Bingöl Üniversitesi Teknik Bilimler Dergisi
Bingol University Journal of Technical Science
Cilt:2, Sayı: 2, Sayfa: 1-10, 2021 *Volume:2, Number: 2, Page: 1-10, 2021*
Derleme Makalesi *Review Article*

Akıllı Şebekeler: Siber Güvenlik Unsurları ile Veri İletimi

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

[1*]Bingöl Üniversitesi, Teknik Bilimler MYO, Bilgisayar Teknolojileri Bölümü, Bingöl, Türkiye.
ORCİD: 0000-0003-4278-7123, mzgunduz@bingol.edu.tr
[2]Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Elazığ, Türkiye.
ORCİD: 0000-0002-6113-4649, rdas@firat.edu.tr

(Alınış/Arrival: 16.12.2021, Kabul/Acceptance: 26.12.2021, Yayınlanma/Published: 31.12.2021)

Özet
Kritik altyapıların ana unsurunu oluşturan elektirik enerjisinin üretim, iletim ve dağıtımında etkinliği sağlamak açısından akıllı şebeke uygulamalarının kullanımı artmaktadır. Günümüz kritik altyapılarının uygulanmasındaki en büyük sorunlardan birisi de siber güvenliğine yönelik tehditler ve saldırılardır. Siber güvenlik, bilgi varlıklarında bulunan açıklıkların tehditler tarafından kullanılması sonucunda bilgi varlığının gizlilik, bütünlük veya erişilebilirliğinin zarar görmesini engelleme süreçlerinin tamamıdır. Akıllı şebekelerin kullanımının yaygınlaşması sürecindeki tehditlerin tanımlanması, sınıflandırılması ve bunlara karşı alınacak önlemlerin belirlenmesine yönelik çalışmalara ihtiyaç duyulmaktadır. Akıllı şebekelerin siber saldırılardan en az seviyede etkilenmesi için bilgi güvenliğinin temel unsurları olan gizlilik, erişilebilirlik ve bütünlük esaslarının diğer gereksinimlerle beraber en üst düzeyde sağlanması gerekmektedir. Bu çalışmada; akıllı şebekelerin tanımlanması, akıllı şebekelerde bilgi güvenliği ve siber güvenlik tehditleri ile ilgili değerlendirmeler yapılarak çözüm önerileri sunulmuştur.

Anahtar Kelimeler: Akıllı şebekeler, siber güvenlik, bilgi güvenliği, kritik altyapılar

Smart Grids: Data Transmission with Cyber Security Principles

Abstract
The use of smart grid applications is increasing in order to ensure efficiency in the generation, transmission and distribution of electrical energy, which is the main element of critical infrastructures. One of the biggest problems in the implementation of today's critical infrastructures is threats and attacks on cyber security. Cyber security is the whole of the processes of preventing damage to the confidentiality, integrity or availabity of information assets as a result of the exploitation of vulnerabilities in information assets by threats. Studies are needed to identify and classify threats in the process of spreading the use of smart grids and to determine the countermeasures to be taken against them. In order to be affected by cyber attacks at the lowest level, the principles of confidentiality, availability and integrity, which are the basic elements of information security, should be provided at the highest level along with other requirements in smart grid applications. In this study; evaluations about the definition of smart grid, information security in smart grid and cyber security threats were made and solution suggestions were presented.

Keywords: Smart grid, cyber security, information security, critical infrastructures

1. GİRİŞ

Enerji üretimi ve tüketimi arasındaki gerçek zamanlı dengeyi izlemeye ve kontrol etmeye olanak sağlayarak muhafaza eden akıllı şebekeler, nesnelerin internetinin en kapsamlı örneği olarak görülebilir [1]. Akıllı şebekelerin sahip olduğu iki yönlü veri ve elektrik iletimi sayesinde; iletim ve dağıtım şebekeleri de dâhil olmak üzere, enerji üretiminden nihai elektrik kullanıcısına kadar elektrik şebekesinin, bilgi iletişim teknolojileri sayesinde yüksek doğrulukla izlenmesi, yönetilmesi ve kontrol edilmesi etkin bir şekilde sağlanabilmektedir [2]. Mevcut elektrik şebekesinin, yalnızca güç iletimi için değil, aynı zamanda gelişmiş izleme ve kontrol uygulamalarıyla veri iletmek için de akıllı cihazları içeren siber-fiziksel bir sistem olarak yeniden yapılandırılması bir ihtiyaç haline gelmiştir. Bunun için, iki yönlü elektrik ve bilgi akışı kullanılarak elektrik şebekesinin geliştirilmesi; kendi kendini onarma, uyarlanabilir koruma ve kontrol, müşteri katılımı ve elektrikli araçlar gibi akıllı özelliklerin kullanımını sağlar.

Akıllı şebekeler, hizmet sağlayıcılar ve tüketiciler arasında gerçek zamanlı olarak büyük miktarda veri üreten, farklı türde düğümler, cihazlar, ağlar, sistemler ve çok sayıda uygulamadan oluşan modernleştirilmiş, karmaşık bir ortamdır. Bu ortamda üretilen veriler, yapıları, kısıtlamaları ve ihtiyaçları nedeniyle karmaşık çözümler, etkili yönetim ve analitik yaklaşımlar gerektirir. Bu veriler, nihayetinde bilgi alışverişi yoluyla şebeke güvenilirliğini, kullanılabilirliğini, güvenliğini ve verimliliğini artırmaya yardımcı olan bilgi ve iletişim teknolojilerine bağlıdır. Artan bu bağımlılık, ağ bileşenlerinin yanlış yapılandırılması, zayıf ağ tasarımı, yazılımdan kaynaklı güvenlik açıkları, güvenlik politikası zaafiyetleri gibi nedenlerden dolayı elektrik güç sistemleri için ek zorluklar ve tehditler de getirmektedir [3].

Akıllı şebeke uygulalamalarının başarılı bir şekilde uygulanması büyük ölçüde iletişim altyapısına bağlıdır. Bu karmaşık, heterojen ağdaki her bir bileşen diğer herhangi bir bileşen ile herhangi bir zamanda, verimli ama aynı zamanda güvenli bir şekilde iletişim kurabilmelidir. Bu iletişimin büyük ölçüde bilgi teknolojilerine bağımlı olması verinin güvenliği ve gizliliği ile ilgili endişeleri ortaya çıkarmaktadır. İletişim ve ağ sistemlerine özgü güvenlik açıkları, akıllı şebeke sisteminin çalışmasını olumsuz etkileyebilir. Eğer siber saldırganlar bu güvenlik açıklarından başarılı bir şekilde yararlanırsa, tüm altyapıya ciddi şekilde zarar vererek ekonominin çökmesi, kaos ortamının oluşması, insanların hayatlarını kaybetmesi gibi durumlara neden olabilirler. Bu nedenle siber güvenlik, bu kritik altyapı uygulamaları için birincil endişedir [4].

Kritik altyapı şebekelerinde meydana gelebilecek siber saldırılar, sabotaj veya ihmallere bağlı olarak gelişebilecek problemler ve kesintiler, tüm kritik altyapıları doğrudan etkileyerek kamu düzeninin sağlanmasında ve günlük yaşamda ciddi sorunlar ve hizmet kesintilerine sebep olacaktır. Akıllı şebekeler ile ülke ve birey bazında kaçak elektrik kullanımının minimum seviyelere düşürülmesi sağlanabilir. Bu bağlamda elektrik üretim, iletim ve dağıtım şebekelerinde olası arızaların tamiri, anormalliklerin tespiti, kaçak kullanım tespiti gibi faydaların sağlanması için şebekelerin uluslararası standartlara uygun olarak yönetilmesini sağlayan “akıllı şebekeler” haline getirilmesi gerekmektedir. Akıllı şebeke terimi, elektrik dağıtım sisteminin modernizasyonunu ifade eder. Bu durum, sistemin birbirine bağlı elemanlarının çalışmasını otomatik olarak optimize etmesine, kendisini izlemesine ve siber saldırılara karşı koruyabilmesi anlamına gelmektedir [5].

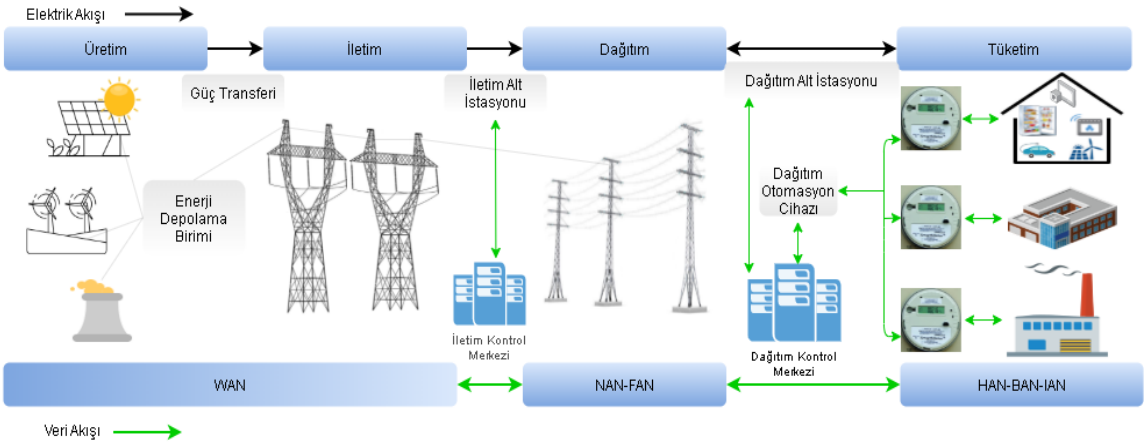
Akıllı şebekeler güç iletim hattı ve veri iletim hattı olarak iki ayrı iletim hattı içerirler. Akım, gerilim, güç ve frekans gibi parametreler ölçülerek sistemin izlenmesi daha otonom ve kolay hale gelir. Alternatif akım elektrik enerjisinin depo edilememesi, şebekenin elektrik enerjisi

talebini güvenle sağlayabilmesi, uzaktan sayaç okuma sistemlerinin etkin kullanılamaması gibi sebeplerden dolayı akıllı şebekelerin kullanımı insan hayatına daha pratik ve kalıcı çözümler sunmaktadır. Akıllı şebeke iletişim altyapısı, iki yönlü olacak şekilde şebeke varlıkları boyunca koordinasyon ve veri akışını sağlar. Enerji depolama teknolojileri, yenilenebilir enerji kaynakları, elektrikli araçlar gibi farklı teknolojilerin akıllı şebekelere entegre edilmesi iletişim altyapısınının karmaşık bir hal almasına neden olmaktadır.

Akıllı şebeke, elektrik enerjisi altyapısının modernizasyonunun bir sonucudur. Yenilenebilir enerji kaynaklarının entegrasyonuna izin vermenin yanı sıra, gelişmiş bilgi işlem ve iletişim teknolojilerinden de yararlanır. Daha iyi enerji yönetimi ve dağıtımı, daha iyi kontrol, verimlilik, şeffaflık ve güvenlik, maliyetlerin düşürülmesi, altyapının güvenilirliğinin, verimliliğinin ve şeffaflığının artırılması akıllı şebekelerin sağlayacağı önemli faydalardandır. Ayrıca, kullanıcıların elektrik tüketim karakteristiklerinin bilinmesiyle gerçekleştirilebilecek pratik uygulamalar ile elektrik faturalarının azaltılması, yenilenebilir enerji kaynak kullanımı, uzaktan okuma sistemlerinin gerçekleştirimi de akıllı şebeke uygulamalarının sağlayacağı faydalardan bazılarıdır. Tüm sistemde güvenliği sağlamak için üç önemli güvenlik ilkesi olan gizlilik, bütünlük ve erişilebilirliğin yerine getirilmesi gerekir [6]. Tüzel veya gerçek bir kişinin enerji kullanım bilgileri gerek ticari gerek kişisel açıdan önemlidir. Bu bakımdan çalışmada veri güvenliğinin temel unsurları olan gizlilik, erişilebilirlik ve bütünlüğün sağlanmasının gerekliliği ve önemi ortaya konmaya çalışılmıştır. Bir akıllı şebeke uygulamasının genel yapısı ve bileşenleri şekil 1'de gösterilmiştir.

Kritik bir altyapı olarak akıllı şebekelerin, izleme ve kontrol işlemleri standart IP tabanlı protokoller aracılığıyla internet altyapısı üzerinden sağlandığı için siber saldırılara maruz kalması olasıdır. Bir saldırgan, gerçek zamanlı enerji üretim ve tüketim dengesini bozarak, cihazlar ile elektrik üretim ve dağıtım şirketleri tarafından oluşturulan verilerin değiştirilmesiyle elektrik iletimini ve işlerliğini sekteye uğratarak sisteme telafi edilemeyecek zararlar verebilir. Dolayısıyla, veri güvenliğinin üç temel bileşeni olan gizlilik, erişilebilirlik ve bütünlük, akıllı şebeke uygulamalarında siber saldırılara karşı sağlanması gereken ilkelerdir ve sistem iletişim ağı bu ilkelere göre oluşturulmalıdır. Kullanıcı ihtiyaçlarına göre kesintisiz olarak güç kaynaklarının erişilebilirliğinin sağlanması, iletilen verilerin bütünlüğünün sağlanması ve kullanıcı verilerinin gizliliğinin sağlanması temel güvenlik bileşenlerinin akıllı şebekelerdeki genel çerçevesini göstermektedir [7].

Bu çalışmada; elektrik enerjisinin etkin kullanımını sağlayan akıllı şebekelerde bilgi güvenliğine yönelik tehditler ele alınmıştır. Tehditler incelenerek değerlendirmeler yapılmış ve çözüm önerileri sunulmuştur. Bu amaçla çalışmanın ikinci bölümünde akıllı şebekelerde siber güvenlik kavramı detaylı olarak incelenmiştir. Üçüncü bölümde ise bu çalışmaya konu olan akıllı şebekelerdeki muhtemel tehditler sıralanmaya çalışılmıştır. Dördüncü bölümde olası tehditlere karşı alınabilecek temel güvenlik önlemleri güvenli veri iletimi bakış açısı ile belirlenmeye çalışılmıştır. Sonuç bölümünde ise akıllı şebekelerde veri güvenliğine yönelik olası tehditler ve önlemler konusunda değerlendirmeler yapılmış olup sonraki çalışmalar için tavsiyelerde bulunulmuştur.

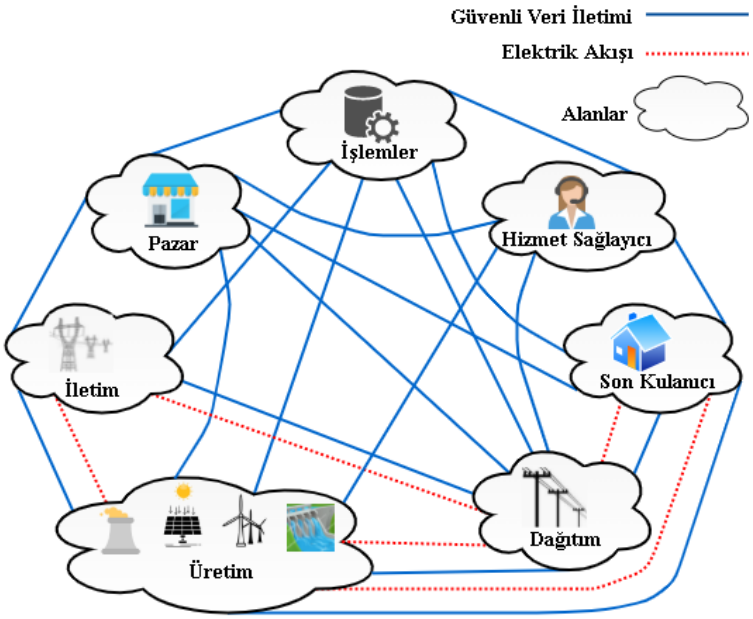


Şekil 1. Akıllı şebeke genel yapısı ve bileşenleri

2. AKILLI ŞEBEKELERDE SİBER GÜVENLİK

Akıllı şebekelerin üretmiş olduğu her tür verinin insanoğlunun hayatını kolaylaştırmada üretim ve tüketim açısından önemli rolü vardır [8]. Bu verilerin toplanmasında ve iletiminde meydana gelebilecek saldırıları engellemek amacıyla bilgi güvenliği tedbirlerinin alınması gerekmektedir. Bilgi güvenliği bilginin bütünlüğünün, gizliliğinin ve erişilebilirliğinin sağlanmasıdır. Bu ilkelerinin bir kısmı teknik olarak sağlanırken bir kısmı ise bilgi güvenliği bilinci oluşturularak gerçekleştirilebilir. Bilgi güvenliği açısından varlık, varlıkta bulunan açıklık ve bu açıklığı kullanacak tehdit bileşenleri çok önemlidir. Bu üç faktörün bir araya gelmesi bilginin gizliliğinin, bütünlüğünün veya erişilebilirliğinin zarar görmesine sebep olabilmektedir. Bilgilerin, bir kısmı cinsiyet, posta kutusu no, doğum tarihi, adres vb. gibi hassas olmayan veriler iken bir kısmı da vatandaşlık no, kredi kartı no, anne kızlık soyadı gibi hassas verilerden oluşmaktadır. Hassas verilerin ele geçirilmesi saldırgana doğrudan fayda sağlayabilir iken hassas olmayan veriler ise dolaylı olarak fayda sağlayabilir [9].

Akıllı şebeke uygulamalarında yer alacak tarafların yedi alanda toplanabileceği belirtilmektedir [6]. Hemen hepsi birbiriyle iletişim halinde olan bu yedi alan kavramsal model olarak şekil 2'de gösterilmiştir. Bu yedi alan arasında yer alan ara yüzlerin her birinde bilginin gizliliği, bütünlüğü ve erişilebilirliği açısından farklı güvenlik gereksinimleri uygulanmalıdır. Bu bağlamda her bir ara yüzde alınacak güvenlik önlemlerinin belirlenmesi gereklidir.



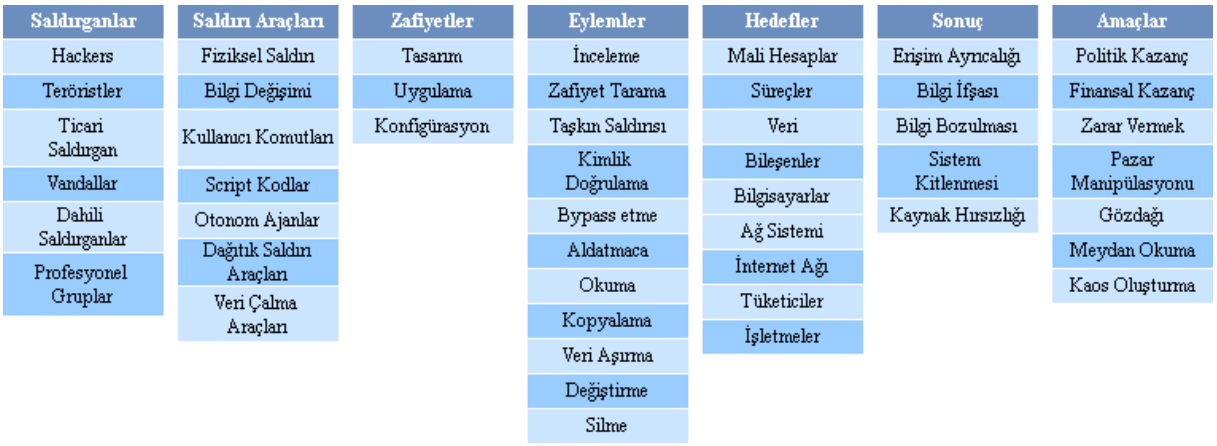
Şekil 2. Akıllı şebekelerin kavramsal modeli

Bir akıllı şebeke uygulaması birbirine bağlı çok sayıdaki cihazdan oluşur. Akıllı şebekede iletilen iki tür veri bulunmaktadır. Bunlar; kullanıcı bilgileri ve komut içeren operasyonel verilerdir. İlk tür verilerin ihlali genellikle mahremiyet ihlaline girer iken, ikincisi ise sistemin çalışmasının topyekün zarar görmesine sebep olabilmektedir. Operasyonel veriler ise gerçek zamanlı akım ve voltaj değerleri, trafo kademe değiştiricileri, kapasitörler, trafo besleyicilerinin akım yükleri, arıza konumları, rölelerin durumu, devre kesicilerin durumu olabilir. Operasyonel veriler, akıllı şebeke sistemlerini, güç kesintisine neden olabilecek herhangi bir güvenlik açığından ve saldırıdan korumak için yüksek düzeyde güvenlik gerektirirler. Akıllı şebekelerin güvenliği, ağırlıklı olarak iletişim kanallarının güvenliğinin sağlanması olarak değerlendirilebilir [2]. Bir akıllı şebeke sisteminde tehditler; fiziksel, çevresel ve siber tehditler olmak üzere üç kategoriye ayrılabilir. Bu bağlamda, güç ve enerji sistemlerinde meydana gelebilecek saldırı bileşenleri şekil 3'deki gibi özetlenebilir. ABD'de bulunan Ulusal Standart ve Teknoloji Enstitüsü (NIST) tarafından listelenen akıllı şebeke üst düzey güvenlik gereksinimleri, iletişim ağını kullanan herhangi bir sistemden farklı değildir. Gizlilik, özel bilgilere yetkisiz erişimi engeller. Bütünlük, bilginin doğruluğunu garanti eder. Erişilebilirlik, hizmet garantisi sağlar. Bununla birlikte, geleneksel iletişim ağlarından farklı olarak, akıllı şebekelerde güvenlik gereksinimlerinin öncelik sıralaması erişilebilirlik, bütünlük ve gizlilik şeklindedir. Akıllı şebeke uygulamalarında birçok güvenlik gereksinimi karşılanmalıdır. Bunlar şu şekilde özetlenebilir [10]:

Bütünlük (Integrity): Bilginin ve sistemin yasadışı kullanıcılar tarafından izinsiz bir şekilde değiştirilmesinin önlenmesidir. İletilen verilerin yetkisiz bir şekilde değiştirilmemesini sağlamaktır. Bütünlük, yetkisiz değişime karşı verinin korunması demektir. Örneğin, akıllı sayaçlar kaynak doğrulaması ve yazılım güncellemesinin bütünlüğünü sağlamalıdır. Akıllı sayaçtaki verinin dağıtım şirketine aktarılması sırasında verilerin bütünlüğünü bozabilecek saldırılar olabilir. Aktarılacak veriler faturalandırmada kullanılan elektrik tüketim verileri olduğundan bütünlüğünün korunması gerekmektedir. Aksi halde bütünlüğü korunamayan bu veriler değiştirilerek şirket ya da son kullanıcı aleyhine maddi zararların doğmasına neden olacaktır. Veri akışının, kontrol mesajlarının veya sensör değerlerinin kötü niyetle şekillendirilmesi veya tekrarlanması sistemin saldırıya uğradığı anlamına gelir ve bütünlük

kaybı olarak adlandırılır. İnkar edememe ve güvenilirlik veri bütünüğünün önemli bileşenleridir. Bütünlük saldırılarının hedefi; fatura bilgisi, müşteri hesap bakiyesi gibi müşterinin bilgileri veya cihazların çalışma durumu, voltaj okumaları gibi ağ operasyon bilgileridir. Diğer bir deyişle, bu tür saldırılar akıllı şebekedeki kritik veri alışverişini bozmak için akıllı şebeke iletişim sistemindeki orijinal bilgileri kasıtlı olarak değiştirmeye çalışırlar [4].

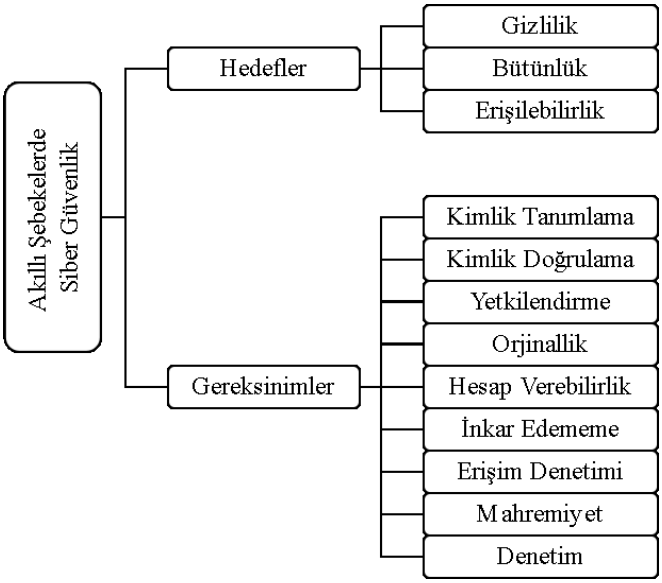
Erişilebilirlik (Availability): Yetkili olan kullanıcıların sisteme erişmesinin sağlanmasıdır. Erişilebilirlik bilgi ve hizmetlerin sürekli ve güvenilir bir şekilde erişimini ve kullanımını içerir. Akıllı şebeke uygulamalarında zamanında bilgiye erişim sağlanmalıdır. Erişilebilirlik, yetkisiz kişilerin veya sistemlerin iletişim ve güç altyapısına da erişememesini garanti eder. Akıllı şebeke uygulamalarında kontrol sistemleri, güvenlik sistemleri, iş istasyonları, üretim sistemleri ve bu sistemlerin aralarında ya da dış dünya ile haberleşmesinde kullanılan iletişim sistemleri gibi tüm bilgi teknolojisi unsurlarının devamlı aktif olması erişilebilirlik ile ifade edilir [12]. Sistem erişilebilirliğini hedefleyen saldırılar, kaynakların kullanılamaması için veri transferini bozmayı hedefleyen hizmet reddi saldırıları (DoS) olarak kabul edilir. DoS saldırıları akıllı şebekelerde bilgileri geciktirebilir, engelleyebilir veya bozabilir. Bu durum güç veya bilgi alışverişi sağlanamamasına neden olur. Erişilebilirliğin kaybolmasında, yetkilendirilmiş bireylere erişim engelleneceğinden, güç dağıtımı etkilenecektir. İletişimin kesilmesi, kontrol mesajlarının veya veri akışının kesilmesi, sistemin kontrolsüz kalması anlamına gelir [13].



Şekil 3. Enerji sistemlerinde saldırı bileşenleri

Akıllı şebeke uygulamalarında bu üç temel güvenlik prensibinin yanısıra olması gereken diğer bazı güvenlik gereksinimleri de vardır. Bu gereksinimler şu şekildedir:
Kullanıcı Mahremiyeti (User's Privacy): Son kullanıcı ile ilgili verilerin, kullanıcının resmi bir onayı olmaksızın farklı amaçlar için kullanılamayacağını, farklı kişilerce elde edilemeyeceğini ve sadece belirlenen amaçlar için kullanılacağının garanti edilmesidir. Örneğin, faturalandırma amacıyla kullanılan enerji tüketimi verileri başka amaçlar için kullanılamaz. Akıllı şebekelerde enerji kullanım verileri incelendiğinde, son kullanıcıya ait çalışma saati, uyku saati, günlük hayata dair planlamaları ile ilgili tahminler yürütebilecek bilgiye sahip olunabilmektedir. Bu bilgilerden yapılacak çıkarımlar, saldırganların ataklarını bu bilgilere göre planlama riskini içerir. Dolayısıyla, akıllı cihazlardan alınan bu tür bilgiler ticari ve stratejik açıdan önemli olabilir. Buradan da anlaşılabileceği gibi enerji kullanım verileri faturalandırmadan daha fazlasıdır. Dolayısıyla, bu verilerin iletiminde mahremiyet öne çıkmaktadır. Yetkilendirme (Authorization): Kimliği doğrulanmış bir nesnenin veya kişinin, bazı kaynaklar üzerinde belli işlemleri gerçekleştirmek için önceden belirlenmiş haklara sahip olduğunun garantilenmesidir. Örneğin, akıllı sayaç üzerinde doğrudan elle yapılandırma yapması gereken görevli, önceden

belirlenen yetki ve erişim kontrol haklarına sahip olmalıdır. Kimlik Doğrulama (Authentication): Akıllı şebekedeki herhangi bir iletişim aygıtının kimliğini belirleme işlemidir. Örneğin, enerji sağlayıcı, ilgili kullanıcıyı faturalandırmak için her bir akıllı sayacın kimliğini doğrulamalıdır. Kullanıcı ve cihaz kimlik doğrulamasındaki bir zafiyet, saldırganların özel bilgilere erişmesine veya cihazların akıllı şebeke kaynaklarına yetkisiz erişimine yol açabilir. Kimlik doğrulamayı sağlayan mekanizma genellikle bütünlük ilkesini de sağlar. Akıllı şebekelerde bu iki ilkenin sağlanması ortadaki adam, kimliğine bürünme, paket manipülasyonu gibi yaygın saldırılara kaşı koruma sağlar. Bu koruma özet fonksiyonlar, anahtar özetleme ve dijital imza gibi siber güvenlik araçları ile sağlanabilir. Kimlik doğrulama protokolleri ile ele alınması gereken saldırılardan biri de saldırganların mesajları yakaladığı ve daha sonra cihazlara yeniden oynattığı replay attack saldırısıdır. İnkâr edememe (Non-Repudiation): Bir sistem veya kullanıcı tarafından gerçekleştirilen belirli bir eylemin daha sonra reddedilemeyeceğini garanti etmektir. Değerli kaynaklar ve bilgiler söz konusu olduğunda inkâr edememe daha önemli bir hale gelir.
Orjinallik (Authenticity), denetim (auditing), hesap verebilirlik (accountability), kimlik tanımlama (identification), erişim denetimi (access control) diğer siber güvenlik gerekliliklerdir. Şekil 4, akıllı şebeke uygulamalarında üst düzey siber güvenlik hedeflerini ve özel güvenlik gereksinimlerini göstermektedir.



Şekil 4. Üst düzey siber güvenlik hedefleri ve özel güvenlik gereksinimleri

3. AKILLI ŞEBEKELERDE SİBER SALDIRILAR ve TEHDİTLER

Önceki bölümde belirtildiği gibi gizlilik, bütünlük, kimlik doğrulama ve yetkilendirme gerekliliklerinin sağlanması için iki yönlü güvenli iletişim kanalı gereklidir. Bu iletişim kanalı çeşitli siber saldırılara maruz kalabilir. Akıllı şebeke güvenliğini tehlikeye atabilecek pasif ve aktif olarak gerçekleşen iki tip saldırı vardır [8]. Pasif saldırının amacı, sistem yapılandırmasını, mimarisini ve normal çalışma davranışını öğrenmek için iletilen verilerin elde edilmesidir. Veriler üzerinde herhangi bir değişiklik yapılmadığından dolayı bu tür saldırıların tespit edilmesi zordur ve bu nedenle saldırının, tespit edilmesinden ziyade önlenmesi üzerine odaklanılmalıdır. Aktif saldırılar ise iletilen veriler üzerinde değişiklik yaparak ya da manipüle edilmiş yanlış veriler ekleyerek sistemin çalışmasını etkileyecek şekilde planlanırlar.

Bilinçli saldırılar, bilgisayar korsanları, organize suç üyeleri, siber suçlular, teröristler, yönetim karşıtları, vandallar ve özellikle güvenlik alanında kapsamlı bilgi sahibi olan şirket çalışanları ve hatta akıllı sayaç sahibi olan son kullanıcıların enerji altyapısına enerji hırsızlığı, dolandırıcılık, sahtekârlık, sabotaj, vandalizm gibi farklı amaçlar için yaptıkları saldırılardır. Bilinçsiz saldırılar, genellikle sistem kullanıcılarının siber güvenlik farkındalıklarının düşük olması nedeni ile ortaya çıkan saldırılardır. Akıllı şebeke saldırılarının üç ana nedeni, manipülasyon, sabotaj ve casusluktur [14].

3.1. Akıllı Şebekelerde Siber Saldırganlar

Siber suç, hacktivizm, siber casusluk ve siber savaş dâhil olmak üzere şebekeye yapılan saldırılara atfedilebilecek birçok sebep vardır. Akıllı şebeke gibi kritik altyapılara saldıran siber saldırganların motivasyonları ekonomik nedenlerden, hoşnutsuz çalışanlardan, sanayi casusluğundan terörizme kadar uzanabilir. Bazı tüketiciler elektrik faturalarını azaltmak amacıyla belli sistem elemanlarına saldırılar düzenleyebilirler. Böyle bir saldırganın en yakınındaki gelişmiş ölçüm altyapısı (AMI) sistemine bağlanması yeterli olacaktır. Bazı son kullanıcılar üretim ve tüketim bilgilerini değiştirerek ya da faturalandırma sistemine erişerek kendilerine maddi fayda sağlamayı amaçlayabilirler.

Akıllı şebekelerdeki zafiyetler, saldırganlar veya kullanıcılar tarafından bilinçli yada bilinçsiz olarak farklı amaçlar doğrultusunda sisteme farklı seviyelerde zarar vermek için kullanılabilirler. Saldırganlar; script kiddies, profesyonel saldırganlar, terörist saldırganlar, çalışanlar, rakip firmalar, ya da müşterilerin kendileri olarak saldırı amaçlarına göre sınıflandırılmaktadırlar. Akıllı şebekelerdeki bu saldırganlar şu şekilde tanımlanabilirler [7], [15], [16] :

Zararsız Saldırganlar: Sistemin güvenliğini ve işleyişini bir bulmaca olarak gören, niyetleri saldırı olmayan saldırganlardırlar. Bu saldırganlar normal olarak entellektüel meydan okuma ve merakla hareket ederler. Hobbyist, script kiddies bu saldırganlara örnektir. Tüketiciler: Diğer tüketicilere karşı intikam ve kin ile hareket ederek, güç sistemlerinin kesilmesi için hareket eden saldırganlardır. Son tüketiciler kendilerine fayda sağlayacak şekilde kendi akıllı sayaç veya ağ geçidi cihazlarına da siber saldırı gerçekleştirebilirler. Teröristler: Terör eylem nedenlerini daha etkin şekilde duyurabilmeyi amaçlayan yasadışı saldırganlardır. Çalışanlar: Kasıtlı ya da kasıtsız olarak saldırıda bulunan çalışanlardır. Çalıştığı ortama kırgın bir çalışan dâhili saldırgan olarak değerlendirilir. Rakip Firmalar: Finansal kazançlar için rakip firmaların birbirlerine siber saldırıları da bulunabilirler. Ayrıca, bir rakip, kişisel bilgileri toplayarak tüketicinin mahremiyetini herkesin erişebileceği şekilde açığa çıkarabilir. Kurumsal veriler, rakip servis sağlayıcıları arasındaki iç rekabet için veritabanından çalınabilir.

Tanımlanmış olan bu saldırgan tiplerinin dışında tanımlanmamış farklı saldırı motivasyonlarına sahip saldırganların olması da mümkündür. Bu saldırganlar, sistem bileşenleri bazında, protokol bazında ve topoloji bazında olmak üzere üç ana kategoride sınıflandırılan çok çeşitli saldırılara neden olabilir. Bileşen bazında saldırılar, Uzak Terminal Birimi (RTU) içeren saha bileşenlerini hedefler. RTU'lar geleneksel olarak mühendisler tarafından akıllı şebeke cihazlarını uzaktan yapılandırmak ve sorun gidermek için kullanılır. Bu uzaktan erişim özelliği, kötü niyetli kullanıcıların cihazların kontrolünü ele geçirmesi ve cihazların kapatılması gibi durumlara olanak tanıyan bir saldırıya zemin hazırlayabilir. Protokol bazlı saldırılar, tersine mühendislik gibi yöntemler kullanarak iletişim protokolünün kendisini hedef alır. Topoloji bazlı saldırılar, genellikle operatörlerin güç sisteminin anlık durumunu tam olarak

değerlendirmesini engelleyen ve yanlış karar vermelerine neden olan bir DoS saldırıları ile ağ topolojisinin hedef alınmasıdır.

3.2. Saldırı Seviyeleri

Zayıf bir siber altyapı, saldırganın zayıf bağlantılar yoluyla güvenliği ihlal etmesine sebep olabilir. Böylece kontrol yazılımına erişim kazanır, sistemin üretim ve tüketim hesaplamalarında istikrarsızlık oluşturmak için fatura bilgilerini ve yük koşullarını değiştirir. Akıllı şebekeler, istihbarat, enerji, politika ve sosyal kaygıların kesişimidir. Bu, saldırganların ve niyetlerin çeşitliliğini açıklar. Sistem bileşenlerine erişme ayrıcalığına sahip olan hoşnutsuz bir çalışan, yazılım algoritmalarını ya da cihazların ayarlarını kendi menfaatlerine göre değiştirebilir. Saldırgan, sistem kullanıcı adları ve parolalarına erişmek için tuş kaydedici yazılımları kullanabilir. Bu tür eylemlerin tespit edilmesi zor olmakla kalmayıp aynı zamanda önlenmesi de zor olabilir.

Güvenilen alanın hem içinde hem de dışında kullanılan dizüstü bilgisayarlar ve USB bellek gibi cihazlar truva atı gibi kötü amaçlı yazılımların bulaşmasına sebep olabilir ve daha sonra sistem içinde kullanıldığında sistemin ele geçirilmesine yardımcı olabilirler. Cihazlar uzaktan güncellenmek istendiğinde İnternet ortamından alınacak olan güncelleme dosyalarındaki donanımın kontrol ayarları yada yazılımın kaynak kodu değiştirilerek cihazlar manipule edilebilir [17].

Akıllı şebekelerde veriler derecelendirilirse bile, en düşük öneme sahip veriler bile insanların çalışma saatleri, uyku saatleri, günlük planlamaları ile ilgili tahminlerin yapılabilmesine olanak sağlayabilir. Veri güvenliği açısından risklerin tanımlanarak azaltılmasına yönelik çalışmaların yapılması gerekmektedir. Bunun için siber saldırıların seviyelerinin risk tanımlaması açısından yüksek-orta-düşük olarak belirlenmesi olası saldırılara karşı proaktif önlemlerin alınmasını sağlayacaktır.

3.3. Güç Sistemlerine Yapılan Geçmiş Saldırılar

Dünya genelinde güç sistemlerine karşı gerçekleştirilmiş siber saldırılar mevcuttur. 1999 yılında Brezilya'nın %70 ini etkileyen ve beş saatten fazla süren bir elektrik kesintisi yaşandı. 2003 yılında ise Kanada ve ABD'nin bir bölümünde ışıklar söndü. Elektrik kesintisi sadece ışıkların sönmesine neden olmadı, havaalanları, metrolar, trenler ve tüneller de kapatıldı. Elektrik gücünün kesilmesi, otomatik kapıların, asansörlerin ve tüm içme suyu hizmetlerinin çalışmasını askıya aldı. Hastaneler yedek jeneratörler tarafından üretilen sınırlı güçle çalıştı. Cep telefonu kuleleri, yazar kasalar ve ATM cihazları hizmet dışı kaldı. 2012 de Hindistan'da 600 milyondan fazla insanı elektriksiz bırakan ve yaklaşık üç saat süren bir elektrik kesintisi yaşandı. 2015 de Türkiye'de iki günden fazla süren ve tüm ülkeyi etkileyen bir elektrik kesintisi yaşandı. Bu saldırılar bağlamında özetlemek gerekirse, sistemsel ve yazılımsal hatalar ve zafiyetler, bu elektrik kesintilerinin arkasındaki ana nedenlerdir, bu nedenle elektrik şebekesinin siber güvenliğinin sağlanması sistemin erişilebilirliği ve güvenilirliği açısından bir zorunluluktur. Özellikle 2011 yılında İran'da nükleer santrale gerçekleştirilen Stuxnet siber saldırısı kritik altyapılarda siber güvenliğin önemini net bir şekilde ortaya koymaktadır [18]. Stuxnet kötü amaçlı yazılımı, şimdiye kadarki en zarar verici siber silahtır. Saldırı vektörleri, şebekenin fiziksel bileşenlerinden iletilen veriye kadar farklı elemanlarını hedef alıyordu. Stuxnet, diğer bileşenlerin yanı sıra binden fazla nükleer santrifüjün yok olmasına neden olabilecek şekilde belirli merkezi denetim ve veri toplama (SCADA) sistemlerini hedef

almıştır. Kötü amaçlı ve karmaşık yapıda tasarlanan bu yazılımın gizliliği ve başarısı, bu tür sistemlerin güvenliği ile ilgili birçok soruyu gündeme getirmiştir.

4. GÜVENLİ VERİ İLETİMİ

Akıllı şebeke iletişim altyapıları, klasik İnternet iletişiminden çeşitli yönlerden farklılık gösterir. Özellikle mimarileri, kullanılan teknoloji ve hizmet kalitelsi (QoS) bakımından farklılıklar vardır. Akıllı şebekelere has güvenlik çözümlerine duyulan ihtiyaç esastır. Akıllı şebeke iletişimi esas olarak makineden-makineye (M2M) iletişimi esas alır, bu da onu geleneksel İnternet trafiğinden daha öngörülebilir kılar. Öngörülebilirlik, anormallik tespitini basitleştirir, ancak kullanımdaki gözlem noktalarına ve protokollere bağlı olarak zorluklar devam eder. Ayrıca, akıllı şebeke ortamları genellikle homojen yapıları tercih eder. Hizmet sağlayıcılar, aygıtların, yazılımların, protokollerin ve ağ topolojilerinin monokültürüyle sonuçlanan bileşenleri bir veya birkaç satıcıdan satın alır. Bu durum, kötü amaçlı yazılımların yayılması için ideal bir ortam sağlayan aynı güvenlik açıklarına sahip cihaz popülasyonlarına yol açabilir. Ayrıca, güvenlik ve gizlilik endişeleri çelişen hedeflerin oluşmasına yol açabilir. Örneğin, enerji tüketimi hakkında veri toplayan ve kullanıcı davranışlarını izleyen akıllı sayaçlar da veri mahremiyeti endişelerini artırmaktadır. Bu veriler, İnternetteki her kullanıcı hakkında toplanan kişisel bilgilerle birleştirilebilir. Ayrıca, birçok akıllı sayaç türü uzaktan bağlantı kesme özelliğine sahiptir. Bu tür özellikler aynı anda birçok hanenin bağlantısını kesmek için kötüye kullanılabileceğinden güvenlik endişelerini artırmaktadır. Akıllı şebeke iletişimini İnternet iletişiminden ayıran özellikleri aşağıdaki gibi belirleyebiliriz:

- Cihaz seçiminde homojenlik (monokültürler).
- Güvenilmeyen taraflarca saha cihazlarına fiziksel erişim ihtimali.
- İnsandan-insana veya insandan-makineye iletişim yerine M2M iletişimin kullanılması.
- Akıllı sayaç, ağ geçiti, sensör, aktüatör gibi farklı cihaz tiplerinde ağ gereksinimi farklılıkları.
- Uzaktan izleme, bakım ve güncelleme ihtiyacı ve desteği.
- Sahadaki kurulumlar için cihaz kullanım ömrünün uzun olması.

Belirtilen özelliklerin etkin kullanımı ile geleneksel güç ağlarını ve bilgi iletişim teknolojilerini birleştirmek, akıllı şebeke konseptinin daha güvenilir olmasını sağlar.

4.1. Akıllı Şebekeler İçin İletişim Teknolojileri

Akıllı şebeke uygulamalarında verinin algılanması, toplanması, iletilmesi, değerlendirilmesi ve depolanması işlemleri birer zorunluluktur. Çok sayıda duyarga donanımlı cihazlardan alınan veriler veri toplama merkezlerinde toplandıktan sonra işlenmek ve değerlendirilmek üzere kontrol merkezlerine aktarılır. Bu bağlamda, akıllı şebekelerdeki iletişim ağları bu veri yükünü karşılayabilecek şekilde tasarlanmalıdır [3]. Elektrik şebekelerinde kullanılan iletişim ağlarının dört farklı seviyeden oluştuğu düşünülebilir. Bunlar:

İlk seviye (çekirdek iletişim) ağları: Bu ağlar çeşitli şalt tesisleri ile şebeke kontrol merkezleri arasındaki veri akışı bağlantısını sağlayan geniş alan ağlarıdır (WAN). Veri akışını sağlamak için yüksek kapasiteli bant genişliğine sahip olmaları gerekmektedir. Bu yüzden genel olarak fiber optik kablolarla tesis edilirler. Ethernet, SONET/SDH, IP/MPLS veya uydu teknolojilerinden yararlanılarak oluşturulurlar.

İkinci seviye iletişim ağları: Uzaktan sayaç okuma için trafo merkezlerine yerleştirilen veri toplama üniteleri ile kontrol merkezleri arasındaki veri iletişimini sağlayan ağlardır. Geniş bant iletişim teknolojileri gerektiren bu ağların güvenilir ve düşük maliyetli olmaları gerekmektedir. 3G, Wimax, LTE, BPL gibi teknolojilerden yararlanılır..

Üçüncü seviye (müşteri iletişim) ağları: Trafo merkezlerinde bulunan veri toplama üniteleri ile akıllı sayaçlar arasında veri iletişimini sağlayan ağlardır. Kablolu ve kablosuz birçok teknoloji bu ağlarda kullanılır. 3G, Wimax, GPS/GPRS, BPL/PLC ve LTE teknolojilerinden yaralanılabilir. WiFi, semt alan ağları (NAN) ve saha alan ağları (FAN) alt ağlar olarak kullanılabilir.

Uç seviye (ev iletişim) ağları: Akıllı şebeke iletişim ağlarının son halkasını oluştururlar. Bu ağlar, ev alan ağları (HAN) olarak adlandırılırlar. Zigbee, WiFi ile PLC standartları üzerine inşa edilen teknolojilerdir. HAN teknolojileri ile oluşturulmuş enerji yönetim sistemi, akıllı ev/bina, akıllı ev aletleri, elektrikli araç vb. uygulamaların yönetilmesine olanak sağlarlar.

Akıllı elektrik şebekeleri açısından bakıldığında ön plana çıkan fiziksel veri iletişim ortamları, fiber, PLC ve radyo kanallarıdır. Fiber optik, elektromagnetik girişim yaratmaması, gürültüye maruz kalmaması ve ayrıca uzun mesafelere yüksek bant genişliğinde iletişim sağlaması nedeniyle ilk seçenektir. Buna rağmen radyo, mikrodalga iletişim sistemleri ilk yatırım ile işletme maliyetlerinin düşük olması ve hızlı tesis edilmeleri nedeniyle iyi bir alternatif oluştururlar.

4.2. Veri İletimi Sorunları

Varlıkların etkileşimi altında ortaya çıkabilecek olası veri iletim güvenlik sorunlarını tanımladıktan sonra, bu bölümde akıllı şebeke varlıklarını etkileyebilecek olası güvenlik sorunları tanımlanacaktır. Aşağıda, akıllı şebeke varlıklarının saldırı hedefi haline gelebileceği bazı senaryolar altında potansiyel tehditleri ve olası sonuçları tartışılmaktadır.

Senaryo1: Servis sunucularından veri çalmayı amaçlayan saldırılar.

Senaryo2: Servis sunucularının kontrolünü ele geçirmeyi amaçlayan saldırılar.

Senaryo3: Servis sunucularını kapatmayı amaçlayan saldırılar.

Yukarıda verilen üç senaryoda da saldırgan, sistem hakkında değerli bilgiler elde etmeyi, sisteme erişmeyi, sistemden veri çalmayı, kontrolü ele geçirmeyi veya devre dışı bırakmayı hedefler. Bunun için akıllı şebekedeki ana servis sunucularını hedef alır. Sistem hakkında değerli bilgiler toplamak, saldırganın sisteme erişirken hedefli bir saldırı planlamasını sağlar, saldırgana sistemle istediği şekilde etkileşime girme fırsatı verir. Sistem hakkında değerli bilgiler toplamanın bir yolu, sistem hakkında halka açık bilgilere İnternet üzerinden erişmek olabilir [19]. Bu tür bilgiler, özellikle sistemin zayıflığını hedef alan bir saldırı planlamasına yardımcı olmak için saldırgana kolaylık sağlar. Sistem hakkında bilgi toplamanın alternatif yolları, aktif bilgisayarlar, kullandıkları ağ hizmetleri, çalıştırdıkları işletim sistemleri vb. hakkında bilgileri ortaya çıkarmak için Nmap gibi ücretsiz olarak kullanılabilen yazılımları kullanarak bağlantı noktası tarama veya ping taramalarını içerebilir. Ayrıca, Nessus gibi güvenlik açığı tarayıcıları saldırganın, sistemin zayıf yönleri, işletim sistemi güvenlik açıkları, uygun izolasyonu sağlamayan kötü ağ tasarımı veya kötü tanımlanmış güvenlik duvarı kuralları hakkında bilgi edinmesine yardımcı olmak için kullanılabilir [20]. Akıllı şebekeye yönelik saldırılar içeriden de gerçekleştirilebilir. Bu tür saldırılar, akıllı şebekenin sunucularına zarar

verme konusunda hem bilgi hem de motivasyona sahip hoşnutsuz çalışanlar tarafından veya sosyal mühendislik saldırıları [21], zayıf platform konfigürasyonlarını kullanarak akıllı şebekenin sunucularına erişmeyi başaran diğer herhangi bir saldırgan tarafından gerçekleştirilebilir [7]. Zayıf platform konfigürasyonları ile kullanıcılara gereksiz erişim hakları verilmesiyle sonuçlanan yetersiz tanımlanmış politikalar, uygun olmayan veya var olmayan kimlik doğrulama mekanizmaları, kırılması kolay parolalarla sonuçlanabilecek zayıf tanımlanmış parola politikaları, ağ üzerinden şifrelenmemiş olarak aktarılan veriler ve veri koklama vb. durumlar verilerin ele geçirilme olasılığını artırır. Hedef sistem hakkında bilgi toplamak veya ona erişim sağlamak, akıllı şebeke sunucularına yönelik olası birçok saldırının ilk adımıdır.

Bu tür saldırılar, kötü amaçlı yazılımların sisteme bulaşmalarını ve DoS saldırılarını içerebilir. Kötü niyetli yazılımlar tarafından SCADA sistemlerine bulaşma olayları, Stuxnet, Flame ve Duqu örneklerindeki gibi geçtiğimiz yıllarda rapor edilmiştir. Bu tür yazılımların muazzam yetenekleri, akıllı şebeke içindeki herhangi bir sistem için büyük bir tehdit oluşturur. Bu tür yazılımlar, genellikle sistemin çalışması için gerekli olan sistem dosyalarını değiştirebilir veya silebilir, dolayısıyla kullanılabilirliğini ciddi sonuçlarla (yüksek etki) riske atabilir. Aynı zamanda log dosyaları, fatura dosyaları gibi sistem dışı dosyalar da hedef alınabilir. Örneğin, bir günlük dosyasını değiştirerek, bir saldırgan izini gizleyebilir veya kendisine karşı yanlış kanıtlar yerleştirebilir (orta etki). Kötü amaçlı yazılımların yetenekleri elbette bahsettiğimiz özelliklerle sınırlı değildir. Geri dönüşü olmayan hasara (yüksek etki) neden olabilecek güçlü yeteneklere de sahip olabilirler. Bu tür sistemlerde DoS saldırıları da mümkündür ve ağ kullanılabilirliğini tehlikeye atabilecekleri için en tehlikeli olanlar arasında kabul edilir [13]. Bu tür saldırılar, sistemin kaynaklarını aşırı yükleme nedeniyle meşru trafiğine artık yanıt veremeyeceği bir düzeye kadar doyurmaya yönelik herhangi bir çabanın sonucu olabilir. Bu durum, şebeke için ciddi veya yıkıcı sonuçlara yol açabilir (yüksek etki). Veriye yönelik yapılan siber saldırılar ağ trafiğinde bulunan veride ekleme, silme ve değiştirme işlemlerinden birini veya birkaçını akıllı şebekeyi yanıltarak gerçekleştirir ve sistemin yanlış kararlar almasını amaçlar.

4.3. Güvenli Veri İletimi

Elektrik tesislerinin operasyonel ve ticari talepleri, hem mevcut işlevleri hem de gelecekteki operasyonel gereksinimleri destekleyen yüksek performanslı bir veri iletişim ağı gerektirir. Böyle bir iletişim ağı, elektrik sistemi otomasyon uygulamalarının özünü oluşturur. Uygun maliyetli ve güvenilir bir ağ mimarisinin tasarımı çok önemlidir.

Bir akıllı şebeke sisteminde iletişim, farklı bant genişlikleri ve tüm cihazların, sertifika yetkililerinin ve sunucuların her zaman bağlanması gereken bağlantılara sahip farklı kanallar üzerinde olacaktır. Elektrik hizmetleri için yapısal bir çatı olarak değerlendirilen akıllı şebeke iletişim ağının otomasyon için yeni iletişim teknolojilerini kullanması ve dolayısıyla karar verme sürecini daha etkin hale getirmesi planlanmıştır. Akıllı şebeke uygulamalarının yapı ve ölçeğinin farklı olması farklı iletişim ağı çözümlerinin kullanılmasını gerektirmektedir. Akıllı şebeke sistemlerinin iletişim altyapısı olan AMI uygulamaları fiziksel ve mantıksal açıdan farklı ağ topolojilerini ve ortamlarını barındırır. İletişim ağının ana omurgası olarak fiber, kablosuz geniş bant veya güç hattı üzerinden geniş bant uygulamaları kullanılabilir. Olası çözümler, verilecek hizmetten istenen güvenilirliğe, çıktıya ve kapsama alanına bağlı olarak WiMax, WLAN, WSN ve kara mobil telsizleri (LMR) içerir. Kablosuz iletişim çözümleri yine sağlanacak hizmetin ihtiyaçlarına bağlı olarak lisanslı veya lisanssız olabilir. En yüksek güvenilirlik için lisanslı olanlar seçilmelidir. Yukarıdaki seçeneklerin her birinin avantajları ve

dezavantajları vardır, ancak tüm çözümler için tutarlı bir şekilde doğru olan şey, ölçeklenebilir bir güvenlik çözümüne sahip olma ihtiyacıdır [2].

Aşağıdaki gibi problem örnekleri belirlenerek anlık çözümler önerilmelidir.
Problem: İnternette belirli uygulamalar oluşturulabilir. Kötü amaçlı yazılımlar ve DoS saldırıları gibi sorunlar, şebeke işlemlerine yönelik tehditlerdir.
Çözümler:

- Akıllı şebeke ağları için TCP/IP kullanımı.
- VPN (IPSec), SSH, SSL/TLS kullanımı.
- İzinsiz giriş algılama ve güvenlik duvarları kullanımı.

5.SONUÇ

Elektrik şebekelerinin akıllı hale getirilmesi gelişen dünyanın kaçınılmaz bir zorunluluğu olmuştur. Bu gelişme veri güvenliği konusunda bazı zafiyet ve endişeleri de beraberinde getirmektedir. Bu zafiyet ve endişeler akıllı şebekelerin uygulanmasında büyük bir engel olarak öne çıkmaktadır. Bu bağlamda şebekelerin akıllı hale getirilmesinde olası tehdit ve zafiyetlerin belirlenerek önlemler alınması zorunludur.

Akıllı şebeke sistemlerinin bilişim sistemlerine bağımlı olması, kritik altyapılara yönelik siber tehditlerin daha karmaşık hale gelmesi, ciddi siber güvenlik tedbirlerinin alınmasını gerektirmektedir. Mevcut güvenlik tedbirlerinin yanısıra yapay zeka metotlarının da entegre edildiği ilave çözümler geliştirilmelidir. Ayrıca kurumlar arası koordinasyın ve işbirliği ile standardizasyon çalışmaları yapılmalıdır. Akıllı sayaç gibi ürünlerin etkin ve ekonomik bir şekilde geliştirilmesi önem arz etmektedir. Akıllı sayaç gereksinimlerinin belirlenmesi, ürün standardizasyonu kapsamında üretici kurum ve şirketlerin işbirliği içinde olmasının çözüme yardımcı olacağı değerlendirilmektedir. Akıllı sayaç standardizasyonu kapsamında yapılacak çalışmaların yetkili bir kamu kurumu liderliğinde gerçekleştirilmesinin daha etkin olacağı söylenebilir.

Akıllı şebeke iletişim altyapısının güvenliğini sağlamak, standart tabanlı son teknoloji güvenlik protokollerinin kullanılmasını gerektirir. Ortaya konan vizyona ulaşmak için atılması gereken birçok adım vardır. Bunların başında akıllı şebeke güvenliği için uyumlu bir dizi gereksinim ve standarda duyulan ihtiyaç gelir. Bu temel adımların hızlı bir şekilde gerçekleştirilebilmesi için NIST'in yönlendirmesi altında başlatılan çalışmalara devam edilmelidir. Uzun yıllar boyunca kullanılacakları için gereksinimlerin ve standartların oluşturulmasına gereken özen gösterilmelidir.

Siber güvenlik sadece teknolojik bir süreç değil, topyekün bir yaklaşım gerektirmektedir. Bu bağamda; sağlam ve verimli bir akıllı şebeke siber altyapısı kurarak sistemin gizliliğini, bütünlüğünü ve erişilebilirliğini geliştirmek gerekir. Saldırı tespiti, saldırı engelleme, kimlik doğrulama ve anahtar yönetimi hala zorlu konular olarak devam etmektedir. Özellikle, makine öğrenmesi yöntemleri siber güvenlik uygulamalarına entegre edilerek etkin yöntemler geliştirilmelidir.

Bu çalışmada, akıllı şebeke uygulamalarında mimari yapı, sistem tasarımı, iletişim altyapısı ve güvenli iletişimin sağlanması için gereksinimler sunulmuştur. Ayrıca akıllı şebeke iletişim

güvenliğinin zorluğu tartışıldıktan sonra teknik uygulamaların siber güvenlik yaklaşımı ile değerlendirmesi ile mevcut araştırma ve çözümler incelenmiştir.

KAYNAKLAR

[1] Gündüz MZ, Daş R. Nesnelerin İnterneti: Gelişimi, bileşenleri ve uygulama alanları, Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi. 2018; 24(2).

[2] Gündüz MZ, Daş R. Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik, Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi. 2020; 10(2).

[3] Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports. 2021.

[4] Yan Y, Qian Y, Sharif H, Tipper D. A Survey on Cyber Security for Smart Grid Communications, IEEE Communications Surveys Tutorials. 2012; 14(4).

[5] Cardenas A. Cyber-Physical Systems Security, University of Bristol. 2019. Erişim adresi: https://www.cybok.org/media/downloads/Cyber-Physical_Systems_KA_-_draft_for_review_January_2019.pdf

[6] Gopstein A, Nguyen C, O'Fallon C, Hastings N, Wollman D. NIST framework and roadmap for smart grid interoperability standards, release 4.0, National Institute of Standards and Technology. 2021. doi: 10.6028/NIST.SP.1108r4.

[7] Wei D, Lu Y, Jafari M, Skare P, Rohde K. An integrated security system of protecting Smart Grid against cyber attacks, Innovative Smart Grid Technologies. 2010. doi: 10.1109/ISGT.2010.5434767.

[8] Komninos N, Philippou E, Pitsillides A. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures, IEEE Communications Surveys Tutorials. 2014; 16(4). doi: 10.1109/COMST.2014.2320093.

[9] Sweeney L. k-anonymity: a model for protecting privacy, International Journal Uncertain Fuzziness Knowledge-Based Systems. 2002; 10(5). doi:10.1142/S0218488502001648.

[10] Pillitteri VY, Brewer TL. Guidelines for Smart Grid Cybersecurity, NIST Interagency/Internal Report (NISTIR) - 7628 Rev 1. 2014.

[11] https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_487 Erişim tarihi: 01.12.2021.

[12] Xiao Y, Security and Privacy in Smart Grids. 2013. CRC Press. https://doi.org/10.1201/b15240

[13] Acarali D, Rao KR, Rajarajan M, Chema D, Ginzburg M. Modelling smart grid IT-OT dependencies for DDoS impact propagation, Computers & Security. 2022; doi: 10.1016/j.cose.2021.102528.

[14] Wagner M, Kuba M, Oeder A. Smart grid cyber security: A German perspective, International Conference on Smart Grid Technology. 2012. doi: 10.1109/SG-TEP.2012.6642389.

[15] Wei D, Lu Y, Jafari M, Skare PM, Rohde K. Protecting Smart Grid Automation Systems Against Cyberattacks, IEEE Transactions on Smart Grid. 2011; 2(4). doi: 10.1109/TSG.2011.2159999.

[16] Nicholson A, Webber S, Dyer S, Patel T, Janicke H. SCADA security in the light of Cyber-Warfare, Computers & Security. 2012; 31(4). doi: 10.1016/j.cose.2012.02.009.

[17] Mo Y. vd, Cyber-Physical Security of a Smart Grid Infrastructure, Proceedings of the IEEE. 2012; 100(1). doi: 10.1109/JPROC.2011.2161428.

[18] Kushner D. The real story of stuxnet, IEEE Spectrum, 2013. https://spectrum.ieee.org/the-real-story-of-stuxnet Erişim Tarihi: 05.12.2021.

[19] Radoglou-Grammatikis P. vd, SPEAR SIEM: A Security Information and Event Management system for the Smart Grid, Computer Networks. 2021; cilt:193, sayı:108008. doi: 10.1016/j.comnet.2021.108008.
[20] Procopiou A, Komninos N. Current and future threats framework in smart grid domain, IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems. 2015. doi: 10.1109/CYBER.2015.7288228.
[21] Gündüz MZ, Daş R. Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri, 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. 2016.