IOT Tabanlı Akıllı Tarım Sisteminde Kullanılan Kablosuz Sensörlerinin Güvenliğinin İncelenmesi ve Saldırılara Karşı Gerçek Ortamdaki Etkisi

Bu tez Bilgi Güvenliği Mühendisliği Yüksek Lisans Programında
Tezli Yüksek Lisans Tez Önerisi Programının bir koşulu olarak

Murat KATIRCIOĞLU
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

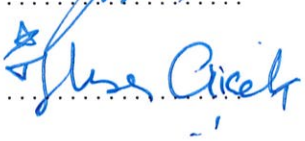
İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Ensar Gül ..... 
(Tez Danışmanı)

Prof. Dr. Nizamettin Aydın ..... 

Dr. Öğretim Üyesi İhsan Çiçek ..... 

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 29.08.2019

MÜHÜR/İMZA: 

Yazarlık Beyanı

Ben, Murat KATIRCIOĞLU, başlığı, 'IOT Tabanlı Akıllı Tarım Sisteminde Kullanılan Kablosuz Sensörlerinin Güvenliğinin İncelenmesi ve Saldırılara Karşı Gerçek Ortamdaki Etkisi' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans Tez Önerisi derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: 

Tarih: 23.08.2019

E=mc2

Proof of Albert Einstein

IOT Tabanlı Akıllı Tarım Sisteminde Kullanılan Kablosuz Sensörlerinin Güvenliğinin İncelenmesi ve Saldırılara Karşı Gerçek Ortamdaki Etkisi

Murat KATIRCIOĞLU

Öz

Sürekli artmakta olan dünya nüfusunun sürdürülebilirliğini sağlamak için birçok bilimsel çalışma yapılmaktadır. Teknolojideki gelişmelere paralel olarak, IoT (Nesnelerin interneti) teknolojisi artan küresel nüfusun gıda taleplerini karşılamada önemli bir rol oynayacaktır. Tarlalara yerleştirilen algılayıcılar, çiftçilerin bölgelerde bulunan topografya ve kaynakların yanı sıra, dijital nem ve sıcaklık, toprak nemi, toprak sıcaklığı, gövde çapı, meyve çapı, yağmur göstergesi ve güneş ışını vb. gibi değişkenleri ayrıntılı şekilde elde etmelerini sağlamaktadır. Geniş arazilerde birçok bireysel aygıt yerine WSN kurularak daha az maliyetle daha yönetilebilir sistem kurulabilir. Bu tezde akıllı tarımda kullanılan IEEE 802.15.4, 6LoWPAN protokolü ve üzerinde yapılan ataklar incelenmiştir. Laboratuvar ortamında IEEE 802.15.4 ve 6LoWPAN kablosuz ağı kurulmuştur. Bu kablosuz ağda ağ haberleşmesi dinlenmiştir. Kablosuz Ağ sinyalleri uygun yazılım ve donanım vasıtasıyla kaydedilip bilgilerin analizi yapılmış atak yapmak için bilgiler elde edilmiştir. Elde edilen bilgilerle atak yapılarak 6LoWPAN kablosuz ağının Ipv6 iletişimi kesilmiştir. 6loWPAN üzerinde çalışan Ipv6 üzerinden DoS atak yapılmıştır. Ipv6 haberleşmesinin kesilmesi ile ilgili açık kaynak işletim sistemi üzerinde atak ile ilgili kural girilmiş ve gerçek hayat senaryoları üzerinde çalışma yapılmıştır.

Anahtar Sözcükler: 802.15.4 destekli algılayıcı, DoS Saldırısı in IEEE 802.15.4

Investigation of Wireless Sensor Security Used in IoT Based Intelligent Agricultural System and Its Impact on Real Environment

Murat KATIRCIOĞLU

Abstract

In order to ensure the sustainability of the ever increasing world population, many scientific studies are being conducted. Meanwhile with the developments in technology, IoT (Internet of Things) technology will play an important role in meeting the food demands of the growing global population. Sensors placed in the fields obtains farmers' topography and resources in the region in detail, as well as variables like digital humidity and temperature, soil moisture, soil temperature, body diameter, fruit diameter, rain gauge and sunlight and so on. such as in detail. In large areas, a more manageable system can be installed at a lower cost by installing WSN instead of many individual devices. In this thesis, IEEE 802.15.4, 6LoWPAN protocol used in smart agriculture and attacks on it was examined. IEEE 802.15.4 network and 6LoWPAN network were established in laboratory environment. In this wireless network, network communication was listened. Wireless Network signals were recorded by means of appropriate software and hardware, information was analyzed and information was obtained to make the attack. DoS attack was made on ipv6 running on 6loWPAN. . An attack rule is applied on the open source operating system for interrupting IPv6 communication and real-life scenarios have been studied.

Key Words: 802.15.4 Sensors, DoS Attacks in IEEE 802.15.4

Teşekkür

Tez danışmanlığımdan ve desteklerinden dolayı Sayın Prof. Dr. Ensar GÜL'e teşekkür ve şükranlarımı sunarım.

Tezin yazımı sürecinde benden desteğini esirgemeyen Fatih TALI ve Mesut BAYRAK'a teşekkürlerimi sunarım

İçindekiler

Şekil Listesi

- IoT Nesnelerin interneti
- WSN Kablosuz Algılayıcı Ağı
- M2M Cihazdan Cihaza Erişim
- BT Bilgi Teknolojileri
- BI İş Zekası
- BTK Bilgi Teknolojileri ve İletişim Kurumu
- RFID Radyo Frekanslı Tanıma
- DoS Servis Engelleme
- DDoS Dağıtık Hizmet Engelleme
- ICMP İnternet Kontrol Mesajlaşma Protokolü
- LPWAN Düşük Güç Geniş Alan Ağı
- IPSP İnternet Profil Destek Protokolü
- RPI Raspberry Pi RPI-1: 1. Raspberry Pi 3 B+
- RPI-2 2.Raspberry Pi 3 B+
- SNMP Basit Ağ Yönetim Protocolü

Bölüm 1

Giriş

1.1 Nesnelerin İnterneti (IoT) Tarihçesi ve Gelişimi

Orijinal adı internet of Things (IoT) olan ''Nesnelerin interneti" teknoloji öncüsü Kevin Ashton tarafından ilk kez 1999 yılında Procter&Gamble şirketi için hazırlanan sunumda kullanıldı. Gelişen teknolojiler sayesinde insanın bilgisayarlar ya da taşınabilir mobil araçlarla internete bağlantısını sağlanmıştır.[1] Milyonlarca cihazı, farklı protokolleri ve farklı platformlarla bir altyapıya bağlayan karmaşık bir ağ üzerine kurulu olan IoT ana vizyonu, gerçek, sayısal ve sanal olan akıllı bir dünya kurulmasıdır.. Enerji, sağlık, ulaşım, şehirler, sanayi, binalar, tarım ve günlük hayatımızın diğer alanlarına daha fazla hızlı akıllı ortamlar yaratmaya çalışmaktadır. Beklenti, sadece herhangi bir "yol", "ağ" ve "herhangi bir hizmet" aracılığıyla, "herhangi bir zamanda" ve "herhangi bir yerde" değil, aynı zamanda "herhangi bir şey" ve "herhangi birini" kullanarak, bilgiye erişimi mümkün kılan milyonlarca akıllı ağ adasının bir araya getirilmesidir. [2] Nesnelerin interneti, potansiyel faydalarını gerçekleştirirken farkında olmadan önemli zorluklar oluşmaktadır. Kablosuz veya internet'e bağlı cihazların, gözetlenme endişeleri ve gizlilik ile ilgili sorunları oluşmaya başlamıştır. İnternet ortamında bulunan cihazların artışı ile IPv6'ya geçiş zorunluluğu doğmaktadır. Bazı ülkeler ve bazı kuruluşların bu geçişi zorlu olmuştur. Bununla birlikte, pratik olarak IPv6 ve bazı M2M dağıtımlarında, bir projedeki tüm ortakların geçişi gerçekleştirmesini gerektiren bir sınırlama faktörünü bile kanıtlayabilir. Örneğin, ortak üniversitelerin bir WSN projesini uygulayabilmeleri için öncelikle IPv6'ya geçmeleri gerekmektedir. 2009 yılında Türkiye Cumhuriyeti Hükümeti, IPv6'ya geçişle ilgili BTK' nu görevlendirmiştir. [3] IPv4'ten IPv6'ya geçiş, internet adresi sorunlarının uzun vadede çözülmesine yardımcı olacaktır, ancak milyarlarca nesnenin kullandığı WSN' nün de IPv6 ya geçmesi gerekmektedir.

Gizlilik ve güvenlik, büyük ölçekli IoT uygulamasında en önemli (ve yakından ilişkili) sorunlardan ikisidir. Gizlilik, güvenlik ve anonimlik, birbiriyle ilişkili, ancak ayrı kavramlardır. Gizlilik (gizlilikle ilgili), hedeflenen hedef kitleyi veri için tanımlama yeteneğidir. Anonimlik, çoğu insan için bilinmeyen bir nitelik veya durumdur. Güvenli bir sistem zayıflıktan veya zayıflıktan kurtulmuş bir sistemdir. Bir güvenlik ihlali, indirilen verilere ve daha sonra nasıl kullanıldığına bağlı olarak mahremiyet kaybına neden olabilir veya olmayabilir. BT'leri düşük gelirli bütçeler için iletişim ve gelirle ilgili faaliyetler için daha büyük fırsatlar sunarken, ilişkili risklerin (mahremiyetin kaybı vb.) dikkate alınması gerekmektedir.[4] Yeterli güvenlik olmazsa, davetsiz misafirler IoT sistemlerine ve ağlarına girebilir, kullanıcılar hakkında potansiyel olarak hassas kişisel bilgilere erişebilir ve yerel ağlara ve cihazlara saldırmak için savunmasız cihazları kullanabilir ve böylece gizliliklerini ihlal edebilir. Gizlilik ve anonimlik ile ilgili başka bir konu, bağlı cihazların adres alanıdır. Bir ağda kullanılan tanımlayıcıların başka bir ağda anlaşılabilir ve / veya kullanılabilir (yani birlikte çalışabilir) olması gerekir. İnternette her şeyden önce, tüketiciler çeşitli nesneleri farklı türlerde kullanmak isteyeceklerdir. Bu sisteme doğru bir şekilde tercüme edilebilecek algılayıcılar ve farklı ağlar tarafından tanınabilecek nesnelerin kimliklerine ihtiyaç duyacaktır. Güvenlik açığı olan IoT cihazları ve servisleri siber atak için potansiyel giriş noktaları olarak kullanılabilir ve veri akışlarını yetersiz korunarak kullanıcı verilerini hırsızlığa maruz bırakabilir. IoT cihazlarının birbirine bağlı doğası, çevrimiçi bağlı iyi bir şekilde korunmayan, korunan cihazın potansiyel olarak internet'in küresel olarak güvenliğini ve esnekliğini etkilemesi anlamına gelir. Bu zorluk, homojen IoT cihazların kitlesel ölçekte dağıtımı, bazı cihazların diğer cihazlara otomatik olarak bağlanma yeteneği ve bu cihazların güvenli olmayan ortamlarda üretilmesi olasılığı gibi diğer faktörlerle güçlenir. Kullanıcıları ve internet'i potansiyel zararlara maruz bırakmamalarını sağlama yükümlülüğünde olunması gerekmektedir. Buna göre, sorunların ölçeği ve karmaşıklığına çok uygun olan IoT güvenlik sorunlarına etkili ve uygun çözümler geliştirmek için işbirliğine dayalı bir yaklaşım gerekmektedir. Gizlilik: Nesnelerin interneti de diğer her şey gibi gizliliğe önem vermelidir. Gizlilik kullanıcı beklentisiyle alakalı bir durumdur. Güvenli bir iletişimin sağlanabilmesinin gerekli olduğu durumlarda IoT'ler de şifreleme özellikleri ile gizliliği sağlayabilir. Birlikte Çalışabilirlik / Standartlar: Ürün ve hizmetler arasında tam birlikte çalışabilirlik her zaman mümkün veya gerekli olmasa da entegrasyon esnekliği, yüksek sahiplik maliyeti ve satıcıya bağlı kalma konusunda endişe varsa, alıcılar IoT ürün ve hizmetlerini satın almak konusunda kararsız kalabilirler. Kötü tasarlanmış ve yapılandırılmış IoT cihazları bağlandıkları ağ kaynakları ve geniş bant internet için olumsuz sonuçlar doğurabilir. Uygun standartlar, referans modelleri ve en iyi uygulamalar, IoT sistemlerinin bozulmasına yol açabilecek cihazların çoğalmasını da engellemeye yardımcı olacaktır. IoT cihazları ve hizmetleri (internet Protokolü gibi) için teknik yapı taşları olarak jenerik, açık ve yaygın olarak kullanılabilen standartların kullanılması, daha fazla kullanıcı avantajı, yenilik ve ekonomik fırsatı destekleyecektir.

Yasal, Düzenleyici ve Haklar: IoT cihazlarının kullanımı birçok yeni yasa ve yasal soruyu beraberinde getirmekte, ayrıca internet üzerindeki yasal sorunları da güçlendirmektedir. Sorular kapsam dahilindedir ve IoT teknolojisindeki hızlı değişim hızı, ilgili politika, yasal ve düzenleyici yapıların uyum sağlama yeteneğini sık sık aşmaktadır. Ayrıca, IoT cihazları tarafından toplanan veriler bazen kötüye kullanıma açıktır, potansiyel olarak bazı kullanıcılar için ayrımcı sonuçlar doğurmaktadır. Gelişen Ekonomi ve Kalkınma Sorunları: Nesnelerin interneti, gelişmekte olan ekonomilere sosyal ve ekonomik faydalar sağlamak için önemli bir avantaj sunar. Bu, diğerleri arasında sürdürülebilir tarım, su kalitesi ve kullanımı, sağlık bakımı, sanayileşme ve çevre yönetimi vb. gibi alanları içerir. Bu nedenle IoT, Birleşmiş Milletler Sürdürülebilir Kalkınma Hedeflerine ulaşmada bir araç olarak söz sahibidir. IoT zorluklarının geniş kapsamı, sanayileşmiş ülkelere özgü olmayacaktır. Gelişmekte olan bölgelerinde IoT' nin potansiyel faydalarını gerçekleştirmek için yanıt vermesi gerekecektir. Ayrıca, altyapı hazırlığı, pazar ve yatırım teşvikleri, teknik beceri gereksinimleri ve politika kaynakları dahil olmak üzere, az gelişmiş bölgelerdeki uygulamaların kendine özgü ihtiyaçları ve zorlukları ele alınmalıdır. Nesneler, çevreleri ve insanlar arasındaki ilişkiler daha sıkı bir şekilde iç içe geçtikçe devrimci, tamamen bağlantılı "akıllı" bir dünya sunmayı vaat ediyor. Ancak, bireylerin, toplumun ve ekonominin gerçekleştirilebileceği potansiyel faydalar için IoT ile ilgili konular ve zorlukların dikkate ele alınması gerekmektedir. Nihayetinde, Nesnelerin interneti'nin faydalarını en üst düzeye çıkarmaya yönelik çözümler, riskleri en aza indirirken, olası tehlikelere karşı IoT' nin vaatlerini yerine getiren kutuplaşmış bir tartışmaya girerek bulunamaz. Aksine, ileriye yönelik en etkili yolları çizmek için bir dizi paydaşa bilgi akışı, diyalog ve işbirliği içerecektir. [5]

Bu çalışmada farkındalık olması için tarımda kullanılan IoT cihazlarının WSN bağlantılarını tehdit eden/edebilecek DoS ataklarını incelenecektir. DoS atakları ile IoT ağının haberleşemez hale getirilmesi amaçlanmaktadır. İncelenecek konu tek bir yerden yapılan atak şeklindedir. Bu çalışmada tarımda kullanılan IoT ağındaki DoS atağı incelenmiş ve etkisi ile nasıl bir uyarı sistemine dahil edilmesiyle ilgili araştırma yapılmıştır. Bu çerçevede Bölüm 2' de IoT' nin akıllı tarımdaki konumu, Bölüm 3' de IoT 'de kullanılan kablosuz algılayıcılar, Bölüm 4' de 6lowPan DoS atakları, Bölüm 5' de IoT 6Lowpan ağının ve atak sisteminin kurulması, Bölüm 6' da çalışmamla günümüz dünyası ile analizlerin yapılması anlatılacaktır.

Bölüm 2

IOT'nin Akıllı Tarımdaki Konumu

2.1 IoT'nin Akıllı Tarımdaki Konumu

Yıllar boyunca tarım, geleneksel yöntemlere sıkı sıkıya bağlı kalmaya devam eden bir endüstri olmuştur. Geleneksel tarım yöntemleri yavaş yavaş tüketilmekte ve artan gıda gereksinimlerine ayak uydurabilmek için tarımın yeni ve yenilikçi yöntemlerle modernize edilmesi zorunlu hale gelmiştir. Tarım ve Tarım endüstrisi, verimliliği artırmak ve kaynakları daha iyi tahsis etmek için yenilikçi fikirlere ve teknolojiye ihtiyaç duymaktadır. [6] Peki, akıllı tarım nedir? Akıllı tarım, kitleler için temiz ve sürdürülebilir bir şekilde gıda yetiştirmenin Modern BİT (Bilgi ve İletişim Teknolojileri)'nin tarıma uygulanmasıdır. IoT tabanlı akıllı tarımda, algılayıcı alanını (ışık, nem, sıcaklık, toprak nemi, vb.) kullanarak ürün alanını izlemek ve sulama sistemini otomatikleştirmek için bir sistem kurulmuştur. Çiftçiler saha koşullarını her yerden izleyebilir. IoT tabanlı akıllı tarım, geleneksel yaklaşımla karşılaştırıldığında oldukça verimlidir. Nesnelerin interneti tarım sektörünün yaygınlaşması ile üretim süreci boyunca makineler birbirleriyle iletişimde kalacak ve üreticiye eş zamanlı bilgiler sunabilir hale gelecektir. [7] IoT tabanlı akıllı tarımın uygulamaları sadece geleneksel, büyük çiftçilik operasyonlarını değil, aynı zamanda organik tarım, aile çiftçiliği (karmaşık veya küçük alanlar, özel sığırlar ve / veya kültürler) gibi tarımda diğer büyüyen veya ortak eğilimleri yükseltmek için de yeni araçlar olabilir. Mahsul verimini artırmak ve israfı azaltmak için, tarım ve çiftlik endüstrilerinin, ileriye doğru hareket eden IoT'ye bel bağlanması gereklidir Geleceğin tarımı daha verimli olmalı ve aynı zamanda çevre kirliliğini azaltmalıdır. GPS hizmetleri, algılayıcılar ve büyük veriler gelecek yıllarda temel tarım araçları haline gelecektir. Çevresel konular açısından, IoT tabanlı akıllı tarım, daha verimli su kullanımı veya girdilerin ve tedavilerin optimizasyonu dahil olmak üzere büyük faydalar sağlayabilir. Tarımda her zaman gündelik hava olayları ve uzun vadeli iklim değişikliği gibi

öngörülemeyen zorluklarla karşı karşıya kalacak olsa da çiftçilere günlük çalışmalarında daha kesin karar vererek aynı veya daha küçük kaynaklardan daha verimli ve yüksek mahsul verimi sağlayabilirler. Hassas tarımsal hizmetler, mantar ilaçları, zirai (tarımsal) ilaçlar ve organik gübrelerin doğru tip ve miktarlarını doğru zamanlarda uygulayarak salgın hastalıklarla mücadele etmek, bitkileri sadece gerekli miktarda suyla sulayarak verimli su tüketimi sağlamak için araçlar sağlamaktadır. [8] Akıllı tarım sistemlerinde toprak veriminin artması ve ürünün daha sağlıklı üretilmesi en büyük amaçtır. İleri teknolojiyle toprakta bulunan ağır metaller e benzer istenmeyen madde analizi, uzaktan operasyon ve kumanda edebilme yeteneği, ürünlerin çürümeden hasat edilebilme imkânı, kaynak kullanımının en aza indirilerek hem israfı ve maliyeti hem de çevre kirliliğini azaltması sağlanır. [3] Akıllı tarımla birlikte çiftçilikte önemli kayıpların azalmasında yardımcı olabilir, veri toplama ve izleme sorunlarını çözebilir ve iklim değişikliklerini azaltabilir. Uzun vadede Dünya'nın karşı karşıya kaldığı sorunların aciliyeti nedeniyle akıllı tarım kullanımına biran evvel geçmekten başka çaremiz kalmamaktadır. IoT tarım uygulamaları, çiftçilerin anlamlı veri toplamasını mümkün kılmaktadır. [9]

Akıllı tarımın amacı, sadece algılayıcılardan veri üretmek değil, aynı zamanda gerekli tepkileri değerlendirme için bu verileri analiz etmektir. Akıllı tarım uygulama alanları arasında çiftlik aracı izleme, hayvan izleme saha gözlem ve depolama izleme bulunmaktadır. Akıllı tarımda veri desteği ile tarımsal teknolojiler; algılayıcılar, haberleşme, veri toplama ve birleştirme, büyük veriyi analiz etme, Bilgi Teknolojisini ve mobil platformları içerir. Bilgi Teknolojisinin görevi, kayıpları azaltmak, iş verimliliğini artırmak ve kaynak yönetimini optimize etmek için üretim döngüsünün tüm aşamalarının otomasyonunu en üst düzeye çıkarmaktır. Hassas tarım, tarım alanında IoT'nin yaygın uygulamalarından biridir ve çok sayıda kurum ve kişi bu tekniği dünya çapında desteklemektedir.

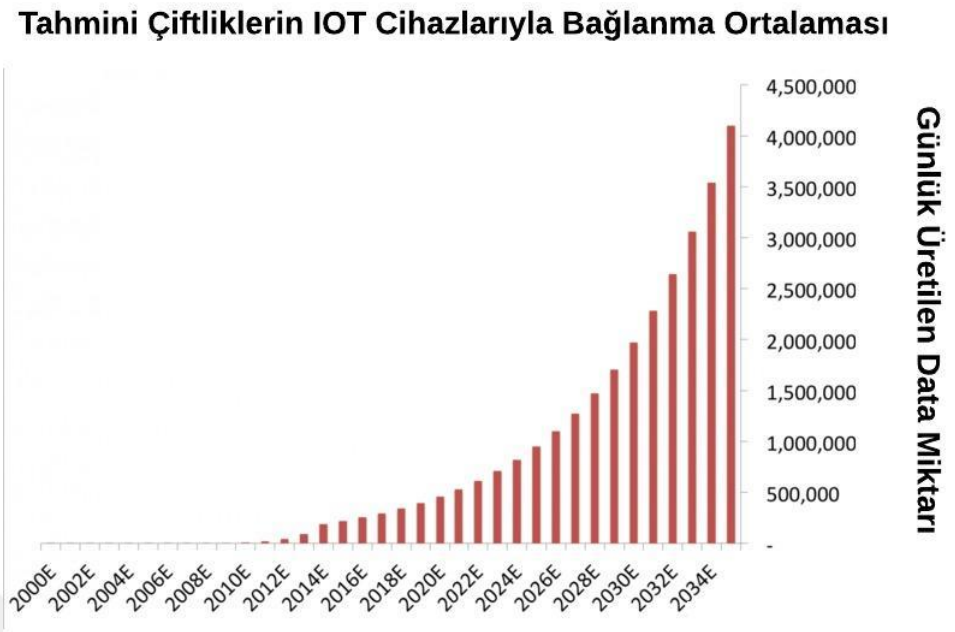
Akıllı tarımda, kızılötesi kameralar ve IHA vb. ekipmanlar kullanılmaktadır. Bağlı cihazlarla gerçek zamanlı izleme ile temel istenen veriler toplanmaya başlanır. Çiftçi tarafından bu verilerin anlamlı halde izlenmesini sağlanabilir. Önümüzdeki birkaç yıl, bu ve diğer hassas tarım teknolojilerinin kullanımının artacağını tahmin edilmektedir. Business Insider'ın araştırma hizmeti olan Business Intelligence (BI), tarımda kullanılan IoT cihazlarının sayısının 2015 yılında 30 milyon iken 2020 yılında 75 milyona yükseleceğini ve bunun da yıllık %20 büyüme oranına ulaşacağını öngörüyor. Şekil6 [10] Örneğin, tarlaya yerleştirilen bir algılayıcı, çiftçilerin bölgedeki topografya ve kaynakların yanı sıra, toprak asitliği ve sıcaklık gibi değişkenleri ayrıntılı bir halde etmelerini sağlar. Çiftçiler akıllı telefonlarını, ekipmanlarını, bitkilerini ve canlı hayvanlarını uzaktan izlemek için kullanabilir ve aynı zamanda hayvanlarını besleme ve üremeleri hakkında istatistikler elde edebilirler. Bu teknoloji ile, bitkileri ve hayvanlar için istatistiksel tahminler yapmak için kullanabiliriz. [6] Goldman Sachs'a göre hassas çiftçilik çözümlerinin getirilmesi ile ekin verimliliğinde biriken artış %70 oranında büyüyebilir ve 2050 yılına kadar 800

Şekil 2.1: Tarımsal kullanımdaki IoT Cihazların kullanılması

milyar dolar ek ürün getirebilir. Üreticilere ve geliştiricilere hassas çiftçilik çözümleri pazarında 2050'de 240 milyar dolarlık bir artış sağlanacak. Bunlar, hassas ekim, hassas sulama, hassas dölleme, püskürtme, tarla izleme ve küçük tarımsal makine verilerini (otonom makineler dahil) analizi için çözümlerdir.[11] Tarımın geldiğini anlamamız ve IoT'nin sektörde yaygınlaşmasıyla (gizlilik ve siber güvenlik artışı gibi) birlikte ortaya çıkabilecek yeni risklere yanıt vermemiz açısından yararlı olacaktır. İlerleyen bölümlerde sistemlere karşı yapılan servis engelleme ataklarını incelenecektir.

2.2 Akıllı Tarımın Çiftçilere Faydaları

IoT platformu, IoT ekosisteminin ve bütünleşmiş IoT projelerinin merkezi bir unsuru olan yüksek dereceli otomasyon, çok sayıda katılımcı ve bağlı cihazlardır. IoT platformu aracı bir rol oynamaktadır: çözümün aygıtları ve bileşenleri, çeşitli iletişim protokollerini kullanarak çok çeşitli formatlarda veri iletebilir. Platform, tüm cihazların ve sistem öğelerinin ortak çalışmasını sağlar ve kullanıcı uygulamaları ve servislerinin geliştirilmesini mümkün kılar. Kural olarak geliştiriciler, çözümlerin hızlı bir şekilde entegrasyonunu sağlamak için, önceden kurulmuş algılayıcıların ve cihazların, standartların, protokollerin ve analitik araçların mümkün olan en kapsamlı listesini desteklemektedir.



Şekil 2.2: Algılayıcı Düğümlerinden ve Analiz Zincirinden Web Tabanlı Karar Destek Sistemine Veri Toplamalarını Gösteren Değer Zinciri

Tüm bu teknikler akıllı tarım veya hassas tarımı, maliyetleri en aza indirmek ve kaynakları korumakla birlikte mahsülü iyileştirmek için uydu görüntüsü ve diğer teknolojileri (algılayıcılar gibi) kullanarak süreç gözlemlemek ve kaydetmek için kullanılır. Tarımın geleceği, verimi en üst düzeye yükseltmek için tarımdaki büyük verilerin toplanması ve analiz edilmesidir. [11]

Akıllı bir tarım çözümü uyguladığınızda elde edeceğimiz bazı inanılmaz faydalar: Gerçek zamanlı veri ve üretim anlayışı: IoT çiftçilere toprak nemini, üretim seviyelerini ve güneş ışığı yoğunluğunu gerçek zamanlı olarak görselleştirme fırsatı veriyor. Olumsuz durumu düzeltmek için kararlar vermek için fırsatlar sunuyor.

Üretimde artış: Verimli ekin, sulama, pestisit (ilaçlama) uygulaması ve hasat dahil olmak üzere geliştirilmiş ve otomatik ürün işleme, üretim oranlarını doğrudan etkiler.

Daha ucuz işletme maliyetleri: Dikim, arıtma ve hasat işlemlerini otomatikleşince insan hatasını, gereksiz kaynak tüketimini ve genel maliyeti azaltırsınız.

Daha iyi hayvancılık: Sağlık sorunları ve hayvanlarda rekor sürede üreme söz konusu olduğunda, algılayıcılar ve makineler işe yarar. Dahası, geofencing konum takibi, hayvanların izlenmesi ve yönetiminde önemli bir rol oynayabilir. Mükemmel tarla ve tarla değerlendirmesi: Akıllı tarımsal bir çözümün uygulanması, çiftçilerin üretim oranlarını doğru bir şekilde zamanla doğru bir şekilde takip etmelerini sağlayacaktır. Bu da gelecekteki mahsul veriminin ve çiftliğin toplam değerinin ayrıntılı tahminine olanak tanır.

Mükemmel tarla ve tarla değerlendirmesi: Akıllı tarımsal bir çözümün uygulanması, çiftçilerin üretim oranlarını doğru bir şekilde zamanla doğru bir şekilde takip etmelerini sağlayacaktır. Bu da gelecekteki mahsul veriminin ve çiftliğin toplam değerinin ayrıntılı tahminine olanak tanır.

Uzaktan izleme: IoT ile hem yerel hem de ticari çiftçiler, dünyanın neresinde olurlarsa olsunlar çeşitli alanları izleyebilirler. Özünde, önemli kararlar anında ve her yerden yapılabilir. [13] Ayrıca, daha az çevresel ayak izi, daha iyi üretim kalitesi, optimize edilmiş ekipman izleme, vb. gibi akıllı tarımdan elde edeceğiniz diğer büyük avantajlar da vardır. Tarımda, IoT teknolojileri, mahsul üretimini arttırmak, korumak ve optimize etmek, aynı zamanda gıdaların depolanmasını ve dağıtımını geliştirmek için kullanılabilir. Son elli yılda tarımsal üretkenlikte büyüme, kısmen büyük sermaye maliyetlerinden dolayı dünyanın gelişmekte olan bölgelerinde çok daha yavaş olmuştur. Benzer şekilde, tarımın kritik bir yönü olan yerel hava durumu verilerini toplamak ve kullanmak, sınırlı kapsama nedeniyle gelişmekte olan bölgelerde önemli bir sorun olmaya devam etmektedir. Syngenta'nın Kilimo Salama ("Güvenli Tarım") projesi, tarımsal olayları izleyen ve sigorta şirketleriyle olan bağlantıları kolaylaştıran bir hava istasyonudur. Amaç, olumsuz hava koşullarıyla ilgili riskleri azaltmak, böylece çiftçiler için tarımsal yatırımı ve gelişmiş geçim kaynaklarını teşvik ederken çok ihtiyaç duyulan bir güvenlik ağını sağlamaktır. Safaricom'un M-Pesa mobil bankacılık sistemi, endeks sigorta primlerini daha hesaplı bir şekilde tutmak için Kilimo Salama'ya yardım eder ve küçük ölçekli çiftçileri sigorta şirketleri için ticari olarak geçerli bir pazar segmentine dönüştürmeye yardımcı olur.[14] Hindistan'da, Nano Ganesh, mikro sulama pompalarını uzaktan kontrol edebilen, küçük çiftliklerde kullanılmak üzere tasarlanmış düşük maliyetli bir çözümdür. Ülke genelinde, tarımsal sulama için yaklaşık 25 milyon su pompası kullanılmaktadır. Bu pompaların çoğu, yağmur suyu koşullarına, elektrik mevcudiyetine ve ürün ihtiyaçlarına göre elle çalıştırılmaktadır. Ortalama küçük ölçekli çiftçi için, bu faktörlerin günden güne değişkenliği, zaman, işçilik ve yakıt maliyetleri açısından ekstra yükler yaratır. Birçok durumda çiftçilerin pompalarına hane halkları erişmek için zor şartlar altında uzun mesafeleri kat etmesi gerekir. Nano Ganesh ünitesi, sulama pompasına takılarak çalışır ve bir çiftçinin basit özellikli telefonundan (2G cep telefonları) temel komutlarla pompayı açıp kapatabilen sistem haline getirilmiştir. Çiftçi, aynı zamanda pompadaki elektriğin bulunup bulunmadığını ve pompanın yakınında su bulunabileceğini de kontrol edebilir (ek bir su algılayıcıile). Ağustos 2014'e kadar, Hindistan'daki yaklaşık yirmi bin çiftçi Nano Ganesh'den faydalanmıştı. Çin, tarımsal üretimi geliştirmek için IoT teknolojilerini uygulamada büyük adımlar atıyor. Tarımsal üretimi artırmak için sera uzaktan izleme, otomatik damla sulama ve süt kaynağı güvenliği bilgi yönetimi dahil olmak üzere çeşitli bilgi tabanlı uygulamalar geliştirilmiştir. Sincan'da "Tarım için Nesnelerin interneti" projesi, tarımsal seraların kablosuz olarak izlenmesini kullanıyor. Kablosuz su

kayağı damla sulama, 2011 yılından beri su kalitesini izlemek ve tatlı su kültüründe su tasarrufu sağlamak için kullanılmaktadır. Ek örnekler, hayvanların izlenmesi için RFID etiketlerinin kullanımını içerir; bu, bireysel hayvanlar için daha kişiselleştirilmiş bakım yapılmasını sağlar. Sri Lanka ve Ruanda'daki çay tarlalarında, toprak neminin yanı sıra karbon, azot, potasyum, kalsiyum, magnezyum ve pH seviyelerini izlemek için WSN'ler kullanılmaktadır. algılayıcılar ve bağlantı modülleri güneş panelleri ile beslenir ve veriler kablosuz olarak iletilir. [15] Türkiye de akıllı tarım ile ilgili örnek projeler bulunmaktadır. Örnek:

Türkiye de akıllı tarım ile ilgili örnek projeler bulunmaktadır.

1. Yerli Otomatik Traktör Dümenleme ve Kontrol (OTAK) Sisteminin Geliştirilmesi Projesi: Bu teknoloji ile, istenilen arazi profiline bağlı olarak, otomatik kontrol sağlanmış ve tamamen yerli bir otomatik dümenleme sistemi prototipi oluúturulmuştur.

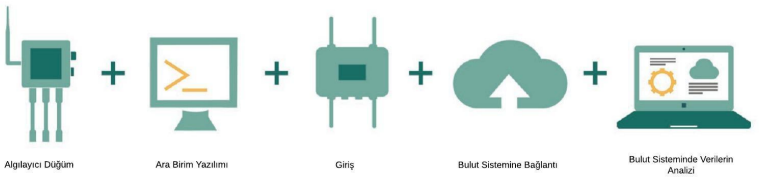
2. Çiftlik Yönetim Sistemi Geliştirilmesi Projesi: Tarım araçları üzerindeki uluslararası ISO 11783 Standart arayüzünde toplanan mesajların, telsiz linki üzerinden uzak mesafeye aktarılarak haberleşmesine, toplanan verilerin harita üzerinde işlenmesine, tarihsel olarak görüntülenmesine ve analiz edilmesine imkan sağlayacak yazılım geliştirilmiştir.

3. İnsansız Hava Aracı ile Görüntü Görüntüleme Temelli Hassas Tarım Uygulamaları Projesi: ASELSAN'ın ARI-1 Döner Kanatlı İnsansız Uçan Sistemi ile toprak, kuraklık, gübre durumu, hasat tahmini, rekolte hesabı ve farklı ürünler için bir kütüphane oluşturulmasına yönelik altyapı kurulacaktır. Altyapı kurulmasıyla, tarım sigortalarına yönelik hasar tespit çalışmalarında da kullanım imkanları doğabilecektir[16].

2.3 Akıllı Tarım Kavramı ve Faydaları

Hassas tarım, diğer endüstrilerde kullanımı iyi olan sensör teknolojilerinden yararlanmıştır. Akıllı Tarım ile ilgili olarak özel algılayıcılar ile, uzak sitelerden kaynaklanan toprak ve ürün davranışı, hayvan davranışları, makine durumu, depolama tankı ve bina dışı durumlar ile ilgili verileri toplar ve anlamlı hale getirilerek çiftçinin anlayacağı duruma getirilmektedir. Tüm M2M uygulamaları için, BT sistemleri verileri toplar, harmanlar, analiz eder ve son kullanıcı tarafından alınan bilgiye uygun bir cevap verecek şekilde sunar. Çiftçiler ve yetiştiriciler için, ilgili çiftçilik türüne bağlı olarak, özel algılayıcılar, toprak ve ürün davranışı, hayvan davranışı, makine durumu, depolama tankı

ve uzak sitelerden kaynaklanan müştemilat durumu ile ilgili verileri toplar. Bu, izleme ve analitik için IT sistemlerine iletilir. Analitiğin sonuçları not edilir ve en uygun gelecekteki kararları ve eylemleri alarak alanda neler olduğuna cevap vermek için kullanılır. Algılayıcı Düğümlerinden ve Analiz Zincirinden Web Tabanlı Karar Destek Sistemine Veri Toplanmasını Gösteren Değer Zinciri



Şekil 2.3: Algılayıcı Düğümlerinden ve Analiz Zincirinden Web Tabanlı Karar Destek Sistemine Veri Toplamalarını Gösteren Değer Zinciri

Tecrübeli çiftçiler, çiftliklerinde dolaşarak en iyi kararları alabilirler ama daha büyük çiftliklerde bu mümkün değildir. Böylelikle alandaki uzak bir göz ya da ahırdaki göz, gerçek zamanlı olarak uzaktan izlemeyi mümkün kılar; Çiftçiler, mahsullerde ve hayvanlarda hastalık belirtilerini, fark edebileceklerinden çok daha fazlasını tespit edebilirler. Özünde, M2M türevli veriler, çiftçilerin daha önce mümkün olandan çok daha yüksek bir tanecik seviyesinde neler olduğunu görmelerini sağlayan bir karar destek sistemine beslenir. Üretim ve hizmet endüstrilerinde iyi bilinen Sürekli İyileştirme Kavramı, hassas çiftçiliğe yararlı bir şekilde uygulanabilir, çiftliklerden toplanan verilerin yanı sıra çeşitli kaynaklardan elde edilen verilerden elde edilen yeni anlayışların eklenmesiyle sürekli bir iyileştirme döngüsü sağlanır. Bunların hepsi çeşitli tarım faaliyetlerinin sonuçlarını etkilemektedir. M2M toplanan veriler, iyi analiz edilmiş, çiftçi faaliyetlerine daha iyi bir bakış açısı kazandırabilir ve bu faaliyetlerde süreç iyileştirmelerine yol açabilir. Analitik sürece eklemek için değerli yardımcı veriler getirilebilir, örneğin:

- Hava durumu ve tahminleri
- Bilimsel bitki oluşumu
- Bitki ve hayvan hastalıkları ve semptomları
- Çiftliğin bulunduğu ülkeye uygulanan kurallar ve düzenlemeler

Toplanan tüm verilerin bir değeri vardır, bazıları mevcut kullanımının ötesinde faydalı olabilir. [17]

2.3.1 Akıllı Tarım Teknlojileri

Akıllı tarım çözümlerinin tasarım ve dağıtımında yer alan teknolojiler çok çeşitli ve çok disiplinlidir. Altta ki şekilde IoT teknolojilerine genel bakış görülebilmektedir.

Şekil 2.4: Akıllı Tarım Teknolojilerine Genel Bakış

Bu çeşitlilik, akıllı tarım çözümlerinin, iletişim servis sağlayıcıları, tarım aracı ve ekipman üreticileri, yazılım geliştiricileri, veri analizleri ve algılama teknolojisi sağlayıcıları gibi farklı pazar aktörleri içermesi anlamına da gelir. Yukarıdaki şekilde gösterilen akıllı tarım teknolojilerinin bir alt kümesini kısaca açıklayalım. Bu teknolojiler, akıllı tarım projelerinde dört temel aşamaya katkıda bulunur; veri algılama, veri toplama, veri iletimi ve veri işleme.

Algılama teknolojileri tüm akıllı tarım faaliyetlerinin altındadır. Tüm akla gelebilecek uygulama türleri için, veriler bir toprak numunesinden mi yoksa bir uydu düzeltme sinyalinden mi geldiği, temel yapı taşıdır. Örneğin, toplanan veri noktaları bir alandaki

mekansal ve zamansal değişkenliği vurgulayabilir. Bu değişikliğe birçok faktör katkıda bulunabilir; her faktörün etkisini anlamak için verilerin istatistiksel analizi kullanılarak ölçülebilir ve yönetilebilir.

Algılayıcılar teknolojileri, toprak kalitesi algılama, hayvan algılama, tank ve silo seviyesi izleme dahil olmak üzere çeşitli uygulamalara sahiptir. Alandaki algılayıcıların ve cihazların düzeni, ihtiyaç duyulan veri tipine göre düzenlenmiştir. Bilgilendirilmiş seçimler şu şekilde yapılmalıdır:

- Algılayıcıların ve ağ geçidinin bulunduğu ve sahada kaç tane ihtiyaç duyulduğu
- Ne sıklıkla veri toplanır?
- Verilerin büyüklüğü ve yükü
- Bir güç kaynağının gerekip gerekmediği (pil, güneş enerjisi).
- Bağlantı Modları

Uzaktan izlemenin kullanıldığı tüm tarımsal uygulamalarda, algılayıcılar tarafından algılanan ve toplanan veriler daha sonra çeşitli iletişim modları aracılığıyla çiftlik yönetim bilgi sistemine gönderilmektedir. Algılayıcı Ağları, tarım sektöründe yaygın olarak kullanılmaktadır. Güvenlik çerçevesi, veri paketlerini etkili bir şekilde yönlendiren ve çoklu iletimi mümkün kılan sensör düğümleri de kullanılmaktadır. WSN genellikle doğada geçicidir ve bir altyapının hazırda bulunması zorunlu değildir. Temel yapı olarak, sensör düğümleri ve son kullanıcı arasında bir ağ geçidi olması gerekmektedir. [18], [19] Büyük tarımsal alanlarda akıllı tarım uygulamaları için bir kablosuz sensör ağının olması gerekmektedir. Akıl tarım sistemdeki düğümler her zaman farklı çevresel koşullar altında çalışır ve bir WSN kurulmasında gerçek bir zorluktur. Bu ağın güvenli hale getirilmeside, ilgili yönlendirme ve yönlendirilmiş protokollerin oluşturulması gerekmektedir. LPWAN'ın (Low Power Wide Area Network) yeni serisi, düşük veri hızında, uzun pil ömründe ve uzun menzilli bağlantı senaryolarında hücresel bağlantının potansiyel ikamesi olarak görülüyor.

WAN seviyesinde bağlantıya ek olarak, ağlarda birkaç orta ve kısa aralıklı bağlantı şekli kullanılmaktadır. Tipik örnek, veri toplayan algılayıcıların ağıdır ve daha sonra bu verileri aynı fiziksel alanda bulunan ağ geçidine iletir. Ağ geçidi daha sonra bir WAN ağı üzerinden çiftlik yönetim sistemi ile iletişim kurmaktadır. Wan bağlantısı gsm üzerinden iletişim sağlanabilir. Algılayıcı ağlar da ise 802.15.4 protokolü vasıtasıyla örgüsel ağlar kurulabilir.

WSN'ler, tarımsal verimi artırmak için uygun maliyetli işlemler olarak kullanılmaktadır. WSN'ler akıllı tarımda, iklimin izlenmesi ve bitkilerin sağlığını ve tarım ürünlerinin

kalitesini tahmin etmek için toprak besin verilerini kullanmak gibi farklı tarımsal uygulamalarda kullanılmıştır. Sulama planlaması, hava koşullarını (sıcaklık ve nem gibi) ve toprağın nemini gözlemleyerek WSN'ler kullanılarak tahmin verileri anlamlı hale getirilebilir. Tarımsal izleme sisteminin parametrelerini iyileştirmek ve ağı ölçeklendirilebilir hale getirmek için mevcut WSN'ye başka sensör düğümleri eklenebilir. Tarımsal alanlardaki WSN'lerde, bazı zorluklar, optimum dağıtım şemaları, ölçüm süreleri, yönlendirme protokolleri, enerji verimliliği, maliyet, iletişim aralığı, ölçeklenebilirlik ve hata toleransı gibi sorunlarla karşı karşıya kalmıştır[20]. Tarım alanı birçok engelle karşılaştığında, sinyal zayıflaması nedeniyle iletişim bağlantısı zayıflayabilir veya kaybolabilir. Akıllı tarım uygulamalarındaki WSN'lerdeki sensör düğümleri, pille beslenir, böylece dağıtım konumundaki ana beslemeye bağlantı yapılmaz. Pil tükenmesini azaltmak ve pil ömrünü uzatmak, sınırlı pil gücü göz önünde bulundurulduğunda WSN' lerin önemi artmıştır. Her ne kadar WSN'lerin uygulanması yıllar içinde sürekli artmış olsa da, pil üretimi aynı oranda gelişmemiştir [21]. Bu nedenle, arazide kullanılan WSN'ler esasen pillerle ile sınırlıdır [22].

Çiftlikler ve baz istasyonları arasındaki uzun mesafeden kaynaklanan sorunlardan dolayı WSN' in önemi artmış olup, verinin bir yere aktarımı gerekliliklerini yerine getirmek için tarımsal alanda veri bağlantı hizmetlerini üstlenmiştir. [23]. Bu bağlantı, sensör düğümlerinin verilerini çiftlik alanının geniş alanı içindeki baz istasyona iletilmesini sağlar. Ancak, bu çözüm WSN'lerin hizmet kalitesi ile sınırlıdır.

Bölüm 3

IOT'de Kullanılan Kablosuz Algılayıcı Ağlar

3.1 IoT'de Kullanılan Kablosuz Algılayıcı Ağlar

WPAN ağları, başlangıçta, tipik olarak TCP/IP olmayan protokolleri desteklemiştir. Bluetooth, Zigbee ve Z-Wave protokol yığınları gerçek bir TCP/IP protokolüyle benzerlik göstermesine rağmen TCP/IP üzerinden iletişim kuramaz. Zigbee üzerinden IP (Zigbee-IP) ve Bluetooth üzerinden 6LoWPAN IP desteklemek için IPSP (internet Protocol Support Profile) kullanan uyarlamalar vardır. Bu bölümde 802.15.4 ve 6LoWPAN protokollerini kullanılarak WPAN örneklerini ele alacağız.

WSN'in önemli bir kısmı, iletişim ara yüzüdür. WSN ilk günlerinde, bu iletişim arayüzlerin standartları oluşturmamıştır. Ama bugün, makineden makineye (M2M) iletişim gereksinimleri (kendinden açıklayan arayüzleri, kendini organize ve kendi kendini iyileştirme) ile uyumludur standartlaştırılmış haberleşme arayüzleri, IoT'nin iletişiminde temel oluşturmuştur. IEEE 802.15.4 fiziksel ve ortam erişim kontrol tabakası tanımlar ve yaygın olarak mevcut WSN kullanılır. Son zamanlarda bu standart, temel ZigBee, WirelessHART ve SP100 gibi özel protokoller için temel olmuştur. Ama bugün, IEEE 802.15.4 de internet Protokolü (IP) için temel olarak kullanılır. Kaynakların IP işlevselliği çok sınırlı kaynakla dağıtılan düşük güç ağları için IPv6 destekli 6LowPAN kullanılabilir durumdadır. Bu bölüm de 6LowPAN bir adaptasyon protokolünü, IEEE 802.15.4 iletişim standardını kullanan, WSN için IPv6 protokolü destekleyen bir iletişim olarak açıklanabilir. 6LoWPAN ile iletişimin çeşitli zorluklarını özel protokollerle, kullanılan uygulamalara entegre edilerek kullanılmaya başlanmıştır. WSN düğümlerindeki düşük güçlü kablosuz cihazlarda, IEEE 802.15.4 üzerinde Zigbee önemli protokollerden biridir.

Bugün, uygulama katmanı ağ geçidi veya proxy çözümleri IP tabanlı ağlarda, kurumsal sistemleri ya da daha yüksek seviyeli hizmetleri için de özel protokolleri destekleyerek, WSN'e entegre etmek için kullanılır. Ağ geçitlerinin aksine uçtan uca bağlanabilirlik, IP tabanlı ağlarda kullanılan yönlendiriciler belirli WSN üzerinde derin bilgiye sahip olmadan ve protokolleri uygulamadan çalıştırılır. WSN' de kullanılan yapısının, IPv4 adresleri yerine IPv6 adreslerine geçişinin sağlanması gerekmektedir. IPv6 2128 'lik adres kapasitesine sahiptir. Yakın zamana kadar IP, kaynak kısıtlaması olan WSN düğümlerinde çalışacak yapıda değildi. Bu bölümde WSN'de kullanılan IEEE 802.15.4 ve 6LoWPAN protokolleri incelenecektir.

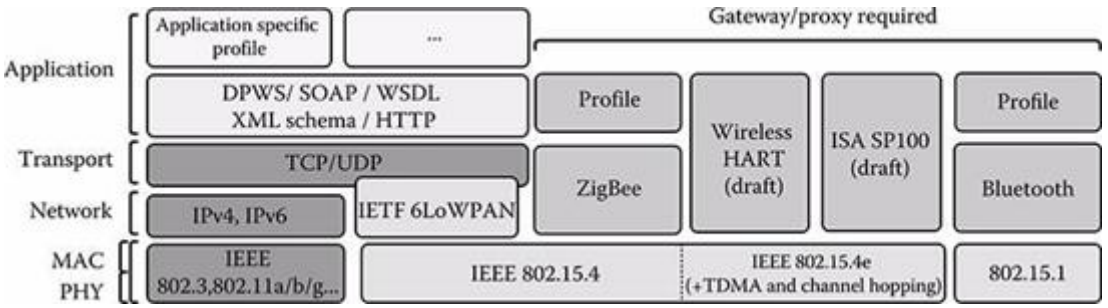
3.2 IEEE 802.15.4

IEEE 802.15.4, IEEE 802.15 çalışma grubu tarafından tanımlanan standart bir kablosuz kişisel alan ağıdır. Model 2003 yılında onaylandı ve Thread, Zigbee, WirelessHART ve diğerleri dahil olmak üzere birçok protokolün temelini oluşturdu. 802.15.4 sadece üst katmanları değil, yığının alt kısmını (fiziksel ve veri bağlantı katmanı) tanımlar. 802.15.4'ün hedefi ve üzerinde oturan protokoller düşük güç tüketimi ile düşük maliyetli WPAN'dır.

Şekil 3.1'te gösterildiği gibi Fiziksel(PHY) - MAC iletişim katmanlarında tanımlanan IEEE 802.15.4'e protokolünün üzerinde de çeşitli üst katman protokolleri bulunmaktadır. Bunlar da IETF 6LoWPAN, ZigBee, Wireles HART, ISA SP100'dür. Tüm protokollerin temel özellikleri aşağıdaki gibidir:

- Düşük güç tüketimi çözümlerle uzun pil ömrü
- Kendini onarabilen ağlar
- Ölçeklenebilirlik ve büyük ağların destek
- Düşük maliyetli düğümü
- Düşük veri hızı

IEEE 802.15.4, düşük veri oranlarına (LR WPAN) sahip kablosuz kişisel alan ağları için bir standarttır. 802.15.4 standardındaki "kişisel alan ağları" (PAN) ifadesi bu noktada yanıltıcıdır çünkü 802.15.4 ağları elbette kişisel kullanımla sınırlı değildir. Yüksek veri çıkışı için Wi-Fi (802.11) ve Bluetooth gibi teknolojiler geliştirilirken, IEEE 802.15.4 ağlarının odağı, düşük veri oranlarıyla sonuçlanan güç farkındalığı ve düşük maliyetli tasarımdır. [24]



Şekil 3.1: IEEE 802.15.4. OSI Katmanı

3.3 IEEE 802.15.4 Mimarisi

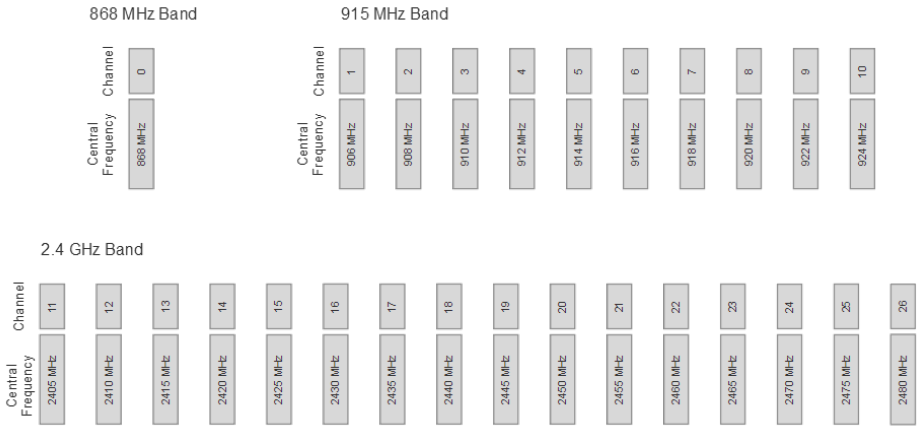
IEEE 802.15.4 protokolü, üç farklı radyo frekansı bandında lisanssız spektrumda çalışır: 868 MHz, 915 MHz ve 2400 MHz'dir. Amaç, mümkün olduğunca geniş bir coğrafi alana erişim sağlamaktır; bu da üç farklı bant ve çoklu modülasyon tekniği anlamına gelir. Düşük frekanslar, 802.15'in RF interferansı veya aralığı ile daha az soruna sebep olurken, 2.4 GHz bandı, dünya çapında en yaygın kullanılan 802.15.4 banttır. Daha yüksek frekans bandı popülaritesini kazanmıştır, çünkü daha yüksek hız, iletim ve almada daha kısa görev döngüleri sağlar, böylece gücü korur. 2.4 GHz bandını popüler yapan diğer faktör ise Bluetooth'un popülaritesi nedeniyle piyasada kabul görmesidir. Tabloda, çeşitli 802.15.4 bantları için çeşitli modülasyon teknikleri, coğrafi alan ve veri hızlarını listelenmektedir.

Frekans Aralığı	Kanal Sayısı	Modülasyon	Veri Hızı	Bölge
868.3	1 channel: 0	BPSK	20	Europe
		O-QPSK	100	
		ASK	250	
902-928	10 channels: 1-10	BPSK	40	North America, Australia
		O-QPSK	250	
		ASK	250	
2405-2480	16 channels: 11-26	O-QPSK	250	Worldwide

Şekil 3.2: Frekans Ayrımı

802.15.4 tabanlı bir protokolününün açık havada kapsama alanı yaklaşık 200Mt'dir. Kapalı alanda yaklaşık 30 m'dir. Menzili uzatmak için daha yüksek güç alıcı-vericileri (15 dBm) ya da ağ örgüsü kullanılabilir. Aşağıdaki grafik, 802.15.4 tarafından kullanılan güç bandı ve frekans dağılımını göstermektedir.

IEEE 802.15.4 bantları ve frekans dağılımları, 915 MHz bandında 2MHz frekans ayrımı kullanılır ve 2.4 GHz bandında 5 MHz frekans ayrımı kullanılır.



Şekil 3.3: Frekans Aralıkları

Paylaşılan bir frekans alanını yönetmek için, 802.15.4 ve diğer birçok kablosuz iletişim kuralı bir çeşit CSMA/CA kullanır. Aynı kanala iletirken bir kanalı dinlemenin imkansız olduğu için, çarpışma tespit şemaları çalışmaz. Bu nedenle çarpışmadan kaçınma kullanılır. CSMA/CA, önceden belirlenmiş bir süre için sadece belirli bir kanalı dinler. Kanal 'boşta' algılanırsa, önce kanalın meşgul olduğu tüm diğer vericilere bir sinyal göndererek iletir. Kanal meşgulse, iletim rastgele bir süre için ertelenir. Kapalı bir ortamda, CSMA/CA ile yüzde 36 kanal kullanımı sağlayacak ancak gerçek ortam senaryolarında, kanalların sadece yüzde 18'i kullanılabilir olacaktır. IEEE 802.15.4 grubu, operasyonel iletim gücünü en az 3 dBm ve alıcı duyarlılığının 2.4 GHz'de -85 dBm ve 868/915 MHz'de -91 dBm olarak tanımlar. Tipik olarak bu, iletim için 15 mA ila 30 mA akım ve alım için 18mA ila 37mA akım anlamına gelir. IEEE 802.15.4 fiziksel katmanında (PHY) 2450 MHz frekansında 250 Kb/s hızı, O-QPSK (Dördün Faz Kaydırmalı Anahtarlama) tekniği ile veri aktarımı sağlar. IEEE 802.15.4 standardı, 2.4 GHz ve 868/915 MHz bant PHY katmanlarında çalışan iki fiziksel (PHY) katman oluşmaktadır. Fiziksel katman kullanıcı tercihine bağlıdır. Lisanssız 2.4 GHz dünya çapında geçerlidir ve 40 Kbps (ABD) ve 20 Kbps veri hızına sahip 868 MHz (AB) bandı olan 915 MHz bandına kıyasla daha yüksek bir veri hızına (250 Kbps) sahiptir. 2.4 GHz bandında 16 kanal, 915 MHz bandında 10 kanal ve 868 MHz bandında 1 kanalda çalışabilir. Protokol yığını sadece OSI modelinin (Fiziksel ve MAC) en alttaki iki katmanından oluşur. PHY, sembol kodlaması, bit modülasyonu, bit de modülasyonu ve paket senkronizasyonundan sorumludur. Ayrıca, gönderme-alma modu anahtarlama ve paket içi zamanlama / alındı gecikme kontrolü gerçekleştirir. Aşağıda, OSI modeliyle karşılaştırıldığında 802.15.4 protokol yığını gösterilmiştir.

Fiziksel katmanın üstünde, fiziksel bağlantıdaki hataları tespit etmek ve düzeltmekle sorumlu veri bağlantı katmanı bulunur. Bu katman ayrıca CSMA/CA gibi protokolleri kullanarak çarpışmadan kaçınmayı ele almak için medya erişim katmanını (MAC) kontrol

eder. MAC'den yığının üst katmanlarına kadar olan arabirim, Hizmet Erişim Noktaları (SAP-Service Access Points) olarak adlandırılan iki arabirim aracılığıyla sağlanır: MAC-SAP: Veri yönetimi için MLME-SAP: Kontrol ve izleme için (MAC katman yönetimi varlığı)

IEEE 802.15.4'te iki tip iletişim vardır: işaret ve işaretsiz iletişim.

İşaret tabanlı ağ için, MAC katmanı, bir cihazın PAN'a girmesine izin verir. Aynı zamanda cihazın iletişime başlayıp kanala girmesi ve giriş zamanlaması için işaretler üretebilir.

İşaret tabanlı ağa ek olarak IEEE 802.15.4, işaretsiz ağ oluşturmaya izin verir. Bu, PAN koordinatörü tarafından hiçbir işaret çerçevesinin iletilmediği çok daha basit bir şemadır. Bununla birlikte, tüm düğümlerin her zaman alıcı modunda olduğunu ima eder. Bu, benekli olmayan CSMA / CA kullanımıyla tam zamanlı çekişme erişimi sağlar. Bu mod, işaret tabanlı iletişimden çok daha fazla güç tüketir. [25]

3.4 IEEE 802.15.4 Topolojileri

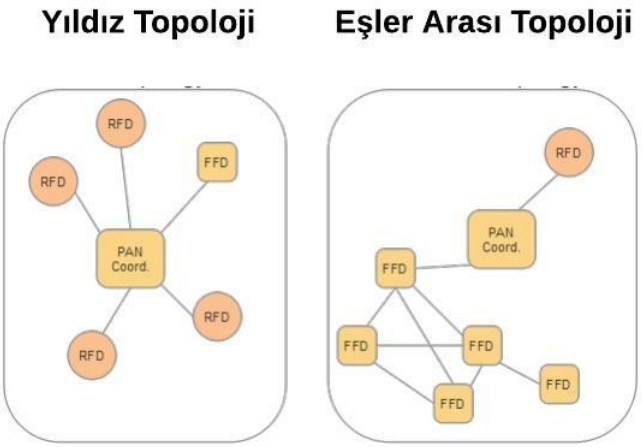
IEEE 802.15.4'te İki Temel cihaz tipi vardır:

FFD-Full Function Device: Herhangi bir ağ topolojisini destekler, bir ağ (PAN) koordinatörü olabilir ve herhangi bir aygıt PAN koordinatörü ile iletişim kurabilir.

RFD-Reduced Function Device: Sadece bir yıldız topolojisi ile sınırlı, bir ağ koordinatörü olarak çalışamaz, sadece bir ağ koordinatörü ile iletişim kurabilir. Yıldız topolojisi en basit olanıdır, ancak eş düğümler arasındaki tüm mesajların yönlendirilmek üzere PAN koordinatörü üzerinden geçmesi gerekir. Eşler arası bir topoloji tipik bir ağdır ve doğrudan komşu düğümlerle iletişim kurabilir. IEEE 802.15.4, diğer düşük güçlü bağlantı katmanları gibi, Şekil 3.4'de gösterildiği gibi, yıldız ve örgüsel ağ gibi birçok topolojiyi destekler. Topoloji içerisinde cihaz, bellek, hesaplama gücü veya enerji açısından minimum kaynak gerektiren hafif uç noktaları oluşturabilir. Biraz daha fazla kaynak mevcut olduğunda, cihazlar, FFD olarak düşünülebilir ve RFD olarak adlandırılan diğer uç noktalar olarak bağlanabilir. Bu FFD ayrıca örgü topolojide yönlendirme işlevleri sağlar. Topolojideki çoğu kaynak, ağı yönetmekten sorumlu olan PAN koordinatörüne ihtiyaç duyar.

PAN koordinatörü, PAN'ı kurmak ve yönetmek için benzersiz bir role sahiptir. Ayrıca ağ işaretlerini iletme ve düğüm bilgilerini saklama görevine de sahiptir. Sürekli yayın alacağı ve özel bir güç hattına bağlı olduğundan dolayı PAN koordinatörü her zaman bir FFD'dir. RFD ve hatta düşük güçlü FFD'ler batarya bazlı olabilir. Rolleri mevcut

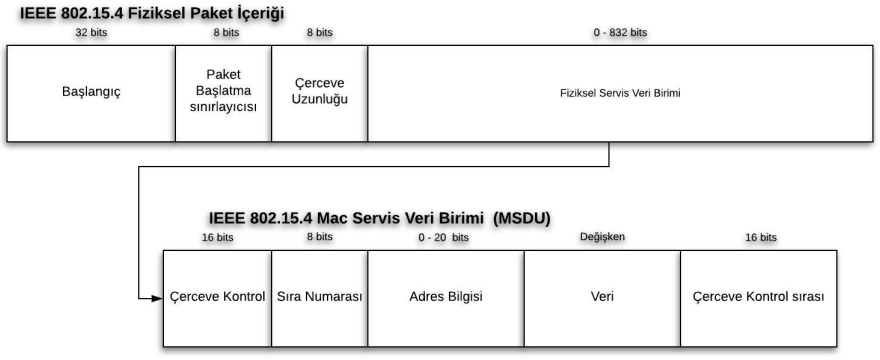
ağları aramak ve gerektiğinde veri transfer etmektir. Bu cihazlar çok uzun bir süre boyunca uyku durumuna geçirilebilir. Aşağıda, yıldızlara karşı örgüsel ağ topolojiye ait bir diyagram gösterilmiştir. [24]



Şekil 3.4: Topoloji Türleri

3.5 IEEE 802.15.4 Adres Modları ve Paket Yapısı

Standart, 64 bitlik adres içermektedir. Bununla birlikte, bant genişliğini korumak ve bu gibi büyük adresleri iletme enerjisini azaltmak için 802.15.4, bir ağa katılan bir cihazın, 16 bitlik kısa bir yerel adres için 64 bit adreslerini 'alıp vermesini' sağlar ve daha verimli iletim sağlayarak düşük enerji harcar. Bu 'takas' süreci PAN koordinatörünün sorumluluğundadır. Bu 16 bitlik yerel adrese PAN ID diyoruz. Tüm PAN ağının kendisinde bir PAN tanımlayıcısı bulunur, çünkü birden fazla PAN mevcut olabilir. Aşağıda şekil 3.5 802.15.4 paket yapısının bir diyagramıdır.



Şekil 3.5: IEEE 802.15.4 PHY ve MAC Paket Kodlaması

Çerçeveler, veri aktarımının temel birimidir ve dört temel tip vardır.

- Veri çerçevesi: Uygulama veri aktarımı
- Onay çerçevesi: Alım teyidi
- İşaret çerçevesi: Super Frame yapısı kurmak için PAN koordinatörü tarafından gönderilir
- MAC komut çerçevesi: MAC katman yönetimi (ilişkilendir, ayır, işaret isteği, GTS talebi)

3.5.1 IEEE 802.15.4 Başlangıç Dizisi:

IEEE 802.15.4, başlangıç, ağ yapılandırması ve mevcut ağların birleştirilmesi için çeşitli süreçler vardır.

- Aygıt, yığını başlatır (PHY ve MAC katmanları).
- PAN koordinatörü oluşturulur. Her bir ağın sadece bir PAN koordinatörü vardır. Devam etmeden önce PAN koordinatörü bu aşamada atanmalıdır.
- PAN koordinatörü, erişimi olan diğer ağları dinler ve yöneteceği PAN'a özgü bir PAN Kimliğini türetir. Bunu çoklu frekans kanalları üzerinden yapabilir.
- PAN koordinatörü, ağ için kullanılacak belirli bir radyo frekansını seçecektir. Bunu, PHY'nin destekleyebileceği frekansları taradığı ve sessiz bir kanal bulmaya çalıştığı bir enerji saptama taraması kullanarak yapar.
- Ağ, PAN koordinatörü yapılandırılarak ve ardından cihaz koordinatör modunda başlatılarak başlatılacaktır. Bu noktada PAN koordinatörü istekleri kabul edebilir.
- Düğümler, tüm frekans kanallarında bir işaret isteği yayınladığı etkin bir kanal taraması kullanarak PAN koordinatörü bularak ağa katılabilir. PAN koordinatörü işaretini tespit ettiğinde, istekte bulunan cihaza geri dönecektir. Alternatif olarak, bir işaret temelli ağda (daha önce ayrıntılı olarak açıklanmıştır), PAN koordinatörü rutin olarak bir işaret gönderir ve cihaz bir pasif kanal taraması gerçekleştirebilir ve işaretini dinleyebilir. Cihaz daha sonra bir ilişkilendirme isteği gönderir.
- PAN koordinatörü, cihazın ağa katılıp katılmayacağını belirler. Bu, erişim denetimi kurallarına dayanabilir veya PAN koordinatörü başka bir aygıtı yönetmek için yeterli kaynağa sahip olsa bile; PAN koordinatörü cihaza 16 bit kısa bir adres atayabilir.(24)

3.5.2 IEEE 802.15.4 Güvenliği

IEEE 802.15.4 standardı, şifreleme ve kimlik doğrulama biçimindeki güvenlik özelliklerini içerir. Mimari ağın güvenliği, maliyet, performans, güvenlik ve güce dayanan esnekliğe sahiptir. Farklı güvenlik özellikleri aşağıdaki tabloda listelenmiştir. AES tabanlı şifreleme, blok şifresini kullanır. AES-CBC-MAC, yalnızca kimlik doğrulama koruması sağlar ve AES-CCM modu, şifreleme ve kimlik doğrulamanın tam paketini sağlar. 802.15.4 protokolü, hangi güvenlik paketinin ve anahtarların kullanılacağını kontrol etmek için bir erişim kontrol listesi (ACL) kullanmaktadır. Cihazlar 255'e kadar ACL bilgisi saklayabilir. MAC katmanı aynı zamanda eski çerçevelerin veya eski verilerin artık geçerli sayılmadığından emin olmak için art arda tekrarlar arasında 'tazelik kontrollerini' hesaplar ve bu karelerin yığından çıkmasını engeller.

Tip	Açıklama	Erişim Kontrolü	Gizlilik	Çerceve Bütünlüğü	Sıralı Tazelik
None	No security				
AES-CTR	Encryption only, CTR	X	X		X
AES-CBC-MAC-128	128-bit MAC	X		X	
AES-CBC-MAC-64	64-bit MAC	X		X	
AES-CBC-MAC-32	32-bit MAC	X		X	
AES-CCM-128	Encryption and 128-bit MAC	X	X	X	X
AES-CCM-64	Encryption and 64-bit MAC	X	X	X	X
AES-CCM-32	Encryption and 32-bit MAC	X	X	X	X

Şekil 3.6: Şifreleme Yöntemleri

Her 802.15.4 alıcı-vericisi kendi ACL'ini yönetmeli ve güvenlik politikaları ile bir "güvenilir komşular" listesi ile doldurmalıdır. ACL, iletişim için temizlenen düğümün adresini, kullanılacak özel güvenlik paketini (AES-CTR, AES-CCM-xx, AES-CBC-MAC-xx), AES algoritmasının anahtarı ve son başlangıç değerini içerir. Aşağıdaki tablo çeşitli 802.15.4 güvenlik modlarını ve özelliklerini listeler.

Simetrik kriptografi, aynı anahtarı kullanarak her iki uç noktaya uygulanır. Anahtarlar, paylaşılan bir ağ anahtarı kullanılarak bir ağ düzeyinde yönetilebilir. Bu, tüm düğümlerin aynı anahtara sahip olduğu ancak anahtarın ele geçirilmesi riski vardır. Benzersiz anahtarların her düğüm çifti arasında paylaşıldığı çift yönlü bir anahtarlama şeması kullanılabilir. Bu mod, özellikle düğümlerden komşulara giden yüksek bir trafiğin olduğu ağlar için ek yük ekler. Grup anahtarlaması başka bir seçenektir. Bu modda, bir dizi düğüm arasında tek bir anahtar paylaşılır ve grubun herhangi iki düğümü için kullanılır. [25]

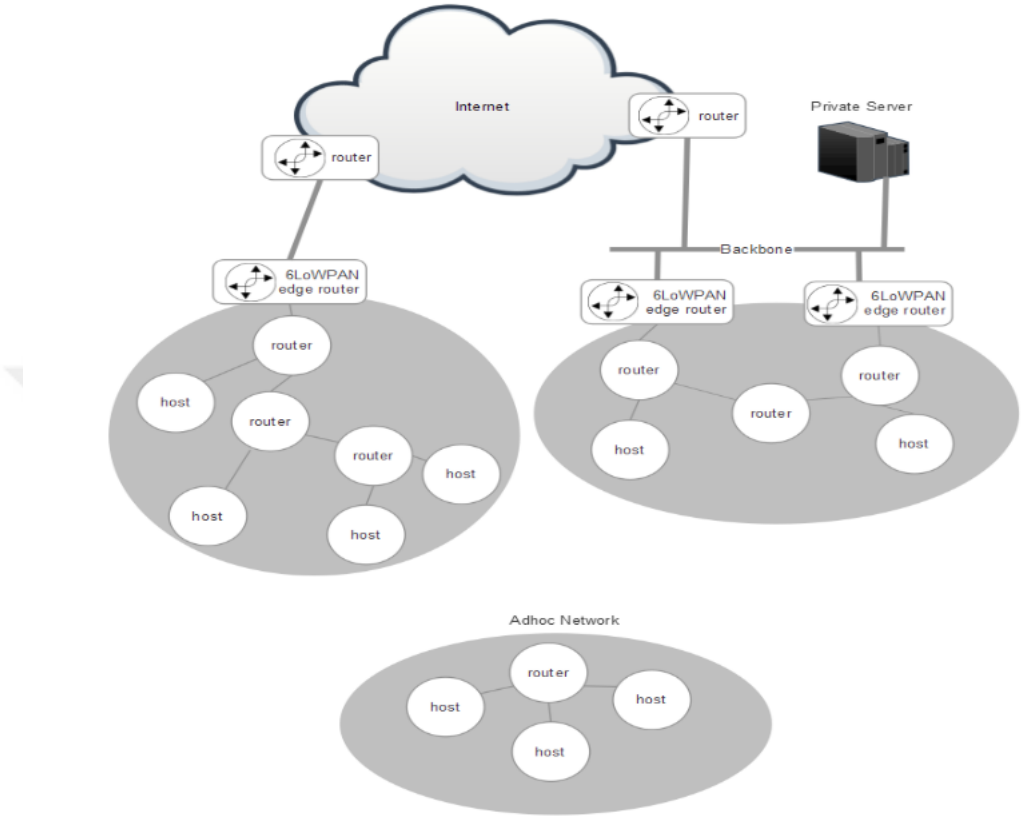
3.6 6LOWPAN

IoT üzerindeki WSN'de kullanılan en küçük ve kaynak kısıtlı cihazlara IP adresi verilebilmesi için 6LoWPAN Protokolü oluşturuldu. 6LoWPAN standardı herkesin kullanması ve uygulanması için açıktır. 6LoWPAN, düşük güçteki WPAN'lar üzerinden IPV6'yı temsil eden bir kısaltmadır. Amaç, güç ve alan kısıtlaması olan ve yüksek bant genişliği ağ hizmetlerine ihtiyaç duymayan aygıtlar için düşük güçlü RF iletişim sistemleri üzerinden IP iletişimi sağlanmasıdır. 6LoWPAN'ın ana avantajı, en basit algılayıcıların IP adreslenebilirliği sahip olmaları ve 3G / 4G / LTE / Wi-Fi / Ethernet yönlendiricileri üzerinden bir ağ cihazı olarak hareket etmeleridir. İkincil bir etki, IPV6'nın 2128 veya 3.4x1038 benzersiz adreslerinin önemli teorik adreslenebilirliğini sağlamasıdır. IETF, IEEE 802.15.4 haberleşme sistemlerini kullanan kablosuz olarak bağlanmış, kaynak kısıtlı ağ düğümlerinde de IP tabanlı iletişim için acil bir ihtiyaç öngörmüştür. Böylece 6LoWPAN çalışma grubu kuruldu. Çalışma grubunun adı şu anda 6LoWPAN çalışma grubunda geliştirilen özel protokol adaptasyonları için kısaltma olarak ve bu 6LoWPAN protokollerini kullanan WSN'lerin adı olarak kullanılmaktadır. [24] RFC 4944'te açıklanan 6LoWPAN, IPv6 paketlerini taşıyabilen IETF standardize 802.15.4 bağlantı protokolüdür ve IP uyumlu LR-WPAN'lar için belirlenmiş standarttır. 6LoWPAN, düğümlerin TCP / IP ağını gerçekleştirdiği sürece 802.15.4 arabirimlerini kullanarak gömülü sistemlerin internete erişmesini mümkün kılar. Paketin içeriği parçalanır ve ardışık taşıma birimlerine iletilir ve isteğe bağlı olarak ağ ve nakil başlıkları, iletim yükünü azaltmak için sıkıştırılır. 6LoWPAN, ağ topolojisini oluşturmak için altyapı sağladığından, ağ seviyesine, IP düzeyindeki yönlendirme tablolarını güncellemek için uygulama düzeyinde protokoller kullanılarak farklı bir şekilde oluşturulabilir.

3.6.1 6LOWPAN Topolojisi

6LoWPAN ağları, daha büyük ağların çevresinde bulunan ağ örgüleridir. Topolojiler esnektir, internete veya diğer sistemlere herhangi bir bağlantı olmadan geçici ve ayrık ağlara

izin verir veya kenar yönlendiricileri kullanarak omurgaya veya internete bağlanabilirler. 6LoWPAN ağları çok kenar yönlendiricilerle birleştirilebilir, buna çoklu arama(multi-homing) denir. Ek olarak, geçici ağlar, bir uç yönlendiricinin internet bağlantısı gerektirmeden de oluşabilir. Bu topolojiler aşağıda gösterilmiştir:



Şekil 3.7: 6LOWPAN Topolojiler

6LoWPAN mimarisi için bir kenar yönlendirici (sınır yönlendirici olarak da bilinir) gereklidir:

- İletişimi 6LoWPAN cihazlara aktarır ve verileri internete aktarır.
- Bir sensör ağında etkinlik için 40 bayt IPv6 üstbilgisini ve 8 bayt UDP başlıklarını azaltarak IPv6 üstbilgilerinin sıkıştırılmasını gerçekleştirir. Tipik bir 40 bayt IPv6 başlığı, kullanıma bağlı olarak 2 ila 20 bayt arasında sıkışabilir.
- 6LoWPAN ağını başlatır.
- 6LoWPAN ağındaki cihazlar arasında veri alışverişi yapar.

Kenar yönlendiriciler, daha büyük geleneksel ağ şekilleri üzerinde 6LoWPAN örgü ağları oluşturur. Ayrıca, gerekirse IPV6 ve IPV4 arasında değiş tokuş yapabilirler. Datagramları, özel protokollere göre bazı avantajları olan bir IP ağında olduğu gibi benzer

bir şekilde ele alınır. Bir 6LoWPAN ağı içindeki tüm düğümler, kenar yönlendiricinin oluşturduğu aynı IPv6 önekini paylaşır. Düğümler, uç yönlendiricilere Ağ Bulma (ND) aşamasının bir parçası olarak kaydolur. ND, yerel 6LoWPAN ağındaki ana bilgisayarların ve yönlendiricilerin birbirleriyle nasıl etkileşime gireceğini denetler. Çoklu hedef, birden çok 6LoWPAN kenar yönlendiricisinin bir ağı yönetmesine izin verir. [25]

6LoWPAN örgü içinde üç tip düğüm vardır: Yönlendirici düğümleri: Bu düğümler, bir 6LoWPAN örgü düğümünden diğerine veri toplar. Yönlendiriciler ayrıca WAN ve internete dışarıdan iletişim kurabilir.

Ana bilgisayar düğümleri: Ağ örgüsündeki ana bilgisayarlar ağdaki verileri yönlendiremez ve yalnızca veri tüketen veya üreten uç noktalarıdır. Ana bilgisayarların uyku durumlarında olmasına izin verilir, bazen veri üretmek veya ana yönlendiriciler tarafından önbelleğe alınan verileri almak için uyanırlar.

Kenar yönlendiriciler: Belirtildiği gibi, bunlar genellikle WAN kenarında ağ geçitleri ve ağ denetleyicileridir. Kenar yönlendiricinin altında bir 6LoWPAN örgü uygulanacaktır.

Düğümler, örgü- düğüm içinde hareket etmek ve yeniden düzenlemek / birleştirmek için serbesttir. Bu bağlamda, bir düğüm, çoklu arama senaryosunda farklı bir kenar yönlendirici ile hareket edip ilişkilendirebilir veya hatta farklı 6LoWPAN düğümler arasında hareket edebilir. Topolojiye yapılan bu değişiklikler, sinyal gücündeki değişiklikler veya düğümlerin fiziksel hareketi gibi çeşitli nedenlerden kaynaklanabilir. Bir topoloji değişimi meydana geldiğinde, ilişkili düğümlerin IPv6 adresi de doğal olarak değişecektir. Kenar yönlendiricisi olmayan özel bir ağda, bir 6LoWPAN yönlendirici düğümü bir 6LoWPAN örgüsünü yönetebilir. WAN'ın internete bağlanması gerekmediğinde bu durum böyle olurdu. Tipik olarak, bu nadiren küçük bir geçici ağ için IPv6 adreslenebilirliğinin gerekli olmadığı şeklinde görülür. [25]

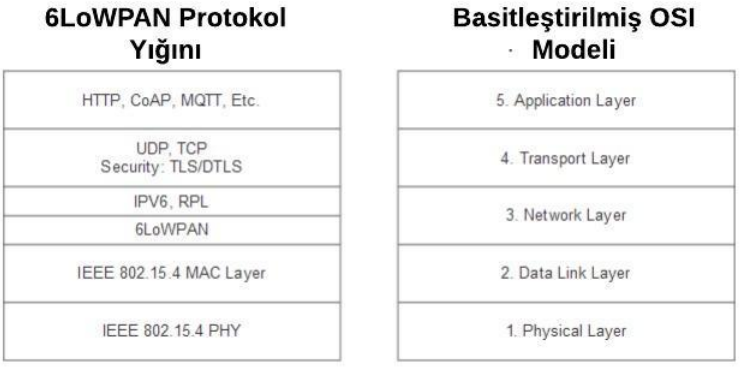
Yönlendirici düğüm bazı işlevleri destekleyecek şekilde yapılandırılır:

- Benzersiz yerel tek noktaya yayın adresi oluşturma
- Komşu keşif ND kaydı gerçekleştirme
- Özel ağ IPv6 öneki, daha büyük olan küresel WAN IPv6 öneki yerine yerel bir önek olacaktır. [25]

3.6.2 6LoWPAN Protokol Yığını

6LoWPAN'i 802.15.4 gibi bir iletişim ortamı biçiminde etkinleştirmek için bir IP protokolünü desteklemek için gerekli olan bir dizi önerilen özellik vardır. Bu özellikler

çerçeveleme, tek noktaya yayın iletimi ve adresleme içerir. Aşağıdaki şekilde gösterildiği gibi, fiziksel katman, veri bitlerinin hava üzerinden alınmasından ve dönüştürülmesinden sorumludur. Bu örnekte, konuştuğumuz bağlantı katmanı IEEE 802.15.4'tür. Fiziksel katmanın üstünde, fiziksel bağlantıdaki hataları tespit etmek ve düzeltmekle sorumlu olan veri bağlantı katmanı bulunur. İşte 6LoWPAN yığını ve OSI modeli arasındaki karşılaştırma:



Şekil 3.8: 6LOWPAN OSI Katmanları

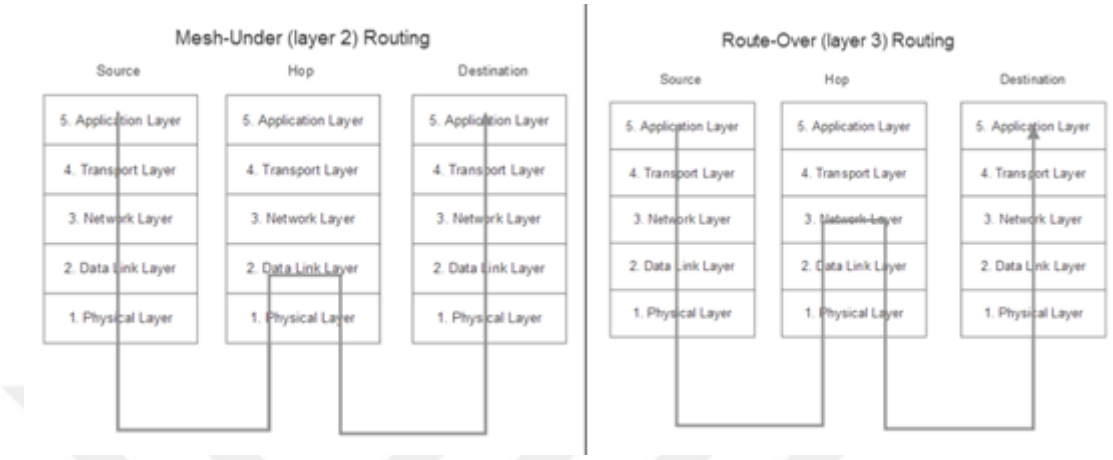
6LoWPAN, fiziksel ve MAC adresini sağlamak için 802.15.4 veya Bluetooth gibi diğer protokollerin üstünde bulunur. IP trafiğini sensör düzeyinde etkinleştirerek, cihaz ile ağ geçidi arasındaki ilişki IP olmayan protokolden IP protokolüne veri dönüştürmek için bir tür uygulama katmanı kullanır. 6LoWPAN, katman üç (ağ katmanı) ve iki tabakanın üstünde (veri bağlantı katmanı) bir uyarlama katmanı sağlar. Bu uyarlama katmanı IETF tarafından tanımlanmıştır. [25]

3.6.3 Örgüsel Adresleme ve Yönlendirme

Örgüsel yönlendirme, paketlerin birden çok atlama kullanılarak bir dinamik ağ boyunca akmasını sağlamak için fiziksel ve veri bağlantı katmanlarında çalışır. 6LoWPAN örgüsel ağları, yönlendirme için iki şema kullanır.

Örgüsel altı ağlar: Ağ tabanlı bir topolojide, yönlendirme şeffaftır ve ağın bütününü temsil eden tek bir IP alt ağını üstlenir. Bir mesaj tek bir alanda yayınlanır ve ağdaki tüm cihazlara gönderilir. Daha önce belirtildiği gibi, bu önemli trafik üretir. Örgüsel altından geçen yönlendirme ağdaki sekmeden sekmeye doğru hareket eder, ancak yığının yalnızca iki katmanına (veri bağlantı katmanı) kadar paketleri ilerletir. 802.15.4, iki katmandaki her atlama için tüm yönlendirmeyi işler.

Güzergah Yönlendirme ağlar: Bir güzergah üstü topolojideki ağlar, yığının üç katmanına (ağ katmanı) kadar paketleri iletme ücretini üstlenir. Yönlendirme şemaları rotaları IP düzeyinde yönetir. Her atlama bir IP yönlendiriciyi temsil eder. Aşağıdaki grafik, örgüsel altı ve güzergah üstü arasındaki farkı göstermektedir:



Şekil 3.9: Layer2 ve Layer3 Farkları

Şekil 3.9 Örgüsel altından ve güzergah yönlendirme ağ iletişimi arasındaki farkı göstermektedir. Aracı atlamalar, paketin her bir yığınının, ağdaki bir sonraki düğüme gitmeden önce ne kadar ileri gittiğini ortaya çıkarmaktadır. Güzergah Yönlendirme ağı, her yönlendirici düğümün eşit derecede yetenekli olduğunu ve çift adres tespiti gibi normal IP yönlendirici olarak daha büyük işlevleri yerine getirebileceğini ima eder. RFC6550 [26] resmi olarak RPL (dalgalanma) protokolünü tanımlar. Güzergah yönlendirme mimarisinin avantajı, geleneksel TCP / IP iletişimiyle benzerliktir. RPL, çok noktadan noktaya iletişim (bir ağdaki aygıtlardan gelen trafiğin internetteki merkezi bir sunucuya iletişim kurduğu) ve noktadan çoklu iletişim (ağdaki aygıtlara merkezi hizmet) sağlar.

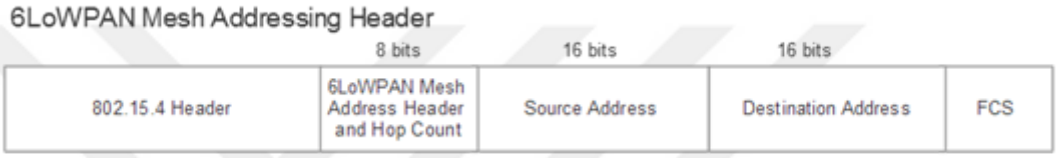
RPL protokolünün rota tablolarını yönetmek için iki modu vardır:

Saklama modu: 6LoWPAN ağındaki yönlendiriciler olarak yapılandırılan tüm aygıtlar yönlendirmelerini ve komşu tablolarını korur.

Depolama dışı modu: Kenar yönlendiricisi gibi sadece tek bir aygıt, yönlendirme ve komşu tablolarını korur. Bir veriyi bir ana bilgisayardan diğerine 6LoWPAN ağında aktarmak için, veri rotasının hesaplandığı ve daha sonra alıcıya iletilip yönlendiriciye gönderilir.

Adından da anlaşılacağı gibi yönlendirme tablosu, örgü yönlendirme yollarını içerirken, komşu tablo her düğümün doğrudan bağlı komşularını korur. Bu, kenar yönlendiricinin her zaman, ağda paketlerin teslim edilmesi için referans alınacağı anlamına gelir. Bu, yönlendirici düğümlerin yönetilmesi için büyük yönlendirme tablolarını yönetme özgürlüğüne izin verir. Ancak kenar yönlendiricisine başvurulması gerektiğinden hareketli

paketlerde biraz gecikme eklenir. Kayıt modu sistemleri, her bir düğümde depolanan yönlendirme tablolarını yönetmek için daha yüksek işleme ve bellek gereksinimlerine sahip olacak, ancak bir rota oluşturmak için daha verimli bir yola sahip olacaktır. Aşağıdaki şekilde atlama sayısı, kaynak adresi ve hedef adres alanları vardır. Bu alanlar adres çözümleme ve yönlendirme aşamasında kullanılır. Sekme sayısı, başlangıçta yüksek bir değere ayarlanır ve daha sonra, paket ağdaki düğümden düğüme doğru yayıldığında her defasında azaltılır. Amaç, sıçrama limitinin sıfıra ulaşması, paketin düşmesi ve ağ gözünden kaybolmasıdır. Bu, ana bilgisayar düğümünün kendisini örgüden çıkarması ve artık erişilememesi durumunda kaçak ağları önlemenin bir yolunu sağlar. Kaynak ve hedef adres 802.15.4 adresleridir ve 802.15.4'ün izin verdiği gibi kısa veya genişletilmiş biçimde olabilir. Başlık aşağıdaki gibi oluşturulur:



Şekil 3.10: 6LOWPAN Mesh Adresleme Başlığı

3.6.4 6LoWPAN Üstbilgi Sıkıştırma ve Parçalanma

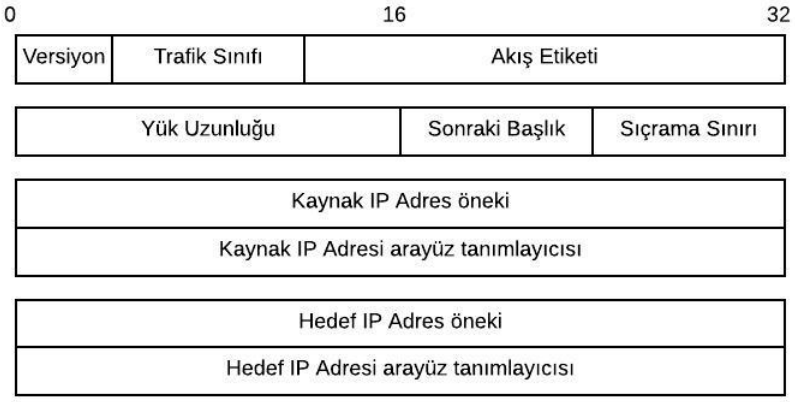
İşler için neredeyse sınırsız IP adreslerine sahip olmanın avantajı önemli bir dönüm noktası iken, IPv6'yı bir 802.15.4 bağlantısına yerleştirmek, 6LoWPAN'ı kullanılabilir hale getirmek için üstesinden gelinmesi gereken bazı zorluklar ortaya çıkarmaktadır. Birincisi, IPv6'nın 1280 baytlık bir Maksimum İletim Birimi (MTU) boyutuna sahip olması, 802.15.4'ün 127 baytlık bir sınırı olmasıdır. İkinci konu, IPv6'nın genel olarak zaten şişirilmiş bir protokole önemli bir mesafe katmasıdır. Örneğin, IPv6 başlıklarında 40 bayt uzunluğundadır. [25] (Not IEEE 802.15.4'nin çerçeve uzunluğu için 127 bayt sınırlaması yoktur.)

3.6.4.1 6LoWPAN Sıkıştırma Başlığı

IEEE 802.15.4 gibi düşük güçlü bağlantı teknolojileri, küçük çerçeve boyutları ile karakterizedir. Tipik bir IEEE 802.15.4 çerçevesi 127 bayttır, MAC başlığı ve güvenlik bilgisi dahil ise üst katlar için 81 bayt bırakılır (en kötü durum yükü = 127–25 bayt MAC başlığı 21 bayt bağlantı katmanı güvenliği = 81 bayt). Yerel bir IPv6-başlık zaten IPv6 uzantısı üstbilgileri dikkate almayan 40 baytlık bir boyuta sahiptir. Bu IPv6 üstbilgisini taşımak için ve örneğin, ek bir UDP başlığı kalan 33 bayta (kalan yük = 81–40 bayt IPv6 üstbilgisi 8 bayt UDP üstbilgisi = 33 bayt) neden olur. IPv6'yı düşük güçlü

bağlantılar üzerinden verimli bir şekilde iletmek için IPv6 üstbilgileri sıkıştırılabilir. Bu sıkıştırmanın amacı, gizli olarak bilinen veya farklı şekilde alınabilen satır içi bilgiden kaçınmaktır. IPv6 başlık alanlarının sıkıştırılması için örnekler aşağıdaki gibidir (bakınız Şekil 3.11):

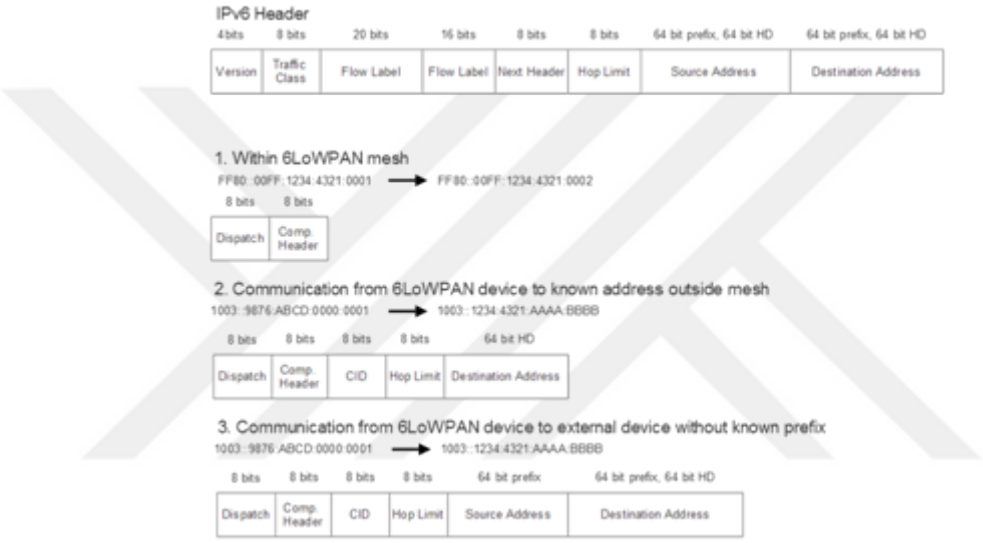
- Protokol sürümü her zaman IPv6'dır. Bu alan ihmal edilebilir.
- Trafik Sınıfı ve Akış Etiketi alanları, ağ tabanlı düşük güçlü ağlarda uygulanamaz ve ihmal edilebilir.
- Alan Yükü Uzunluğu gereksizdir ve ihmal edilebilir, çünkü bu bilgi zaten IEEE 802.15.4 başlığında taşınır.
- Çerçevede bir sonraki başlık taşınmazsa sonraki başlık alanı ihmal edilebilir.
- Hop Limiti alanı sıkıştırılamaz ve tamamen dahili olarak taşınmalıdır.
- Kaynağın ve hedef uç noktaların IPv6 adres örnekleri zaten bilinebilir ve / veya aynı olabilir, örneğin her iki uç nokta aynı 6LoWPAN'da ise ve 6LoWPAN'in tamamı için bir önek kullanılır. Bu durumda, ö örnekler ihmal edilebilir veya sıkıştırılabilir.
- IPv6 arabirimi tanımlayıcıları uç noktaların MAC adreslerinden üretilirse, kaynağın ve hedefin IPv6 arabirim tanımlayıcıları da gereksiz olabilir. Bir IEEE 802.15.4'teki iletişim için, MAC adresleri 802.15.4 çerçevelerinde zaten taşınır ve IPv6 başlıklarında ihmal edilebilir / sıkıştırılabilir.



Şekil 3.11: Doğal IPv6 Başlığı

Belirli bir senaryoya bağlı olarak, yerel IPv6 üstbilgileri yalnızca birkaç bayta kadar sıkıştırılabilir. IPv6 başlık sıkıştırmasına benzer şekilde, 6LoWPAN protokolleri UDP başlık sıkıştırmasını da açıklar, böylece UDP başlığı en iyi durumda 8 bayttan 4 bayta

kadar sıkıştırılabilir. [24] Başlık sıkıştırması, verimlilik nedenleriyle IPv6 standart üst-bilgisindeki fazlalıkların sıkıştırılması ve kaldırılması için bir araçtır. Normalde, başlık sıkıştırması durum temellidir, yani statik bağlantılar ve kararlı bağlantılar içeren bir ağda, oldukça iyi çalışır. 6LoWPAN gibi bir örgü ağda, bu işe yaramaz. Paketler düğümler arasında geçiş yapar ve her atlamada sıkıştırma / açma işlemi gerektirir. Ek olarak, yollar dinamiktir ve değişime izin verilir ve uzun süre boyunca yollar mevcut olmayabilir. Bu nedenle, 6LoWPAN paylaşılan içerik sıkıştırmayı kabul etti. Sıkıştırma türü, RFC4944'ün RFC6922 üzerinden kullanılması gibi, belirli özelliklerin karşılanıp karşılanmadığının yanı sıra, bir paketin kaynağının ve hedefinin nerede olduğu gibi aşağıdakilerden de etkilenebilir:



Şekil 3.12: 6LoWPAN'de Başlık Sıkıştırma

Güzergâhın yerel ağ içinde, ağın dışında, bilinen bir adreste mi yoksa bilinmeyen bir adrese ağın dışında mı olduğuna bağlı olarak, 6LoWPAN için üç ana başlık sıkıştırma vakası bulunur. 40 baytlık başlıklı standart IPv6'ya kıyasla, 6 LoWPAN 2 ila 20 bayt arasında sıkışabilir. Birinci durumda (bir önceki resimde), yerel bir ağdaki düğümler arasındaki en iyi durum iletişimidir. Bu sıkıştırılmış başlık formatı ile WAN'a hiçbir veri gönderilmez. İkinci durumda, verilerin WAN'a bilinen bir adrese dışarı gönderildiği ve son durumun da bilinen bir adrese benzediği ima edilmektedir. En kötü durum olan üçüncü durumda bile, sıkıştırma hala trafikte yüzde 50'lik bir düşüşe neden olur. 6LoWPAN ayrıca UDP sıkıştırmasına da izin verir. [25]

3.6.4.2 6LoWPAN Parçalanma Başlığı

IPv6 standardı, bağlantı katmanı tarafından desteklenecek en az 1280 bayt MTU gerektirir. Ancak IEEE 802.15.4 gibi düşük güçlü bağlantı teknolojileri, tipik olarak 1280

baytlık gerekli MTU'nun çok altında olan küçük çerçeve boyutları ile karakterize edilir. Böylece 6LoWPAN protokolleri için bir parçalanma tabakası tanımlanmıştır. Bu katman, katman 2.5'de, yani MAC ile adresleme arasında yer alır ve böylece adresleme katmanını 3 gerekli MTU ile şeffaf bir şekilde sağlar. Böyle adanmış ve şeffaf bir parçalanma tabakası kullanarak, alt katmanlar hala küçük veri çerçevelerinin enerji verimliliğini kullanabilirken, üst tabakalar yine de IPv6 uyumlu paket boyutlarından yararlanabilir. Parçalanma, MTU boyutlarının 1280 baytta 802.15.4 (127 bayt) ve IPv6 arasında uyumsuz olmasından dolayı ikincil bir sorundur. Parçalanma sistemi, her bir IPv6 çerçevesini daha küçük parçalara bölecektir. Alıcı tarafta, fragmanlar yeniden monte edilecektir. Parçalanma, düğüm konfigürasyonu sırasında seçilen yönlendirme türüne bağlı olarak değişecektir. Parçalanma ve kısıtlama türleri şu şekilde verilir:

Örgüsel altı yönlendirme fragmantasyonu: Fragmanlar sadece son varış noktasında yeniden kurulacaktır. Yeniden montaj sırasında tüm parçaların hesaba katılması gerekir. Varsa, paketin tamamı yeniden iletime ihtiyaç duyar. Bir yan not olarak, örgüsel tabanlı sistemler tüm parçaların derhal iletilmesini gerektirir. Bu, bir trafik patlaması oluşturacaktır. **Güzergah yönlendirme fragmantasyonu:** Parçalar, ağdaki her sıçramada yeniden birleştirilecektir. Rotadaki her düğüm, tüm parçaları yeniden oluşturmak için yeterli kaynak ve bilgi taşır.

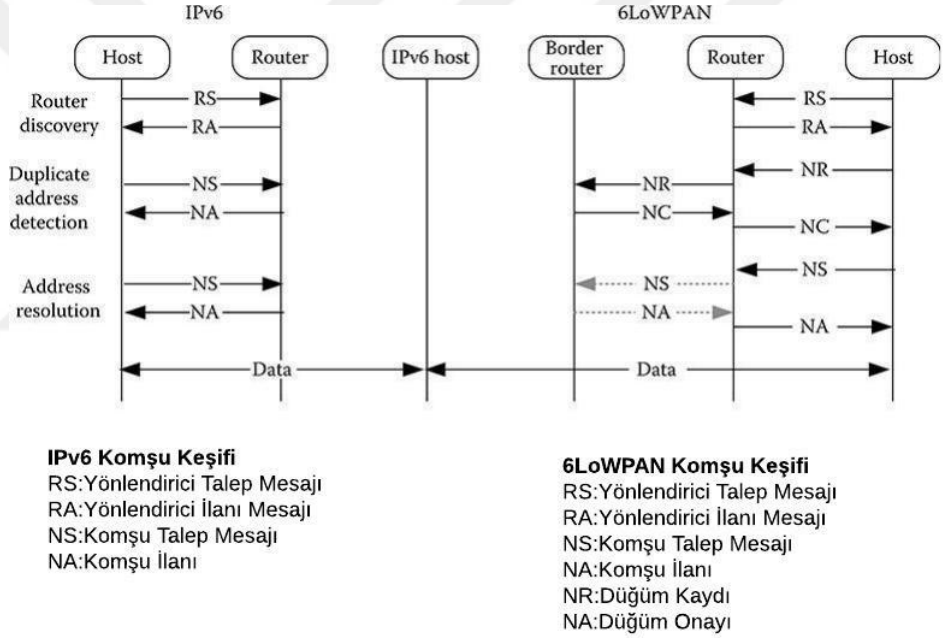
Şekil 3.13: Başlık bilgileri

Parçalanma, batarya tabanlı bir sensör düğümüne ek olarak uygulayabilen işlem ve enerji kabiliyeti gerektiren, kaynak açısından ağır bir görevdir. Veri boyutlarını (uygulama düzeyinde) sınırlamak ve büyük bir ağdaki güç ve kaynak kısıtlamalarını azaltmak için başlık sıkıştırmasını kullanmanız önerilir. Parçalanma başlığı, parçalara ayrılmamış verilerin toplam boyutunu belirten bir Datagram Boyutu alanı içerir. Datagram Tag alanı, bir yüke ait olan fragman setini tanımlar ve Datagram Ofset, parçanın bir faydalı yük dizisine ait olduğunu gösterir. Not, yeni bir parça dizisinin ofset sıfır olarak başlamalı olarak gönderilen ilk fragman için datagram ofset kullanılmaz. [25]

3.6.5 Komşu Bulma

Komşu keşfi (ND), tek bir yönlendirme protokolü olarak RFC4861 tarafından tanımlanır. Örgüdeki komşu düğümler arasındaki iletişimdir ve düğümlerin birbirleriyle iletişim kurmasını sağlar. ND, yeni bir komşunun keşfi, bir ağın büyümesi, küçülmesi ve dönüşmesi

ile yeni ve değişen komşuluk ilişkilerinin ortaya çıkmasıdır. Adres alanının genişletilmesi genellikle IPv4'ten IPv6'ya yapılan büyük değişiklik olarak kabul edilirken, bu değişiklik yalnızca biçimi etkiler. Bununla birlikte, Komşu keşif, IPv6'nın arkasındaki en önemli özelliktir. IPv6'nın Komşu bulması, geçerli bir (global kapsam) IP adresi ve varsayılan yönlendirici adresi gibi diğer ağ yapılandırma parametrelerini almak için IPv4 mekanizmalarının yerini alır. Yerel IPv6 ağlarında, her uç nokta alt ağdan sorumlu yönlendirici ile aynı bağlantılıdır. Bu yönlendiriciden, uç nokta, ağ öneki, vb. gibi adres bilgilerini alır. Ancak WSN / 6LoWPAN gibi örgüsel topolojilerde, uç noktalar 6LoWPAN alt ağından sorumlu olan sınır yönlendiricisi ile doğrudan iletişim aralığında olmayabilir. Sınır yönlendiricisi ile uç nokta arasında, yönlendirme yönlendiricisi olarak görev yapan 6LoWPAN bir cihaz daha gerekebilir. Bu nedenle, 6LoWPAN ağları için, komşu bulma protokolü, doğal IPv6 ağlarına kıyasla topoloji farklılıkları ile baş etmek üzere değiştirilmiştir (Şekil 3.14). [24]



Şekil 3.14: 6LoWPAN Komşu Bulma- IPv6 Komşu Bulma

ND sırasında ortaya çıkan çatışmalar olabilir. Örneğin, bir ana bilgisayar düğümü bir yönlendirici ile ayrılır ve aynı ağda farklı bir yönlendirici ile bir bağlantı kurar. ND yinelenen adresleri ve ulaşılamaz komşuları bulmak için gereklidir. DHCPv6 için komşu keşif ile kullanılabilir. 802.15.4 özellikli bir cihaz, fiziksel ve veri bağlantı katmanlarından sonra 6LoWPAN komşu keşfini gerçekleştirebilir ve ağı büyütebilir. Bu işlem aşağıdaki şekilde ve sonraki şekilde gösterildiği gibi devam edecektir:

1. Düşük güçlü kablosuz için uygun bir bağlantı ve alt ağ bulma.

2. Düğüm tarafından başlatılan kontrol trafiğinin en aza indirilmesi.

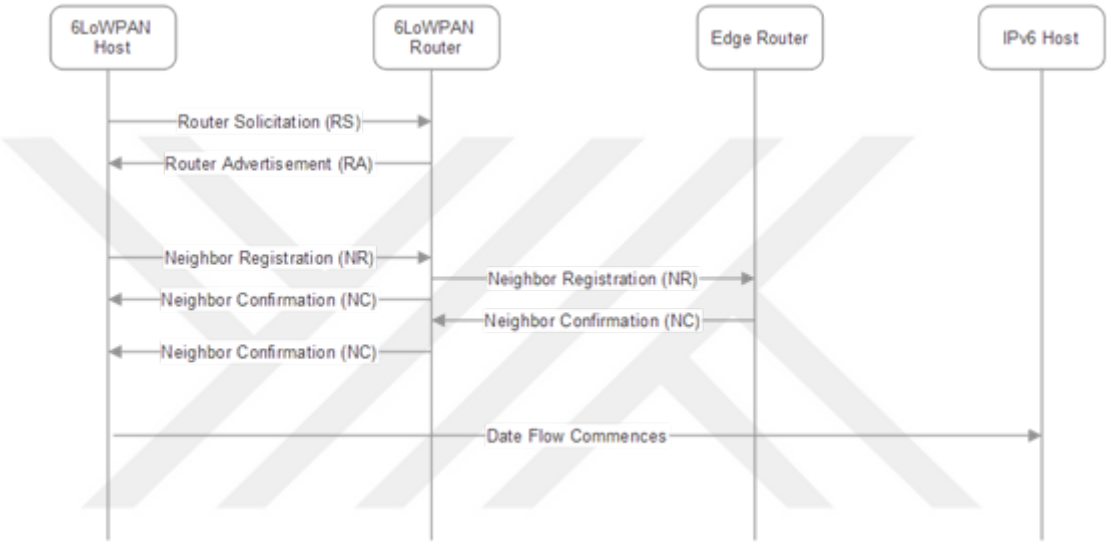
3. Ana bilgisayar ağ örgüsü önekini istemek için RS mesajını gönderiyor.

4. Yönlendirici önek ile yanıt veriyor.

5. Ev sahibi kendisine bir bağlantı yerel tek noktaya yayın adresi (FE80:: IID) atar.

6. Bu link-local tek noktaya yayın adresini bir NR mesajında örgüsel ileten ev sahibi

7. Ayarlanmış bir süre için bir NC'yi bekleyerek Yinelenen Adres Saptama (DAD) gerçekleştirme. Zaman aşımı süresi dolduğunda, adresin kullanılmadığını varsayar.



Şekil 3.15: 6LoWPAN örgü düğümünden örgü yönlendiriciden kenar yönlendiriciye ve daha sonra geniş alan ağına kadar basitleştirilmiş komşu keşif şekli

Şekil 3.15: 6LoWPAN örgü düğümünden örgü yönlendiriciden kenar yönlendiriciye ve daha sonra geniş alan ağına kadar basitleştirilmiş komşu keşif şekli. Örgüsel altından yönlendirme kullanılıyorsa, beşinci adımda alınan bağlantı yerel adresi, 6LoWPAN ağındaki herhangi bir başka düğüme iletişim kurmak için kullanılabilir. Bir rota üzerinde şemada, link-local adresi sadece tek bir atlama olan düğümlerle iletişim kurmak için kullanılabilir. Bir atlamadan daha büyük bir şey, tam yönlendirilebilir bir adres gerektirecektir. [25] .

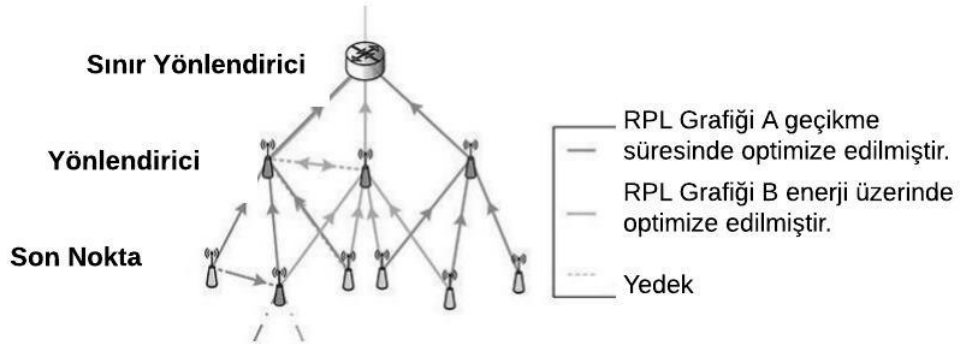
3.6.6 Yönlendirme

Gelişmekte olan 6LoWPAN protokolleri nedeniyle, IETF bu tür ağlar için ayrılmış düşük güçlü IP ağlarında kullanılmak üzere uygun bir yönlendirme çözümü sağlamak zorundaydı. Bu nedenle, ROLL (Düşük Güç ve Kayıp Ağlar Üzerinden Yönlendirme) çalışma grubu oluşturulmuştur. ROLL içinde, IPv6 yönlendirme protokolü RPL'i geliştirilmiştir

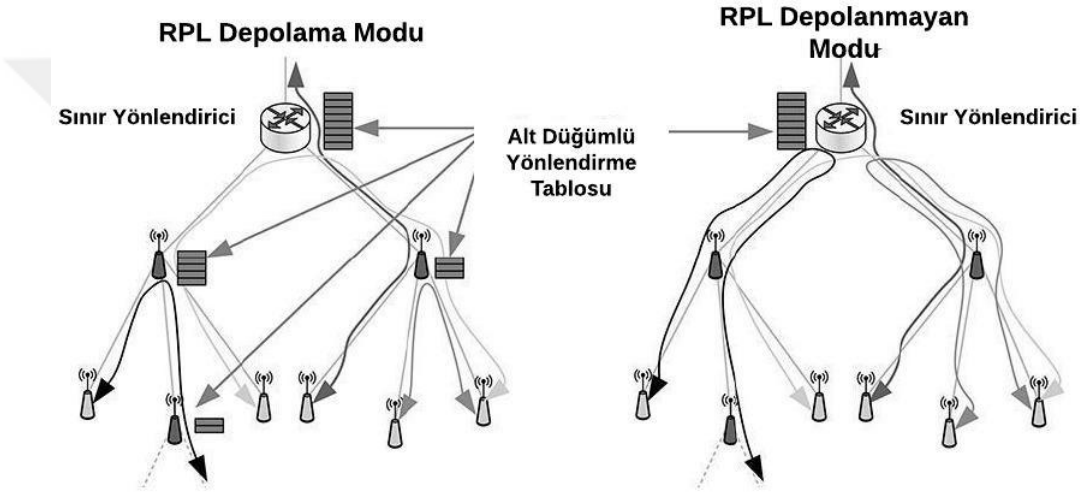
(Düşük Güç ve Kayıp Ağlar için IPv6 Yönlendirme Protokolü Ripple) RPL, IPv6'nın üstünde bulunur. Böylece, 6LoWPAN'larda olduğu gibi diğer IPv6 tabanlı ağlarda da kullanılabilir. RPL, 6LoWPAN ağlarda kullanım için optimize edilmiştir. RPL, verileri 6LoWPAN'dan diğer kısıtlanmamış omurga ağlarına çekmek veya itmek için optimize edilmiştir. Bu nedenle, RPL, Sınır Router'a yönelik yönlendirilmiş bir topoloji oluşturur. Şekilde de görüldüğü gibi birçok kullanım durumuna göre 6LoWPAN'ın sınır yönlendiricisi olacaktır, ancak RPL bununla sınırlı değildir. Grafik (yönlendirme ağacı), yol boyunca enerji tüketimini en aza indirgemek, minimum sıçrama sayımı veya rota yolu üzerindeki yönlendiricilerin kaynaklarına (CPU, RAM, enerji) bağlı olarak trafik yükünü yaymak gibi birkaç ölçüm için optimize edilebilir. 6LoWPAN'da böyle bir şekle sahip olmak bile mümkündür, bu sayede, bir kaynaktan bir Sınır Routera ulaşmak için farklı özelliklere ve metriklere sahip farklı yollar bulunabilir (bkz. Şekil 3.15).

Yönlendiriciler sırayla Sınır (Border) Yönlendiriciye daha yakın yönlendiricilere veya doğrudan yönlendirme topolojisinin Sınır Yönlendiricisine atanır, bu nedenle daha yakın kullanılan metrikle ilgili olarak daha az maliyetli anlamına gelir ve mutlaka fiziksel mesafeyi ifade etmez. Her yönlendirici Sınır Yönlendiricinin varlığını ve hangi uç noktalara veya yönlendiricilere bağlı olduğunu bildirir. Sonuç olarak, Sınır Yönlendiricisi tüm RPL ağını bilmektedir. Yönlendirme topolojisinden iletişim için (yani, alt yönlendiricilerde sınır yönlendiricisine doğru başlayan), bir kaynak yönlendirmesi kullanılır. Bu kaynak yönlendirmesinde, gezilecek tüm ara yönlendiriciler, Sınır Yönlendirici tarafından pakete dahil edilir. Topolojiden yukarı doğru iletişim (yani alt ağdan başlayarak ve Sınır Router'a doğru) veya topolojideki uç noktalar arasındaki iletişim için iki farklı mod mevcuttur (bkz. Şekil 3.17). Her yönlendiricinin ağır ve depolama yoğun yönlendirme tablolarını korumasını önlemek için, yönlendiriciler tüm trafiği Sınır Yönlendiriciye iletebilir ve Sınır Yönlendiriciden yine kaynak yönlendirme kullanılır. Bu moda depolanmayan mod denir. Veri paketlerinin Sınır Yönlendiriciye kadar ilerlemesini ve daha sonra tekrar aşağı inmesini önlemek için, yönlendiriciler kendi yönlendirme tablolarını tutabilir, böylece paketler yalnızca kaynak ve hedefin ilk ortak atağına kadar seyahat etmek zorunda kalır. Bu moda depolama modu denir. [24]

IETF'deki ROLL çalışma grubu tarafından daha fazla durumsuz yönlendirme çözümleri geliştirilmektedir. Bu durumsuz yönlendirme çözümleri, örneğin, iyi bilinen Trickle algoritmasına [RFC2606] dayanmaktadır ve kontrollü bir taşma davranışı denilen yeteneğe sahiptir. Bu davranıştan ötürü, bu tür çözümler örnek olarak düşük güçlü ağlarda IP–Multicast iletişimi kullanılır. [24]



Şekil 3.16: RPL yönlendirme topolojisi



Şekil 3.17: RPL depolama ve depolanmayan modu

Bir WPAN sisteminde iletişimi dinlemek kolay olduğundan, 6LoWPAN birden fazla seviyede güvenlik önlemi uygulanabilir. Protokolün 802.15.4 seviyesinde, 6LoWPAN, AES-128 şifreleme verisini destekler. Ek olarak, 802.15.4 şifreleme ve bütünlük kontrolü sağlamak için CBC-MAC modu (CCM) ile bir çözüm sağlar. Bir 802.15.4 çoğu yonga çipleri, performans iyileştirme için bir donanım şifreleme özelliğine sahiptir.

Protokolün üçüncü katmanında (ağ katmanı), 6LoWPAN IPsec standart güvenliğini (RFC4301) kullanma seçeneğine sahiptir.

Kimlik Doğrulama İşleyicisi (AH): Bütünlük koruması ve kimlik doğrulaması için RFC4302'de tanımlandığı gibi

Encapsulating Security Payload (ESP): RFC4303'te, paketlerde gizliliği sağlamak için şifreleme

ESP, en yaygın üç katmanlı güvenlik paket biçimidir. Ek olarak, bir ESP modu, katman-üç şifreleme için de (RFC4309) katman-iki donanımında kullanılan yeniden kullanılan AES / CCM'yi tanımlar. Bu katmanlı 6LoWPAN düğümleri için üç güvenlik katmanını uygun hale getirir.

Bağlantı katmanı güvenliğine ek olarak, 6LoWPAN ayrıca UDP trafiği için TCP trafiği ve Datagram Aktarım Katmanı Güvenliği (DTLS) için Aktarım Katmanı Güvenliğini (TLS) ile sağlar. [25]

Bölüm 4

6LOWPAN Tabanlı IOT Sistemlerinde Hizmet Reddi Tespiti

4.1 6LOWPAN Tabanlı IOT Sistemlerinde Hizmet Reddi Tespiti

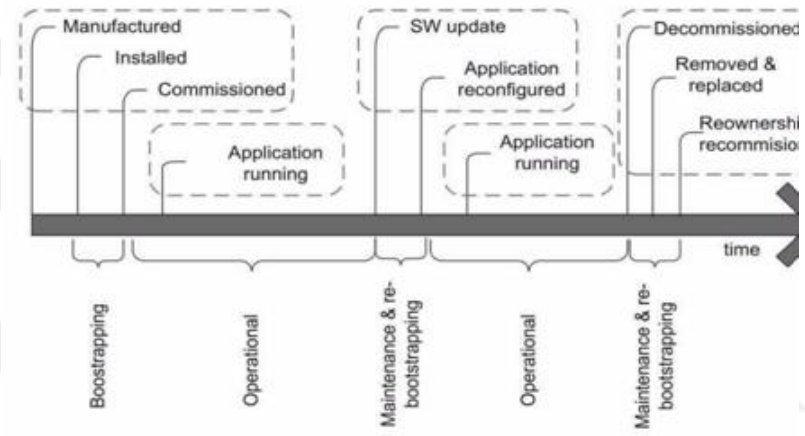
Kablosuz cihazlar günlük hayatımızda giderek daha yaygın ve zorunlu hale geldiğinden, güvenlik kritik bir konu haline gelmiştir. Bu cihazlar ve teknolojiler, yeterince bilinçli yönetilmezse gelecekte daha fazla tehdit oluşturabilirler. Yeterli önlem alınmamış, IoT cihazlar ve kameralar üzerinden yapılan devasa büyüklükteki DDoS ataklarını örnek gösterilebilir. Kötü niyetli birisi, farklı atak türlerini başlatmak için bu zayıflıklardan yararlanabilir. Daha spesifik olarak, hizmet reddi ataklarının WSN'lerin iletişimini kesmede olumsuz etkileri olduğu kabul etmek gerekir. Günümüzde Akıllı Tarımda kullanılan WSN'ler için DoS ataklarına karşı etkili güvenlik mekanizmaları henüz ele alınmamıştır.

IoT'lerde 6LoWPAN'ın zayıflıklarını kullanarak yapılan DoS/DDoS ataklarını tespit etme ve önleme zorlukları bulunmaktadır. Bu sorunları giderebilmek için güvenlik mimarisinin geliştirilmesi ve son kullanıcı tarafında dikkatli konfigürasyonların yapılması gerekmektedir. IoT'de DoS ataklarını tespit etmek için yeni bir güvenlik mimarisi sunulması ve bilinçlenmek gerekmektedir. Profesyonel sistemler ise uçtan uca güvenlik ve sürdürülebilir özellikleri barındırmaya çalışmaktadır.

4.2 IOT'de Güvenlik

IoT, IP ve WSN'ler gibi düşük güçlü radyo teknolojilerini bir araya getirdiğinde, her iki teknoloji de zayıf noktalar bünyesinde barındırmaktadır. WSN güvenliği konusunda

birçok araştırma yürütülmektedir. WSN'lerin DoS ataklarına ve savunmalarına ilişkin araştırmalar yapılmaktadır. IP tabanlı WSN'ler için tehditler ve olası karşı önlemler hakkında bazı çalışmalar yapılmıştır. Bu çalışmalar algılama mimarisini tasarlamak için faydalı olmuştur. Bir IoT' nin yaşam döngüsü, Şekil 4.1'de gösterildiği gibi üç ana aşamaya ayrılabilir: üretim, yükleme / önyükleme ve operasyonel. Bu aşamaların her biri, bir veya daha fazla atağa açıktır. Kısıtlı kaynaklara sahip 6LoWPAN IoT cihazlarına klasik güvenlik çözümlerinin hepsi uygulanmakta ve sınırlı çözümler sağlanmaktadır. Güvenlik mekanizmalarının çoğu temel güvenlik gereksinimlerini garanti etmeyi amaçlamaktadır: Gizlilik, entegrasyon ve kimlik doğrulama gibi[27]. Ancak, WSN'lerin DoS ataklarında kurtulabilecek kadar güçlü özellikleri barındırmadığını, 5. Bölümdeki örnek topoloji üzerine yapılan ICMP Flood atağıyla WSN ağını etkilendiğini göreceğiz.



[27]

Şekil 4.1: IoT Yaşam Döngüsü

Algılayıcı ağları özellikle gizlilik, trafik analizi, fiziksel ataklar ve en önemlisi DoS ataklarını ile ilgili ataklara karşı hassastır. Bazı araştırmalarda algılayıcı düğümlerin güç kaynaklarını hedefleyen uyku reddi ataklarını üzerinde yoğunlaşmıştır. Bu tip ataklar ile güç kaynağının uzun yıllar dayanabilen pil ömrünü aylar hatta günler mertebesine düşürüp ağın pasif duruma düşmesine sebep olabilecektir. Tasarımlar gereği algılayıcılar sadece pasif değil aktif durumda da bulunmaktadır[28]. 6LoWPAN ile ilgili protokoller potansiyel güvenlik açıkları dikkatlice analiz edilmelidir.

4.3 Hizmet Reddi Saldırıları (DoS)

Kablosuz ortamda kurulan ağlarda verileri aktarmak için, gönderme işlemi çeşitli güvenlik riskleri ve tehditlere tabidir. Algılayıcı düğümlerinin kaynakları sınırlıdır. Bu nedenle, bunları gelişmiş güvenlik protokolleri ve teknikleriyle korumak çoğu zaman mümkün değildir. WSN'ler içindeki güvenlik protokolleri ve mekanizmaları, mümkün olduğu kadar

az kaynak kullanarak ağı tatmin edici bir düzeyde güvenceye alacak şekilde geliştirilmiştir. Algılayıcı düğümlerinin aksine saldırgan, sinyal yayımı için güçlü antenler, sabit güç kaynağı, güçlü işlemci ve bellek kapasitesi gibi daha büyük kaynakları ve yetenekleri olan cihazları kullanabilir. Bu, WSN'lere yönelik atak sayısının artmasının nedenlerinden biridir.

WSN'lere yönelik atakların, ağı tehlikeye atması amaçlandığından dolayı, ağ içinde aktarılan verilerin kötüye kullanılması, casusluk yapmak veya ağa müdahale etmeyi amaçlamaktadır. Saldırılar, saldırdıkları protokolün OSI katmanına göre sınıflandırılabilir. WSN'lere yapılan en yaygın ve tüm protokol yığını katmanlarından geçen ataklardan biri DoS' dur. Bu atağın asıl amacı ağın düzgün çalışmasını engellemektir. Saldırgan veya saldırganlar, çeşitli atak türlerini kullanarak meşru ağ düğümlerinin ağ kaynaklarını kullanmasını önler. Ağ birden fazla kaynak tarafından atağa uğradığında, bu duruma DDoS atağı denir. Bu tür bir atak, ağ işleyişinde tek bir düğüme yapılan ataklardan çok daha fazla soruna neden olabilir. Saldırgan, WSN'nin bir parçası olmayan bir dış düğüm olabilir veya saldırgan tarafından ele geçirilen meşru düğümlerden biri olabilir.

DoS saldırısının göstergelerinden bazıları:

- Ağ performansında azalma,
- Ağ parçalarına yanıt verdirmeme,
- Spam mesajlarının arttırılması,
- Paketlerin gecikmesi veya kaybı ve onayları,

Şekil 4.2'de, en yaygın DoS ataklarını protokol yığını katmanlarına göre sınıflandırılmış olarak gösterilmiştir.

DOS saldırılarının OSI katmanlarına göre sınıflandırması Bu bölümde, protokol yığını katmanlarına göre sınıflandırılmış farklı tipte DoS ataklarını açıklanmaktadır. [28]

İletişim ağları için en önemli şey cihazların kullanılabilirliğidir. Ağın iletişimini azaltan, kesen veya tamamen ortadan kaldıran herhangi bir olay DoS atağı olarak kategorize edilir. Sistemin çalışırlılığının ortadan kalkmasından dolayı; DoS ataklarını önemli bir güvenlik olayı olarak kabul edilir. Bazı DoS ataklarını uzak konumlardan gerçekleştirilebilir ve bir çok noktadan yapılan atağa DDoS denir. Hizmet kullanılamıyor hale gelmeden önce bir DoS atağı bulmak oldukça zordur. Aşağıda OSI katman seviyesinde ataklar anlatılmaktadır. [29]

Katman	Saldırılar
Fiziksel Katman	Jamming Interference Node tampering and destruction
Bağlantı Katman	Collision Exhaustion Unfairness
Ağ Katman	Sybil Selective forwarding Sinkhole Hello flooding Wormhole
Taşıma Katman	Flooding Desynchronization
Uygulama Katman	Overwhelming sensors (sensor overload) Path based attack

Şekil 4.2: DOS Saldırısı

4.4 Fiziksel katmandaki DoS saldırıları

Jamming (Yayını Bozma): Algılayıcı ağı tarafından kullanılan radyo frekanslarına müdahale etmek için başka bir radyo sinyalini kullanmak anlamına gelir. Jamming sürekli veya aralıklı olarak yapılabilir. Her iki durumda da, ağ ciddi bir şekilde zarar görecektir. Jamming saldırısı genellikle "operasyonel aşama" sırasında gerçekleştirilir. Jamming, çarpışmalar oluşturmak için sahte paketler göndererek bağlantı düzeyinde gerçekleşir. WSN'lere yapılan en yaygın DoS saldırılarından birisidir. Saldırılar sürekli girişim içinde, rastgele, aldatıcı ve reaktif işlevler olarak sinyal yayar. Sel saldırısı, saldırgan ağ içindeki meşru bir düğüm gibi davranır ve sürekli veri göndererek gerçekleşir. Ayrıca saldırgan ağ içinde iletişim olduğunu fark ettiğinde, jamming sinyali yayar. Özellikle, bir süre kestikten sonra, radyo kanalını kapatır ve "uyku" moduna girer. Bir süre uyuduktan sonra iletişimi algıladığında yayını bozmaya devam edecektir. Saldırgan ağın gerçek bir parçası gibi gözükmek için ağa belirli aralıklarla bilgi gönderir. [29]

Karşı önlemler: Spread spektrum tekniği bu tür atakların önlenmesinde yardımcı olur. Yayılmış spektrum tekniğinin yanı sıra, düğümlerin jamming ataklarına karşı koymak için kendi stratejilerine sahip olmaları gerekir. Yayını bozma sinyali süresince, uyku verimliliğini korumak için düğümü uyku moduna geçirmek, ayrıca jamming sinyalinin hala aktif olup olmadığını kontrol etmek için periyodik olarak düğümleri uyandırma yaparak jamming sinyalinin olup olmadığını kontrol edilebilir [30]. Nancy, J. T.' nin makalesinde [31], yayını bozma ataklarından korunma ve tespit için yeni yaklaşım anlatılmıştır. Bu yaklaşım, WSN'deki parazit seviyesini belirleyen iki modül kullanır. İlk modül, ağı daha önce büyük miktarlarda jamming sinyali yayan düğümler olarak işaretlenmiş dahili düğümlerden korumak. İkinci modül yeni potansiyel saldırgan düğümlerini tespit etmektir.

Ghildiyal makalesinde gösterilen sonuçlar, bu yaklaşımın yüksek düzeyde saldırgan tespitini sunduğunu ortaya koymaktadır.[30]

Interference (Parazit), saldırganın, ağın çalışmasını engellemek amacıyla periyodik olarak veya sürekli olarak radyo dalgaları şeklinde büyük miktarda ağ trafiği oluşturması durumunda ortaya çıkar.

Karşı önlemleri: Bu sorunu çözmek için duraklama sırasında anahtarların gecikmeli sinyal ile simetrik anahtar algoritması kullanılır [32]. Danyang ve arkadaşları (2013)[33], daha etkin bir frekans aralığı elde etmek için önceden belirlenmiş bir eşik değerine dayanan uyarlamalı filtreleme mekanizmasının kullanılması önerilmektedir. Bu girişimin azalmasına ve kaynakların WSN içinde daha verimli kullanılmasına katkıda bulunur.

Node tampering and destruction (Düğüm kurculama ve imhası), Bu sorunu çözmek için duraklama sırasında anahtarların gecikmeli sinyal ile simetrik anahtar algoritması kullanılır [32]. Danyang ve arkadaşları (2013)[33], daha etkin bir frekans aralığı elde etmek için önceden belirlenmiş bir eşik değerine dayanan uyarlamalı filtreleme mekanizmasının kullanılması önerilmektedir. Bu mekanizma girişimin azalmasına ve kaynakların WSN içinde daha verimli kullanılmasına katkıda bulunur.

Düğüm kurculama ve imhası (Node tampering and destruction), Saldırgan düğüme fiziksel erişim sağladığında ve işlevini devre dışı bıraktığında veya düzgün çalışmasını sağlayan bilgileri değiştirmek amacıyla belleğine erişebildiği zaman meydana gelir. Arızalı düğüm iletişimde girişime neden olur.

Karşı önlemler: Düğüme fiziksel erişime karşı korumanın yolu, onu korumak için fiziksel bir paket kurmak veya düğümü zor erişilen bir yere yerleştirmektir.[32]

Nesnelerin klonlanması: Bu istismar, “üretim süreci” sırasında ve “işletme aşamasında yapılır. İlk durumda, bir iç saldırgan yetkisiz amaçlar için önceden programlanmış olanla orijinal bir yazılımın yerine geçebilir. "İşletim aşaması" sırasında, bir düğüm yakalanabilir ve çoğaltılabilir ve bunlar genellikle düğüm çoğaltma ataklarını olarak bilinir. Düğüm yakalama, aşağıdaki gibi başka ataklara da yol açabilir: Güvenlik parametrelerinin çıkarılması, donanım yazılımı değiştirme ataklarıdır.

Dinleme: Bu güvenlik zayıflığı, tüm kablosuz iletişimin "bağlantı gönderme aşamasında" ortaya çıkar; Saldırgan çeşitli bilgileri konfigürasyonları işletim kanalını pasif olarak dinleyerek alabilir; daha sonra bunları kullanarak, saldırgan meşru bir düğüm olarak ağa katılabilir ve başka ataklar gerçekleştirebilir. Daha sonra, ortadaki bir adamın atağına yol açabilir.

Veri bağlantı katmanında DoS saldırıları Çarpışma, iki düğüm aynı frekansta aynı anda paket göndermeye çalıştığında ortaya çıkar. Mesaj gönderen vericide paket kaybı

veya toplam kontrol hatası görülür. Kötü niyetli düğüm, paketin meşru düğümden alıcıya gelmesini engellemek için aynı anda meşru düğümler olarak veri göndermeye çalışır.

Karşı önlemler: Bu sorunun üstesinden gelmek için ECC (hata düzeltme kodu) kullanılmalıdır. Kodların çoğu daha az çarpışmayı düzeltir, ancak ek işlemci kapasitesi ve iletişim kaynakları gerektirir. Asıl sorun, saldırganın düzeltilebilecek olandan daha fazla hata üretme yeteneğine sahip olmasıdır [32]. (Dbibih ve diğerleri, 2016)[34] Makalesinde CAMAC'a erişimi sınırlandırmak için yeni bir algoritma tasarlamıştır. Bu algoritmanın işlevi, çarpışma sayısını en aza indirmek için her mesaja öncelik vermektir.

Tükenme: kanalın tamamen tıkanmasına neden olan sürekli çarpışmalarda meydana gelir. Genellikle saldırgan çok sayıda RTS gönderir (gönderme istekleri).

Karşı önlemleri: Bunun çözümlerinden biri, MAC'in (Orta Erişim Kontrolü) belirli bir düğümden gelen çok sayıda talebi reddetmesidir [35]. Bu atak için başka bir çözüm, zaman çoğullamayı kullanmak, yani erişim ortamı için bir zaman sınırı belirlemek ve bu şekilde saldırganın aşırı sayıda talebini reddetmek şeklindedir.[30]

4.5 Ağ katmanında DoS saldırıları

Yönlendirme döngüleri oluşturmak, ağ trafiğini çekmek veya püskürtmek, kaynak rotalarını uzatmak veya kısaltmak için IoT'deki yönlendirme bilgisi taklit edilebilir, değiştirilebilir veya tekrarlanabilir. Diğer olası yönlendirme ataklarını şunlardır: flooding, silkhole attack, selective forwarding, wormhole attack ve sybil atağıdır. Daha fazla analiz, paket parçalanma ataklarını gibi 6LoWPAN'a dayalı ataklarve sıralama atakları, yerel onarım ataklarını gibi RPL protokolleri de mümkündür.

Sybil, kötü amaçlı düğüm ağdaki diğer düğümlere birden fazla kimlik sunduğunda gerçekleşir. Bir düğüm birden fazla yerde veya tek bir ağda birden çok kez görülebilir. Saldırganın, her bir komşu düğüm çiftinin başlatılması veya genişletilmiş aralıktaki bulunan frekans atlaması için benzersiz bir anahtar kullandığı ağda, bu tür bir atağı iletmesi çok karmaşık olabilir. Yönlendirme protokolleri atağa uğradığında Sybil ataklarıyla, kötü niyetli düğüm birden fazla düğümün içinden geçmesine yol açan çoklu düğümlerin kimliğini alır.

Karşı önlemler: Sybil ataklarına karşı savunma, kimlik kontrolü ve kimlik bazlı anahtar ve yer tabanlı anahtar kullanımı ile sağlanır [36]. Sybil ataklarını sorgulamalarla tespit etmenin yolu açıklanmıştır.[37] Bu, kümedeki ana düğümler tarafından kümedeki düğümlere sorgu gönderilerek gerçekleştirilir.

Selective Forwarding (Seçmeli iletme atağı), kötü niyetli düğüm alınan paketlerin bazılarını reddettiği ve diğerlerini ilettiği zaman meydana gelen bir ataktır. Saldırgan paketleri belirli kriterlere göre reddedebilir. Bu nedenle, belirli bir düğümden alınan tüm paketleri iletebilir ve tüm paketleri başka bir düğümden reddedebilir. Bu tür atakların özel bir örneği tüm paketlerin reddedilmesidir, ancak bu durumda komşu düğümler kötü niyetli düğümü kolayca tespit eder ve alternatif yollar kullanmaya başlar.

Karşı önlemler: Bu tür bir atağın çözümü birden fazla yol kullanmaktır [28]. Mathur ve diğerleri, 2015 makalesinde[46] , güvenli yönlendirme için değiştirilmiş protokol açıklanmıştır. Bu protokol, yönlendirme gibi seçmeli yönlendirme gibi ataklarını tespit etme yeteneğine sahiptir.

Wormhole, kötü niyetli düğüm, belirli bir alandaki tüm veri trafiğinin içinden geçirileceği şekilde konumlandırıldığında rolü, alınan tüm paketleri reddetmektir. Kötü niyetli düğüm, çevreleyen düğümler tarafından veri göndermek için en etkili düğüm olarak tanımlanır. Düğüm bunu, güçlü bir verici kullanarak sınır yönlendiriciye atlama sayısını azaltarak başarır. Ağda ne kadar uzun süre çalışan kötü niyetli düğüm çalışırsa, veri gönderen düğümlerin sayısı o kadar artar. Yapay bir faydalı yol kullanılarak bir wormhole atağı gerçekleştirilebilir. Bu tür atakta saldırganın diğer düğümlerden daha fazla hesaplama ve iletişim gücü vardır ve baz istasyonuyla yüksek kaliteli bir tek sekmeli bağlantı kurmayı başarır. Daha sonra komşularına yüksek kaliteli yönlendirme mesajını yayar. Bundan sonra, tüm komşular, davetsiz misafirleri geçmek için trafiğini baz istasyonuna yönlendirir ve wormhole atağı başlatılır[28]

Karşı önlemler: Bu tür atakların çözümlerinden biri, coğrafi yönlendirme protokolünün kullanılmasıdır[28]. Wazid ve ark.[47], 2013 yılındaki makalede, bu tür ataklarını tespit eden ve önleyen algoritmalar açıklanmaktadır.

Hello Flooding, saldırgan güçlü bir emisyon gücüne sahip ekipmanları kullanarak merhaba mesajı gönderdiğinde gerçekleşir. İleti, asıl saldırgan genellikle düğümden uzak ve gerçekte menzilinin dışında olmasına rağmen, çevresindeki düğümleri saldırgan olarak algılayan çok sayıda düğüm tarafından alınır. Meşru düğümler saldırgana mesaj gönderir ve saldırganın bu mesajları alması durumunda onları başka şekillerde reddeder veya kötüye kullanır. Mesajların saldırgan düğümüne iletilmemesi durumunda içeriği kaybolur. Yani, çok sayıda protokol, her bir düğüm tarafından 'merhaba' mesajı gönderilmesini gerektirir [28]. Her düğüm mesajı komşularına sunar, böylece onunla iletişim kurabilirler. Bu tür bir atak için, saldırgan genellikle sensör düğümlerinden daha güçlü bir yapılandırmaya sahip bir dizüstü bilgisayar kullanır.

Karşı önlemler: Bu tür bir atağın çözümü, üçüncü düğüm [37] veya coğrafi yönlendirme protokolü [32] tarafından kimlik doğrulama kullanımıdır. Raporda (Maheswari 2016)[48]

yeni güvenlik yönlendirme şeması sunmuştur. Bu şema, gelişmiş yönlü doğrulama şemasına dayanmaktadır. Saldırgan, ağ içindeki düğümlerin ortalama sinyal gücü kontrol edilerek belirlenebilir, bu nedenle daha büyük sinyal gücüne sahip olan düğüm, daha sonra çevresindeki düğümler potansiyel saldırgandır [38].

SinkHole, saldırgan, ağın bir kısmı ile diğeri arasındaki veri trafiğini doğrudan yavaş hızlı bağlantı kullanarak tünelediğinde gerçekleşir. Bu atak için genellikle biri sınır yönlendiriciye yakın olan iki kötü niyetli düğüm kullanılır. Bir düğüm diğer verileri çevreleyen düğümlere veri iletmek için en iyi düğüm olarak sunulur. Yönlendirme, genellikle iki kötü niyetli düğüm arasındaki bir tüneli kullanarak tek atlamada çalıştırılabilir görünmektedir.

Karşı önlemler: Coğrafi yönlendirme protokolü yoluyla bu tür bir atağın olası olarak en aza indirilmesi sağlanabilir; Sinkhole atağı ile aynıdır[28]. Goyal et al.[49], 2015 makalesinde solucan deliği ataklarına karşı savunmalar şu kategorilere ayrılır: konum ve zamansal temelli savunma yaklaşımı, (zaman senkronizasyonu ve gizli anahtarların dağıtımına dayanır), bağlantıya ve çevresindeki düğümlere dayalı savunma yaklaşımı (atlama sayımı ve komşu düğümlerin listelenmesine dayanır) ve topolojiye dayanan yaklaşım (ağ izlemesi ile ilgilenen fazladan unsurlar eklenmesine dayanır).

Uygulama Katmanı saldırısı: Uygulama Katmanı atağı: CoAP, 6LoWPAN için uygulama katmanı protokolü olarak standartlaştırılmıştır. Hala gelişmekte olduğundan, gelecekte birçok güvenlik sorunu ortaya çıkabilir. Bazı olası güvenlik açıkları SYN Flood, protokol ayrıştırma, URI'yi işleme, proxy oluşturma ve önbellekleme, amplifikasyon riski, IP adresi sahtekarlığı atağı, çapraz protokol ataklarıdır.

Overload, saldırgan, algılayıcıları uyararak düğümü aşırı yüklemeye çalıştığında oluşur; bu, büyük miktarda veri trafiğinin sınır yönlendiriciye doğru iletilmesine neden olur. Bu saldırı bant genişliğini aşırı yükler ve düğümün gücünü boşa harcıyor.

Karşı önlemler: Bu tür bir atak, algılayıcıların hassasiyetini ayarlayarak ve düğümlerden gelen veri gönderme hızını sınırlayarak önlenebilir [32]. Bant genişliğini sınırlama ve verimli toplama, bu atağın etkinliğini başarıyla azaltabilir.

Replay Routing Information, saldırgan iki düğüm arasındaki iletişimi uçtan uca geçirmek için tekrar paketler enjekte ettiğinde gerçekleşir. Baz istasyonuna giden yoldaki her düğüm paketi iletir ve çok sayıda sahte paket gönderilirse bunların tümü meşgul olur. Bu nedenle, bu atak ağ bant genişliğini ve düğümlerin enerjisini tüketir [28].

Karşı önlemler: Çözüm, iyi bir kimlik doğrulama yöntemi veya tekrar oynatma koruması seçmektir.

4.6 IoT Üzerinde Yapılan DoS Çalışmaları

WSN bağlamında çeşitli DoS atak savunma mekanizmaları ve karşı önlemleri için çalışmalar bulunmaktadır. IP tabanlı WSN'lerle ilgili genel QoS tehditleriyle ilgili bir çalışma [38] 'da açıklanmıştır. Ancak IoT dünyasında DoS ataklarını tamamen bertaraf edebilecek hiçbir önlem veya savunma mekanizması bulunmamaktadır.

WSN'lerde yapılan araştırmalar, WSN'lerin ataklarını savunmak için çeşitli teknikler önermektedir. Genel olarak, merkezi çözümler ölçeklenebilir değildir; dağıtılmış ve işbirlikçi yaklaşımlar daha verimli ve sağlam olabilir, ancak uzun süreli tutarlılık ve istikrar ciddi konulardır. Sistemi tüm DoS tehditlerinden korunmak gerekli hale gelir. IoT ile ilgili son çalışmalar, aşağıdaki güvenlik önlemleri sınıflarını önermektedir:

Güvenli Önyükleme: Önyükleme, bir aygıtın bir ağ parçası veya benzeri aygıtlarla ilişkilendirildiği veya bağlandığı bir işlemdir. Önyükleme aşamasında, benzersiz bir kimlik ve diğer güvenlik parametreleri her cihazla ilişkilendirilir. Güvenli önyükleme, yalnızca kimliği doğrulanmış cihazların ağa erişmesini sağlar. İlk kurulumun gerçekleştirilmesi için en basit mekanizma (güvenlik parametreleri, düğüm kimliği) fiziksel arayüz (USB, kablo, algılayıcı, bağlantı vb.) üzerindendir. Kablosuz önyükleme gizlilik sağlayan gelişmiş şifreleme mekanizmaları kullanılarak önlense bile gizli konuşmaya neden olabilir [39]. Anahtar dağıtım mekanizmasını optimize etmek için, WSN'lerin [40], literatürde WSN cihazları arasında güvenli iletişim ve kimlik doğrulamayı desteklemek için birkaç anahtar yönetim şeması önerilmiştir.

Uygulama Katmanı Güvenliği: Taşıma Katmanı Güvenliği (TLS) IoT'de çok önemli bir güvenlik fonksiyonu olarak kabul edilmektedir [39]. Aslında, mevcut ve öngörülen IoT uygulamaları daha hassas verileri ele alıyor; Tüm bu verilerin güvence altına alınması, IoT için büyük bir gerekliliktir. Bunları yalnız tutmak, IoT için temel güvenlik gereksinimleri sağlayabilir. Bazı çalışmalarda teknolojilerdeki uygulama katmanı güvenliğine odaklanmaktadır: IKEv2 / IPsec, TLS / SSL, DTLS, HIP, PANA ve EAP.

IDS çözümleri: IDS'ler, herhangi bir güvenlik sistemi için ilk savunma hattını sağlar. Gizlenmiş bir atağı tespit etmenin önemli bir güvenlik özelliği olduğu düşünülüyor. IDS'ler, iki ana tespit yöntemine göre sınıflandırılabilir: yanlış kullanım veya imza bazlı tespit ve anomali tespiti. Birincisinde, önceden tanımlanmış bir dizi kural IDS'ye yüklenir ve ağın olaylarıyla eşleşir; şüpheli bir olay tespit edildiğinde bir uyarı tetiklenir. Anomaliye dayalı tespitlerde normal ağ davranışı kaydedilir ve mevcut ağ durumuyla karşılaştırılır ve ağ anormal davrandığında bir olayı tetikler. Yanlış algılama, yeni ataklara açıktır, oysa anomali saptama yöntemi, daha yanlış pozitif olaylar yaratır. Bu iki teknik, hatalı pozitif olayları azaltarak algılama doğruluğunu arttırmak için bir araya getirilebilir: ortaya çıkan yaklaşıma Hibrit Algılama denir. Literatürde WSN'ler için çeşitli

IDS çözümleri önerilmiştir [41], [42], ancak çoğu IP tabanlı WSN ortamında uygulanabilir değildir. IP tabanlı IoT için özel olarak tasarlanmış bir Host Based IDS sistemler bulunmaktadır. Mevcut IDS çözümlerinin karşılaştırmalı bir çalışması aşağıdaki tabloda açıklanmaktadır.

Şema	Benzeşme / OS	Algılama Metodu	Açıklama
SVELTE (IDS for IoT)[24]	Cooja (Contiki)	Karışık	Host based IDS, 6Mapper (Reconstructs RPL's network information)
RIDES (IP-Based WSNs)[25]	ns2	Karışık	Bloom Filters, CUSUM charts
Specification Based IDS for RPL (IP-Based WSNs) [18]	-	Tanımlama	Finite state machine design to detect RPL based attack.
Novel Hybrid IDS (WSNs)[26]	-	Karışık	Clustered approach to save energy
Energy Efficient Hybrid-IDS (WSNs)[27]	Omnet++	Karışık	Cluster Based, Energy Efficient
An Experimental Study of Hierarchical IDS (WSNs) [28]	NesC in TinyOs	Suistimal	Hierarchical Model.

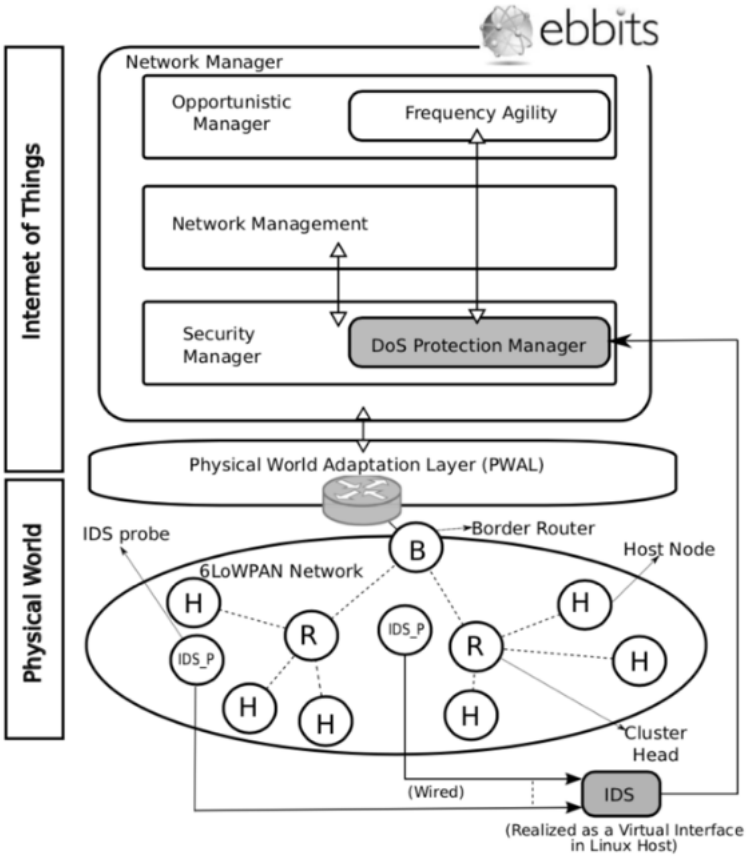
Şekil 4.3: IDS Şemalarının Analizi ve Karşılaştırılması

SoTA analizi, mevcut çözümlerin sınırlarını belirledi. IDS'lerin dezavantajlarını :

Mevcut IDS'lerin Dezavantajları: Önerilen stratejilerin çoğu, hafif ya da verimli algoritmalar ya da bir ya da daha fazla kaynak kısıtlı WSN düğümü içinde programlanabilen benzer yöntemler içerir. Önerilen IDS'lerin çoğu IP tabanlı WSN'ler için tasarlanmamıştır. Bu programlar merkezi ya da dağıtılmış halde iken merkezi sistemler tek bir başarısızlık noktasına doğru gider. Programlanan düğümler, komşuları ile aynı sınırlı yeteneklere sahiptir, bu nedenle DoS ataklarının çoğundan eşit derecede zarar görürler. Bir atak tespit ederse, bu düğümler aynı "kablosuz kanal" üzerinden mesajı gelişmiş algılama işlemleri (imza eşleştirme veya anomali tespiti) için grup / küme kafalarına veya baz istasyonlarına (daha güçlü bir cihaz) iletir. Flooding ve Jamming gibi DoS atakları, kablosuz kanalı kullanılamaz hale getirir, dolayısıyla IDS'nin en temel amacı başarısız olur. 5. Bölümde yaptığımız çalışma da kablosuz kanalı kullanılmaz hale getirerek sadece ağ geçidi tarafında uyarı mekanizmasıyla farkındalık elde edilmiş olacaktır.

4.7 Örnek Gösterilen EBBITS Projesindeki DDoS Çalışması ve Çözüm Önerileri

Ebbits Projesindeki önerilen çözümün, 6LoWPAN ağlarındaki DoS ataklarında kesintiye uğramadan önce tespit etmek ve ağ kullanılabilirliğini arttırmayı amaçlayan karşı önlemlerin uygun şekilde yürütülmesini hedeflemiştir. 6LoWPAN'da DoS ataklarının etkili bir şekilde tespit edilmesini desteklemektir. IDS'ler söz konusu olduğunda, geleneksel çözümlerin geniş kapsamlı atakları, özellikle DoS atağını tespit etmede etkili olduğu kanıtlanmıştır.



Şekil 4.4: DoS Algılama Mimarisi

A. DoS Algılama Mimarisi IoT'deki DoS ataklarını tespit etmek için, algılama sisteminin DoS ataklarına karşı önlemlerinin olması gerekir. Ayrıca ölçeklenebilir ve gerçek dünya IoT senaryolarının çoğuna uygulanabilir olmalıdır. Bu tasarım kriterleri, IoT için DoS algılama mimarisi geliştirilirken göz önünde bulundurulur. DoS algılama mimarimiz, ağlarındaki DoS ataklarını tespit etmek için tasarlanmıştır. Şekil 4.4'de bildirildiği gibi DoS algılama mimarisi, ebbit'lerin ağ sistemi ile bütünleşmiş 6LoWPAN ağını temsil eder. IDS probu (IDS_P), IDS'nin 6LoWPAN ağ trafiğini dinlenmesine yardımcı olur.

Bu araştırmanın en önemli katkıları DoS koruma sistemi ve eBits ağ sistemi ile güvenlik sistemi olarak entegre edilen IDS'dir. Aşağıda, öncelikle ağ yöneticisini ve bileşenleri kısaca açıklanmakta; daha sonra önerilen DoS koruma sistemi ve bileşenleri ayrıntılı olarak açıklanmaktadır. Mevcut önerilen mimari, geniş kapsamlı ataklarını tespit edebiliyor olabilir. Bununla birlikte, ataklara karşı savunma mekanizmaları, yani izinsiz giriş önleme sistemleri (IPS) sağlanması bu çalışmanın kapsamı dışındadır ve bu çalışmanın bir sonraki adımı olacaktır.

Fiziksel dünya: Şekil 4.4'de gösterilen fiziksel dünya, gerçek dünya algılayıcılarıinden veri toplamayı amaçlayan basit bir 6LoWPAN ağını temsil eder. Birkaç ana bilgisayar (H) düğümü, ağı kendi küme düğümleriyle (R) birlikte oluşturur; küme düğümlerinden elde edilen toplu ağ verileri, bir sınır yönlendiricisi (B) aracılığıyla ağ yöneticisine iletilir. Gerçek dünyadaki senaryoda fiziksel dünyayı oluşturmak için birçok akıllı nesne (RFID, Sensör, Akıllı Telefon vb.) Bir araya getirilmiştir. Fiziksel dünya adaptasyon katmanı (PWAL), ebbits'lerin özel bir ağ bileşenidir ve fiziksel cihazlar / akıllı nesneler ve ebbits ağ yöneticisi arasındaki düşük seviye etkileşimi sağlar.

eBits Ağ Yöneticisi: Ağ yöneticisi, üç ana alt bileşeni birleştirir: ağ yönetimi, fırsatçı yönetici ve güvenlik müdürü olmak üzere üç ana alt bileşeni birleştirir.

Ağ yönetimi, ağ izleme ve yapılandırma hizmetleri sunar. Ağı izleyerek performans bilgisi sağlar: Parazit seviyesi, gecikme süresi ve çarpışmalar gibi performans bilgilerini tespit etmeyi sağlar. Ağ yönetiminin rolü, fırsat bilgisini, ve güvenlik yöneticisini ve herhangi bir zamanda sağladığı ağ bilgisini sağlayarak birlikte çalışabilir hale getirmektir.

Fırsatçı yönetici, ebbits çerçevesi için iletişim esnekliği ve optimizasyonu sağlar. Sistemin her zaman mevcut en iyi ağ iletişimi ile çalışmasını sağlar. WSN / 6LoWPAN'lara gecikmeye dayanıklı ağ iletişimi (DTN) ve frekans çevikliği (FA) yetenekleri sağlar [43]. FA, kanal doluluk durumlarını gerçek zamanlı olarak analiz ederek ağın parazit seviyesinden haberdar olmasını sağlayan bir mekanizmadır. Amaç, mevcut en iyi kanalı belirlemektir. Sistem parazit seviyesinin belirli bir eşiği aştığını tespit ettiğinde, FA mekanizması işletim kanalını mevcut en iyi kanala [43] çevirmek için bir prosedür başlatır.

Güvenlik yöneticisi, Şifreleme ve politika uygulama gibi ağda güvenlik mekanizmaları sağlar. Şifreleme ve güven mekanizmaları sağlayarak, ebbits ağ yöneticisi ve ara katman yazılımı arasında güvenli iletişim kurulmasını sağlar. Bu çalışmada, DoS korumayı ebbits'in güvenlik sistemi bünyesinde tanıtılmıştır.

DoS koruma yöneticisi: DoS koruma yöneticisi, izinsiz giriş denemeleri olduğunda IDS'den uyarılar alır. Daha sonra, diğer ebbits yöneticilerinden (ağ yönetimi ve fırsat yöneticisi) bilgi parçalarını (girişim oranı, paket bırakma oranı vb.) Çıkarır ve gerçek bir atağı doğrulamak için analiz eder. DoS koruma yöneticisinin ana bileşeni, atağın

tespitinde rol alan IDS'dir. Bu hibrid yaklaşım, diğer ebbits yöneticileri tarafından toplanan aynı ağla ile ilgili ek verilerden yararlanılarak, IDS uyarılarının yanlış alarm oranını azaltır.

IDS: Önerilen IDS, ağ tabanlı bir IDS'dir (NIDS). Genellikle ağ paketini yakalayıp inceleyerek çalışır. 6LoWPAN trafiğini izlemekten ve ağda herhangi bir yanlış davranış durumunda uyarıları yükseltmekten sorumludur. Bu IDS aracısı, Şekil 25' de gösterildiği gibi ağ içinde yayılan birden fazla IDS_P'den elde edilen ağla ilgili bilgilerin işlenmesinden sorumludur. Bu IDS_P, karışık modda çalışır, hedef adreslerinden bağımsız olarak tüm mesajları dinleyebilir. Büyük ölçekli ağları yönetmek için çoklu probeların kullanılması gerçekten gereklidir. Bu gibi probeların 6LoWPAN işletim sisteminin dışında olduklarından ve ağ faaliyetlerine katılmadıklarından bahsetmek önemlidir. Aktif bir DoS atağı gerçekleştirildiğinde, kablosuz kanal bozulur ve IDS_P'ler aracılığıyla alınan mesajlar güvenilir olamaz, bu nedenle onları ve IDS'i bağlamak için kablolu bağlantı kullanılır. Bilinen ve bilinmeyen atakları yüksek hassasiyetle tespit etme kabiliyetine sahip olmak için, bir hibrit tespit modelinin daha iyi çalıştığı ve dolayısıyla geliştirme için kabul edildiği kullanıldığı kabul edilir. Özetle, önerilen sistem, 6LoWPAN'ın ağ trafiğini, karışık modda çalışan bir ya da daha fazla IDS_P aracılığıyla izler ve hibrit IDS tespit yöntemini kullanarak atağı tespit eder. DoS koruma yöneticisi, uyarıları aldığınızda, diğer ağ yöneticisi bileşenleri tarafından sağlanan bilgileri kullanarak atağı onaylar. Bu atak tespit yaklaşımı genel olarak herhangi bir ağ yöneticisiyle uygulanabilir.

Senaryo Önerilen mimarinin uygulanmasını açıklamak için, basit bir üretim senaryosu düşünelim. Ekipmanın hızlanmasını, üretim ayarında yer alan alanın basıncının ve sıcaklığının izlenmesini gerektirir. Bu senaryoda, herhangi bir DoS atağı, üretim kalitesini düşürebilir. DoS algılama mimarisinin işleyişi aşağıda yazılmıştır. Burada bir sıkışma atağının gerçekleştiğini varsayıyoruz. atak bir hedef 6LoWPAN ağına doğru gerçekleştirilir. DoS koruma yöneticisi bir uyarı aldığında IDS'den sıkışma atağı hakkında bildirim sonrası ayrıca algılamayı aşağıdakilerle doğrular.

- Mevcut işletim kanalında tespit edilen parazit seviyesini kontrol etme bilgisini FA yöneticisinden elde edilir.
- İzlenen ağdaki kayıp oranı hakkında toplanan bilgilerin doğrulanması ağ yönetim yöneticisinin kontrol sağlaması
- İzlenen ağdaki kayıp oranı hakkında toplanan bilgilerin doğrulanması ağ yönetim yöneticisinin kontrol sağlaması

Önerilen DoS algılama mimarisi, yukarıda bahsedilen çalışmalara göre aşağıdaki avantajların elde edilmesine katkıda bulunur. IDS_P ve IDS arasındaki kablolu bağlantı,

kablosuz sıkışma ve diğer DoS ataklarına karşı önlem sağlar, böylece IDS her zaman güvenilir ağ bilgileri alabilir. İşlem, bir Linux ana bilgisayarında çalışan güçlü bir IDS ajanı ile merkezileştirilerek, geleneksel düşük güçlü cihazlarda bulunan kaynak kısıtlamalarının üstesinden gelinir. IDS'nin yanlış pozitif olayları, diğer ağ yöneticilerinden edinilen bilgilerden yararlanılarak azaltılabilir. Önerilen mimari, güvenilirlik ve bulunabilirliğin en önemli güvenlik gereksinimleri olduğu gerçek zamanlı endüstriyel ortamlara uygundur.

Önerilen DoS algılama sistemi endüstriyel ortam kablo güvenliği kolay bir şekilde sağlanabileceği için bu tip ataklar için ideal bir çözüm sunduğu düşünülebilir. Ama Akıllı tarım uygulamalarında bu sistemi kurulum ve işletme maliyetinin çok daha fazla olacaktır. Örneğin 100 dönüm büyüklüğünde bir domates tarlasında 6LoWPAN ağını kurulduğunda, IDS_P dediğimiz IDS ajanlarını tarla da uygun şekilde konumlandırmak gerekecektir. atak anında ajanların çalışabilmesi için kabloların çekilmesi ve kablonun zarar görmemesi içinde ayrıca bir çaba gösterilmesi gerekmektedir.

Bölüm 5

6LOWPAN Ağının Kurulması

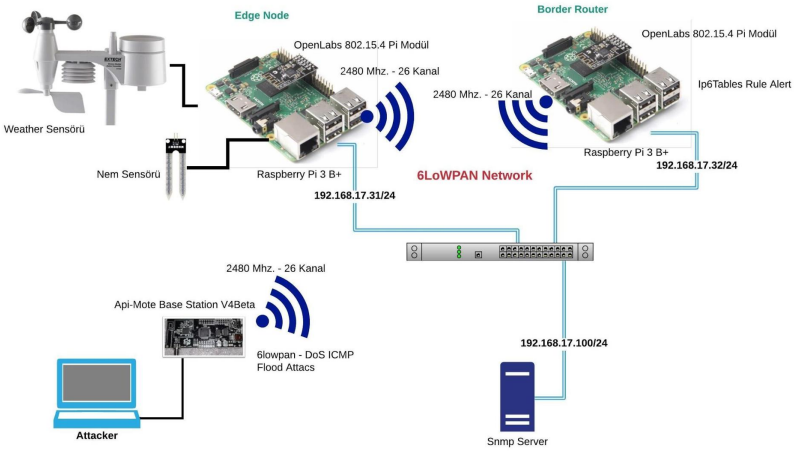
5.1 Low Power Wireless: 6LoWPAN,802.15.4 ve Rapsberry PI

Akıllı tarımda uygulamalarına örnek olarak düz ve geniş bir arazi üzerinden olan domates tarlasında çalışması yapılmıştır. Domates tarlasında birden fazla algılayıcılı IEEE 802.15.4 ve 6LoWPAN protokolleri kullanılarak ağ kurulmuştur. Ağda kullanılan ürünlerin detaylı açıklamaları aşağıda yapılacaktır. Lower Power ağlarının nasıl kurulum yapılacağını adım adım gösterilecek ve yapılan kurulumlarda IEEE 802.15.4 ve 6LoWPAN ağının kurulması detaylı şekilde anlatılacaktır. Buradaki bileşenler wireless algılayıcı modülü ve yapının çalışması için gereken Raspberry ile yapılmıştır. Sistem, kablosuz ve düşük güçte olacak şekilde tasarlanmıştır. Gerçek ortamda çok büyük arazi üzerinde böyle bir düşük güçlü kablosuz ağ kurulumu yüzlerce modülün çalıştırılmasını gerektirecektir.

6LoWPAN için fiziksel katman IEEE 802.15.4 ile belirlenmiştir ve kullanılan modüller 20 metre kapsama alanında, 2.4 Ghz kablosuz bandı ve 250 Kb/s veri aktarım hızları kullanılarak iletişimi kurar.

IEEE 802.15.4' ün üstüne çeşitli protokoller gelebilir. Bunlara örnek olarak zigbee, z-wave, thread vb. Bu çalışma sadece 6LoWPAN' ı kapsamaktadır. 6LoWPAN için IEEE 802.15.4 kablosuz üzerinden IPv6 desteklenmiş hali diyebiliriz. IPv6 mevcut internet için, IEEE 802.15.4 ise farklı bir ortam için tasarlanmıştı. Bu iki farklı seviye birlikte ele alınmıştır.

Cihaz katmanı, fiziksel donanım seçimlerinin devreye girdiği yerdir. Linux, AT86RF230 serisi, MRF24J40 ve diğerleri gibi çeşitli aygıtları destekler. Çekirdeğin, bu aygıt sürücülerinin dinamik olarak yüklenebilir modüller halinde derlenmiş veya mevcut olması gerek.



Şekil 5.1: 6LowPAN Ağ Topolojisi

Ağ katmanında 6LoWPAN desteği gerektirir. Yine, çekirdeğin bunun derlenmiş ya da modül olarak mevcut olması gereklidir. Bu modüller, IEEE 802.15.4 destekli 6LoWPAN, IEEE 802.15.4 veya MAC 802.15.4 modülleridir.

5.2 Raspberry Pi ve OpenLabs Raspberry Pi 802.15.4 radio özellikleri ve kurulması

Raspberry Pi, tamamen gelişmiş bir linux bilgisayardır. GPIO pinleriyle, algılayıcı birimlerle balantı kurabilir, ethernet ile LAN veya WAN'ın bir parçası olabilir. Bu çalışmada IEEE 802.15.4 modülleri ile mevcut ve bir RPI' yı tam işlevli bir 6LoWPAN cihazına dönüştürülmüştür. RPI üzerinde Openlabs Raspberry Pi 802.15.4 radio modülünü kullanıldı. Modül üzerinde atmel AT86RF233 radyosu bulunmaktadır.

Raspberry Pi 3 Model B+ Çalışmada kullandığım Raspberry ürünü Pi 3 B+ dır. Raspberry Pi 3 ailesinin en son ürünü olan Raspberry Pi 3 B+ modeli yenilenen özellikleriyle işlem gücü ve bağlantı hızlarının arttırılması ile piyasaya çıkmıştır. Raspberry Pi 3 model B+ önceki model B ile aynı tasarım ile birlikte gelmektedir. Ama yeni model üzerinde bazı farklar bulunmaktadır. Şekilde de gösterildiği gibi RPI küçük bir bilgisayardır. [44]

Raspberry Pi 3 Model B ile B+ arasındaki temel farklar:

- Raspberry Pi 3 B+ önceki modele göre fazladan +200Mhz daha hızlı işlemci ile birlikte gelmektedir. Ayrıca işlemcide bulunan metal kapak ile daha iyi soğutma imkânı sunar.

- Yeni işlemci daha hızlı olmasına karşın daha az enerji tüketimi yapmaktadır. (Daha verimli işlemci)
- Yenilenen B+ 802.11 b/g/n/ac desteği ile birlikte gelmektedir bu da 2.4GHz ve 5GHz kablosuz bağlantı imkanı sunar.
- Raspberry Pi 3 B+ Ethernet bağlantısı üzerinden güç beslemesi imkânı sunar bunun için PoE HAT genişletme kartı gerekmektedir.
- Yenilenen Ethernet bağlantısı ile 330 Mbit bağlantı imkânı sunar.

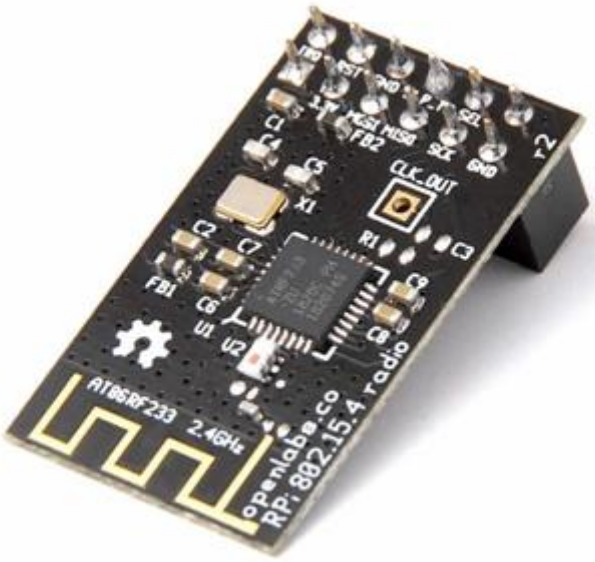
Raspberry Pi Model B+ 3 - Raspberry Pi 3 B+ Özellikleri:

- BCM2837B0, Cortex-A53 64-bit 1.4GHz işlemci
- 1 GB LPDDR2 SDRAM
- 2.4GHz ve 5GHz IEEE 802.11.b/g/ n/ac kablosuz LAN, Bluetooth 4.2, BLE
- USB 2.0 üzerinden Gigabit Ethernet (maksimum çıkış 300 Mbps)
- Genişletilmiş 40 pinli GPIO başlığı
- Tam boyutlu HDMI
- 4 USB 2.0 bağlantı noktası
- CSI kamera portu
- DSI dokunmatik ekran portu
- Video ve ses çıkış portu (4'lü jack çıkışı)
- İşletim sisteminizi yüklemek ve veri depolamak için Micro SD port
- 5V / 2.5A DC güç girişi
- Ethernet üzerinden Güç (PoE) desteği

5.3 Openlabs Raspberry Pi 802.15.4 Radio

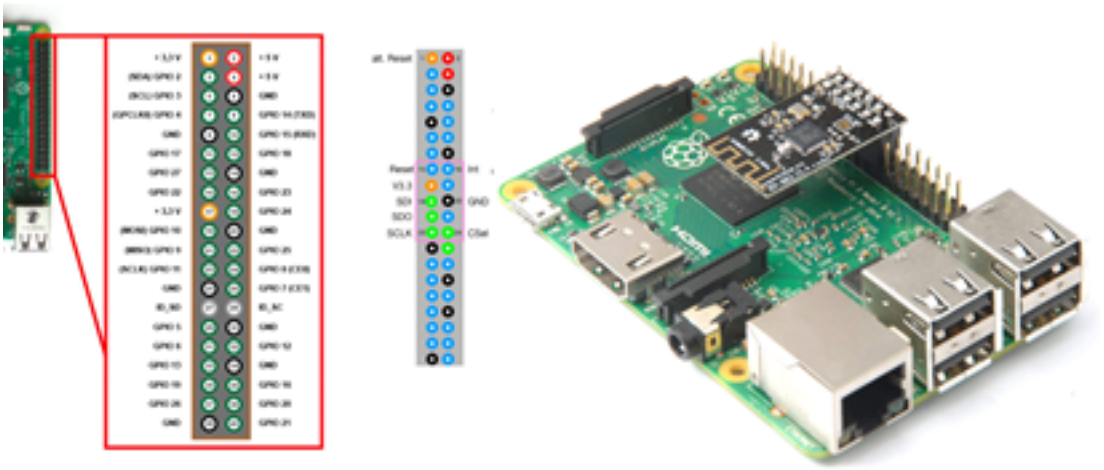
Aşağıdaki şekildeki modül OpenLabs Raspberry Pi 802.15.4 Radio modülüdür. Raspberry Pi 802.15.4 radio modülü 6LoWPAN protokolüne desteklemektedir. Yukarıdaki 6LoWPAN topolojisi için bu modülün seçimi yapılmıştır. Topolojinin çalıştırılması için Raspberry Pi 3 B+ üzerindeki GPIO çıkışlarına kurulum yapılmıştır. 31) Bu modülü

Şekil 5.2: Raspberry Pi 3 Model B+



Şekil 5.3: Raspberry Pi 802.15.4

seçilmesinin nedeni devre tasarımın açık kaynaklı olması ve 6LoWPAN ağının sorunsuz kurulum yapılabilmesidir[50].



Şekil 5.4: Raspberry Pi 802.15.4 uçları

Modülün çalışması için, RPI üzerindeki P1 soket başlangıcından itibaren 15-26 soket girişlerine gelecek şekilde bağlanır. Şekil 5.4

Bu çalışmada RPI için standart Raspbian dağıtımını kullanıldı[51]. Bu kernel üzerinde kullanılan AT86RF233 modülünü tanımlama da sorun yaşandı. İlk standart Raspbian dağıtımındaki kernel problem çıkardı, içinden gelen overlay datası ile kernel içerisinde kodlanmış data olan aynı değildi, kernel downgrade edildi. [52]

rpi-update 936a8dc3a605c20058fbb23672d6b47bca77b0d5

Problemsiz kernel aşağıdaki versiyona düşürülmüştür. Bir çekirdek oluşturmak çok fazla dosya derlemek anlamına gelir ve RPI' da çok yavaştır. Çoğu kişi çapraz derlemeyi önermektedir, ancak bu daha karmaşıktır.

Linux raspberrypi 4.9.80-v7+ 1098 SMP Fri Mar 9 19:11:42 GMT 2018 armv7l GNU/Linux

Kernel versiyonu düşürüldükten sonra RPI 'ın bir AT86RF233 telsiz ile 6LoWPAN'ı desteklemesi sorununu aşılmış oldu

RPI üzerinde aşağıdaki komutları ekleyerek NL802154 netlink inteface aktif hale getirtilir.

/boot/overlays/at86rf233.dtbo

Aşağıdaki /boot/config.txt dosyası içine eklememiz gerekmektedir.

toverlay=at86rf233

RPI üzerine NL802154 netlink Interface erişmek için ve ayrıca ağ bağlantısı kontrol etmek için size WPAN aracını yüklemeniz gerekmektedir[53]. Bununla birlikte 6LoWPAN yığınını yapılandırmak için buna ihtiyacımız bulunmaktadır.

sudo apt install libnl-genl-3-dev libnl-3-dev tar xf

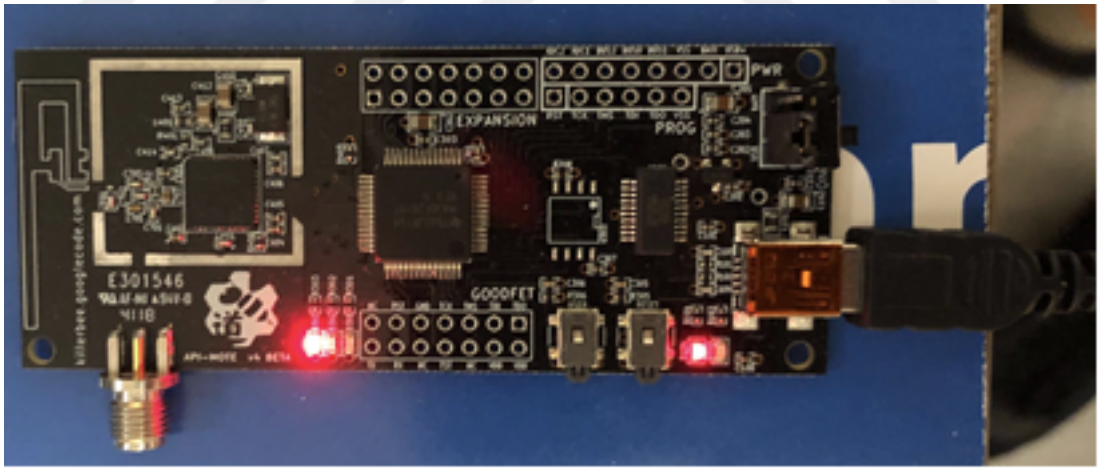
http://wpan.cakelab.org/releases/wpan-tools-0.7.tar.xz cd wpan-tools-0.7/

./configure make make install

Wpan-tools kurulumundan sonra; RPI'nın birincisindeki iwpan komutuyla Openlabs RPI 802.15.4 Radio durumu görülmektedir. 6LoWPAN cihazımız şimdi RPI sistemi tarafından biliniyor durumdadır. RPI üzerinde yeni kernel update edilmiş ve AT86RF233 modülü tanıtılmış durumdadır. Wireless Networkler de SSID'ye sahip olan Wi-Fi ağlarına her bilmektedir. IEEE 802.15.4 ağları benzer bir konsepte sahiptir, bir PAN ID sahiptir. İki cihaz sadece aynı PAN ID'ye sahiplerse aynı ağ üzerinde olacaktır. Bunu ayarlamak için iwpan kullanılarak PAN ID belirlenir.

5.4 RiverLoopSecruity APIMOTE Modülü ve Çalıştırılması

Api-Mote v4 beta versiyonu, öğrenciler, araştırmacılar, mühendisler ve güvenlik uzmanlarının IEEE 802.15.4, Zigbee ve 6LowPan sistemlerinin güvenliğini öğrenmek ve değerlendirmek için kullandıkları beta donanımıdır. Api-Mote Modülünü usb kablosu ile notebook üzerinden tanıtıp testler yapılacaktır.



Şekil 5.5: RiverLoopSecruity APIMOTE Modülü

Api-Mote modülünün Linux platformunda bir bilgisayarda çalışması için scapy ve Killerbee paketlerinin yüklenmesi gerekmektedir.

apt-get install python-gtk2 python-cairo python-usb python-crypto python-serial python-dev libgcrypt-dev

git clone https://github.com/secdev/scapy

cd scapy

python setup.py install

git clone

https://github.com/riverloopsec/killerbee.git

cd killerbee python

setup.py install

Bu şekilde Linux platformunda çalışan bilgisayarda scapy ve Killerbee kurulumu tamamlanmış oldu. Bundan sonra IEEE 802.15.4 ve 6LoWPAN ağlarındaki kablosuz iletişimi dinlebilir veya atak yapılabilir duruma gelmiş olduk. Killerbee kurulumundan sonra Killerbee komutları ile işlem yapılabilir. Bu komut setleri aşağıda açıklaması yapılmıştır.

zbid: Killerbee ve ilgili araçlar tarafından kullanılabilecek arayüzleri gösterir. zbdump: Tcpdump benzeri IEEE 802.15.4 çerçevelerini yakalayarak paket yakalama dosyasına kaydedebilir. Yakaladığı dosyaya yazarken tcpdump gibi gerçek zamanlı istatistikleri göstermez.

Killerbee komutu olarak zbid komutuyla interfacelerde çalışan usb cihazlar aşağıdaki gibi görülebilir.. /dev/ttyUSB0 Interface altında Api-Mote bulunmaktadır.

root@ituser-Inspiron-15-3567: zbid

Dev Product String Serial Number

1:11 CC2531 USB Dongle None

/dev/ttyUSB0 GoodFET Api-Mote v2

RPI üzerinde IEEE802.15.4 ağının kurulması ve kablosuz iletişimin dinlenmesi

Laboratuvar ortamındaki 2 adet RPI üzerindeki tanımların doğruluğu için IEEE 802.15.4 protokolü üzerinden tanımlar yapıldı. . Short_Addr, Pan_id ve Kanal frekans tanımlarını komut satırından yapıldı.. Aşağıdaki komut satırında Wpan0 IEEE 802.15.4 Interface ismidir. IEEE 802.15.4 tanımlarından sonra iki RPI protokol katmanı seviyesinde pingleyebilir duruma getirildi.

RPI-1 içindeki tanımlar:

ip link set wpan0 down

iwpan phy0 set channel 0 15

iwpan dev wpan0 set pan_id 0x1111

iwpan dev wpan0 set short_addr 0x0001

RPI-2 üzerindeki tanımlar:

ip link set wpan0 down

iwpan phy0 set channel 0 15

iwpan dev wpan0 set pan_id 0x1111

iwpan dev wpan0 set short_addr 0x0002

ip link set wpan0 up

L2 ping başlatıp test edeceğiz. RPI-1 üzerinde aşağıdaki komutu yazarak RPI-2 den ping isteği gelmesin durumunda kabul etmesi sağlanıyor. RPI-1 dinleme moduna dönüşüyor.

wpan-ping -d 0x0002 # Listen for sort address 0x0000

RPI-2 den RPI-1 short_addr pingliyoruz.

wpan-ping -a 0x0001 -s 5 -c5 PING 0x0001 (PAN ID 0x1111) 5 data bytes

5 bytes from 0x0001 seq=0 time=4.9 ms

5 bytes from 0x0001 seq=4 time=4.7 ms

Wpan0 Interface üzerinde pan_id 0xbeef olarak pan_id belirliyoruz.

iwpan dev wpan0 set pan_id 0xbeef

phy0 Interface üzerinde kanal 26 ayarlanarak 2480 Mhz bandında yayını alıp vermeye başlayacaktır.

iwpan phy0 set channel 0 26

Her iki RPI üzerinde iwpan phy komuyutla fiziksel Interface durumunu görmekteyiz.

root@raspberrypi-master: # iwpan phy

wpan_phy phy0

supported channels:

page 0: 11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

current_page: 0

current_channel: 26, 2480 MHz

cca_mode:

(1) Energy above threshold

cca_ed_level: -77

tx_power: 4

capabilities:

iftypes: node,monitor

channels: page 0:

[11] 2405 MHz, [12] 2410 MHz, [13] 2415 MHz,

[14] 2420 MHz, [15] 2425 MHz, [16] 2430 MHz,

[17] 2435 MHz, [18] 2440 MHz, [19] 2445 MHz,

[20] 2450 MHz, [21] 2455 MHz, [22] 2460 MHz,

[23] 2465 MHz, [24] 2470 MHz, [25] 2475 MHz,

[26] 2480 MHz

tx_powers:

4 dBm, 3.7 dBm, 3.4 dBm, 3 dBm, 2.5 dBm, 2 dBm,

1 dBm, 0 dBm, -1 dBm, -2 dBm, -3 dBm, -4 dBm,

-6 dBm, -8 dBm, -12 dBm, -17 dBm,

cca_ed_levels:

-91 dBm, -89 dBm, -87 dBm, -85 dBm, -83 dBm, -81 dBm,

-79 dBm, -77 dBm, -75 dBm, -73 dBm, -71 dBm, -69 dBm,

-67 dBm, -65 dBm, -63 dBm, -61 dBm, cca_modes:

(1) Energy above threshold

(2) Carrier sense only

(3, cca_opt: 0) Carrier sense with energy above threshold (logical operator is 'and')

(3, cca_opt: 1) Carrier sense with energy above threshold (logical operator is 'or')

min_be: 0,1,2,3,4,5,6,7,8

max_be: 3,4,5,6,7,8

csma_backoffs: 0,1,2,3,4,5

frame_retries: 0,1,2,3,4,5,6,7 lbt: false

Yukarıdaki çıktı görselindeki radio kanalı 26 ve 2480 Mhz de yayın yaptığı görülmektedir. "iwpan dev" komutuyla bağlı olan RPI üzerindeki fiziksel Interface listesi alınmıştır. Bu komut içerisinde tanımlama yapılan Pan ID görülmektedir. Aşağıdaki çıktıda radyo modülün extended_addr bilgisi de görülmektedir. Bu adres RPI-1 de 0x18c0ffee1ac0ffed ' dir.

RPI-1 üzerindeki iwpan dev çıktısı:

root@raspberrypi-master: # iwpan dev

phy#0

Interface wpan0

ifindex 3

wpan_dev 0x1

extended_addr 0x18c0ffee1ac0ffed

short_addr 0xffff

pan_id 0xbeef

type node

max_frame_retries 3

min_be 3

max_be 5

max_csma_backoffs 4

lbt 0

ackreq_default 0

RPI-2 üzerindeki iwpan dev çıktısı:

root@raspberrypi-master: # iwpan dev

phy#0

Interface wpan0

ifindex 3

wpan_dev 0x1

extended_addr 0x18c0ffee1ac0ffee

short_addr 0xffff

pan_id 0xbeef

type node

max_frame_retries 3

min_be 3

max_be 5

max_csma_backoffs 4

lbt 0

ackreq_default 0

RPI-2 de 0x18c0ffee1ac0ffee ‘ dir. Wpan Interface status bilgisinde

RPI-1 üzerinde ifconfig wpan0 komutunu çalıştırdığımızda IEEE 802.15.4 protokolündeki belirtilen 123 Byte MTU boyutunu, extended_addr ve Interface durumunu görmekteyiz.

root@raspberrypi-master: # ifconfig wpan0

wpan0:

flags=195 <UP,BROADCAST,RUNNING,NOARP> mtu 123

unspec 18-C0-FF-EE-1A-C0-FF-ED-00-00-00-00-00-00-00-00 txqueuelen 300 (UNSPEC)

RX packets 100 bytes 9814 (9.5 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 135 bytes 14885 (14.5 KiB)

TX errors 0 dropped 0 overruns 0 car

RPI-2 de ifconfig wpan0 komutu çalıştırıldığında aşağıdaki bilgileri görmekteyiz.

root@raspberrypi: # ifconfig wpan0

wpan0:

flags=195<UP,BROADCAST,RUNNING,NOARP> mtu 123

unspec 18-C0-FF-EE-1A-C0-FF-EE-00-00-00-00-00-00-00-00 txqueuelen 300 (UNSPEC)

RX packets 12628 bytes 1204322 (1.1 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 19960 bytes 2375679 (2.2 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

RPI-1 ile RPI-2 cihazlarının IEEE 802.15.4 protokolü ile WSN oluşturulmasıyla birlikte RiverLoopSecruity Api-Mote Modülü tanımlama yaparken Killerbee programı yüklenmişti. Killerbee yüklemesi yapıldıktan sonra kendi kütüphanesinde derlenen komutlar gelmiştir. RiverLoopSecruity Api-Mote Modülü yardımıyla kablosuz iletişimi dinlemek için aşağıdaki komut yardımıyla **test.pcap** dosyasına yakalanan veriler kaydedildi.

zbdump -i /dev/ttyUSB0 -c 26 -w test.pcap -v

Bir saldırgan IEE 802.15.4 ağını hedef aldığında ilk önce Pan ID ile birlikte frekansı tespit etmek isteyecektir. Pan ID ve frekansın bulunması ile saldırgan ağa dahil olma girişiminde bulunma şansını yakalayacaktır. WSN ağının kullanılandığı frekans kanalı API-Mote ile deneme yanılma yolu ile ya da özel programlar ile tespit edilebilir. 2.4 GHz bandında 16 kanal tek tek denenerek frekans tespit edilmiştir.

Yakalanan test.pcap dosyası incelendiğinde önemli detaylar gözükmektedir.

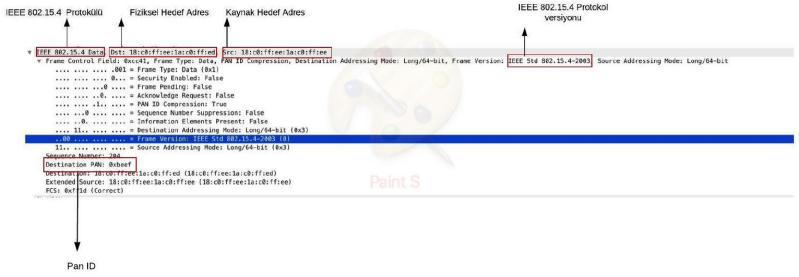
Öncelikli olarak ilk detay yakaladığımız haberleşme protokolünün IEEE 802.15.4 olmasıdır. Wireshark ile yakalanan trafiğin ekran görüntüsü Şekil 5.6' de gösterilmiştir.

WSN ağına ait kaynak ve hedef adres bilgilerinin yanı sıra kritik bilgi olan PAN id bilgisi de tespit edilmiştir.

RPI üzerine takılan OpenLabs Raspberry Pi 802.15.4 Radio modülünün yakalanan haberleşmesinde şifreleme olmadığı görülmektedir.

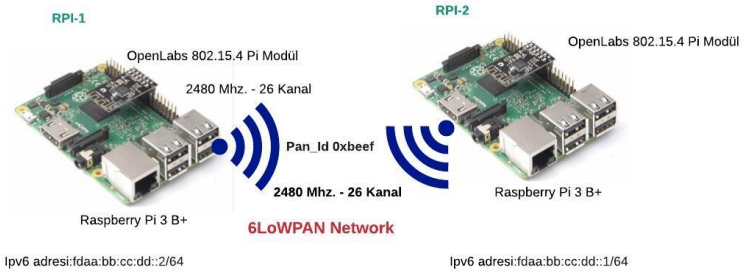
Bu bilgiler saldırganın işini kolaylaştıracak içeriklerdir. Bu zayıflıklar IEEE 802.15.4 radyo modülünün konfigürasyonu yapılırken AES tabanlı şifreleme veya erişim kontrol listesinin oluşturulmasından kaynaklanmaktadır.

RPI üzerinde 6LoWPAN ağının kurulması ve kablosuz iletişimin dinlenmesi



Şekil 5.6: Yakalanan trafiğin Wireshark görüntüsü

Laboratuvar ortamında bulunan 2 adet RPI üzerindeki modül ile 6loWPAN protokolü üzerinden WSN ağı kuracağız. RPI üzerindeki Openlabs RPI 802.15.4 Radio modülü üzerinden 6LoWPAN ağını kurmak için aşağıdaki komutları kullanıyoruz. Öncelikle lowpan0 ve wpan0 interface' ni kapatıyoruz. Pan_Id 0xbeef ve kanal frekansı 26 tanımı yapıyoruz. Wpan0 üzerine lowpan interface' ni ekleme yapıyoruz. 6LoWPAN ağı için de Ipv6 adresinin da tanımı yapıyoruz.



Şekil 5.7: Kurulan 6LowPAN Topolojisi

ip link set lowpan0 down

ip link set wpan0 down

iwpan dev wpan0 set pan_id 0xbeef

iwpan phy0 set channel 0 26

ip link add link wpan0 name lowpan0 type lowpan

ip link set wpan0 up

ip link set lowpan0 up

ip addr add fdaa:bb:cc:dd::2/64 dev lowpan0

RPI-1 ipv6 adresi fdaa:bb:cc:dd::2/64 ‘dir. Tanımlama yapıldığında wpan0 ve lowpan0 up yapılır. RPI-2 de aynı benzer tanımlar yapılır. RPI-2 nin ipv6 adresi fdaa:bb:cc:dd::1/64 ‘dir.

ip link set lowpan0 down

ip link set wpan0 down

iwpan dev wpan0 set pan_id 0xbeef

iwpan phy0 set channel 0 26

ip link add link wpan0 name lowpan0 type lowpan

ip link set wpan0 up

ip link set lowpan0 up

ip addr add fdaa:bb:cc:dd::1/64 dev lowpan0

RPI-1 ve RPI-2 6LoWPAN ağına dahil ettik. Kanal 26 da, Pan_Id olarak 0xbeef olarak ortak ağa kriterlerine sahip durumdalar. RPI-1 ile RPI-2 birbirlerine ipv6 üzerinden ping6 ile ping edebilir durumdayız. wpan0 ve lowpan0 Interface durumlarını aşağıdaki gibidir.

RPI-1 wpan0 ve lowpan0 Interface durumları aşağıdaki gibidir. Burada Interface wpan0 ve lowpan0 interrface durumları up’ dır.

root@raspberrypi-master: # ifconfig wpan0

wpan0:

flags=195<UP,BROADCAST,RUNNING,NOARP> mtu 123

unspec 18-C0-FF-EE-1A-C0-FF-ED-00-00-00-00-00-00-00-00 txqueuelen 300 (UNSPEC)

RX packets 100 bytes 9814 (9.5 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 135 bytes 14885 (14.5 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@raspberrypi-master: # ifconfig lowpan0

lowpan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280

inet6 fe80::1ac0:ffee:1ac0:ffed prefixlen 64 scopeid 0x20<link>

inet6 fdaa:bb:cc:dd::2 prefixlen 64 scopeid 0x0<global>

unspec 18-C0-FF-EE-1A-C0-FF-ED-00-00-00-00-00-00-00-00 txqueuelen 1 (UNSPEC)

RX packets 112 bytes 11328 (11.0 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 136 bytes 14566 (14.2 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

RPI-2 wpan0 ve lowpan0 Interface durumları aşağıdaki gibidir.

root@raspberrypi: # ifconfig wpan0

wpan0:

flags=195<UP,BROADCAST,RUNNING,NOARP> mtu 123

unspec 18-C0-FF-EE-1A-C0-FF-EE-00-00-00-00-00-00-00-00 txqueuelen 300 (UNSPEC)

RX packets 12628 bytes 1204322 (1.1 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 19960 bytes 2375679 (2.2 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@raspberrypi: # ifconfig lowpan0

lowpan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280

inet6 fdaa:bb:cc:dd::1 prefixlen 64 scopeid 0x0<global>

inet6 fe80::1ac0:ffee:1ac0:ffee prefixlen 64 scopeid 0x20<link>

unspec 18-C0-FF-EE-1A-C0-FF-EE-00-00-00-00-00-00-00-00 txqueuelen 1 (UNSPEC)

RX packets 11068 bytes 1194242 (1.1 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 11709 bytes 1943352 (1.8 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions0

RPI-1 den RPI-2' ye ping6 atılması. Başarı bir şekilde ping işlemi yapılmış durumdadır.

root@raspberrypi: # ping6 fdaa:bb:cc:dd::1

PING fdaa:bb:cc:dd::2(fdaa:bb:cc:dd::1) 56 data bytes

64 bytes from fdaa:bb:cc:dd::1: icmp_seq=1 ttl=64 time=14.4 ms

64 bytes from fdaa:bb:cc:dd::1: icmp_seq=2 ttl=64 time=14.2 ms

64 bytes from fdaa:bb:cc:dd::1: icmp_seq=3 ttl=64 time=12.4 ms

64 bytes from fdaa:bb:cc:dd::1: icmp_seq=4 ttl=64 time=15.1 ms

64 bytes from fdaa:bb:cc:dd::1: icmp_seq=5 ttl=64 time=13.3 ms

RPI-2 den RPI-1 e ping6 atılması. Başarı bir şekilde ping işlemi yapılmış durumdadır.

root@raspberrypi: # ping6 fdaa:bb:cc:dd::2

PING fdaa:bb:cc:dd::2(fdaa:bb:cc:dd::2) 56 data bytes

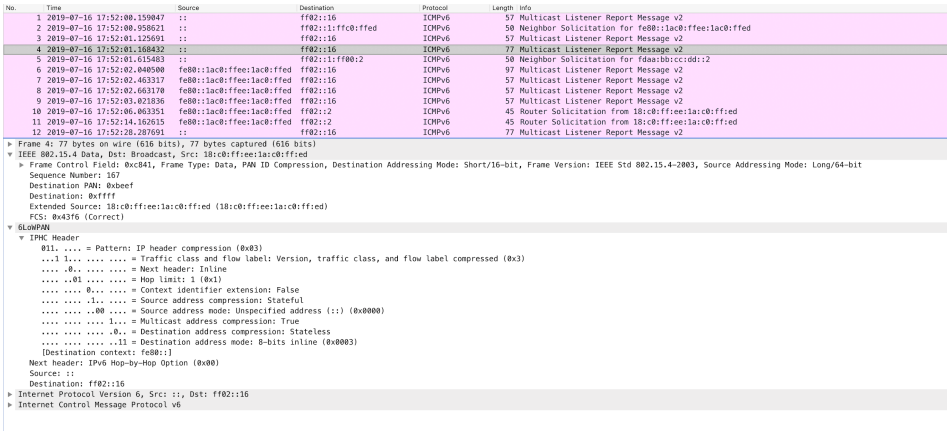
64 bytes from fdaa:bb:cc:dd::2: icmp_seq=1 ttl=64 time=14.5 ms

64 bytes from fdaa:bb:cc:dd::2: icmp_seq=2 ttl=64 time=14.2 ms

64 bytes from fdaa:bb:cc:dd::2: icmp_seq=3 ttl=64 time=12.6 ms

64 bytes from fdaa:bb:cc:dd::2: icmp_seq=4 ttl=64 time=15.5 ms

64 bytes from fdaa:bb:cc:dd::2: icmp_seq=5 ttl=64 time=13.2 ms



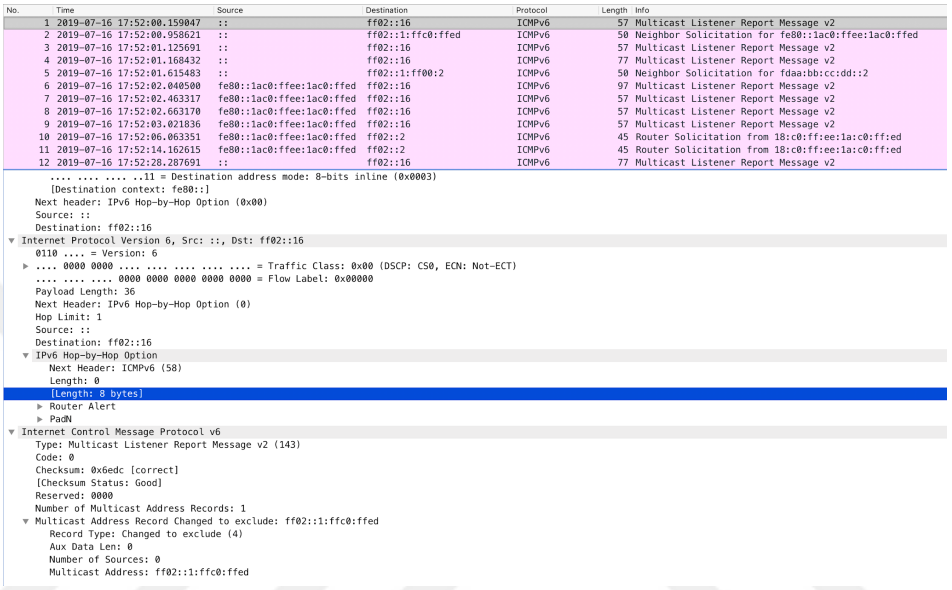
Şekil 5.8: Modülün WSN ilk giriş esnasındaki dinleme

RPI-1 ile RPI-2 arasında ilk açıldıklarında icmpv6 nın adımlarını yukarıdaki şekil 5.8 de görülmektedir. Icmpv6 aşağıdaki adımlara göre çalışmaktadır. Bu adımları şekil 5.8 deki info kolonunda görmekteyiz.

- Multicast Listener Report Message V2
- Neighbor solicitation(Komşu talep mesajı)

- Router Solicitation (Yönlendirici talep mesajı)

Şekil 5.9 Multicast Listener Report Message V2 içeriğinde ise ICMPv6' nın tip alanında 8 bit ve türü 143 olarak görülmektedir.RFC 3810 da geniş bir şekilde anlatılmıştır [54]. Bu mesajlar, çok noktaya yayın dinleyicilerinin mevcut durumunu bildirmek (komşu yönlendiricilere) veya çok noktaya yayın dinleyicilerinin durumunu veya arabirimlerini değiştirmek için tüm düğümlere gönderilir.



Şekil 5.9: Multicast Listener Report Message V2 içeriği

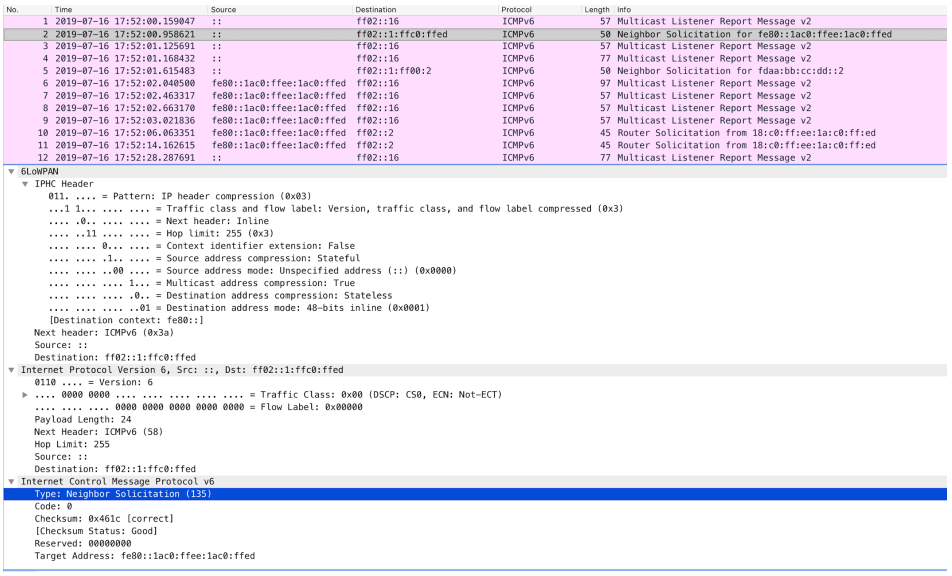
Şekil 5.10 Komşu talep mesajında , komşu ana varlığını belirlemek için parametreler ve yöntemlerin alışverişini resmileştirmek fonksiyonudur. Bu görevler IPv6 yeni adresi çözümleme yöntemi, hem de sonraki atlama belirlenmesi ve komşu erişilememesi algılama süreçlerini kapsar. Komşu talep mesajı bir ana bilgisayar veya yönlendirici varlığını teyit ve ayrıca gerektiğinde adres bilgileri katmanı sağlar. İleti Türü: 135' dir, RFC 2461 detaylı şekilde anlatılmıştır[55].

Şekil5.11'Yönlendirici talep mesaj içeriği görülmektedir. İleti türü 133' dür, RFC 2461 detaylı şekilde anlatılmıştır[55]. Yönlendirici bildirimlerini veya Yönlendirici Uyarıları üretmek kullanılır.

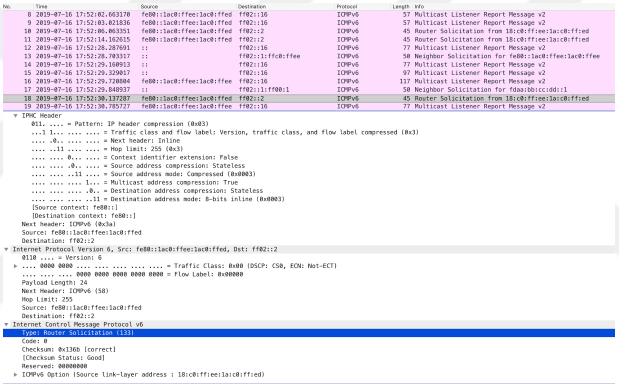
Şekil5.12'da api-mote ile 6LoWPAN ağını dinlemesinde IEEE 802.15.4 broadcast paketinin yakalandığını görülmektedir. Burada pan_id de görülmektedir.

Şekil 5.12'da Api-Mote ile 6LoWPAN ağının dinlenmesiyle 6LoWPAN broadcast paketinin yakalandığı görülmektedir.

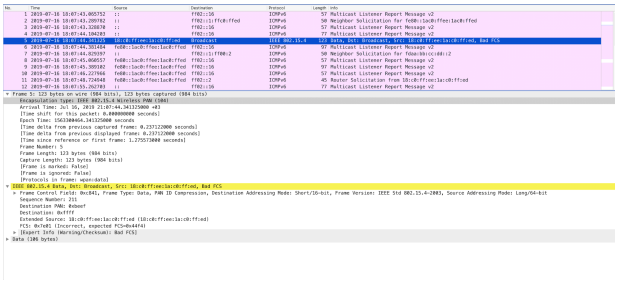
RPI-1 ve RPI-2 karşılıklı ping atıldığından 20 Kbpslik trafik oluşturmaktadır. Şekil 5.15'da lowpan0 Interface icmp paketlerinin yarattığı trafik görülmektedir. Bu trafiği



Şekil 5.10: Komşu talep mesaj içeriği



Şekil 5.11: Yönlendirici talep mesaj içeriği

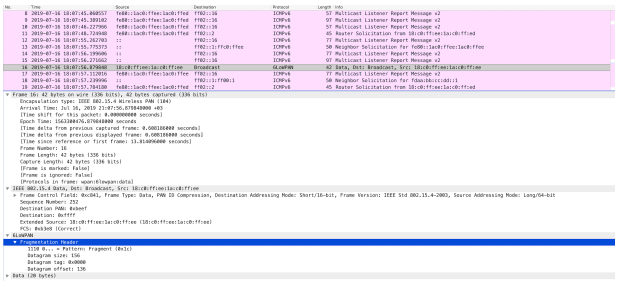


Şekil 5.12: IEEE 802.15.4 broadcast trafiği

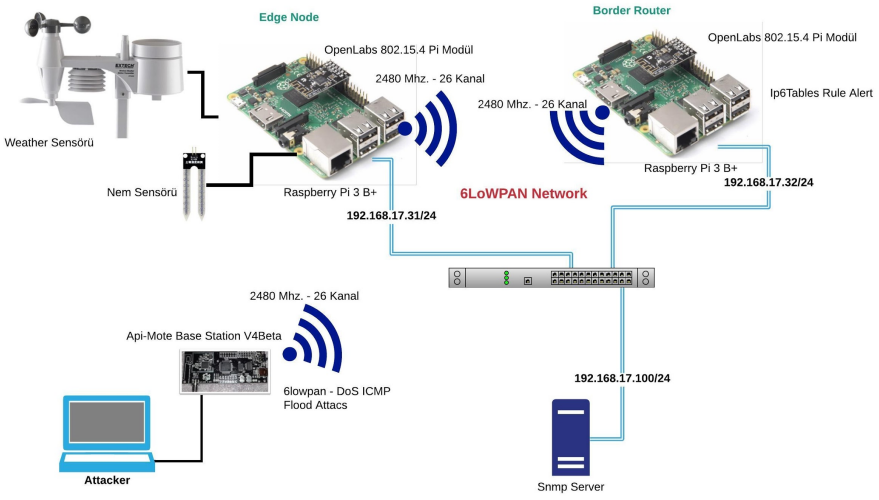
izlemek ve atak olduğu zamanı görmek için her iki RPI aynı network switch bağlayarak ipv4 adresi verildi.

RPI-1 ipv4 adresi:192.168.17.31 RPI-2 ipv4 adresi:192.168.17.32

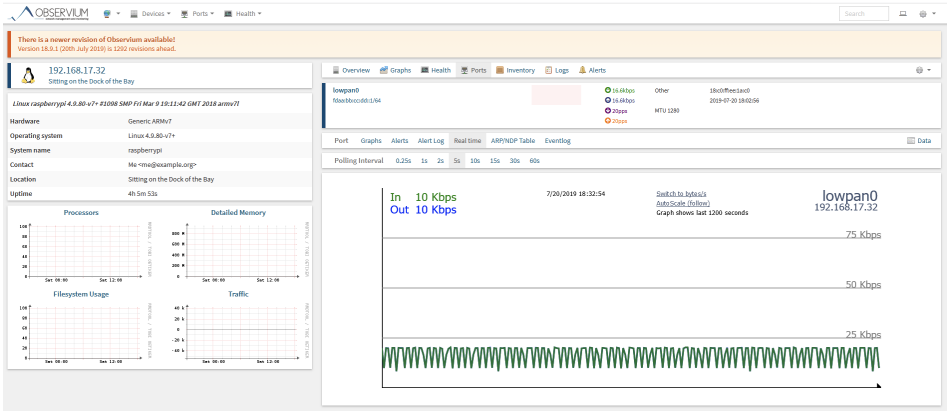
Atak ve ağ geçidi RPI üzerindeki Interface trafiğini görmek için şekil 5.14' deki network topolojisi oluşturuldu.



Şekil 5.13: 6LoWPAN Broadcast trafiği



Şekil 5.14: RPI kablolu bağlantısı ve SNMP Sunucu



Şekil 5.15: Lowpan0 arabiriminin trafik grafiği

Attacker bilgisayarına fping kurulumu yapılarak fping üzerinden icmp flood atağı yapacağız.

sudo apt-get install fping

Ağgeçidi üzerinde ip6table üzerine icmp paketiyle ilgili bir alert oluşturuldu. Bu normal icmp ‘ nin üzerinde gelir ise icmp flood atak olarak algılayarak alarm oluşturuldu.

ip6tables –new-chain RATE-LIMIT

ip6tables -A INPUT -p icmpv6 –icmpv6-type echo-request -j RATE-LIMIT

ip6tables -A INPUT -p icmpv6 –icmpv6-type echo-reply -j RATE-LIMIT

ip6tables –append RATE-LIMIT –match limit –limit 20/sec –limit-burst 20 –jump

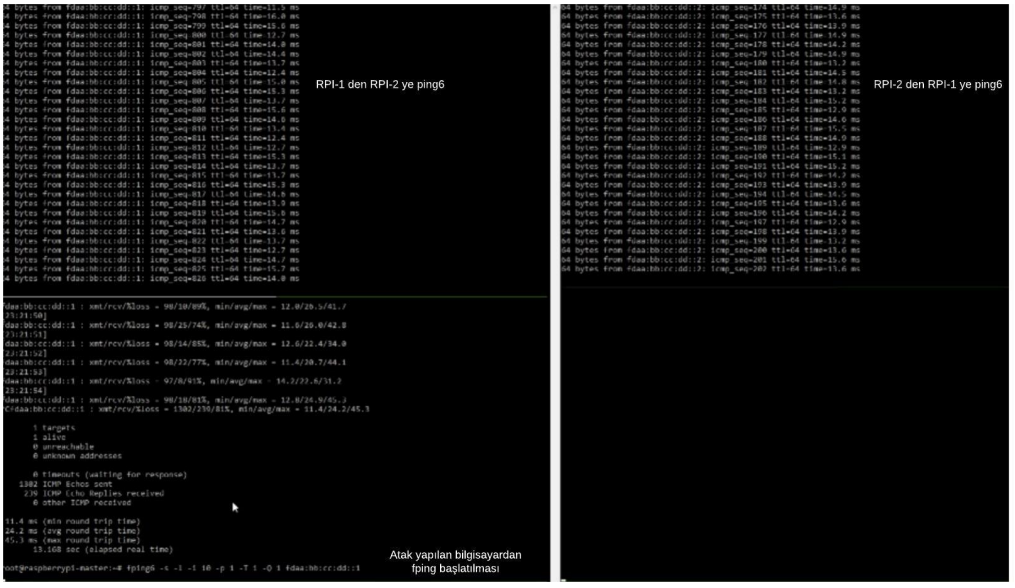
ACCEPT

ip6tables –append RATE-LIMIT –match limit –limit 20/sec –limit-burst 20 –jump LOG –log-prefix "echo req asti"

Aşağıdaki komut ile icmp flood atağını gerçekleştiriyoruz.

fping -s -l -i 10 -p 1 -T 1 -Q 1 fdaa:bb:cc:dd::1

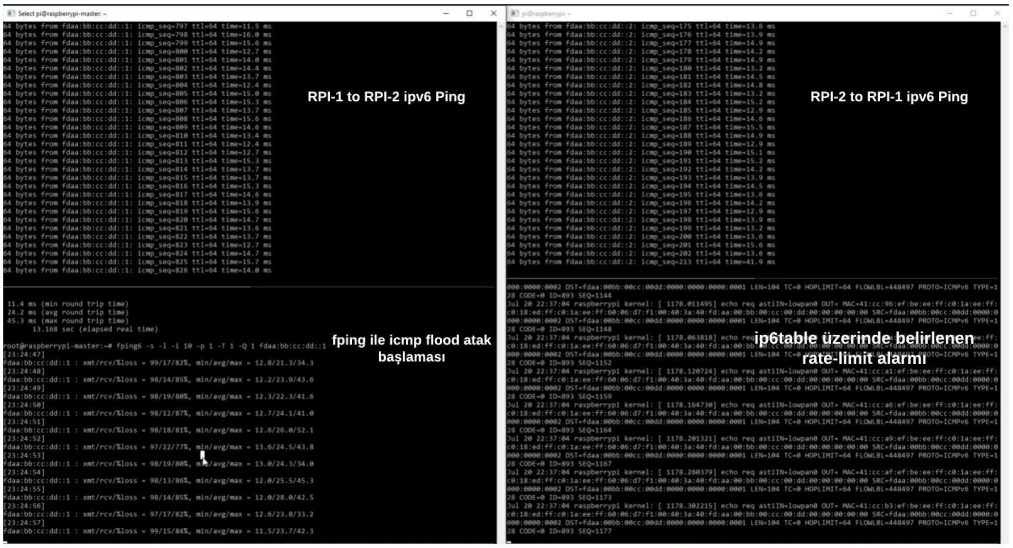
RPI-1 ve RPI-2 arasında karşılıklı ping atılması. Atak yapılacak bilgisayardan lowpan0 Interface üzerinden fping başlatılarak lowpan0 interface'ni etkileyeceğiz.



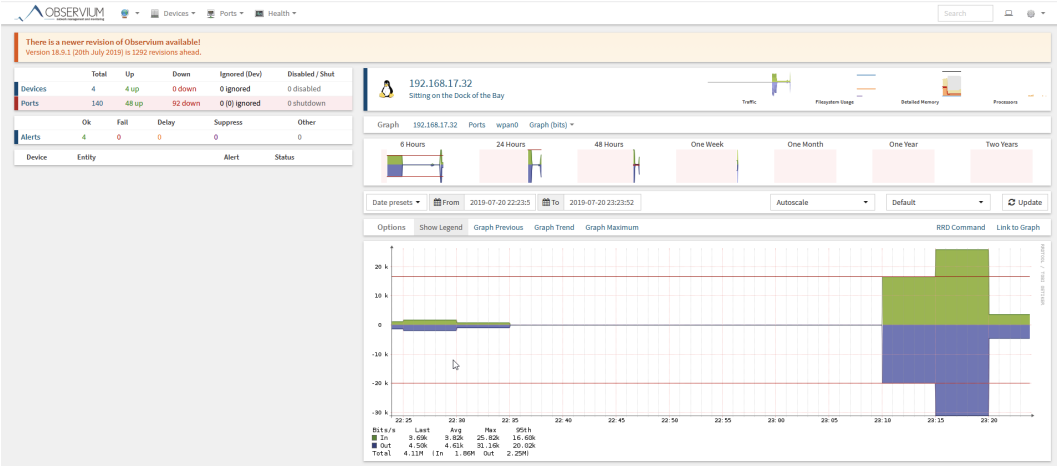
Şekil 5.16: 6LoWPAN ağında ping6 ve fping6 komutu

Ip6tables üzerinde icmp için tanımlama yapmıştık. bu tanımlamaya göre fping başlar ve icmp flood atak olarak algılamasını sağladık. Şekil 5.16'de görüldüğü gibi.

Ip6table da yapılan rate limit ile alarm oluşturduğu görülebilir. Snmp sunucu üzerindeki Interface grafiğine göre de atak olduğunda bandwidth'in yükseldiğini ve iletişimi durdurduğumuzu tespit ettik. Şekil 5.18'de interface üzerindeki bandwidth aşımı olduğunu tespit ettik. Bu tespit ile icmp flood atağına örnek oluşturmuştur.



Şekil 5.17: Fping6 ile icmp flood atak atılması ve ip6table log detayı



Şekil 5.18: Atak yapılan RPI lowpan arabirimi trafiğinin grafiği

Bölüm 6

Sonuç ve Öneriler

IoT dünyası bileşenleri çok sınırlı donanım ve yazılım kaynaklarına sahiptir. IoT cihazlarının en temel özelliği zaten basit yapıda küçük bileşenler şeklinde olmasıdır. Aksi durumda IoT cihazlarının büyük bir bilgisayardan farkı kalmayacaktır. IDS çözümleri sınırlı kaynaklar sebebiyle gelişmiş ataklarını algılamakta yetersiz kalmaktadır. Kaynakların bu kadar yetersiz olduğu bir ortamda IPS çözümlerinden bahsetmek çok da kolay gözükmemektedir.

IoT cihazlar IEEE 802.15.4 Zigbee ve 6LoWPAN protokolü ile geniş bir kapsama alanında hizmet sağlamasına rağmen bant genişliği ise genel olarak 250 Kb/s ile sınırlıdır. Bant genişliğinin sınırlı olması her ne kadar gerekli olan iletişimi sağlasa da DOS/DDOS ataklarına karşı savunmasız bırakmaktadır. Yapılan çalışmalarla bant genişliğinin arttığı görülmektedir.

Akıllı Tarım sistemlerinde de benzer sorunlar bulunmaktadır. Akıllı Tarım sistemlerinin tasarımları gereği daha dayanıklı yapılara sahip olmaktadır. Sıvı temasına, sıcak ve soğuk hava şartlarına dayanıklı yapılmaktadır. Fiziksel olarak dayanıklı oldukları gibi ataklara karşı ise çözümler göz ardı edilmektedir. Teoride özellikle sertifika ile koruma önlemlerinden bahsedilmektedir. Bunun yanı sıra firmware güncellemesi ile yeni özellikler gelmekte ve geliştirme süreçleri devam etmektedir. Akılı tarım uygulama alanlarının zorluğu göz önüne gelince firmware güncellemeleri de zor olmaktadır. Bir de IoT dünyasında ise güncelleme polikasınından söz etmek zordur. Bilgisayar sistemlerindeki bilinçlenme IoT dünyasında zor işlemektedir.

Birlikte çalışabilirlik, farklı üreticilerin aygıtlarının veri alışverişinde bulunma yeteneğidir. İletişim yığında katmanlar üzerinde birlikte .alışmayı sağlamak için, test prosedürleri ve birlikte çalışabilirlik testlerini tanımlayan birçok ittifak ve organizasyon vardır. Bazı

standartlar OSI modelinde bir veya iki katman üzerinde birlikte çalışabilirliği tanımlamaktadır. IEEE, IETF ve diğerlerinden standartlar benimseyen ve bunları tam bir birlikte çalışabilirliği sağlamak için bunları bir baştan sona sertifikalandırma programları oluşturmak için kullanan birkaç kurum ve ittifak vardır. 6LoWPAN'ı kullanılan her türlü cihazda güvenlik farkındalığının gelişmesi ve adaptosyana ihtiyacı vardır. 6LoWPAN pazarda oldukça yenidir. 6LoWPAN ile yönetilebilir bir ağ oluşturulmaktadır. Günümüzde dağıtımlar, büyük ağ topolojisi, güçlü iletişim ve çok düşük güç tüketimi desteği dahil olmak üzere IEEE 802.15.4 avantajlarından yararlanılmaktadır. Son 30+ yıl boyunca geliştirilen birçok uygulama ile IP iletişimi, 6LoWPAN'ın açık standartlar, uzun ömür, kolay öğrenme eğrisi ve şeffaf Internet entegrasyonu ile iyi bir konuma getirmektedir.

IoT sistemleri için güvenlik bir zorunluluktur ve her zaman bir zorluk oluşturur. IoT'nin çoğu durumda çok sınırlı performansı olan birçok düğüme sahip olması nedeniyle, dış saldırgan için daha fazla giriş noktası bulunmaktadır. 6LoWPAN, IEEE 802.15.4'te tanımlanan güçlü AES tabanlı şifreleme ve erişim kontrol listesi ile bağlantı katmanı güvenliğini artırmaktadır. Link katmanı güvenliği link doğrulama ve şifreleme sağlar. Bağlantı katmanı güvenliğine ek olarak, taşıma katmanı güvenliği (TLS) 6LoWPAN sistemlerinde çalışmaktadır. Ama gerçek dünyada bu algılayıcıların kullanılmasında firmaya bağımlılık veya açık kaynak kodlu olmasından dolayı güvenlik ön planda tutulmadan çalışır duruma getirilmektedir. Bu çalışmada gerçek ortamın benzeri çalışır duruma getirilmiştir. Kablosuz trafik dinlenerek gerçek ortamda kurulan ağ bilgileri elde edilmiştir. Basit bir atak mekanizması tasarlanmıştır. atağın algılanmasıyla ilgili çalışma yapılmıştır.

Kaynakça

[1] Nesnelerin İnterneti URL https://www.rfidjournal.com/articles/view?4986

[2]Teknolojinin Sektörlere Etkisi URL http://dergipark.ulakbim.gov.tr/makufebed

[3] Nesnelerin İnternetinin Getirdiği Yenilikler ve Sorunları URL http://industryolog.com/teknolojinin-sektorlere-etkisi-akilli-tarim

[4] Internet of Things IoT URL http://turkishstudies.net/files/turkishstudies/1278323770_4KelesAyturk-Ali-btb-53-66.pdf

[5] Internet of Things (IoT) system for data-driven agriculture URL https://internetofthingsagenda.techtarget.com/definition/internet-of-Things-IoT

[6] Teknolojinin sektörlere etkisi Akıllı Tarım URL https://www.geospatialworld.net/blogs/internet-of-things-system-for-agriculture

[7] Design and implementation of a cloud-based IoT scheme for precision agriculture URL http://industryolog.com/teknolojinin-sektorlere-etkisi-akilli-tarim

[8] IoT Applications in Agriculture URL https://ieeexplore.ieee.org/document/7847850

[9] Why IoT, big data smart farming are the future of agriculture URL https://www.IoTforall.com/IoT-applications-in-agriculture

[10] Precision Farming: Cheating Malthus with Digital Agriculture URL ://www.businessinsider.com/internet-of-things-smart-agriculture-2016-10

[11] IoT, big data smart farming are the future of agriculture URL https://docdrop.org/static/drop-pdf/GSR_agriculture-N1sH6.pdf(page8)

[12] IoT for Agriculture URL http://www.businessinsider.com/internet-of-things-smart-agriculture-2016-10

[13] Agriculture in Senegal URL http://intelzone.com/agriculture

[14] ICT in agriculture connecting smal holders to knowledge networks, and institution update edition URL https://www.syngentafoundation.org/agriservices/wherewework /senegal

[15] Türkiye'de Akıllı Tarımın Mevcut Durum Raporu URL http://documents.worldbank.org/curated/en/522141499680975973/ICT-in-agriculture-connecting-smallholders-to-knowledge-networks-and-institutions

[16] URL http://www.tarmakbir.org/haberler/atp/atprapor.pdf

[18] Ioanna Mampentzidou, Eirini Karapistoli, Anastasios A. Economides "Basic Guidelines for Deploying Wireless Sensor Networks in Agriculture" 978-1-4673-2015-3/12/ @c 2012 IEEE

[19] Ajay Mittal, Chetan K. P. , Srinivasan Jayaraman, Bhushan G. Jagyasi, Arun Pande, Balamuralidhar "mKRISHI Wireless Sensor Network Platform for Precision Agriculture" 978-1-4673-2248-5/12 @c 2012 IEEE

[20] Ojha T., Misra S., Raghuwanshi N.S. Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. Comput. Electron. Agric. 2015;118:66–84. doi: 10.1016/j.compag.2015.08.011.

[21] Tuna G., Gungor V.C. Energy harvesting and battery technologies for powering wireless sensor networks. In: Kolavennu S., editor. Industrial Wireless Sensor Networks. Woodhead Publishing; Sawston, UK: 2016. pp. 25–38.

[22] Tan Y.K., Panda S.K. Review of energy harvesting technologies for sustainable wireless sensor network. In: Seah W., editor. Sustainable Wireless Sensor Networks. InTech; Rijeka, Croatia: 2010. pp. 15–43.

[23] Valente J., Sanz D., Barrientos A., Cerro J.D., Ribeiro A., Rossi C. An air-ground wireless sensor network for crop monitoring. Sensors.2011;11:6088\T1\textendash6108. doi:10.3390/s110606088.

[24] Industrial Communication Technology Handbook, 2nd Edition By Richard Zurawski

[25] Internet of Things for Architects

[26] Denial-of-Servicedetectionin6LoWPANbasedInternetofThingsURLhttps://tools.ietf.org/html/rfc6550

[27] Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks URLhttps://www.researchgate.net/publication/261128514_Denial-of-Service_detection_in_6LoWPAN

[28] URL http://www.scielo.org.co/pdf/iei/v38n1/0120-5609-iei-38-01-00130.pdf

[29] Xu, W., Ma, K., Trappe, W., Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. IEEE Network, 20(3), 41-47.

[30] Ghildiyal, S., Mishra, A. K., Gupta, A., Garg, N. (2014). Analysis of denial of service (dos) attacks in wireless sensor networks. IJRET: International Journal of Research in Engineering and Technology, Vol. 3, eISSN: 2319-1163, pp.140-143.

[31] Nancy, J. T., VijayaKumar, K. P., Kumar, P. G. (2014). Detection of jammer in Wireless Sensor Network. International Conference on Communications and Signal Processing (ICCSP), IEEE, 1435-1439. DOI: 10.1109/ICCSP.2014.6950086

[32] Raymond, D.R., Midkiff, S.F. (2008). Denial of Service in Wireless Sensor Network: Attacks and Defenses. IEEE Pervasive Computing, Vol. 7, Issue 1, pp.74-81. DOI: 10.1109/MPRV.2008.6

[33] Danyang, Q., Lin, M., Erfu, W., Hongbin, M., Qun, D. (2013). An interference suppression mechanism for WSN. International Conference on Sensor Network Security

[34] Dbibih, I., Iala, I., Aboutajdine, D., Zytoune, O. (2016). Collision avoidance and service differentiation at the MAC layer of WSN designed for multi-purpose applications. Cloud Computing Technologies and Applications (CloudTech), 2016 2nd International Conference, IEEE, 277-282. DOI: 10.1109/CloudTech.2016.7847710

[35] Amara, S. O., Beghdad, R., Oussalah, M. (2013). Securing Wireless Sensor Networks: A Survey. EDPACS, 47(2), 6-29. DOI: 10.1080/07366981.2013.754207

[36] Shahzad, F., Pasha, M., Ahmad A. (2017). A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. International Journal of Computer Science and Information Security, Vol. 14, No. 12. arXiv preprint arXiv:1702.07136

[37] Yong, W., Garhan, A., Byrav, R. (2006). A Survey Of Security Issues In Wireless Sensor Networks. IEEE Communications Surveys Tutorials, Volume 8. DOI: 10.1109/COMST.2006.315852

[38] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: a study on qos security threats and countermeasures using intrusion detection system approach," International Journal of Communication Systems, vol. 25, no. 9, pp. 1189–1212, 2012.

[39] O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen, "Security considerations in the ip-based internet of things." IETF (work in progress) Available [Online] URL http://tools.ietf.org/html/draft-garcia- core-security-05, Mar. 2013.

[40] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," Computer communications, vol. 30, no. 11, pp. 2314–2341, 2007.

[41] A. H. Farooqi and F. A. Khan, "Intrusion detection systems for wireless sensor networks: A survey," in Communication and networking, pp. 234–241, Springer, 2009.

[42] A. Mitrokotsa and A. Karygiannis, "Intrusion detection techniques in sensor networks," Wireless Sensor Network Security, ed. J. Lopez and J. Zhou, pp. 251–272, 2008.

[43] R. Tomasi, H. Khaleel, F. Penna, C. Pastrone, R. Garello, and M. Spirito, "Frequency agility in ipv6-based wireless personal area networks (6LoWPAN)," in Wired/Wireless Internet Communications (E. Osipov, A. Kassler, T. Bohnert, and X. Masip-Bruin, eds.), vol. 6074 of Lecture Notes in Computer Science, pp. 146–157, Springer Berlin Heidelberg, 2010.

[44] Raspberry Pi 3 B+ (Raspberry Pi Model B Plus 3): URL https://www.direnc.net

[45] URL https://fping.org/fping.1.html

[46] Mathur, A., Newe, T. (2015). Medical WSN: Defense for selective forwarding attack. Sensing Technology (ICST), 2015 9th International Conference, IEEE, 54-58. DOI: 10.1109/ICSensT.2015.7438364

[47] Wazid, M., Katal, A., Sachan, R. S., Goudar, R. H., Singh, D. P. (2013). Detection and prevention mechanism for blackhole attack in wireless sensor network. Communications and Signal Processing (ICCSP), 2013 International Conference IEEE, 576-581. DOI: 10.1109/iccsp.2013.6577120

[48] Maheswari, S. U., Usha, N. S., Anita, E. M., Devi, K. R. (2016). A novel robust routing protocol RAEED to avoid DoS attacks in WSN. Information Communication and Embedded Systems (ICICES), 2016 International Conference, IEEE, 1-5. DOI: 10.1109/ICICES.2016.7518942

[49] Goyal, S., Bhatia, T., Verma, A. K. (2015). Wormhole and Sybil attack in WSN: A review. Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference, IEEE, 1463-1468.

[50] Raspian URL https://github.com/RIOT-Makers/wpan-raspbian /wiki/Create-a-generic-Raspbian-image-with-6LoWPAN-support

[51] 6LoWPAN Raspbian image URL https://www.raspberrypi.org/downloads/raspbian/

[52] linux-wpan URL https://github.com/RIOT-Makers/wpan-raspbian/wiki/Create-a-generic-Raspbian- image-with-6LoWPAN-support

[53] Multicast Listener Discovery Version 2 (MLDv2) for IPv6 URL http://wpan.cakelab.org

[54] Neighbor Discovery for IP Version 6 (IPv6) URL https://tools.ietf.org/html/rfc3810

[55] URL https://datatracker.ietf.org/doc/rfc2461/