Elektrik Elektronik Mühendisliği / *Electrical Electronic Engineering* **DOI: 10.21597/jist.655990**
Derleme Makalesi / *Review Article*

Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 10(2): 970-984, 2020
Journal of the Institute of Science and Technology, 10(2): 970-984, 2020
ISSN: 2146-0574, eISSN: 2536-4618

Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik

Muhammed Zekeriya GÜNDÜZ[1]*, Resul DAŞ[2]

ÖZET: Akıllı şebekeler, mevcut elektrik şebekelerinin bilgi iletişim teknolojileri ile donatılmış yeni nesil güç sistemlerine dönüştürülmesidir. Gelişmiş bilgi iletişim teknolojilerinin ve yenilenebilir enerji kaynaklarının etkin bir şekilde mevcut elektrik şebekelerine entegre edilmesi geleceğin güç sistemlerinin verimlilik ve etkinliğini artıracaktır. Siber-fiziksel bir sistem olan akıllı şebekeler sağladıkları olanakların yanı sıra siber güvenlik ile ilgili ciddi sorunları da beraberinde getirmektedirler. Bu sorunları engellemek, tespit etmek ve sistemi bunlara karşı korumak için iletişim altyapısının verimli, güvenilir, güvenli ve etkin bir şekilde tasarlanması gerekmektedir. Bu çalışmada akıllı şebeke iletişim altyapısındaki siber güvenlik gereklilikleri, ağ zafiyetleri, güvenli iletişim mimarileri ve protokolleri ile siber saldırıların engellenmesi konuları ele alınmıştır. Ayrıca, akıllı şebekelerde öne çıkan siber güvenlik zafiyetlerinin ve çözümlerinin derinlemesine anlaşılması sağlanarak, konu ile alakalı gelecekte yapılacak çalışmalara yol gösterilmesi amaçlanmıştır.

Anahtar Kelimeler: Siber fiziksel sistem, Akıllı şebekeler, Siber güvenlik, İletişim altyapısı

Communication Infrastructure and Cyber-Security in Smart Grids

ABSTRACT: Smart grids are the evolution of existing electricity grids into the new power systems equipped with information-communication technologies. The integration of advanced information-communication technologies and renewable energy sources into the existing electricity networks will increase the efficiency and qualification of future power systems. Smart grids are cyber-physical systems. Commonly, cyber-physical systems come with some cyber-security issues as well as the opportunities they provide. The communication infrastructure has to be designed efficiently, reliably, securely and effectively to protect the systems and to prevent and detect these security issues. In this context, cyber-security requirements, network vulnerabilities, secure communication architectures and protocols, and the prevention of cyber-attacks in smart grid networks are discussed in the study. Moreover, it is aimed to give a roadmap in smart grid network security for future studies by providing an in-depth understanding of cyber-security vulnerabilities and solutions.

Keywords: Cyber-physical system, Smart grid, Cyber security, Communication infrastructure

[1] Muhammed Zekeriya GÜNDÜZ (**Orcid ID:** 0000-0003-4278-7123), Bingöl Üniversitesi, Teknik Bilimler MYO, Bilgisayar Teknolojileri Bölümü, Bingöl, Türkiye
[2] Resul DAŞ (**Orcid ID:** 0000-0002-6113-4649), Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Elazığ, Türkiye

*Sorumlu Yazar/Corresponding Author: Muhammed Zekeriya GÜNDÜZ, e-mail: mzgunduz@bingol.edu.tr

Geliş tarihi / *Received:* 06-12-2019
Kabul tarihi / *Accepted:* 25-01-2020

GİRİŞ

Endüstriyel ve sosyal alandaki gelişmeler enerjiye olan ihtiyacı artırmaktadır. Mevcut güç sistemlerinin kapasite yetersizliği, farklı yenilenebilir enerji kaynaklarının elektrik üretiminde kullanılması, elektrik ihtiyacının artması gibi sebepler geleneksel elektrik şebekelerinin gelişmiş bilgi iletişim teknolojileri ile güçlendirilmesi gerekliliğini ortaya çıkarmıştır (Ahmed ve ark., 2019). Ayrıca geleneksel elektrik şebekelerinde kömür, petrol gibi fosil yakıt kaynakları ile rüzgâr, su ve güneş enerjisi gibi yenilenebilir enerji kaynakları dâhil birçok farklı enerji kaynağının etkin yönetiminin sağlanması önemli bir sorundur (Colak ve ark., 2016). Bu eksikliklerin akıllı şebeke sistemleri ile giderilmesi için önde gelen kuruluşlar tarafından ortak projeler ve çalışmalar yapılmaktadır. Özellikle, bünyesinde birçok resmi ve özel kuruluşu barındıran National Institute of Standards and Technology (NIST) tarafından yayınlanan kapsamlı çalışmalar dünya genelinde akıllı şebekelerde standartlaşmanın sağlanmasında önemli katkılar sağlamaktadır (NIST, 2014).

Akıllı şebekeler yüksek bant genişliği, çift yönlü iletişim ve interaktif enerji yönetimine olanak sağlayan "akıllı ölçüm" olarak da adlandırılan AMI (Advanced Metering Infrastructure) sistemlerine sahip olacak şekilde tasarlanırlar. Bu durum sağlam bir iletişim altyapısını gerektirir (Usman ve Shami, 2013). Ancak bilgi iletişim teknolojilerine bağımlı ve karmaşık bir yapıda olan bu sistemler, iletişim ve ağ sistemleri ile ilgili olası güvenlik zafiyetlerini de beraberinde getirmektedirler. Saldırganlar tarafından sisteme zarar verme veya veri hırsızlığı amacıyla kullanılabilecek bu olası zafiyetler, müşteri bilgilerinin çalınmasından, sistemin tamamen çökmesine kadar büyük sorunlara sebep olabilirler. Ayrıca konunun öneminin daha iyi kavranması açısından yakın geçmişte siber-fiziksel sistemlere yapılan birçok saldırı olduğu da bilinmelidir (Eder-Neuhauser ve ark., 2017; Gündüz ve Daş, 2020).

Akıllı şebeke iletişim ağları siber güvenlik gerekliliklerini sağlayacak şekilde tasarlanmalıdır. Güvenlik zafiyetlerinin ve siber güvenlik tehditlerinin doğru tanımlanması siber ataklara karşı etkin önlemlerin alınmasına olanak sağlar. Erişilebilirlik, bütünlük ve gizlilik siber güvenliğin sağlanması açısından temel güvenlik gerekliliklerdir. Bu bağlamda; çalışmada akıllı şebeke veri iletim ağlarında kritik öneme sahip siber güvenlik amaçları ve gereklilikleri sunulmuştur. Ayrıca, akıllı şebekelerde güvenli iletişimin sağlanması için temel güvenlik gerekliliklerini ihlal eden atakların analizi, mevcut siber güvenlik çözümlerinin değerlendirilmesi ve güvenli ağ protokolü mimarisi tasarımına yönelik siber güvenlik merkezli bir bakış açısı oluşturulması amaçlanmıştır.

Çalışmanın ikinci bölümünde akıllı şebekelerde iletişim ağ mimarisi sunulmuştur. Üçüncü bölümde siber güvenliğin amaçları ve gereksinimleri belirtilmiştir. Dördüncü bölümde akıllı şebeke iletişim ağına yönelik saldırılar ve önlemler değerlendirilmiştir. Tartışma ve sonuç beşinci bölümde yapılmıştır.

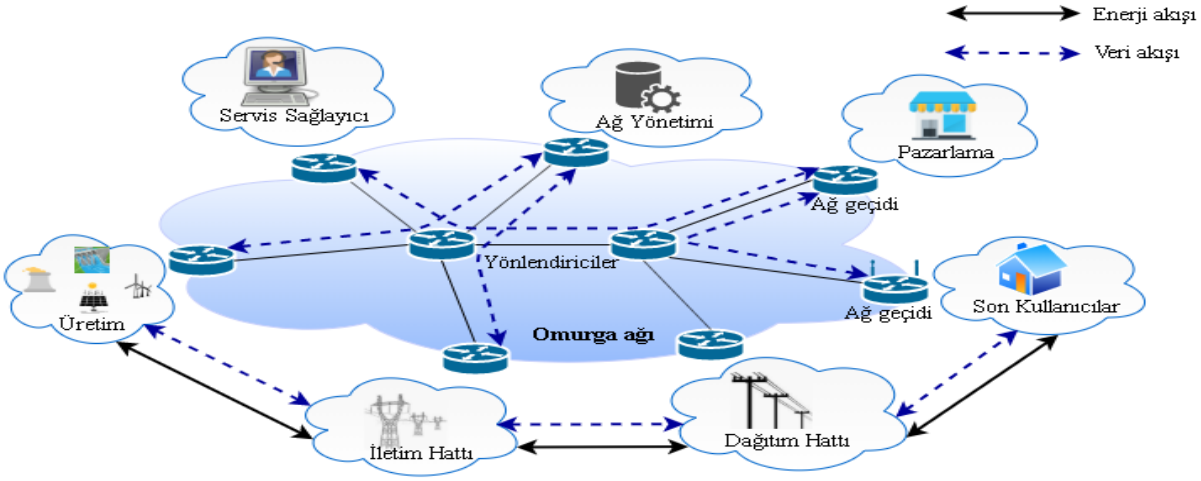
Akıllı Şebekelerde İletişim Ağ Mimarisi

Bu bölümde akıllı şebeke iletişim ağ mimarisinde yaygın olarak kullanılan iletişim teknolojileri ve protokollerinin temelleri sunulmuştur.

Ağ altyapısı temelleri

Bilgi iletişim teknolojilerinin entegre edildiği güç şebekeleri oldukça karmaşık yapıya sahip olan siber-fiziksel sistemlerdir. Bu karmaşıklığı minimize etmek için NIST tarafından akıllı şebeke kavramsal modeli önerilmiştir (NIST, 2014). Buna göre bir akıllı şebeke sisteminde; üretim, iletim, dağıtım, son kullanıcı, pazarlama, servis sağlayıcı ve ağ yönetimi olmak üzere 7 tane mantıksal alan vardır. İlk dört alan çift yönlü veri ve güç akışına sahiptir. Diğerleri ise akıllı şebekede verinin toplanması ve güç

yönetiminin sağlanması ile ilgilidir. Bu alanların haberleşmesi için iletişim ağı, Şekil 1'de gösterildiği gibi dağıtık ve hiyerarşik bir yapıda oluşturulmalıdır (Wang ve Lu, 2013).



Şekil 1. Akıllı şebeke ağ mimarisi

Şekil 1'deki omurga ağı mantıksal alanlar arası haberleşme için kullanılan altyapıyı göstermektedir. Altyapıda bulunan ağ geçidi cihazları alanların iletişim altyapısına bağlanmasını sağlar iken yüksek bant genişliğine sahip yönlendirici cihazları ise mesajların alanlar arasında yönlendirilmesini sağlamaktadır. Alanlar arasındaki kablolu haberleşme genellikle omurga altyapısında bulunan ve yüksek bant genişliğine sahip fiber optik kablolar ile sağlanır (Lopez ve ark., 2015).

Her bir alan bir yerel alan ağı (Local Area Network-LAN) olarak değerlendirilebilir. LAN ağları barındırdıkları ağ cihazları sayesinde alan içindeki iletişimi sağlarlar. Alan içindeki haberleşme genellikle sınırlı bant genişliğine ve işlem yeteneğine sahip olan akıllı sayaçlar, sensörler ve akıllı elektronik cihazlardan oluşan amaca özel olarak oluşturulan ad-hoc ağlar şeklindedir. Ad-hoc ağlar, herhangi bir kablosuz erişim noktasına ihtiyaç duymadan veri aktarımının sağlandığı ağlar olarak tanımlanabilmektedir. Bu ad-hoc ağlar genellikle sensör ağlar, hücresel ağlar, bilişsel radyo ağları gibi kablosuz iletişim teknolojilerini kullanırlar (Bedi ve ark., 2018). Akıllı şebekelerde kablosuz iletişimin kullanılması mobilitenin sağlanması, altyapı maliyetlerinin azaltılması, karmaşıklığın azaltılması gibi birçok avantaj sağlar. Bu yüzden akıllı şebekeler için yeni kablosuz iletişim cihazları ve protokollerinin geliştirilmesi teşvik edilmektedir (Wang ve Lu, 2013).

Örneğin AMI sistemlerinde bulunan ev alan ağı (Home Area Network-HAN) cihazları ve akıllı sayaç gibi uygulamalar için zigbee protokolü ile çalışan cihazların kullanımı yaygınlaşmaktadır. Bu yüzden, geleneksel elektrik şebekeleri ile karşılaştırıldığında akıllı şebekelerin geniş ölçekli, dağıtık ve hiyerarşik olan iletişim altyapısının, özellikle kablosuz ağ teknolojileri sayesinde geliştirilmesi amaçlanmaktadır. Böylesine karmaşık bir sistemde güvenli ve güvenilir bir şekilde işlemlerin gerçekleştirilmesi için kendine özgü niteliklere sahip kapsamlı güvenlik mimarilerinin oluşturulması gerekir (Tan ve ark., 2017). İletişim altyapı mimarileri ilk oluşturuldukları zamanlarda güvenlik öne çıkan bir konu değildi. Verinin eksiksiz ve zamanında iletiminin sağlanması en önemli problemdi. Ayrıca, ağ sistemlerine yönelik siber saldırılar mevcut bile değildi. Ancak, günümüzde sistemlerin siber güvenliğine zarar verecek birçok saldırı türü mevcuttur. Dolayısıyla, güvenlik gereksinimleri ağ mimarisinin içinde katmanlara özel ve dağıtık bir şekilde gerçekleştirilmelidir. Akıllı şebeke iletişim ağları genellikle dört katmanlı olarak tasarlanırlar. Bu katmanlar yukarıdan-aşağıya sırası ile uygulama, ağ/taşıma, MAC, ve fiziksel katman şeklindedir (Wang ve Lu, 2013).

İletişim ağları ve protokolleri

Akıllı şebeke iletişim ağları karmaşıklık ve hiyerarşik yapı bakımından internete benzerdir. Fakat bu iki karmaşık sistem arasında bazı temel farklılıklar vardır. İnternetin temel fonksiyonu kullanıcılar için sanal gezinti, veri indirme gibi servisler sağlamaktır. İnternet mimarisi tasarımında yüksek bant genişliği ve bunun kullanıcılar arasında adil bir şekilde dağıtılması oldukça önemlidir. Akıllı şebeke iletişim altyapısında ise sistemin güvenilir bir şekilde çalışmasının garanti edilmesi, güvenlik, gerçek zamanlı olarak veri gönderiminin sağlanması ve gerçek zamanlı/zamansız şekilde sistemin gözlemlenebilmesi ve yönetilmesi oldukça önemlidir. Ayrıca akıllı şebekelerde veri iletiminde gecikmenin olmaması, bant genişliğine dayalı yapılan iş çıktısından daha önemlidir. Akıllı şebeke uygulamalarında zaman kaybı yaşamaması gereken veri paketleri uygulama katmanından doğrudan MAC katmanına geçirilebilir. Bu durum, akıllı şebeke iletişim ağlarındaki performans ölçütleri, veri trafiği modeli, zamanlama gereklilikleri, iletişim modeli ve protokol gruplarının internet ağından farklı olduğunu gösterir (Wang ve Lu, 2013).

Akıllı şebeke ağlarında veri trafik akışının büyük bir kısmı periyodiktir. Bu durum HAN ağlarında belli aralıklarla akıllı sayaç okumalarının sağlanması, alt güç merkezlerinden ham verilerin örneklenmesi gibi işlemlerin verimli bir şekilde yapılabilmesi için gereklidir. İnternette ise periyodiklik genellikle söz konusu olmadığından bu iki sistemin veri trafiği modelleri farklıdır.

İnternette noktadan-noktaya iletişim modeli prensibi esastır. Geleneksel güç sistemlerinde en yaygın kullanılan iletişim modeli, elektronik cihazların durumlarını merkeze bildirdikleri tek yönlü iletişimdir. Akıllı şebekede ise merkezden-cihaza ve cihazdan-merkeze olacak şekilde iki yönlü iletişim prensibi vardır. Akıllı şebekelerde, noktadan-noktaya iletişim de desteklenmektedir. Ancak bunun kullanımı güvenlik endişelerinden dolayı sınırlıdır.

İnternet, IPv4 ve IPv6 protokollerini esas alır iken akıllı şebekelerde sadece IPv6 protokolü ağ/taşıma katmanı protokolü olarak kullanılır. Ancak akıllı şebekelerde ağın ihtiyaç ve fonksiyonlarına bağlı olarak Ipv6 den başka protokol takımları da kullanılabilir. Örneğin, ATM anahtarlama diğer adıyla hızlı paket anahtarlama, zaman kritik mesajların teslim edilmesinde hizmet kalitesi garantisi sağladığı için tercih edilebilir. Sonuç olarak, akıllı şebeke uygulamaları heterojen protokol yığınları içerirler. Mevcut iletişim protokollerinin bu farklılıklardan dolayı bazı güvenlik zafiyetleri olabilir, bu yüzden otomasyon ve iletişim ağları için daha güvenli standartlar geliştirilmelidir.

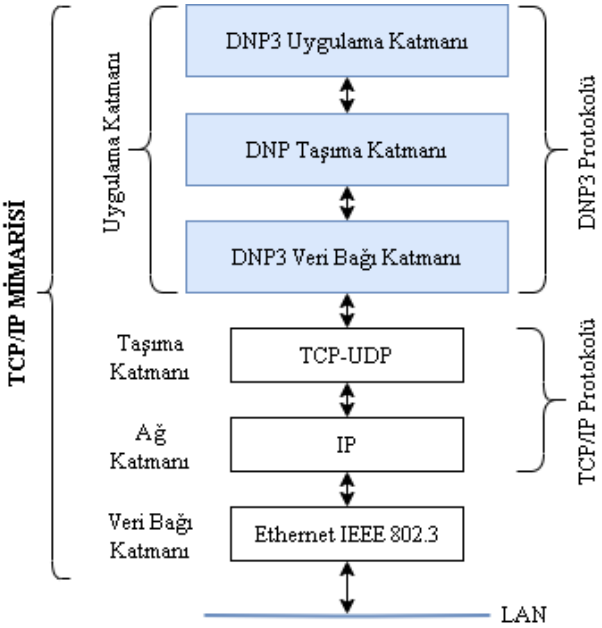
İnternet üzerinde, çoğu IP trafiği en iyi erişimi gerektirir. En iyi erişim, bağlantının devamlılığının sağlanmasını gerektirir. İnternet ağları, gecikmeye duyarlı trafik, ses ve multimedya servislerini desteklemek için 100-150 milisaniyelik gecikme gereksinimlerine sahiptir (Wang ve Lu, 2013). Bununla birlikte, akıllı şebekeler milisaniyeden dakikalara kadar daha geniş bir gecikme gereksinimi yelpazesine sahiptirler (NIST, 2014). Örneğin, trafo merkezlerindeki kontrol mesajları 3 milisaniye gecikme sınırına sahiptirler. Bu nedenle, akıllı şebekeler mesaj iletimi konusunda İnternet'ten çok daha katı "zamanlama gereksinimi" gerektirir. Tablo 1, internet ve akıllı şebeke iletişim ağları arasındaki temel farklılıkları göstermektedir. Bu farklılıklar güç tesislerinin enerji yönetiminin verimli, sağlam ve güvenli veri dağıtımını sağlaması için akıllı şebeke iletişim ağlarının tasarımının kapsamlı bir şekilde gözden geçirilmesi gerektiğini göstermektedir.

Güç sistemleri için iletişim protokolleri standart olacak şekilde geliştirilmeye devam etmektedir. DNP3 (Distributed Networking Protocol 3.0), IEC61850, Modbus, IEEE Std. C37.118 bu protokollerden bazılarıdır (Mrabet ve ark., 2018). DNP3, General Electric tarafından 1993 yılında geliştirilmiştir. TCP/IP tabanlı bir protokol olan DNP3 şu anda Kuzey Amerika güç sistemlerinde kullanılan yaygın bir standarttır. Elektrik, su, petrol, doğalgaz, güvenlik gibi alanların SCADA sistemlerinde yaygın

kullanılan bir protokoldür. DNP3 başlangıçta fiziksel, veri bağı, taşıma ve uygulama katmanı olmak üzere dört katmanlı tasarlanmış idi. Günümüzde ise yeni iletişim teknolojilerini ve noktadan noktaya iletişimi desteklemesi için TCP/IP protokolünün üzerine üç katmanlı olacak biçimde Şekil 2'de gösterildiği gibi yerleştirilmiştir.

Tablo 1. İnternet ve akıllı şebeke iletişim ağları arasındaki temel farklılıklar

Kriter	İnternet Ağları	Akıllı Şebeke İletişim Ağları
Performans	İşlem hacmi	Mesaj gecikmesi
Ağ trafiği	Bant genişliği	Periodik
Zamanlama gereksinimi	Gecikme duyarlı (100 ms)	Zaman açısından kritik (3 ms)
İletişim modeli	Uçtan uca iletişim	İki yönlü iletişim, Kısıtlı uçtan-uca iletişim
Protokol takımı	IPv4, IPv6	IPv6, Heterojen, Tescilli özel iletişim protokolleri



Şekil 2. Güncelleştirilmiş DNP3 protokolü

IEC 61850, koruma, kontrol, ölçüm ve izleme gibi tüm trafo fonksiyonlarının entegrasyonunu sağlayan uluslararası iletişim standardıdır. Ethernet temelli iletişimi sağlayan IEC 61850 protokolü alt-istasyon otomasyon sistemlerinde kullanılmak üzere International Electrotechnical Commission (IEC) tarafından geliştirilmiştir. IEC 61850'nin kendine ait olan TCP/IP ve UDP/IP'nin de dâhil olduğu protokol takımları vardır. IEC 61850, alt-istasyon merkezlerinde bilgi ve veri değişimi için zamanlama gereksinimlerini açıkça tanımlar. Örneğin zaman açısından kritik mesajlar doğrudan uygulama katmanından MAC katmanına geçirilebilir. IEC 61850, alt-istasyonların haberleşmesinde DNP3'ün yerini almayı amaçlamaktadır. Mevcut IEC 61850, bir alt-istasyon merkezi içinde sınırlıdır, ancak IEC 61850'nin gelecekteki enerji sistemlerinde dış alt-istasyon merkezi iletişimi için potansiyel olarak kullanılabilmesi için çalışmalar yapılmaktadır. IEEE Std. C37.118 protokolü ağırlıklı olarak WAN ağlarına uygulanırken, IEC61850 ise alt-istasyon otomasyonu için en iyi seçimdir (Rizzetti ve ark., 2015).

Seri haberleşme protokolü olan Modbus 1979 yılında Modicon tarafından PLC cihazlar için geliştirilmiştir. Modbus sunucu/istemci tabanlı bir protokol olup endüstri ortamında en çok kullanılan protokollerdendir. Kullanımının kolay olması ve herkes tarafından telif ücreti gerektirmeden kullanılabilmesi tercih edilmesinin en büyük sebepleri arasındadır (Rizzetti ve ark., 2015).

DNP3 ve IEC 61850 protokolleri ilk tasarlandıklarında sadece haberleşme özelliklerine odaklanılmış idi. Bu yüzden herhangi bir güvenlik mekanizmasına sahip değildiler. Veri paketlerinde saldırganlar tarafından yapılacak değişikliklere karşı bir önlem içermiyorlardı. Ancak, salt veri iletişimi günümüz SCADA kontrol sistemleri için yetersiz bir durumdur. Bu yüzden günümüzde akıllı şebekelerde güç, ağ ve güvenlik çalışmaları birlikte yapılarak güvenlik gereksinim ve amaçlarını da sağlayan protokollerin tasarlanması amaçlanmaktadır. Güç santrallerindeki RTU ve PLC bileşenleri genellikle iletişim amacıyla MODBUS veya DNP3 protokollerini kullanırlar. MODBUS protokolü yetkisiz girişlere karşı güvenlik sağlamaz. Bu yüzden IP bağlantısına sahip bir saldırgan, istenmeyen sistem çalışmasına yol açacak şekilde PLC veya RTU birimlerini bozabilir.

Mevcut siber güvenlik çözümleri, akıllı şebeke siber-fiziksel sistem güvenliği endişeleri için uygun veya verimli olmayabilir ve alana özgü yaklaşımlar ve çözümler gerektirir (Tong ve ark., 2016). Bu nedenle, akıllı şebekedeki siber güvenlik, DNP3.0, Modbus, IEEE Std. C37.118 ve IEC 61850 gibi özel iletişim protokollerini gerektirir. Akıllı şebekeye yönelik siber güvenlik konusundaki öncelikli araştırma alanları arasında gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama ve güvenlik açığı değerlendirmesi bulunmaktadır.

Akıllı Şebekelerde Siber Güvenlik Amaçları Ve Gereksinimleri

Akıllı şebeke iletişim altyapılarının siber güvenlik esaslarına göre tasarlanması için güvenlik amaç ve gereksinimlerinin bilinmesi gerekmektedir. Bu bölümde akıllı şebekelerde siber güvenlik amaç ve gereksinimleri konularına odaklanılmıştır.

Siber güvenlik amaçları

NIST tarafından akıllı şebekelerde siber güvenlik konusunda önde gelen birçok organizasyonun işbirliği ile kapsamlı bir rapor yayınlanmıştır. Bu raporda belirtilen akıllı şebeke siber güvenlik amaçları üç tanedir. Sağlanması gereken bu güvenlik amaçlarının öncelik sıralaması İnternet ağlarında gizlilik, bütünlük, erişilebilirlik şeklince iken akıllı şebekelerde erişilebilirlik, bütünlük, gizlilik şeklindedir (Pillitteri ve Brewer, 2014).

Erişilebilirlik: Yetkili tarafların ihtiyaç duyduğunda bilgiye erişebileceği anlamına gelir. Akıllı şebekelerde bilgiye zamanında ve güvenli bir şekilde erişme ile bilginin kullanımının kesintisiz olarak sağlanması garanti altına alınmalıdır. Erişilebilirliğin kaybolması, veri kullanımının ve erişiminin engellenmesi küçük veya büyük çaplı elektrik kesintilerine sebep olur. Erişilebilirliğin engellenmesine sebep olan ataklar genellikle DoS atakları olarak adlandırılır. Bu ataklar akıllı şebekedeki veri iletişimini geciktirmeyi, engellemeyi ve bozmayı amaçlar.

Bütünlük: Veriler üzerinde yetkisiz taraflarca değişiklik yapılmasının imkânsız olduğu veya tespit edildiği ve ayrıca yetkili kullanıcılar tarafından yapılan değişikliklerin ise izlendiği anlamına gelir. Veri bütünlüğünün zarar görmesi, verinin yetkisiz kişiler tarafından değiştirilmesi veya bozulmasını ifade eder. Bu durum sistem yönetiminde ileri düzeyde yanlış kararlar verilmesine sebep olur. Veri üzerinde yapılacak yetkisiz değişikliklerin engellenmesi ve bütünlüğün sağlanması için verinin sahibince inkâr edilememesi ve orijinalliğinin yani aslına uygunluğunun sağlanması gereklidir. Bütünlüğü hedef alan saldırılar, akıllı şebekedeki veri değişimini kasıtlı ve yasadışı olarak değiştirmeyi veya engellemeyi amaçlarlar.

Gizlilik: Belli bir veri kümesine erişim sağlayacak kişi veya birimlerin belirlenmesidir. Bilgilerin yalnızca erişmeye yetkili taraflarca görülebileceği veya kullanılabileceği anlamına gelir. Gizlilik, kişilere veya kamuya açık olmayan verilerin yetkisiz taraflarca açığa çıkarılmasını önlemek için gereklidir. Özellikle içerisinde banka, kimlik, tüketim bilgileri gibi kişisel ve mahrem bilgileri bulunduran akıllı sayaç cihazlarında gizlilik ilkesi öne çıkmaktadır. Akıllı şebekelerde gizliliği hedef alan saldırılar ağ kaynaklarından yetkisiz olarak bilgi edinmeyi amaçlamaktadır.

Akıllı şebekelerde sistemin güvenli bir şekilde devamlı olarak çalışması bakımından erişilebilirlik ve bütünlük en önemli güvenlik amaçlarıdır. Gizlilik ise diğerlerine göre daha az kritiktir. Fakat AMI, talep ihtiyacı gibi uygulamalar sayesinde son kullanıcılar ile etkileşime olanak sağlayan akıllı şebeke sistemlerinde gizlilik ilkesi daha da önemli olmaya başlamıştır.

Siber güvenlik gereksinimleri

Akıllı şebekelerin geleneksel şebekelere göre daha geniş bir coğrafi alana yayılması ve internete bağlı olmasından dolayı daha açık bir iletişim ortamına sahiptirler. Bu yüzden sistemde bulunan tüm bileşenleri ağ saldırılarına karşı %100 güvence altına almak mümkün değildir. Dolayısıyla, iletişim ağında siber atakların sebep olacağı anormal süreçlerin belirlenmesi ve tanımlanması için profil tanımlama, test işlemleri ve ağ trafik durumunun izlenmesi sürekli olarak sağlanmalıdır. Ayrıca, akıllı şebekeler anormal durumlarda ve hatta siber saldırıların gerçekleştiği zaman diliminde bile ağ işlemlerini devam ettirebilmek için kendisini onarabilme yeteneğine sahip olmalıdır. Bu bağlamda, akıllı şebekelerde erişilebilirlik, bütünlük ve gizlilik yüksek öncelikli siber güvenlik amaçlarıdır. Ayrıca, bazı spesifik siber güvenlik gereksinimleri de bulunmaktadır. Bu gereksinimlerin bir kısmı bilginin korunmasına yönelik iken bir kısmı da ağ sisteminin güvenli çalışmasını temin eder.

Yetkilendirme: Sistem kaynaklarıyla ilgili cihaz ve kullanıcı ayrıcalıklarını veya erişim düzeylerini belirlemek için kullanılan bir güvenlik mekanizmasıdır. Yetkilendirme, sistemde bulunan cihazların veya bireylerin kimliklerini temel alarak sistem nesnelerine erişmelerini sağlar. Yetkilendirme kullanıcı kimliğinin geçerliliğinin tespiti için kimlik doğrulamadan önce gerçekleştirilir.

Kimlik doğrulama: Cihazın veya kişinin iddia ettiği taraf olduğunun garanti edilmesidir. Ancak kimlik doğrulama cihazın veya kişinin erişim haklarıyla ilgili hiçbir şey belirtmez. Kimlik doğrulama yetkilendirmeden farklıdır.

Orijinallik: Bir mesajın, işlemin veya veri alışverişinin mesajın ana kaynağı olduğunu iddia eden tarafça aslına uygunluğunun doğrulanmasıdır. Orijinallik, veriyi gönderen tarafın kimliğinin denetlenmesini gerektirir. Kimlik doğrulama işlemi sayesinde verinin orijinalliği sağlanabilir.

Denetim: Bir organizasyonun bilgi iletişim teknolojisi altyapısının, politikalarının ve faaliyetlerinin incelenmesi ve değerlendirilmesidir. Denetim, hesap verebilirliği sağlamak ve büyük çaptaki endişe verici güvenlik olaylarını önlemek için etkili bir yöntemdir.

Hesap verebilirlik: Bir sistemdeki kullanıcı, süreç ve cihaz işlemlerinin kayıt altında tutulup gerektiğinde incelenebilmesidir. Kullanıcı kimliği ve kimlik doğrulaması kullanımı hesap verebilirliği destekler iken paylaşılan kullanıcı kimlikleri ve şifrelerin kullanılması ise hesap verebilirliği ortadan kaldırır.

Mahremiyet: Gizlilik ilkesi altında bulunur. Özellikle son kullanıcıların mahrem ve hassas bilgilerinin korunmasını esas alır.

Kimlik Tanımlama: ID numarası gibi bir kullanıcı tanımlayıcısının bir insana, bilgisayara veya ağ bileşenine eşleştirilmesi işlemidir.

Erişim Denetimi: Belirlenmiş kaynaklara sadece doğru bir şekilde tanımlanmış teknik personel ve son kullanıcıların erişiminin sağlanmasıdır. Ağ iletişimindeki güvenlik riskini önemli derecede azaltan temel kavramdır. Kullanıcıların ve varlıkların yetkilendirilmesi, kimlik tanımlaması ve kimlik doğrulaması işlemlerini içerir.

İnkâr Edememe: İletilen bir mesajın hangi şahıs ya da cihaz ile ilişkili olduğunu kanıtlayabilmektir. Kimlik tanımlama ve kimlik doğrulama hizmetlerinin bir uzantısı olarak görülebilir.

Akıllı şebekeler milyonlarca elektronik cihazı ve kullanıcıyı barındırır. Bir kullanıcı veya cihazın doğrulanması bakımından; kimlik tanımlama ve kimlik doğrulama, iletişim altyapısında kaynaklara erişimin güvenliğini sağlamak açısından ön koşul olarak önemli gerekliliklerdir. Erişim kontrolü sürecinde, yetkisiz kullanıcıların hassas verilere erişimi ve kritik altyapı elemanlarında kontrol yetkisi engellenmelidir. Bu gerekliliklerin karşılanması, verilerin şifrelenmesi ve kimlik doğrulamanın gerçekleştirilmesinin sağlanması için akıllı şebekedeki her bir bileşen temel düzeyde de olsa kriptografik süreçlere dâhil edilmelidir. Ayrıca, güvenlik ve güvenilirlik terimleri arasındaki fark, güvenliğin kasıtlı tehditlere karşı koruma sağlaması iken güvenilirliğin kasıtlı olmayan tehditlere karşı koruma sağlamasıdır. Bir sistemin güvenilirliğinin tam olarak sağlanabilmesi için kasıtlı olmayan güvenlik tehditlerine de karşı koruma sağlayabilecek şekilde tasarlanması gerekir (Otuoze ve ark., 2018).

Erişim kontrolü, tanımlama ve kimlik doğrulama tüm iletişim ağında sıkı bir şekilde gerçekleştirilmelidir. Çünkü geleneksel iletişim ağlarından farklı olarak akıllı şebeke iletişim ağlarında, özellikle iletim ve dağıtım sistemlerinde, veri paketleri kesinlikle hem zamanında hem de güvenli olarak iletilmelidir. Ancak veri paketlerinin hem zamanında hem de güvenli olarak iletilmesinin aynı anda sağlanması genellikle mümkün olmamaktadır. Bu durum bazı performans metriklerinde tavizlerin verilmesini gerektirebilir. Bu yüzden akıllı şebeke ağlarında her zaman güvenli, fiziksel olarak korunmuş, yüksek bant genişliğine sahip iletişim kanalları kullanılamaz. Buna çözüm olarak akıllı şebeke ağ mimarisi ve iletişim protokollerinin tasarımında verinin güvenliğini ve iletişimin verimliliğini dengelemek için ağın özellik ve kullanım durumuna göre tercihler belirlenmelidir (Wang ve Lu, 2013).

Sonuç olarak akıllı şebekelere özel, siber güvenlik açısından güvenli ve verimli iletişime olanak sağlayan protokoller tasarlanmalıdır. Ayrıca mimarinin tüm katmanlarında oluşturulacak ağ protokollerinde güvenlik işin içine dâhil edilmelidir. Saldırı tespit ve önleme sistemleri iletişim ağının her yerinde uygulanmalıdır. Bahsedilen siber güvenlik amaç ve gereklilikleri göz önüne alındığında, akıllı şebekelerin iletişim ağ yapısının etkili ve güvenli bir şekilde sağlanması için internetten daha katı güvenlik gereksinimleri gerektirdiği görülmektedir. İletişim ağlarındaki bu siber güvenlik gereksinimlerinin karşılanması, etkili yönetim politikalarının uygulanması ve sağlam fiziksel altyapıların tasarlanması, "enerji interneti" hedefine ulaşmak için kapsamlı güvenlik yeteneklerine sahip olan akıllı şebekelerin siber ortamlarda daha güvenilir olmasını sağlayacaktır.

Akıllı Şebeke Ağına Yönelik Tehditler Ve Çözümler

Akıllı şebekelerde, geniş ölçekli elektrik kesintileri ve güç elemanlarına fiziksel ya da siber açıdan zarar verilmesi kesinlikle meydana gelmesi istenmeyen durumlardır. Sistemin geniş ölçekli ve karmaşık bir yapıya sahip olmasından dolayı olası tüm saldırıları sıralamak pratik bir çözüm değildir (Mendel, 2017). Bu yüzden akıllı şebekelere yönelik yapılabilecek olası siber atakların spesifik olarak incelenmesi gereklidir. Erişilebilirlik ilkesine zarar vermeyi amaçlayan siber ataklar DoS saldırıları olarak bilinir. Bu saldırılar, akıllı şebekelerdeki veri iletişiminin gecikmesini, engellenmesini ya da bozulmasını amaçlar. Bütünlük ilkesine zarar vermeyi amaçlayan siber ataklar, akıllı şebekelerde kasıtlı olarak ve yasal olmayan bir şekilde veri içeriğinin manipüle edilmesini ya da bozulmasını amaçlar.

Gizlilik ilkesine zarar vermeyi amaçlayan siber ataklar ise akıllı şebekelerde, ağ kaynaklarından yetkisiz olarak bilgi elde edilmesini amaçlar (Cintuglu ve ark., 2017).

Akıllı şebekelerin kritik öneme sahip olmasından dolayı iletişim ağında gerçekleştirilecek siber saldırıların otomatik tespiti ve sistemin saldırının türüne göre uygun çözümler üretmesi ağın erişilebilirliğini sağlamak için gereklidir. Akıllı şebeke uygulamaları bağlayıcı güvenlik gereksinimlerini karşılamalıdır. Akıllı şebekenin çalışmasını etkileyebilecek tüm cihazlar ve kullanıcılar için güçlü bir kimlik doğrulaması süreci gereklidir. Bu bağlamda çalışmanın bu bölümünde akıllı şebeke güvenlik amaçlarına göre sınıflandırmada öne çıkan saldırılar ele alınmaktadır. Saldırıların özellikleri genel olarak belirtilmekte ve öne çıkan bazı saldırılar detaylı olarak incelenmektedir. Özellikle DoS saldırılarına karşı alınabilecek önlemler incelenmekte ve mevcut çözümler ile çözülemeyecek olası sorunlar tartışılmaktadır.

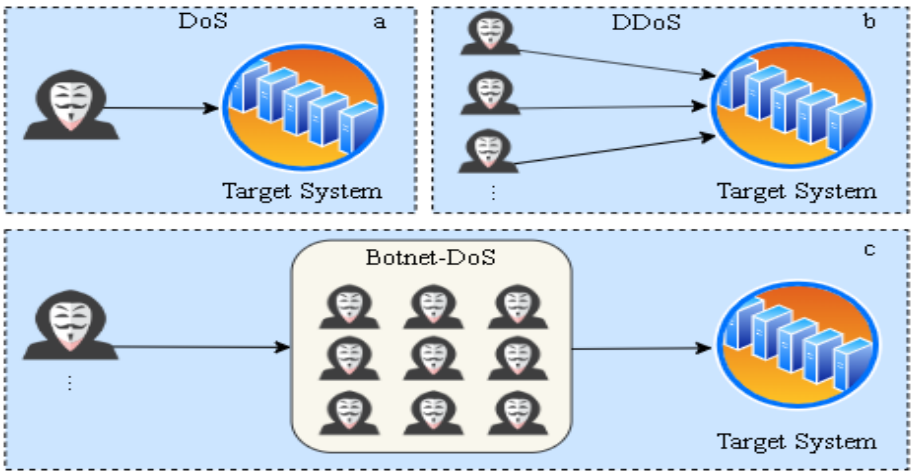
Erişilebilirliğe yönelik ataklar

Akıllı şebekelerde erişilebilirlik sağlanması gereken en önemli güvenlik amacıdır. Bu yüzden DoS ataklarının önlenmesine yönelik birçok çalışma yapıldığı görülmektedir (Kaur ve ark., 2014; Rawat ve Bajracharya, 2015; Shapsough ve ark., 2015). Bu bölümde akıllı şebeke iletişim ağlarına karşı yapılan bu atakların özet bir derlemesi sunulmaktadır. Dos ataklarının nasıl gerçekleştirildiğinin bilinmesi erişilebilirlik ilkesinin anlaşılması açısından önemlidir. Şekil 3a'da bir saldırgan tarafından gerçekleştirilen klasik bir DoS saldırısı gösterilmektedir. Saldırıyı gerçekleştiren tek bir saldırgandır. Saldırgan, hedef sistemin bant genişliğini meşgul ederek, sistemin iletişim hızını düşürmek için kendi cihazından devamlı olarak gereksiz bağlantı istek paketleri göndermektedir. Şekil 3b'de ise birden fazla saldırgan aynı anda hedef sistemden yoğun bağlantı isteğinde bulunmaktadır. Bu saldırı DDoS olarak adlandırılır. Burada amaç bant genişliğini gereksiz bağlantı istek paketleri ile doldurarak sistem iletişim hızını yavaşlatmak ya da kullanılamaz hale getirmektir. Şekil 3c'de ise en kapsamlı DoS atağı şekli görülmektedir. DDoS saldırısı gerçekleştirecek olan saldırgan veya saldırganlar kendilerine web üzerinde bir saldırı ordusu oluştururlar. Bu saldırı ordusu botnet olarak adlandırılır. Botnet ağındaki saldırgan cihazlar gönüllü kullanıcılara ait olabilir. Ancak bu ağdaki cihazlar genellikle arka kapı ve truva atı zararlı yazılımları ile ele geçirilip, kullanıcılarının haberi bile olmadan kullanılan cihazlardır. Literatürde DDoS saldırılarının genellikle botnet ağları üzerinden gerçekleştirildiği ifade edilmektedir. Botnet-DoS terimi tarafımızdan önerilmiştir. Bir botnette bulunan saldırganlar içerisinde gönüllü saldırganların yanısıra cihazları izinsiz olarak ele geçirilmiş kullanıcılar da vardır.

Dos atakları akıllı şebekelerin en önemli güvenlik amacı olan erişilebilirlik ilkesine zarar verirler (Yi ve ark., 2014). Bu yüzden, iletişimin performansını ve elektronik cihazların işlerliğini bozan ya da azaltan Dos ataklarının akıllı şebekelerde hangi güvenlik zafiyetlerinden dolayı meydana geleceği ve sonuçlarının incelenmesi önemlidir. Mevcut Dos saldırı türleri farklı katmanlarda gerçekleştirilebilir. Örneğin; Buffer flooding, traffic flooding taşıma katmanında (L3), jamming ataklar fiziksel katmanda (L1) gerçekleşir. Özellikle traffic flooding ve worm atakları veri transfer hızında ciddi performans kayıplarına sebep olurlar (Lopez ve ark., 2015).

Jamming ataklar, özellikle kablosuz ağlarda L1 seviyesinde meydana gelen en etkili Dos ataklarındandır. Çünkü saldırganın sadece iletişim kanalına bağlanması saldırıyı başlatması için yeterlidir. Akıllı şebeke uygulamalarında bulunan iletişim ağlarında kablosuz iletişim teknolojilerinin - özellikle LAN ağlarında - yaygın olarak kullanılacak olması bu atakların L1 seviyesinde öne çıkan siber ataklar olacağını göstermektedir. Jamming atakların alt güç sistemlerinin performansına ciddi ölçüde

zarar verdiği tespit edilmiştir (Peng ve ark., 2019). Zaman açısından kritik öneme sahip komut paketlerinin iletiminin geciktirilmesi bunun en açık delilidir.



Şekil 3. Dos saldırı şemaları

Noktadan-noktaya iletişimin gerçekleştiği MAC katmanında gerçekleşen ARP spoofing saldırısı ise hem erişilebilirlik hem de bütünlük ilkesine zarar verir (Khelifa ve Abla, 2015). Bu saldırıda paketteki MAC parametreleri değiştirilerek sistemde gereksiz veri trafiğine sebep olunur. Bu Dos saldırısı çeşidi diğerlerine göre erişilebilirlik ilkesinin engellenmesi açısından daha etkisizdir. Multi-hop iletişimin gerçekleştiği ağ katmanlarında distributed traffic flooding ve worm propagation saldırısı gibi Dos atakları uçtan-uca iletişimin performansına ciddi zarar verebilirler.

Alt seviyelerde gerçekleştirilen Dos atakları iletişim kanalındaki iletişimin bant genişliğini tıkamayı hedefler. Uygulama katmanı Dos atakları ise elektronik cihazlara ait işlemci ve I/O birimleri gibi bileşenlerin kaynaklarını tüketmeyi amaçlar. Dolayısıyla, akıllı şebekelerde sınırlı işlem ve iletişim yeteneğine sahip olan yüzlerce elektronik cihaz, uygulama katmanı Dos ataklarının potansiyel hedefleri olabilir.

Akıllı şebekelerde gerçekleştirilebilecek bir Dos saldırısının iletişimde oluşturacağı en küçük etki, zaman açısından kritik öneme sahip olan kontrol veri paketlerinin az da olsa zaman kaybı yaşamasına sebep olacağından güç sisteminde yıkıcı bir etkiye neden olur. Sonuç olarak Dos atakları akıllı şebekelerdeki iletişim ağları için ciddi güvenlik tehdidi oluşturmaktadırlar. Geçmişte gerçekleştirilen büyük ölçekli Dos ataklarının internet performansını ciddi oranda düşürdüğü görülmektedir (Kumar ve ark., 2019). Bu durum başarılı olacak Dos saldırılarının akıllı şebekelerin ağ performansında da ciddi oranda düşüşe sebep olabileceğini göstermektedir. Bu yüzden erişilebilirlik akıllı şebekelerde kesintisiz olarak sağlanmak zorundadır.

Bütünlük ve gizliliğe yönelik ataklar

Akıllı şebekelerde verilerin manipüle edilmesini ya da ele geçirilmesini amaçlayan bu ataklar genellikle uygulama katmanında gerçekleştirilir. Bütünlük ilkesine zarar vermeyi amaçlayan ataklar kritik veri iletişimini bozmak için veriyi değiştirmeyi amaçlar (Kimani ve ark., 2019). Hedef, hem fatura bilgisi, talep miktarı gibi müşteri bilgileri hem de cihazların çalışma durumu, voltaj okumaları gibi güç sistemlerinin anlık durum verileri olabilir. Bu tür veriler hem son kullanıcılar hem de üreticiler için önemlidir. Veri bütünlüğünü korumak için güç sistemlerinde hata-toleransı ve bütünlük kontrolü yöntemleri kullanılır.

False-data-injection ataklarının da akıllı şebekeler için ciddi sorunlar oluşturdukları gözlemlenmiştir (Baig ve Amoudi, 2013). Load-redistribution bu saldırının özel bir tipidir. Bu atak akıllı şebekelerin güvenliği alanında araştırılmaya açık bir saldırı tipi olarak durmaktadır. Ayrıca bu ataklar finansal kayıplara da sebep olabilirler.

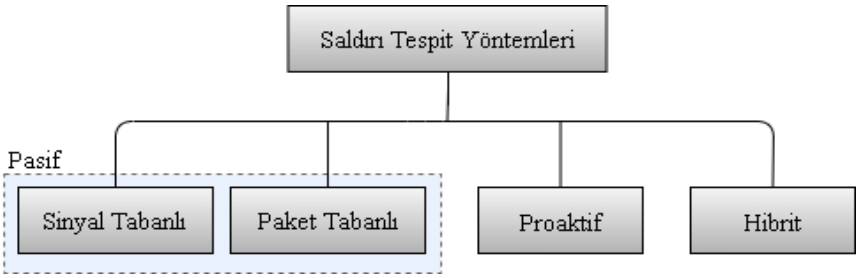
Bütünlük ilkesini hedef alan saldırganlar ile kıyaslandığında gizliliği hedef alan saldırganların güç sisteminde iletilen veriyi değiştirmek gibi bir niyetleri olmadığı anlaşılır. Çünkü bu ilkeyi hedef alan saldırganlar genelde pasif durumda kalırlar. Yani müşterinin hesap numarası, elektrik kullanım miktarı gibi ele geçirmeyi istedikleri verileri güç ağının iletişim kanallarındaki veri trafiğini dinleyerek elde ederler. Wiretapping ve traffic-analyzer atakları bunun tipik örnekleridir.

Gizlilik ilkesini hedef alan saldırıların genellikle akıllı şebekelerde iletişim ağının işlerliğine olumsuz etki etmedikleri düşünülebilir. Fakat müşterilerin mahremiyetinin önemi ve artan farkındalıkları ile sosyal etkilerinden dolayı mahremiyet ilkesine yönelik yapılan saldırılar son yıllarda daha fazla dikkat çekmektedir. Özellikle müşteri verilerinin toplu olarak sızdırılabilme olasılığı konuyu daha hassas hale getirmektedir.

Saldırganların şebeke ya da iletişim ağına kimlik doğrulanmış şekilde bağlanmış olmaları ve hassas verilere erişim sağlayabilmeleri, bütünlük ve gizlilik ilkelerine karşı yapılan atakların başlaması için öncül koşuldur. Bu yüzden kimlik doğrulama ve erişim denetimi bu tür ataklardan akıllı şebekeleri korumak için gereklidir. Dolayısıyla kimlik doğrulama ve erişim denetimi güvenlik gereksinimleri, sistemin her tarafında tüm veri akışı boyunca mutlaka sağlanmalıdır.

Akıllı şebekelerde saldırı tespiti

Siber fiziksel sistemlerden olan akıllı şebekeler, yapısı gereği birinci öncelikli olarak erişilebilirlik güvenlik ilkesini sağlamalıdır. Bu yüzden iletişim ve kontrol sistemlerinin erişilebilirliklerine anlık etki edebilecek DoS atakları akıllı şebekelerde en önemli ağ güvenliği tehdidi olarak görülmektedir. Bu ataklarının tespiti ve engellenmesi, ağ trafiğinin gözlemlenmesi ve filtrelenmesi gibi ağ önlemlerine oldukça bağlıdır. Bu yüzden DoS ataklarına karşı etkili ağ güvenliği yaklaşımları sağlamak gereklidir. Mevcut DoS ataklarının tespiti için Şekil 4'de gösterildiği gibi sinyal tabanlı tarama, paket tabanlı tespit, proaktif metot ve hibrit metot olmak üzere dört yöntem kullanılabilir (Wang ve Lu, 2013).



Şekil 4. DoS saldırısı tespit yöntemlerinin sınıflandırılması

Sinyal tabanlı taramada fiziksel katmandaki bir dedektör bir saldırının olup olmadığını tespit etmek için alınan sinyalin gücünü ölçebilir. Eğer bu değer belirlenen bir eşik değerinden büyük ise atak tespit dedektörü bir saldırının varlığını bir alarm ile bildirebilir. Paket tabanlı tespit yöntemi DoS atak tespitinde kullanılan genel ve etkili bir yöntemdir. Çünkü DoS atakları her zaman paket kaybının veya gecikmenin yaşanması bakımından ağ performansının düşmesine sebep olur. Bu yöntemdeki çözümler, paket iletiminin başarısızlığındaki artışı tanımlayarak olası atakları tespit etmek ve paketlerin iletim başarısını ölçmek için her katmanda kullanılabilir. Proaktif tespit yöntemi DoS atağı henüz başlamadan

olası saldırganların durumunu tanımlamayı amaçlar. Bu olası saldırganların durumunu test etme ve ölçme işlemi, kontrol paketleri gönderilerek yapılır. Hibrit metot önceki üç yöntemin ortak kullanımının sağlanması ile oluşturulur. Kablosuz ağlardaki jamming ataklarını etkili bir şekilde tespit etmek için sinyal-tabanlı ve paket-tabanlı yöntemlerin beraber kullanılması hibrit yönteme bir örnektir.

Sinyal tabanlı ve paket tabanlı yöntemler sadece ağı dinleyerek kontrol yaptıkları için pasif yöntemlerdir. Bu yüzden DoS atak tespiti için var olan metotlar akıllı şebekelerdeki iletişim ağlarında doğrudan uygulanabilirler (Radoglou-Grammatikis ve Sarigiannidis, 2019). Örneğin sinyal-tabanlı dedektör kablosuz akıllı şebeke uygulamalarında, paket-tabanlı metot ise AMI sistemlerinde DoS atak tespitinde kullanılabilir.

Güvenli ağ protokolleri ve mimarileri tasarımı

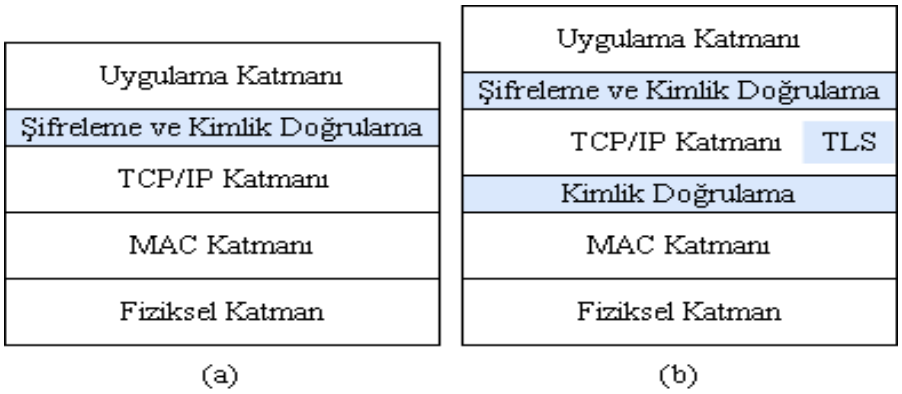
Akıllı şebekelerdeki olası güvenlik tehditleri ile başa çıkmak için güvenlik önlemleri ve stratejileri, ağ protokol ve mimarilerine entegre edilmelidir. Bu yüzden, geleneksel şebeke sistemlerine kıyasla, akıllı şebekeler, tüm ağda güvenli ve verimli iletişimi sağlamak için tam teşekküllü iletişim protokolleri ile donatılmalıdır.

Akıllı şebekelerde güvenli iletişim protokolleri oluşturmak için birçok çalışma yapılmaktadır. Bu çalışmalar genellikle IPSec ve TLS gibi mevcut protokol takımlarının geliştirilmesi ile gerçekleştirilmektedir (Shapsough ve ark., 2015). Ayrıca, güç iletişim protokollerinin güvenlik açısından geliştirilmesi ve standardizasyonun sağlanması literatürdeki ana konulardan biridir. Bu bölümde, güç sistemlerinde yaygın olarak kullanılan DNP3 ve IEC 61850 iletişim protokollerinin güvenlik açısından nasıl geliştirildiği sunulmaktadır.

DNP3 günümüzde hem alt-istasyon içi hem de alt-istasyonlar arasındaki iletişimlerde yaygın olarak kullanılmaktadır. DNP3 ilk tasarlandığında sadece temel iletişim gerekliliklerini karşılayacak şekilde tasarlanmıştı ve bu yüzden herhangi bir güvenlik mekanizması içermiyordu. DNP3 tabanlı çalışan mevcut güç sistemlerini, yeni iletişim protokolleri ile çalışabilecek şekilde tasarlamak çok pratik değildir. Dolayısıyla mevcut güç sistem cihazlarının güvenlik gereksinimlerine ayak uydurabilmelerini sağlamak için DNP3 gibi protokollerin güvenlik gereksinimlerini geliştirmek daha pratik bir çözümdür. DNP3 protokol kümesine güvenlik mekanizmaları eklemek için orijinal protokolü yapısal olarak değiştirmek, alt katmanlardaki konfigürasyonlara bakmaksızın sadece DNP3 de güvenlik gerekliliklerini karşılar. Ayrıca, hem DNP3 de yapısal değişikliklerin yapılması hem de güç cihazlarının dâhil olduğu iletişim altyapılarının yazılımsal ve donanımsal olarak güncelleştirilmesi gerekir. Bu durum uygulamada zorluklar içermektedir. Dolayısıyla, DNP3'ün bu sorununu çözmek için TCP/IP katmanı ile uygulama katmanının arasına bir güvenlik katmanı yerleştirilmiştir. Bu durum Şekil 5'de gösterildiği gibi DNP3 protokol kümesinde yapısal bir değişiklik yapılmasını gerektirmez ve böylece eski sistemlerin akıllı şebeke ile protokol çeviri cihazlar üzerinden iletişim kurması sağlanır.

Bu açıklamalar ışığında, DNP3 ve TCP/IP arasına bir güvenlik katmanının yerleştirilmesi ile eski aygıtların akıllı şebeke uygulamaları ile uyumlu hale getirilmesinin daha uygun olacağı sonucuna varılabilir. Bu güvenlik katmanının amacı, DNP3 protokolünün özellikle bütünlük ve gizlilik güvenlik gereksinimlerinin sağlamasına yardımcı olmaktır. Veriyi gönderen tarafta, güvenlik katmanı TCP/IP katmanına dağıtılacak olan DNP3 paketlerini yakalar, verileri şifreler, ardından şifreli paketleri TCP/IP katmanına gönderir. Alıcı tarafta ise, güvenlik katmanı TCP/IP katmanlarından gelen veri paketlerini çözer ve bunları uygulama katmanına (DNP3 katmanları) iletir. DNP3 paketlerinde bütünlük ve gizliliğin korunmasını sağlamak için hem simetrik hem de asimetrik algoritmalar kullanılabilir. Örneğin,

MAC tabanlı kimlik doğrulama, dağıtım otomasyon sistemleri için DNP3 tabanlı iletişimin güvenlik uzantısı olarak tasarlanır ve uygulanır.



Şekil 5. Geliştirilmiş DNP3 ve IEC 61850 ile IEC 62351

Alt-istasyonların iletişimi için bir standart olan IEC 61850 kendi güvenlik mekanizmalarına sahip değildir. IEC 61850'nin güvenliği, bir dizi iletişim protokolünde güvenliği sağlamak için önerilen bir standart olan IEC 62351'e dayanır. IEC 62351, IEC 61850 iletişimi için hem kimlik doğrulama hem de şifreleme mekanizmalarını tanımlar. Şekil 5b'de gösterildiği gibi, iki temel güvenlik katmanı içerir.

1. TC/IP katmanının üstündeki bir kimlik doğrulama ve şifreleme katmanı, TLS'yi mesajın gizliliğini ve aslına uygunluğunu sağlamak için simetrik şifreleme ve MAC'ler kullanmaya zorlar. Bu katman, alt istasyonlardaki TCP/IP'ye dayanan ve zaman açısından daha az kritik olan mesajlar için kullanılır.

2. MAC ve IP katmanları arasındaki bir kimlik doğrulama katmanı, IEC 61850'deki kritik zaman iletilerinin doğrulanması için kullanılır. Bu tür mesajların zamanında iletilebilmesini sağlamada IEC 62351, bu katman için veri şifreleme mekanizması tanımlamamaktadır. Bu nedenle IEC 61850'deki zaman kritik mesajlar yalnızca aslına uygunluklarını sağlamak için korunmaktadır.

Güvenlikli DNP3 ile karşılaştırıldığında, IEC 62351 ve IEC 61850'in, güç sistemlerindeki farklı mesaj türleri için iki farklı güvenlik katmanı kullanarak güvenlik ve zaman kritikliği arasındaki dengeyi sağlayan modern birer güç iletişim protokolü oldukları görülür. Akıllı şebeke uygulamalarındaki mesaj iletim süreçlerinde hem güvenlik hem de hizmet kalitesi gerekliliklerini sağlayacak daha kapsamlı güvenli katman mekanizmaları önerilebilir.

Enerji şebekesi iletişiminde uçtan-uca güvenliği sağlamak için güvenli DNP3 ve IEC 62351 ile IEC 61850 önerilmektedir (Shapsough ve ark., 2015). Bu tür uçtan-uca güvenlik protokollerinin yanı sıra, akıllı şebeke uygulamaları için güvenli veri toplama protokolleri de önerilmektedir. Çünkü aşağıdan yukarıya veri akış modeli (cihazdan merkeze); SCADA ağında cihaz izleme ve AMI ağında ölçüm okuma gibi işlemler için güç sistemlerinde yaygın olarak kullanılır. Böyle bir iletişim modelinde, ağ içinde veriyi işleyebilen veri toplama protokolleri, her bir düğümün merkeze kendi yolunu bulmaya çalıştığı uçtan-uca yönlendirme protokollerinden daha verimli olacaktır (Wang, 2017).

Güvenli veri toplama süreci, birçok bilgi işlem kaynağının kullanımını gerektirir. Bu durum daha fazla zaman gecikmesine sebep olur. Dolayısıyla mevcut çalışmalar, iletişim trafiğinde zaman açısından daha az kritik olan AMI için güvenli veri toplama protokollerine odaklanırlar. Mevcut yaklaşımlarla ilgili hala bazı sorunlar vardır. Örneğin, bir saldırgan aktif olarak kendisini veri toplama işlemine dâhil edebilir ve toplama sonuçlarını işlemek için kendi verilerini oluşturabilir. Bir veri toplama süreci saldırı nedeniyle bozulursa, veri toplama merkezi büyük miktarda bilgi kaybedebilir. Buna göre, akıllı

şebekelerde kullanılacak güvenli veri toplama protokollerinin, hem veri bütünlüğünü hem de veri gizliliğini sağlamaları ve ayrıca siber saldırılara karşı dirençli olmaları gerekir.

Genel olarak akıllı şebeke için güvenli ağ mimari tasarımı; ağ oluşturma, güvenilir işlemler ve şifreleme sistemleri gibi çok geniş kapsamlı konular içerir. Ayrıca, akıllı şebekeler karmaşık güvenlik gereksinimleri, politikaları, ağ ve varlık modelleri hakkında kapsamlı bir bakış açısı gerektirir.

SONUÇ

Bu çalışmada akıllı şebekelerin iletişim altyapısındaki siber güvenlik sorunları kapsamlı bir şekilde sunulmuştur. İletişim mimarisi ve temel güvenlik gereksinimleri detaylı incelenmiş, önemli güvenlik açıkları analiz edilmiş, akıllı şebeke saldırı önleme ve savunma yaklaşımları değerlendirilmiştir. Ayrıca, akıllı şebekelerde verimli ve güvenli veri iletimini sağlamak için güvenli ağ protokollerinin tasarımı sunulmuştur. Bu çalışmada elde edilen bulgular genel olarak değerlendirildiğinde, akıllı şebeke uygulamalarının geliştirilmesi büyük ölçüde güç sistemi iletişimine ve veri iletişim altyapılarına bağlıdır. Akıllı şebeke uygulamalarında, güç sağlayan kurumlar ve müşteriler hem kablolu hem de kablosuz iletişim ağlarını kullanırlar. Akıllı şebeke iletişim ağının heterojen cihazlara ve ağ mimarilerine sahip olması, ölçeklenebilirlik ve gömülü sistemlerinin farklı yapıları gibi özellikleri güçlü güvenlik yaklaşımlarının tüm ağ sisteminde uygulanmasını zorlaştırmaktadır. Bilgi iletişim teknolojilerinin entegrasyonu, güç sisteminin yeteneklerini artırırken, siber tehditlere karşı güvenlik açıkları da büyük ölçüde artmaktadır. Elektrik enerjisi sistemlerinde veri güvenliği özellikle dikkate alınması gereken bir konudur. Dolayısıyla, akıllı şebeke uygulamaları için siber güvenlik çözümleri hala geliştirilme aşamasındadır. Akıllı şebekelerin siber güvenliği konusu, hükümetlerin, endüstrinin ve akademinin ilgisini çeken önemli bir araştırma alanıdır. Bu bağlamda, akıllı şebekelerde siber güvenlik konusunda önemli çalışmalar yapılmakla birlikte, bu konu bilgi iletişim teknolojilerinin yapısı gereği bir sorun olarak varlığını devam ettirecektir. Etkin siber güvenlik çözümleri için, akıllı şebeke iletişim altyapıları özellikle farklı ağ uygulamalarını kapsayacak şekilde detaylıca tasarlanmış güvenlik yaklaşımları gerektirir.

KAYNAKLAR

Ahmed S, Gondal TM., Adil M, Malik SA, Qureshi R, 2019. A Survey on Communication Technologies in Smart Grid. IEEE PES GTD Grand International Conference and Exposition Asia, 7-12.

Baig ZA, Amoudi A, 2013. An Analysis of Smart Grid Attacks and Countermeasures. Journal of Communications, 8(8): 473-479.

Bedi G, Venayagamoorthy GK, Singh R, Brooks RR, Wang K, 2018. Review of Internet of Things (IoT) in Electric Power and Energy Systems. IEEE Internet of Things Journal, 5(2): 847-870.

Cintuglu MH, Mohammed OA, Akkaya K, Uluagac AS, 2017. A Survey on Smart Grid Cyber-Physical System Testbeds. IEEE Communications Surveys and Tutorials, 19(1): 446-464.

Colak I, Sagiroglu Ş, Fulli G, Yesilbudak M, Covrig CF, 2016. A survey on the critical issues in smart grid technologies. Renewable and Sustainable Energy Reviews, 54: 396-405.

Eder-Neuhauser P, Zseby T, Fabini J, Vormayr G, 2017. Cyber attack models for smart grid environments. Sustainable Energy Grids and Networks, 12: 10-29.

Gunduz MZ, Das R, 2018. Analysis of cyber-attacks on smart grid applications. International Conference on Artificial Intelligence and Data Processing, 1-5.

Gündüz MZ, Daş R, 2019. Analysis of cyber-attacks in IoT-based critical infrastructures. International Journal of Information Security Science, 8(4): 122-133.

Kaur R, Sangal AL, Kumar K, 2014. Modeling and simulation of DDoS attack using Omnet++. International Conference on Signal Processing and Integrated Networks, 220-225.

Khelifa B, Abla S, 2015. Security concerns in smart grids: Threats, vulnerabilities and countermeasures. International Renewable and Sustainable Energy Conference, 1-6.

Kimani K, Oduol V, Langat K, 2019. Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25: 36-49.

Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A, 2019. Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. IEEE Communications Surveys and Tutorials, 21(3): 2886 - 2927.

Lopez C, Sargolzaei A, Santana H, Huerta C, 2015. Smart Grid Cyber Security: An Overview of Threats and Countermeasures. Journal of Energy and Power Engineering, 9(7): 632-647.

Mendel J, 2017. Smart Grid Cyber Security Challenges: Overview and Classification. e-mentor, 1(68): 55-66.

Mrabet ZE, Kaabouch N, Ghazi HE, Ghazi HE, 2018. Cyber-security in smart grid: Survey and challenges. Computers and Electrical Engineering, 67: 469-482.

NIST, 2014. Framework and Roadmap for Smart Grid Interoperability Standards. https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-30. (Erişim Tarihi:15.12.2019)

Otuoze AO, Mustafa MW, Larik RM, 2018. Smart grids security challenges: Classification by sources of threats. Journal of Electrical Systems and Information Technology, 5(3): 468-483.

Pandey RK, Misra M, 2016. Cyber security threats-Smart grid infrastructure. National Power Systems Conference, 1-6.

Peng C, Sun H, Yang M, Wang Y, 2019. A Survey on Security Communication and Control for Smart Grids Under Malicious Cyber Attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(8): 1554-1570.

Pillitteri VY, Brewer TL, 2014. Guidelines for Smart Grid Cybersecurity. https://www.nist.gov/publications/guidelines-smart-grid-cybersecurity. (Erişim Tarihi:14.12.2019)

Radoglou-Grammatikis PI, Sarigiannidis PG, 2019. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. IEEE Access, 7, 46595-46620.

Rawat DB, Bajracharya C, 2015. Cyber security for smart grid systems: Status, challenges and perspectives. IEEE SoutheastCon Conference.

Rizzetti TA, Wessel P, Rodrigues AS, Silva BM, Milbradt R, Canha LN, 2015. Cyber security and communications network on SCADA systems in the context of Smart Grids. 50th International Universities Power Engineering Conference, 1-6.

Shapsough S, Qatan F, Aburukba R, Aloul F, Ali ARA, 2015. Smart grid cyber security: Challenges and solutions. International Conference on Smart Grid and Clean Energy Technologies, 170-175.

Tan S, De D, Song WZ, Yang J, Das SK, 2017. Survey of Security Advances in Smart Grid: A Data Driven Approach. IEEE Communications Surveys and Tutorials, 19(1), 397-422.

Tong W, Lu L, Li Z, Lin J, Jin X, 2016. A Survey on Intrusion Detection System for Advanced Metering Infrastructure. Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control, 33-37.

Usman A, Shami SH, 2013. Evolution of Communication Technologies for Smart Grid applications. Renewable and Sustainable Energy Reviews, 19: 191-199.

Wang W, Lu Z, 2013. Cyber security in the Smart Grid: Survey and challenges. Computer Networks, 57(5): 1344-1371.

Wang Z, 2017. An Identity-Based Data Aggregation Protocol for the Smart Grid. IEEE Transactions on Industrial Informatics, 13(5): 2428-2435.

Yi P, Zhu T, Zhang Q, Wu Y, Li J, 2014. A denial of service attack in advanced metering infrastructure network. IEEE International Conference on Communications, 1029-1034.