küçük çerçeveler üzerinde işlem yapan bir protokol olma özelliğini taşımaktadır. DTLS aynı zamanda bir sonraki bölümde incelenecek olan CoAP protokolü ile beraber güvenliği sağlamada günümüzde aktif olarak kullanılmaktadır.

DTLS protokolü, TLS'e benzer şekilde iki alt katmandan oluşmaktadır. Alt katman Record Protocol olarak adlandırılırken, üst katman kendi içerisinde dört alt protokolden oluşmaktadır: Handshake, ChangeCipherSpec, Alert, Application Data. Record Protokol, gizliliğin sağlanması için gerekli simetrik şifreleme ve bütünlüğün kontrolü için gerekli özüt hesaplama işlemlerini gerçekleştirmektedir. Alt katmanda yer alan protokoller ise güvenli kanalın açılmasından önceki parametrelerin ayarlanması ve oturum anahtarının üretilmesinden (Handshake protokol), güvenli iletişim başlamadan önce her iki tarafın karşılıklı destekledikleri şifreleme ortamlarını değişmesinden (ChangeCipherSpec), Hadshake protokolü esnasında karşılaşılabilecek çeşitli durumlarda hata ve uyarı mesajlarının iletilmesinden (Alert Protocol) ve uygulama katmanından gelen verinin alt parçalara ayrıştırılması, sıkıştırılması, şifrelenmesinden (Application data) sorumludur.

Yukarıda genel hatları ile bahsedilmiş olan ve UDP için güvenliği sağlamadan sorumlu olan DTLS'in 6LoWPAN ağlarına adaptasyonu için Branchmann vd. [83] IoT ağlarının güvenliğinin sağlanması için DTLS'in kullanımının nasıl adapte edilebileceğine dair bir çalışma gerçekleştirmişlerdir. Yazarlar tarafından iki önemli açık ortaya konmuştur: Internete bağlantı uçlarında DTLS/TLS dönüşümü için gerekli mekanizmaların olmayışı ve DTLS'in şu an için multicast trafiği desteklemiyor olması. Kothmayr vd. DTLS'in 6LoWPAN'da RSA algoritması için donanım desteği alabilmek amacıyla Güvenilir Platform Modülü (GPM) ile beraber kullanımını iredelemiştir. Fakat önerdikleri çalışmada DTLS mesajlarının sıkıştırılabilirliği hakkında herhangi bir inceleme yapılmadığı gibi önerilen yöntem CoAP ile uyumsuzdur. Raza vd. [84] DTLS başlık bilgilerinin sıkıştırılabileceğine ve böylelikle iletişimden kaynaklı yükün hafifletilebileceğine çalışmalarında vurgu yapmışlardır. Fakat DTLS'in doğrulama ve anahtar üzerinde karar verme aşamalarından kaynaklı işlem yükünün irdelenmesi gerçekleştirilmemiştir. Sıkıştırılmış DTLS'in uygulanabilir olması için ise gerek Internet uyumlu LoWPAN'in sınır yönlendiricilerinde gerekli dönüşümün uygulanması veya Internet hostlarında sıkıştırılmış DTLS'in desteklenmesi gerekmektedir. DTLS'in multicast trafik ile olan uyumsuzluğuna vurgu yapılan Oscar vd. [85] güvenlik gateway'i tanımlayarak multicast grupların oluşturulabileceğini göstermişlerdir. Kontrolcü olarak çalışan gateway gruptaki her birim ile başlangıç mesajlaşmasını gerçekleştirmekten ve güvenli CoAP grup haberleşmesi için gerekli anahtarları göndermekten sorumludur. Rene vd. [86] ise, düşük güçlü ağlarda işlem yükü gerektiren güvenlik sertifikalarının kullanımının etkisi incelenmiştir. İki farklı yaklaşım önerdikleri çalışmalarında, ilk yaklaşım handshake mesajlarının gönderilmesinden önce security gateway'in sertifikaların geçerliliğini kontrol etmesini sağlamaktadır. Diğer yaklaşım ise haberleşen taraflar arasında oturumun kapanmasından sonra dahi minimal ölçüde belirli oturum bilgilerinin tutulmasını gerektirir. Böylece bir sonraki güvenli haberleşmenin başlatılması esnasında, tekrar DTLS handshake protokolünün devreye sokulmasına gerek kalmayacaktır. Literatürdeki bazı çalışmalarda TCP'nin Kablosuz Duyarga Ağlarına adaptasyonu incelenirken [87, 88], 6LoWPAN ağları göz ardı edilmiştir. SSNAIL ve Sizzle olarak adlandırılan iki farklı çalışma ise, TCP üzerinde çalışan SSL protokolünün Kablosuz Duyarga Ağlarına adaptasyonunu hedeflemiştir [89, 90].

Literatür genel olarak değerlendirildiğinde: DTLS'in kaynak sınırlı ağlar üzerinde etkin olarak kullanılabilmesi için protokol üzerinde modifikasyonların önerilmesi, doğrulama ve bütünlük kontrolü için iletim katmanındaki güvenliğin sağlanmasında Eliptik Eğri Şifrelemenin kullanılabilirliği, sertifikaların yönetiminden kaynaklı işlem yükünün aza indirilmeye çalışılması, DTLS'in multicast trafiği destekleyecek şekilde adapte edilebilmesi alanlarında çalışmalar mevcuttur. Bahsi geçen alanlar halen araştırma ve geliştirme aşamasında olup, yeni yöntemlerin önerilebilmesi için açık alan oluşturmaktadır.

5.5. Uygulama Katmanında Güvenlik (Application Layer Security)

Uygulama katmanı protokolleri Nesnelerin İnterneti cihazlarının kullanmış olduğu farklı yapıdaki uygulamaların birbirleri ile haberleşmesine olanak sağlamaktadır. Bu özellikleri sayesinde her uygulama için özel olan tasarımlardan (semantik, içerik tasarımları) bağımsız olarak uygulamalar kendi aralarında haberleşebilmektedirler. Tablo 3'te görüldüğü gibi çeşitli istekleri karşılamak için geliştirilmiş farklı prorokoller vardır. Uygulama protokolleri haberleşme kapsamlarına göre D2D(Device to Device-(Cihaz-Cihaz)) ve D2S(Device to Server-(Cihaz-Sunucu)) olmak üzere ikiye ayrılmaktadırlar [91]. D2D protokolleri akıllı cihazların "Yayın/Kayıt(Publish/Subscribe)" modeline dayanarak birbirinden bağımsız olarak haberleşmesi için tasarlanmıştır. Tüm haberleşme global veri alanına okuma ve

Tablo 3. Nesnelerin İnterneti-Uygulama protokolleri (Internet Of Things- Application layer protocols)

Nesnelerin İnterneti Protokolleri				
	Protokoller	TCP/IP	Yöntem	Amacı
MQTT	Message Queue Telemetry Transport	TCP	Yayın/Kayıt İstek/Yanıt	Kısıtlı kaynaklara sahip cihazların Web ortamıyla etkileşim kurabilmesi için geliştirilmiş bir protokoldür.
DDS	Data Distribution Service	UDP	Yayın/Kayıt İstek/Yanıt	Cihazlardan toplanan verinin yine cihazlar tarafından kullanılmasına olanak sağlayan standarttır
XMPP	Extensible Messaging and Presence Protocol	TCP	Yayın/Kayıt İstek/Yanıt	XMPP protokolü birbirinden uzak noktalar arasında haberleşme için adres sağlamaktadır.
RestFull HTTP	Advanced Message Queuing Protocol	TCP	İstek/Yanıt	RESTful, sunucu ve istemci arasındaki veri alışverişini platform bağımsız ve olabilecek en az veri yüküyle sağlamayı amaçlayan bir protokoldür.
CoAP	Constrained Application Protocol	UDP	İstek/Yanıt	CoAP web üzerinde Internet kaynaklarına erişmek için geliştirilmiş protokoldür.

yazma olarak temsil edilmektedir. D2S protokolleri cihazlardan toplanan verilerin sunucuya iletimi ve sunucudan cihazlara veri iletimi için tasarlanmıştır ("İstek/Yanıt(Request/Response)" modeli).

Yukarıda uygulama katmanında popüler olarak kullanılan protokoller verilmiştir. Bu yayın kapsamında detaylı bir şekilde CoAP protokolünden bahsedilmesinin nedeni: zaman içerisinde HTTP protokolünün neredeyse global hale gelmesi ve CoAP'ın da HTTP'nin Nesnelerin İnternetinde karşılığı olmasıdır denilebilir. Ayrıca birçok firma ürettikleri Nesnelerin İnterneti cihazında CoAP'ı kullanmaktadır [92].

CoAP (Constrained Application Protocol – Kısıtlı Uygulama Protokolü), IETF tarafından tasarlanmış bir uygulama katmanı protokolüdür. Adından da anlaşılabileceği gibi birincil amacı kısıtlı kaynaklara sahip cihazlar üzerinde çalışmak olan CoAP, tasarımı basit tutmak için UDP üzerinde çalışır. CoAP, uygulama uç birimleri arasında etkileşimli bir istek/yanıt modeli sunar; servisler ve kaynakların keşfi için yerleşik desteğe sahiptir; URI gibi anahtar web kavramlarını barındırır.

HTTP'nin istemci/sunucu modeline benzeyen CoAP protokolü makineden-makineye çalıştığı için hem istemci hem sunucu rollerini üstlenir. HTTP'den farklı olarak bu etkileşim UDP üzerinde asenkron olarak gerçekleştirilir. Bu süreç, opsiyonel olarak güvenilirliği desteklemek için mesaj katmanlarının mantıksal kullanımı ile gerçekleştirilebilir [13, 93]. CoAP mesajların şifrelenmesi için iletim katmanındaki güvenlik mekanizması olan DTLS kullanılır. Bu nedenle DTLS'in güvenliğinin sağlanması CoAP protokolünün de güvenilirliğinin sağlanması anlamına gelmektedir. Fakat güvenlik aynı zamanda uygulama katmanında CoAP'ın sahip olduğu farklı güvenlik modları ile de sağlanabilmektedir ve kendi içerisinde tanımlı üç güvenlik modu vardır: PreSharedKey, RawPublicKey ve Certificates modları. Her mod ile beraber CoAP protokolü kendi mesajlarının gizliliğini, aitliğini, bütünlüğünü ve tekrarlanmadığının kontrolünü sağlar. Doğrulamanın ve anahtar üzerinde karar verme aşamaları ise her üç mod için farklılık gösterecektir. PreSharedKEy modunda iken haberleşme yapacak olan cihazlarda, şifreleme için kullanılacak olan anahtar değerlerinin ön yüklemesi gerçekleştirilir. Her bir cihaz için veya belirli bir grup cihaz için belirli bir anahtar kullanan uygulamalar için ideal bir güvenlik modudur. RawPublicKey modunda ise CoAP protokolü, cihaz doğrulamayı genel anahtar şifreleme kullanarak fakat genel anahtar altyapısını (PKI) gerektirmeden gerçekleştirmektedir. Cihazın kimliği kullanılan anahtar değerinden elde edilirken, iletişime geçebilecek olduğu uçlarda yine aynı anahtar değerine göre belirlenecektir. Certificates modunda ise, sertifikaların doğrulanabilmesi amacıyla cihazla bir sertifika zincirine bağlıdır. Bu nedenle de önceden kurulmuş bir güvenlik altyapısının ilgili ağda mevcut olması zorunludur. Eliptik Eğri Şifreleme yöntemi şu an için CoAP tarafından RawPublicKey ve Certificates modlarını gerçekleştirme esnasında kullanılmaktadır. Eliptik Eğri Şifrelemenin 6LoWPAN ağları uygulamalarına yönelik olarak donanımsal ve yazılımsal olarak optimizasyonu başlı başına bir çalışma konusudur. Aynı zamanda hız etkin yeni genel anahtar şifreleme yöntemlerinin de Eliptik Eğri Şifrelemeye bir alternatif oluşturabilecek şekilde irdelenmesi, uygulama katmanındaki güvenliğin performans etkin olarak sağlanabilmesi için önemlidir.

CoAP protokolü güvenliğin sağlanmasında DTLS'den faydalandığı için DTLS'in optimizasyonu üzerine gerçekleştirilen çalışmalar doğrudan CoAP protokolünün performansını da etkilemektedir. [94]'te gerçekleştirilen çalışmada, büyük handshake mesajlarının 6LoWPAN fragmantasyon aşamasındaki etkisi incelenmiş ve handshake mesajlarının CoAP mesajlarının bir payload'u olarak gönderilmesine karar verilmiştir. CoAP protokolünün kendi içerisinde yeni güvenlik mekanizmaları öneren çalışmalarda literatürde mevcuttur [95-97]. DTLS seviyesinde, CoAP içerisinde veya hibrit yaklaşımların enerji ihtiyacı ve hesaplama maliyetini de göz önünde bulundurarak önerilmesi ilgili alandaki bir araştırma konusudur.

6. NESNELERİN İNTERNETİ GÜVENLİĞİNİN SAĞLANMASINDAKİ ZORLUKLAR (OPEN RESEARCH ISSUES FOR INTERNET OF THINGS)

Nesnelerin İnternetinde haberleşmenin korunması için analiz edilen yöntemlerin kullanımı sorun oluşturmaktadır fakat aynı zamanda bu sorunlar yeni araştırma alanlarının ortaya çıkmasına katkı sağlamaktadır. Alt bölümlerde katmanlarda var olan zorluklardan ve bu zorluklara karşı alınması gereken tedbirlerden bahsedilecektir.

6.1. Fiziksel ve Ortam Erişim Katmanlarında Karşılaşılan Zorluklar ve Önerilen Yöntemler

(Research Challenges and Proposals for Security at the Physical and Medium Access Control Layers)

IEEE 802.15.4 standardı belli bir düzeyde olmasına rağmen, MAC katmanı tarafından desteklenen güvenlik hizmetlerinin nasıl eklenmesi gerektiği konusunda çeşitli kısıtlamalar mevcuttur.

Başlangıç vektörü yönetim problemleri, çoklu ACL girişinde aynı anahtar kullanılması ve yaşanabilecek güç kesintileri nedeniyle ACL durumunun kaybolması şeklinde ortaya çıkabilir. En çok 255 taneye kadar ACL girişi, ilgili nonce'ları ve farklı anahtarları depolamak için kullanılabilir. Göndericiler alıcı adreslerine göre uygun ACL belirlerler. Bununla birlikte eğer aynı anahtar iki farklı ACL girişinde kullanılırsa problem oluşur. Bu durumda büyük olasılıkla tesadüfen nonce yeniden kullanılacaktır. Bazı durumlarda bütünlük değişmemesine rağmen gizlilik ortadan kalkabilir. Bir gönderici nonce değerini dikkatlice yönetmek şartıyla, aynı anahtarı kullanarak iki farklı alıcıya iki mesajı güvenli bir şekilde yollayabilir. Burada en kolay yöntem tek bir ACL girişi kullanmaktır. Gönderici önce birinci mesajı iletecek, daha sonra ACL girişindeki alıcı adresini değiştirerek ikinci mesajı yollayacaktır. Nonce'un tekrar kullanımını önlemek

için genel prensip, nonce durumunun asla anahtardan ayrılmamasıdır. Düğüm bir güç kesintisi ile karşılaştığında ACL durumu kaybolursa ciddi sorunlar oluşabilir. Bu durum için önlem alınmaz ise güç kesintisi giderilene kadar düğüm ACL tablosunu sıfırlar. Bundan sonra düğümün yazılımı uygun anahtar ile ACL tablosunu yeniden oluşturur. Nonce durumuyla ilgili ne olacağı açık değildir. Eğer tüm nonce'lar sıfırlanırsa (örneğin sıfır gibi bilinen bir değer ile değiştirilirse) güvenliğin sağlanması için nonce'lar yeniden kullanılacaktır. Bu sorunu çözmek için öncelikle düğümler bir güç kesintisinden sonra yeni anahtarlar oluşturabilmelidirler. Böylelikle aynı anahtar ile aynı nonce'u iki kez kullanmamış olacaklardır.

Anahtar yönetim problemleri grup anahtarlama için destek sağlanamaması, ağ paylaşımlı anahtar ile tekrar saldırılarına karşı koruma arasındaki uyumsuzluk ve eşleşme anahtarlamasının yeterince desteklenmemesi olarak meydana gelmektedir. IEEE 802.15.4 altında grup anahtarlama desteği yaygın değildir ve çalışma açısından çok fazla sorun içerdiğinden kullanıma pek uygun değildir.

Uygulamada tek bir ağ paylaşımlı anahtarlama kullanıldığında, tekrarlama saldırılarına karşı koymak için herhangi bir yöntem yoktur. Grupta fazla kullanıcı olduğunda ağ paylaşımlı anahtar ile tekrarlama korumasının kullanımı engellemek uygun bir yöntem olmaktan çıkar.

Anahtar yönetim problemleri ile ilgili zorlukların kısmen kaynağı nonce'un ve tekrarlama sayacının kafa karıştırıcı rolüdür. Paketlerde gönderilen nonce iki amaca hizmet eder. Birincisi, tekrarlanmayan bir değer sağlar ve gizliliği korur. İkincisi ise monoton olarak artan sayaç sağlar ve bu da tekrarlama saldırılarını engeller. Gizliliği korumak için, göndericinin aynı anahtar için aslı aynı nonce'u iki kez kullanmadığından emin olması gerekir. Tekrarlama saldırılarından korunmak için alıcı her göndericinin aynı anahtarı paylaşan bir önceki mesajda, daha büyük bir nonce değeri bulduğuna emin olmaya ihtiyaç duyar. Birinci gereksinim, nonce'un kuvvetli biçimde anahtara bağlı olmasını önerir. Herhangi bir zamanda anahtar şifreleme için kullanılır ve farklı bir nonce değeri kullanmalıdır. Bu yüzden anahtarın her kullanımında farklı ACL girişlerinde bile olsa, tek bir nonce değeri kaydı paylaşmalıdır. Diğer taraftan ikinci gereksinim ise, tekrarlama sayacının kuvvetli bir biçimde gönderici adresine bağlı olmasını önerir. Çoklu ACL girişinde aynı anahtar görülür ise her kullanıcı için farklı bir en yüksek işaret sağlanır.

Anahtar yönetim mekanizmaları uçtan uca güvenliği sağlamak için üst katmanlarda tasarlanabilir böylece bağlantı katmanında ACL yönetimini kısıtlayan grup ve ağ paylaşımlı anahtarlama sorunu ortadan kalkabilir. Ayrıca bağlantı katmanı desteği olmadan IEEE 802.15.4'deki mevcut ACL depolama alanından yararlanılarak anahtar yönetim yaklaşımları tasarlanabilir. Tek başına AES-CCM donanımsal şifreleme, ağ ve daha üst katmanlarda etkili şifreleme sağlayabilir. IEEE 802.15.4 standardı bütünlük veya gizlilik ile ilgili onay mesajlarının güvenliğini sağlamaz. Saldırgan sahte onay mesajları yayarak paketin içindeki sıra numarasını öğrenebilir ve bunu hizmet engellemede kullanabilir.

Güncel araştırma konularından biri de IEEE 802.15.4e standardını kullanan zaman paylaşımlı bağlantı katmanı iletişim ortamları altında yatmaktadır. Daha önceden belirtildiği gibi, uygulamalar böyle ağlardaki iletişim mekanizmasından sorumludur ve güvenlik mekanizmaları zaman eşleşmesini ve kanal atlamalı iletişimini kullanan MAC katmanından faydalanarak tasarlanabilir. Yaklaşımlardan biri, anahtar yönetim ve saldırı tespiti için kötücül düğümlerin belirlenmesi gibi ihtiyaç duyulan güvenlik operasyonlarını destekleyen slot tabanlı güvenlik mekanizmaları olabilir. IETF çalışma grubu 6tisch modu için güvenlik çözümleri üzerine çalışmalar yapmaktadır.

6.2. Ağ Katmanında Karşılaşılan Zorluklar ve Önerilen Yöntemler

(Research Challenges and Proposals for Security at the Network Layer)

Geçmiş analizlerde, mevcut 6LoWPAN standardı sadece genel güvenlik tehditlerini ve gerekliliklerini tartışırken, RFC 4944 [10] açık bir şekilde 6LoWPAN adaptasyon katmanında uygun güvenlik mekanizmalarını tanımlamaktadır. Yapılan çalışmalarda, 6LoWPAN'ı kullanan Nesnelerin İnterneti teknolojisindeki ağ katmanı haberleşmesinin korunmasına yönelik çözümler önerilmektedir.

İnternet Güvenlik Protokolü (IPsec) mimarisi belirli bir iletişim oturumu bağlamında uçtan uca güvenliği garanti eden Sanal Özel Ağlar (VPN) için destek sunar [98-100]. Uçtan uca ağ katmanı güvenliğinin avantajlarına rağmen, uçtan uca güvenliği sağlamak adına hiçbir özel güvenlik mekanizması şimdiye kadar 6LoWPAN adaptasyon katmanı için ortaya konmamıştır. 6LoWPAN'daki IPsec ve IKE gibi ağ katmanı güvenlik protokollerinin tipik kablosuz duyarga platformlarının işlemci ve bellek kaynaklarıyla gerçeklenmesi oldukça zordur. Bu kısıtlamalar yakın zamanda yapılan birçok araştırmanın ana temasını oluşturur [9, 102]. Bu araştırmaların sonuçlarından da anlaşılabileceği gibi 6LoWPAN adaptasyon katmanıyla uyumlu çalışan ve uçtan uca güvenlik mekanizmalarını mümkün kılacak çözümlere ihtiyaç vardır.

Var olan İnternet Protokol Güvenliğinin kapsülleme güvenlik yükü (ESP) ve kimlik doğrulama başlığı (AH) gibi aynı amaç ile 6LoWPAN uygunluk katmanı için sıkıştırılmış güvenlik başlıklarının tasarımına odaklanan birkaç araştırma önerisi şu anda mevcuttur [98-100]. Bu yaklaşım öncelikli olarak [103]'de önerilmiştir. Yapılan çalışmalar, algılama platformlarında var olan güvenlik donanımları yardımıyla geliştirilen algoritmaların sıkıştırılmış güvenlik protokolü başlıklarını adaptasyon katmanında işlemek için kullanılabileceğini ortaya koymuştur. Platform donanımlarında var olan AES/CCM şifreleme kullanarak ve tanımlanmış uygulama güvenlik profillerini kullanarak 6LoWPAN için ESP ve AH sıkıştırılmış güvenlik

başlıklarının işlenebileceği deneysel olarak ortaya konmuştur [104, 105]. Donanım tabanlı şifreleme yöntemleriyle ağ katmanında güvenliğin sağlanması enerji verimliliği adına büyük bir fırsat sunmaktadır. Haberleşmede yer alan katmanlardan bağımsız, uzun süreli ve etkili güvenliği garanti altına almak için anahtar güncellemesi gereklidir. 6LoWPAN'da tartışılan diğer önemli katmanlar arası güvenlik beklentisi ise kimlik doğrulama ile ilişkili olan anahtar yönetimidir. Herhangi bir spesifik anahtar yönetimi sunulmadığından, RFC 6568 [106] geçerli İnternet anahtar yönetimi çözümlerinin basitleştirilmiş versiyonlarının adaptasyonunu tanımlamıştır. Örneğin, sadeleştirilmiş IKEv2 standart Internet özelliklerini korumakla birlikte kısıtlı kaynaklara sahip cihazlar için İnternet anahtar yönetimini uyumlu hale getirmeyi amaçlar [107]. Diğer bir yaklaşım ise 6LoWPAN IP başlık sıkıştırmasını kullanan veri yükü bilgisi ve IKE başlıklarının sıkıştırılmasıdır [85]. Roman vd. açık anahtarlı yönetim yaklaşımlarının hala gereğinden fazla enerji kullandıklarını ifade etmişlerdir [31]. Bu nedenle enerji verimliliğini göz önünde bulunduran anahtar yönetim sistemlerinin tasarlanması gerekmektedir.

6.3. İletim Katmanında Karşılaşılan Zorluklar ve Önerilen Yöntemler
(Research Challenges and Proposals for Security at the Transpor Layer)

İletim katmanında güvenliğin sağlanmasında yaygın olarak kullanılan DTLS'in kaynak kısıtlamalı ağlardaki etkisi önemli bir inceleme konusudur. İşlem karmaşıklığı ve işlemci bağımlılığı açısından daha etkin bir algoritma olan ECC (Elliptic Curve Cryptography-Eliptik Eğri Kriptografisi)'nin doğrulama ve anahtar kararlaştırma aşamasında kullanımı için adaptasyonu önemli bir araştırma konusudur. DTLS'in Nesnelerin İnterneti ortamlarında kullanılabilecek şekilde optimizasyonu, iletim katmanındaki güvenliğin irdelenmesi alanında en yaygın uğraşılan konular arasında yer almaktadır. Diğer taraftan DTLS'in, CoAP protokolünün özelliklerini de kullanabilecek şekilde modifiye edilmesi de bir diğer araştırma alanıdır. Orjinal DTLS protokolünde var olan el sıkışma(handshake) mesajlarının boyutları, 6LoWPAN seviyesinde veri parçalama ve birleştirme işlemlerini gerektirmektedir. Aynı zamanda ilk el sıkışmanın tamamlandığını gösteren mesajların hesaplama maliyeti yüksektir. Mesajların parçalanması, ağ üzerinden iletilen paketlerin yeniden gönderimi ve karşı tarafta yeniden düzenlenmeleri ile sonuçlanabilir. Bu bağlamda, özellikle DTLS'in handshake aşamasının 6LoWPAN ağlarında etkinliğini artırabilecek şekilde optimizasyonu önemli bir araştırma konusudur.

ECC algoritmasının 6LoWPAN ağlarındaki kullanımı ve performans ölçümleri de yine araştırmacılar tarafından ilgilenilen bir araştırma alanı olmuştur. DTLS ile beraber gelen en önemli dezavantajlardan biri ise protokolün multicast haberleşmeye izin vermemesidir. Oysaki multicast trafik birçok Nesnelerin İnterneti ortamları için gereklidir. DTLS protokolünün multicast trafiği destekleyecek şekilde adaptasyonu da iletim katmanındaki güvenlikteki araştırma alanlarından biridir. CoAP ile beraber multicast trafiğin desteklenmesi durumunda ise, DTLS grup anahtar yönetimini sağlamadığı için problem oluşmaktadır. DTLS'in kayıt (record) katmanının çoklu gönderiyi destekleyecek şekilde adaptasyonunun sağlanması literatürde ilgi gösterilen bir alandır. DTLS tarafından ihtiyaç duyulan ve maliyeti yüksek işlemlerin donanımsal açıdan kuvvetli güvenlik geçitlerine aktarılması ise iletim katmanında güvenliğin irdelenmesindeki bir diğer araştırma konusudur. Özellikle DTLS'in getirdiği işlemsel maliyetin donanımsal açıdan güçlü ek aygıtlar ve adaptasyon protokolleri ile sağlanması son yıllarda uğraşılan bir konu olmuştur. İleriye dönük olarak, Nesnelerin İnterneti ortamlarının bir standardı haline dönüşen iletim katmanındaki güvenlik protokolü olan DTLS'in, kaynak sınırlılığının da göz önüne alınarak modifikasyonu ilgilenilmesi gereken bir konu olarak göze çarpmaktadır. ECC algoritması yerine işlemsel maliyeti daha da düşük genel anahtar şifreleme yöntemlerinin araştırılması, sertifika yönetiminde yeni yöntemlerin önerilebilmesi, multicast trafiğin ve grup anahtar paylaşımının etkin bir şekilde yönetilebilmesi ileriye dönük araştırma konuları olarak görülmektedir.

6.4. Yönlendirme Katmanında Karşılaşılan Zorluklar ve Önerilen Yöntemler
(Research Challenges and Proposals for Routing Security)

IETF RPL temel güvenlik işlemleri ile birlikte yönlendirme kontrol mesajı güvenlik sürümlerini tanımlamaktadır fakat önemli operasyonları gerçekleştirmek için kullanılan mekanizmalar yeterince iyi değillerdir. RPL protokol standardının güncel halinde yukarıda bahsedilenlerden başka güvenlik mekanizmaları tasarlanmamıştır. IETF ROLL grubu tarafından oluşturulan diğer kaynaklar da özelleşmiş güvenlik mekanizmaları içermeyen genel güvenlik gereksinimleri ve amaçları tartışılmıştır. Dışardan gelen ataklara karşı güvenli yönlendirmeyi sağlayan RPL incelendiğinde, araştırmalar RPL'in çalışmasını engelleyecek tehdit modellerinin belirlenmesi ve içerden gelen ataklara karşı önlem alınması üzerine olmalıdır.Önceki yapılan çalışmalar RPL'de var olan güvenlik sorunlarına ek olarak içerden yapılan saldırılar ve saldırganlara karşı mekanizmaları ve tehdit modellerini ele almaktadırlar. Bu öneriler gelecekte belki de RPL standardındaki diğer güvenlik mekanizmalarının adaptasyonuna katkıda bulunabilir. Geçmişte duyarga ağlarında yönlendirme protokolleri için kapsamlı bir araştırma oluşturulmuş durumdadır ve bu araştırma gelecekte RPL güvenliğinin sağlanmasında rehber olarak kullanılabilir. Düğümlerin doğrulanmasını ve anahtar değişimini tanımlamayan RPL; bu ihtiyaçları gidermek için ileriki zamanlarda asimetrik kriptografi kullanan güvenlik mekanizmaları önerebilir.

6.5. Uygulama Katmanında Karşılaşılan Zorluklar ve Önerilen Yöntemler (Research Challenges and Proposals for Security at the Application Layer)

Daha önce de belirtildiği gibi, CoAP protokolünü kullanan uygulama katmanında güvenlik için DTLS incelenmiştir. Uygulama katmanı güvenliği için DTLS bazı kısıtlar

içerdiğinden, araştırmacıları yeni güvenlik mekanizmaları geliştirme konusunda motive etmektedir. Farklı özelliklere sahip duyarga platformlar üzerinde CoAP'ın etkisini değerlendirmek önemlidir çünkü IEEE 802.15.4 duyarga platformlarda AES-CCM etkili bir şekilde kullanılabildiğinden, DTLS el sıkışma mekanizmasının kısıtlı kaynaklara sahip cihazlar üzerindeki kullanımı ileriki çalışmalarda optimize edilebilir.

IETF kısıtlı kaynaklara sahip cihaz üzerinde DTLS'in kullanımını araştırmak üzere bir çalışma başlatmıştır. DTLS protokolünün bazı özellikleri sınırlı kaynaklara sahip cihaz üzerinde etkili çalışmasını engellemektedir:

- DTLS handshake protokolü adaptasyon katmanındaki büyük mesajların parçalanmasından dolayı sorun oluşturabilir.
- 6LoWPAN çevrelerinde eliptik eğri şifrelemenin desteklenmesi yakın gelecekte üzerinde durulacak konulardan biri olmalıdır.
- Gelecekteki Nesnelerin İnterneti cihazları özellikle CoAP güvenlik modu için X.509 sertifikasını destekleyen mekanizmaları kullanabilir. Bu amaçla tasarlanacak ve adapte edilecek mekanizmalar ayrı bir çalışma konusu oluşturmaktadır.

Güncel araştırma konuları CoAP haberleşmesini güvenli hale getirmek için alternatif yaklaşımların ve iletim katmanı güvenliği yerine nesne güvenlik yaklaşımlarının kullanımı üzerinedir. Belirtilen yaklaşımlar, CoAP protokolüne entegre edilerek güvenlik sağlanabilir. Granjal vd. güvenliği desteklemek için yeni CoAP seçeneklerinin kullanımı üzerine çalışma yapmışlardır [96]. Kullanımlardan biri CoAP istemcisinin yetkilendirilmesi ve doğrulanması için gerekli olan verilerin iletilmesidir. Diğer kullanım ise CoAP mesajlarının şifrelenmesi için gerekli olan verilerin iletilmesidir. Bu yaklaşımlar mesajlar için güvenlik sağlamakla birlikte; çoklu kimlik doğrulama mekanizmalarının kullanımını da desteklemektedir.

CoAP güvenliğinin sağlanmasında hala çeşitli sorunlar mevcuttur. CoAP çoklu gönderim(multicast) haberleşmesinde güvenlik için uygun anahtar yönetim mekanizmasının olmayışı önemli sorunlardan biridir. Grup anahtar yönetim mekanizmaları ya CoAP dikkate alınmadan ya da grup cihazlar üzerinde oturum anahtarını desteklemek için DTLS yöntemiyle bütünleşik olarak geliştirilebilir. DTLS başlık sıkıştırma mekanizmalarının kullanımı ile ilgili olarak, varolan eklentilerden gerekli desteğin sağlanması istenebilir veya DTLS ile sıkıştırılmış DTLS arasında eşleşmiş mekanizmalar tasarlanabilir. Böyle mekanizmalar uçtan uca güvenli CoAP haberleşmesi için TLS ve DTLS arasında eşleşme sağlayan İnternet bağlantısı bulunan düşük güçlü cihazları birbirine bağlayan ağ geçitleri tarafından desteklenebilir.

CoAP güvenliği için açık anahtarlı şifreleme ve sertifika üretimi önemli araştırma konularından biri olarak ortaya çıkmıştır. İnternet üzerinden sertifikaların doğrulanması için OCSP [108] veya RFC 6066 [109]'de tanımlanan TLS yöntemi ile OCSP yöntemlerinin birleşimi kullanılabilir. OSCP sertifika yetkilisi sorunları yerine doğrulama hizmetlerine katılan kaynak maliyeti doğmasına sebep olmaktadır. Diğer önemli bir sorun ise ECC'nin mevcut duyarga cihazları üzerindeki etkisidir. Bu bağlamda, IEEE 802.15.4 platformlarda donanımsal AES-CCM'e benzer olarak ECC'in de gerekli optimizasyonlar yapılarak desteklenmesi sağlanmalıdır.

7. SONUÇLAR (CONCLUSIONS)

Bu makalede Nesnelerin İnterneti için düşünülen güncel protokol parçaları tanıtılarak, oluşabilecek güvenlik zafiyetleri protokol yığınının her katmanı için irdelenmiştir. Yapılan çalışmadan anlaşılabileceği gibi Nesnelerin İnterneti güvenliği gelecek nesil İnternet'in güvenliğinin ayrılmaz bir parçası olarak düşünülmelidir ve bu bağlamda düşük karmaşıklığa ve yüksek güvenilirliğe sahip çözümler Nesnelerin İnterneti ağları için yapılandırılmalıdır. Bu gözlemlerimiz yakın zamanda dünya çapında ortaya çıkan hizmet engelleme saldırılarının küçük cihazları kullanmış olduğu gerçeğiyle de daha anlamlı hale gelmektedir [109]. Bu bağlamda gelecek nesil İnternet'i oluşturacak 6LoWPAN, 6TiSCH, CoAP ve benzeri protokollerin güvenliğin ön planda olduğu bir anlayışla tasarlanması büyük bir önem arz etmektedir.

Güvenlik mekanizmaları tasarlanırken her Nesnelerin İnterneti cihaz katmanı güvenlik gereksinimleri dikkate alınarak tekrar ele alınmalıdır. Fiziksel ve ortam erişim katmanlarında boğma ve dinleme saldırılarına dayanıklı yöntemler geliştirilmelidir. Bu anlamda TSCH boğma ve dinleme saldırılarına karşı etkili bir yöntem sunmaktadır. Bu bağlamda TSCH'in sağladığı güvenlik avantajlarını etkin kullanacak yöntemler geliştirilmelidir. 6Top/6LowPAN gibi kablosuz Nesnelerin İnterneti katmanlarına özel güvenlik mekanizmalarına ihtiyaç vardır. Örneğin kaynak ayırma için kullanılan 6Top protokolünün güvenliği için özel güvenlik mekanizmaları geliştirilmelidir. Bu mekanizmalar TSCH ortam erişim protokolüyle birlikte düşünülmelidir. Ağ katmanı için ise RPL, IP katmanı ver diğer katmanlara ait güvenlik gereksinimleri birlikte değerlendirilmelidir ve mümkün olduğunca uygulamaya uygun güvenlik mekanizmaları belirlenmelidir. Bu nedenle uygulama katmanı güvenlik gereksinimlerini diğer katmanlarla paylaşmalı ve protokol yığını katmanlarında uygulanacak güvenlik seviyesi uygulamaya göre belirlenebilmelidir. Bu anlamda CoAP protokolü güvenlik gereksinimlerinin düğümler arasında paylaşılması için kullanılabilir. CoAP güvenliği için ise en uygun protokol olarak ise DTLS protokolü karşımıza çıkmaktadır. Tabii ki DTLS için de uygulamaya ve ağın yeteneklerine özgün özelleştirmeler yapılmalıdır. Bütün bu katmanlar arası güvenlik mekanizmalarına ek olarak, heterojen Nesnelerin İnterneti ağlarını dikkate alan güvenlik mimarisi önerilerek heterojen ağların güvenlik gereksinimleri karşılanmalıdır. Ayrıca, farklı ağ mimarileri türü için kesin birleşik kimlik doğrulama mekanizması, E2E kimlik doğrulaması, anahtar anlaşma mekanizması, Ortak Anahtar Altyapısı (PKI- Public key

infrastructure), kablosuz PKI, güvenlik yönlendirmesi ve saldırı tespiti ayarlanmalıdır. IoT uygulama alanlarının genişlemesiyle birlikte oluşan çok boyutlu sensör verilerini temel alan yeni algoritmalar geliştirilmelidir. TM (Trust Management-güven yönetimi), IoT kuruluşları arasındaki güven ilişkilerini değerlendirmek için etkili bir yaklaşım olabilir. Mevcut asimetrik şifreleme teknikleri kısıtlı cihazlarda kullanılabilecek şekilde optimize edilerek IoT teknolojisine uyumlu hale getirilmelidir. Ayrıca geleneksel ağlarda etkin olarak kullanılan simetrik/asimetrik şifreleme teknikleri gerekli sadeleştirmeler yapılarak kısıtlı kaynaklara sahip cihazlarda donanımsal olarak gerçekleştirilmelidir. IoT sistemlerinin güvenliği, katmanlı yapıların (fiziksel, ortam erişim, vb..) sağlamış olduğu güvenlik mekanizmaları göz önünde bulundurularak tasarlanmalıdır.

KAYNAKLAR (REFERENCES)

1. Özdağ R., Kablosuz algılayıcı ağlarda hedef kapsama problemi için algılayıcı dağıtımı ile ağın yaşam süresinin optimizasyonu, Journal of the Faculty of Engineering and Architecture of Gazi University, 32 (4), 2017.
2. Fan Z., Kulkarni P., Gormus S., Efthymiou C., Kalogridis G., Sooriyabandara M., Chin W.H., Smart grid communications Overview of research challenges, solutions, and standardization activities, IEEE Commun. Surv. Tutorials, 15 (1), 21-38, 2013.
3. Lu D., Liu T., The application and development of iot. International Symposium on Information Technology in Medicine and Education, 15 (1), 991-994, 2012.
4. Dave E., The Internet of Things How the Next Evolution of the Internet Is Changing Everything. http://www.cisco.com/c/dam/en us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Yayın tarihi Nisan 9, 2011. Erişim tarihi Temmuz 29, 2016.
5. Wood A.D., Stankovic J. A., Denial of service in sensor networks, Ad Hoc Networks, 35 (10), 54-62, 2002.
6. Karlof C., Wagner D., Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1 (2), 293-315, 2003.
7. Wood A.D., Stankovic J.A., A taxonomy for denial-of-service attacks in wireless sensor networks, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, 739-763, 2004.
8. Ganesan D., Govindan R., Shenker S., Estrin D., Highly-resilient, energy-efficient multipath routing in wireless sensor networks, ACM SIGMOBILE Mobile Computing and Communications Review, 5 (4), 11-25, 2001.
9. Shelby Z., Bormann C., keshi. ubiwna. org/ 2015IotComm /6LoWPAN The Wireless Embedded Internet.pdf. Yayın tarihi Kasım 8, 2009. Erişim tarihi Temmuz 14, 2016.
10. Internet Engineering Task Force (IETF) IPv6 over Low Power Wireless Personal Area Networks (6lowpan) Working Group. http:// datatracker. ietf.org/ wg/ 6lowpan/. Yayın tarihi Nisan 7, 2010. Erişim tarihi Aralık 17, 2016.
11. IETF. IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch). https://datatracker.ietf.org/wg/6tisch/charter/. Yayın tarihi Ekim 14, 2015. Erişim tarihi Ekim 28, 2016.
12. IEEE 802.15 WPAN 4e Task Group. IEEE 802.15 WPAN 4e Task Group. http://www.ieee802.org /15/pub/TG4e.html.Yayın tarihi Şubat 6, 2012. Erişim tarihi Kasım 7, 2016.
13. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol. https:// tools. ietf.org/ html/rfc7252. Yayın tarihi Haziran, 2014. Erişim tarihi Ekim 28, 2016.
14. MQ Telemetry Transport. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html. Yayın tarihi Ekim 29, 2014. Erişim tarihi Aralık 17, 2016.
15. Internet Engineering Task Force (IETF) Routing over Low Power and Lossy Networks (ROLL) Working Group. http://datatracker.ietf.org/wg/roll/. Yayın tarihi 2010. Erişim tarihi Aralık 17, 2016.
16. Hui J., Thubert P., Compression format for IPv6 datagrams over IEEE 802.15. 4-based networks. Yayın tarihi Eylül 2011. Erişim tarihi Ağustos 10, 2016.
17. Kushalnagar N., Montenegro G., IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. https://tools.ietf.org/pdf/rfc4919.pdf. Yayın tarihi Ağustos 2008. Erişim tarihi Temmuz 17, 2016.
18. Internet Eng. Task Force (IETF). https:// datatracker. ietf.org/wg/6lowpan/charter/. Yayın tarihi Nisan 2012. Erişim tarihi Temmuz 14, 2016.
19. Winter T., Thubert P., Brandt A., Kelsey R., Levis P., Pister K., Struik R., Vasseur J.P., Alexander R., Internet Eng. Task Force (IETF). RPL: IPv6 routing protocol for low-power and lossy networks. 2012.
20. Levis P., Patel N., Culler D. ve Shenker S., Trickle: A self-regulating algorithm for code propagation and maintenance in wireless sensor networks. Proc. of the 1st USENIX/ACM Symp. on Networked Systems Design and Implementation, USENIX Association Berkeley, A.B.D, 25, 2004.
21. Jin Y., Gormus S., Kulkarni P., Sooriyabandara M., Content centric routing in IoT networks and its integration in RPL. Comput. Commun., 89–90, 87-104, 2016.
22. Drath R., Horch A., Industrie 4.0: Hit or Hype [Industry Forum]. IEEE Ind. Electron. Mag., 8 (2), 56-58, 2014.
23. Görmüş S., Synchronisation in 6Tisch networks, 2015 23nd Signal Processing and Communications Applications Conference (SIU), Malatya-Türkiye, 535-539, 16-19 Mayıs, 2015.
24. Stanislowski D., Vilajosana X., Wang Q., Watteyne T., Pister K.S., Adaptive Synchronization in IEEE802.15.4e Networks, Industrial Informatics, IEEE Trans. Ind. Inf., 10 (1), 795-802, 2014.
25. Menezes A.J., Van Oorschot P.C., Vanstone S.A., Handbook of applied cryptography, CRC press, New York, A.B.D., 1996.

26. Stallings W. Cryptography and network security: principles and practices, http:// www. inf.ufsc.br /~bosco.sobral /ensino /ine5680/ material-cripto - seg/2014-1/ Stallings/Stallings_ Cryptography_and_ Network_Security.pdf. Yayın tarihi Kasım 16, 2005. Erişim tarihi Haziran 11, 2016.

27. Shi E., Perrig A., Designing secure sensor networks, IEEE Wireless Communications, 11 (6), 38-43, 2004.

28. Akyol S., Alataş B., Automatic Mining of Accurate and Comprehensible Numerical Classification Rules with Cat Swarm Optimization Algorithm, Journal of The Faculty of Engineering and Architecture of Gazi University, 31 (4), 839-857, 2016.

29. Perrig A., Szewczyk R., Tygar J.D., Wen V., Culler D.E., SPINS: Security protocols for sensor networks. Wireless networks, 8 (5), 521-534, 2002.

30. Mahalle P.N., Anggorojati B., Prasad N.R., Prasad R, Identity authentication and capability based access control (iacac) for the internet of things, Journal of Cyber Security and Mobility, 1 (4), 309-348, 2013.

31. Roman R., Alcaraz C., Lopez J., Sklavos N., Key management systems for sensor networks in the context of the Internet of Things, Comput. Electric. Eng., 37 (2), 147-159, 2011.

32. Yasmin R., Ritter E. ve Wang G., An authentication framework for wireless sensor networks using identity-based signatures, Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, Bradford-Birleşik Krallık, 882-889, 2010.

33. Yeh H.L., Chen T.H., Liu P.C., Kim T.H., Wei H.W., A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors, 11 (5), 4767-4779, 2011.

34. Yurttutan G., Group Key Management in IEEE 802.15.4 Wireless Networks, Yüksek Lisans Tezi, Boğaziçi Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2006.

35. Messerges T.S., Cukier J., Kevenaar T.A., Puhl L., Struik R. ve Callaway E., A security design for a general purpose, self-organizing, multihop ad hoc wireless network, Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Virginia-A.B.D, 1-11, 2003.

36. Karlof C., Sastry N. ve Wagner D., TinySec: a link layer security architecture for wireless sensor networks, Proceedings of the 2nd international conference on Embedded networked sensor systems, Marilend-A.B.D, 162-175, 2004.

37. Lighfoot L.E., Ren J. ve Li T., An energy efficient link-layer security protocol for wireless sensor networks, 2007 IEEE International Conference on Electro/Information Technology, Chicago-A.B.D, 233-238, 2007.

38. Luk M., Mezzour G., Perrig A., Gligor V., MiniSec: a secure sensor network communication architecture, Proceedings of the 6th international conference on Information processing in sensor networks (IPSN 07), Massachusetts-A.B.D, 479-488, 2007.

39. Rogaway P., Bellare M., Black J., OCB A Block-cipher Mode of Operation for Efficient Authenticated Encryption, ACM Trans. Inf. Syst. Secur., 6 (3), 365-403, 2003.

40. SOYLU S., Tasarsız ağlar için eliptik eğriye dayalı Diffie Hellman grup anahtar yöntemi. Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2007.

41. Szczechowiak P., Oliveira L.B., Scott M., Collier M. ve Dahab R., NanoECC: Testing the limits of elliptic curve cryptography in sensor networks. Wireless sensor networks, Bologna-İtalya, 305-320, 2008.

42. Schwartz G.G., Olsson A.G., Ezekowitz M.D., Ganz P., Oliver M.F., Waters D., Effects of atorvastatin on early recurrent ischemic events in acute coronary syndromes: the MIRACL study: a randomized controlled trial. Jama, 285 (13), 1711-1718, 2001.

43. Moteiv Corporation. https:// www. scribd. com/ document/ 249935619/Tmote-Sky-Datasheet, Yayın tarihi Haziran 2, 2006. Erişim tarihi Ekim 2, 2016.

44. Crossbow Technology. https:// www. eol.ucar .edu//isf//facilities//isa//internal//CrossBow//Doc//MPR -IB_ Series_User_ Manual_ 74 30 -0021-05_A.pdf. Yayın tarihi Aralık 2003. Erişim tarihi Ekim 21, 2016.

45. Liu A., Ning P., TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks, Information Processing in Sensor Networks, IPSN'08. International Conference on, Washington-A.B.D, 245-256, 2008.

46. Raza S., Duquennoy S., Höglund J., Roedig U., Voigt T., Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN, Security and Communication Networks, 7 (12), 2654-2668, 2014.

47. Zhao K. ve Ge L., A survey on the internet of things security, Computational Intelligence and Security (CIS), 2013 9th International Conference on, Leshan-Çin, 663-667, 2013.

48. Granjal J., Monteiro E., Silva J.S., Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tutorials, 17 (3), 1294-1312, 2015.

49. Lupu T.G., Rudas I., Demiralp M., Mastorakis N., Main types of attacks in wireless sensor networks, WSEAS International Conference. Proceedings, Recent Advances in Computer Engineering, Budapeşte-Macaristan, 180-185, 2009.

50. Diaz P.A., ValleCarcamo G.D. ve Jones D., Internal Vs. External Penetrations: A Computer Security Dilemma, Proceedings of the 2010 International Conference on Security and Management, 2010.

51. Le A., Loo J., Lasebae A., Vinel A., Chen Y., Chai M. The impact of rank attack on network topology of routing protocol for low-power and lossy networks, IEEE Sens. J., 13 (10), 3685-3692, 2013.

52. Jing Q., Vasilakos A.V., Wan J., Lu J., Qiu D., Security of the Internet of Things: perspectives and challenges, Wireless Networks, 20 (8), 2481-2501, 2014.

53. Borgia E., The Internet of Things vision: Key features, applications and open issues, Comput. Commun., 54, 1-31, 2014.

54. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Commun. Surv. Tutorials, 17 (4), 2347-2376, 2015.

55. Alabaa F.A., Othmana M., Hashema I. A. T., Alotaibib F., Internet of Things security: A survey, Journal of Network and Computer Applications, 88, 10-28, 2017.

56. Wong K.H.M, Zheng Y, Cao J. ve Wang S., A dynamic user authentication scheme for wireless sensor networks, Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on, Taichung, Tayvan, 32-58,5-7 Haziran, 2007.

57. Das M.L., Two-factor User Authentication In Wireless Sensor Networks, IEEE Transactions on Wireless Communications, 8 (3), 1086-1090, 2009.

58. He D., Gao Y., Chan S., Chen C., Bu J., An Enhanced Two-factor User Authentication Scheme In Wireless Sensor networks, Ad hoc and sensor wireless networks, 10 (4), 361-371, 2010.

59. Khan M.K., Alghathbar K., Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks', Sensors, 10 (3), 2450-2459, 2010.

60. Chen T.H., Shih W.K., A robust mutual authentication protocol for wireless sensor networks, ETRI Journal, 32 (5), 704–712, 2010.

61. Yeh H.L, Chen T.H., Liu P.C, Kim T.H., Wei H.W., A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, 11 (5), 4767-4779, 2011.

62. Song R., Advanced smart card based password authentication protocol, Computer Standards and Interfaces, 32 (5), 321-325, 2010.

63. Xu J., Zhu W.T., Feng D.G., An improved smart card based password authentication scheme with provable security, Computer Standards and Interfaces, 31 (4), 723-728, 2009.

64. Sen J., A survey on wireless sensor network security, International Journal of Vommunication Networks and Information Security(IJCNIS), 1 (2), 55-78, 2010.

65. Babar S., Stango A., Prasad N., Sen J. ve Prasad R., Proposed embedded security framework for internet of things (iot). Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, Hindistan, 1-5, 2011.

66. Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E., Wireless sensor networks: a survey, Comput. Networks, 38 (4), 393-422, 2002.

67. The IEEE 802.15.4–2003 Standard. http:// www.ieee802.org/ 15/pub/TG4.html. Yayın tarihi 2003. Erişim tarihi Temmuz 17, 2016.

68. Gutierrez J.A., Naeve M., Callaway E., Bourgeois M., Mitter V., Heile B., IEEE 802.15. 4: a developing standard for low-power low-cost wireless personal area networks, IEEE network, 15 (5), 12-19, 2001.

69. Texas Instruments. CC2538 Powerful System-On-Chip for 2.4-GHz IEEE 802.15. 4, 6LoWPAN and ZigBee Applications. http:// www.ti. com/lit/ds /symlink /cc2538.pdf. Texas Instruments. Yayın tarihi Aralık 2012, Erişim tarihi Haziran 14, 2016.

70. Texas Instruments. Single-Chip 2.4 GHz IEEE 802.15.4 Compliant and ZigBee Ready RF Transceiver. http://www.ti.com/product/cc2420. Yayın tarihi Mart 7, 2013. Erişim tarihi Kasım 3, 2016.

71. Sciancalepore S., Piro G., Boggia G., Grieco L. A., Application of IEEE 802.15.4 security procedures in OpenWSN protocol stack., IEEE Standards Education e-Magazine, 4 (2), 66-77, 2014.

72. Bellare M., Kilian J., Rogaway P., The security of the cipher block chaining message authentication code. J. Comput. Syst. Sci. Int., 61(3), 362-399, 2000.

73. Whiting D., Housley R., Ferguson, N. Counter with CBC-MAC (CCM). http://www.rfc-editor.org/info/rfc3610. Yayın tarihi Eylül 2003, Erişim tarihi Mayıs 14, 2016.

74. Raza S., Duquennoy S., Chung T., Yazar D., Voigt T. ve Roedig U., Securing communication in 6LoWPAN with compressed IPsec. 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barselona-İspanya, 1-8, 2011.

75. Palattella M.R., Accettura N., Vilajosana X., Watteyne T., Grieco L. A., Boggia G., Dohler M., Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutorials, 15 (3), 1389 – 1406, 2013.

76. Thubert P., Objective function zero for the routing protocol for low-power and lossy networks (RPL). https://tools.ietf.org/html/rfc6552. Yayın tarihi Mart 2012. Erişim tarihi Nisan 12, 2016.

77. Atzori L., Iera A., Morabito G., The internet of things: A survey. Computer networks, 54 (15), 2787-2805, 2010.

78. Dohler M., Watteyne T., Winter T., Barthel D., Routing requirements for urban low-power and lossy networks. https://tools.ietf.org/html/rfc5548. Yayın tarihi Mayıs 2009. Erişim tarihi Haziran 10, 2016.

79. Pister K., Thubert P., Dwars S., Phinney T. Industrial routing requirements in low-power and lossy networks. https://tools.ietf.org/html/rfc5673. IETF. Yayın tarihi Ekim 2009. Erişim tarihi Mayıs 12, 2016.

80. Brandt A., Porcu G. Home automation routing requirements in low power and lossy networks. https://tools.ietf.org/html/rfc5826. IETF. Yayın tarihi Nisan 2010. Erişim tarihi Nisan 14, 2016.

81. Martocci J., Vermeylen W., Riou N., Mil P. D. Building automation routing requirements in low power and lossy networks. https://tools.ietf.org/html/rfc5867. IETF. Yayın tarihi Haziran 2010. Erişim tarihi Haziran 11, 2016.

82. Richardson M.C. 6tisch secure join using 6top. https://tools.ietf.org/pdf/draft-richardson-6tisch--

security-6top-05.pdf. Yayın tarihi Kasım 20, 2015. Erişim tarihi Ağustos 10, 2016.

83. Brachmann M., Keoh S.L., Morchon O.G. ve Kumar S.S., End-to-end transport security in the IP-based internet of things, 2012 21st International Conference on Computer Communications and Networks (ICCCN), Münih-Almanya, 1-5, 2012.

84. Raza S., Voigt T. ve Jutvik V., Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, Proceedings of the IETF workshop on smart object security, İspanya, 2012.

85. Garcia M., Kumar S., Dijk E., Keoh S. DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs). https:// tools. ietf. org/ id/ draft –keoh -dtls-multicast-security-00.txt. Yayın tarihi Temmuz 6, 2013. Erişim tarihi Eylül 12, 2016.

86. Hummen R., Ziegeldorf J.H., Shafagh H., Raza S. ve Wehrle K., Towards viable certificate-based authentication for the internet of things, Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy, Macaristan, 37-42, 19-19 Nisan, 2013.

87. Zheng T., Ayadi A. ve Jiang X., TCP over 6LoWPAN for industrial applications: An experimental study. New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on, Fransa, 1-4, 7-10 Şubat, 2011.

88. Braun T., Voigt T. ve Dunkels A., TCP support for sensor networks, 2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services, Avusturya, 162-169, 24-26 Ocak, 2007.

89. Jung W., Hong S., Ha M., Kim Y.J., Kim D., SSL-based lightweight security of IP-based wireless sensor networks, Advanced Information Networking and Applications Workshops, 2009. WAINA'09. International Conference on, Birleşik Krallık, 1112-1117, 26-29 Mayıs, 2009.

90. Gupta V., Wurm M., Zhu Y., Millard M., Fung S., Gura N., Shantz S.C., Sizzle: A standards-based end-to-end security architecture for the embedded internet, Pervasive Mob. Comput., 1 (4), 425-445, 2005.

91. Cronin M.J., Smart products, smarter services: strategies for embedded control. Cambridge University Press, New York, A.B.D, 2010.

92. Rahman R.A., Shah B., Security analysis of IoT protocols: A focus in CoAP. 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), IEEE, Umman, 1-7, 15-16 Mart, 2016.

93. Shelby Z., Vial M., Koster M., Groves C. Reusable Interface Definitions for Constrained RESTful Environments. Internet Engineering Task Force (IETF). https://tools.ietf.org/html/draft-ietf-core-interfaces-06. Yayın tarihi Ekim 28, 2016. Erişim tarihi Kasım 15, 2016.

94. Kumar S., Shelby Z., Keoh S. Profiling of DTLS for CoAP-based IoT Applications. https:// tools.ietf.org /id/draft-keoh-dtls-profile-iot-00.txt. Yayın tarihi Haziran 12, 2013. Erişim tarihi Mart 23, 2016.

95. Yegin A., Shelby Z., CoAP Security Options. http://tools.ietf.org/html/draft-yegin-coap-security-options-00, IETF, Yayın tarihi Ekim 14, 2012. Erişim tarihi Temmuz 3, 2016.

96. Granjal J., Monteiro E., Silva J.S., Application-layer security for the WoT: extending CoAP to support end-to-end message security for internet-integrated sensing applications, International Conference on Wired/Wireless Internet Communication, Tsaoussidis, Springer-Verlag Berlin, Rusya, 140-153, 2013.

97. Wang W., Zhu L., Wang L., Yu F. CoAP Option Extensions: Profile and Sec-flag. Internet Engineering Task Force (IETF). https://tools.ietf.org/html/draft-wang-core-profile-secflag-options-00. Yayın tarihi Temmuz 2, 2012. Erişim tarihi Haziran 22, 2016.

98. Kent S., Seo K. Security architecture for the internet protocol. IETF. https://tools.ietf.org /html/ rfc4301. Yayın tarihi Aralık 2005. Erişim tarihi Mart 20, 2016.

99. Kent S., Atkinson R. RFC 2402: IP authentication header. Network Working Group. https://tools.ietf.org /html/rfc2402.Yayın tarihi Kasım 1998. Erişim tarihi Mayıs 10, 2016.

100. Kent S., Atkinson R. IP Encapsulating Security Protocol (ESP). RFC 2406. https://tools. ietf.org/ html/ rfc2406.Yayın tarihi Kasım 1998. Erişim tarihi Haziran 3, 2016.

101. Riaz R., Kim K.H., Ahmed H.F., Security analysis survey and framework design for ip connected lowpans. 2009 International Symposium on Autonomous Decentralized Systems. Yunanistan, 1-6, 23-25 Mart, 2009.

102. Granjal J., Silva R., Monteiro E., Silva J.S., Boavida F., Why is IPSec a viable option for wireless sensor networks. 2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, A.B.D, 802-807, 29 Aralık-2 Ocak, 2008.

103. Granjal J., Monteiro E., Silva J.S., Enabling network-layer security on IPv6 wireless sensor networks. Global Telecommunications Conference (GLOBECOM 2010), A.B.D, 1-6, 6-10 Kasım, 2010.

104. Granjal J., Monteiro E., Silva J.S., Network-layer security for the Internet of Things using TinyOS and BLIP. Int. J. Commun. Syst., 27 (10), 1938-1963, 2014.

105. Kim E., Kaspar D. Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Engineering Task Force (IETF). https://tools.ietf.org/html/rfc6568. Yayın tarihi Nisan 2012. Erişim tarihi Mayıs 25, 2016.

106. Hummen R., Wirtz H., Ziegeldorf J. H., Hiller, J., Wehrle K., Tailoring end-to-end IP security protocols to the Internet of Things. 2013 21st IEEE International Conference on Network Protocols (ICNP), Almanya, 1-10, 7-10 Ekim, 2013.

107. Santesson S., Myers M., Malpani A., Galperin S., Adams C. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP. RFC 6960, Internet Engineering Task Force. https:// tools.

ietf.org/html/rfc69680. Yayın tarihi Haziran 2013. Erişim tarihi Ağustos 12, 2017.

108. Transport Layer Security (TLS) Extension Definitions. IETF. https://tools.ietf.org/ html/rfc6066. Yayın tarihi Ocak 2011, Erişim tarihi Kasım 2, 2016.

109. Symantec. IoT devices being increasingly used for DDoS attacks. https:// www.symantec .com /connect /blogs/ iot-devices- being-increasingly -used-ddos-attacks. Yayın tarihi Eylül 22, 2016. Erişim tarihi Kasım 17, 2016