

HÜCRESEL ŞEBEKELERDE MAKİNELER ARASI İLETİŞİM VE GÜVENLİK ÖNERİLERİ

Serdar SARIKOZ¹, Mustafa KÜÇÜKALİ²

¹Bilgi Teknolojileri ve İletişim Kurumu, sksarikoz@gmail.com

²Bilgi Teknolojileri ve İletişim Kurumu, mustafa.kucukali@btk.gov.tr

Özet:

İnternet teknolojilerinin gelişimi ve İnternet'in yaygınlaşması ile birlikte hayatımızda önemli değişiklikler meydana gelmiştir. Her yerden ve herhangi bir zamanda bilgiye ulaşma ve analiz edilmesi ihtiyacı; akıllı cihazlar arasında herhangi bir yöntem ile haberleşmenin gelişmesini sağlamıştır. Nesnelere arası İnternetin (IoT) en önemli parçalarından birisi olarak kabul edilen, makineler arası iletişim (M2M) olarak ta adlandırılan teknolojik gelişim ile makinelerin bağlantı ve birlikte çalışabilirliğinin sağlanması amaçlanmaktadır. Mobil haberleşme teknolojilerindeki yenilikler ile birlikte günlük hayatımızın ayrılmaz bir parçası haline gelecek M2M uygulamalarının devletlerin, yerel yönetimlerin ve bireylerin hayatında birçok kolaylıklar kazandırdığı gibi kişisel verilerin gizliliği, yaşam hakkının ihlali ve ülkeler arası siber saldırılarda önemli bir araç olarak kullanılma potansiyeline sahiptir. Yeterli güvenlik altyapısına sahip olmayan makineler arası iletişim çözümlerinin üçüncü taraflarca erişilecek sistemlerden dolayı verilerinin elde edilebildiği, bozulabildiği veya servis engellemesine maruz kalabileceği değerlendirilmektedir. Bu çalışma kapsamında Nesnelere arası İnternet (IoT), makineler arası iletişim (M2M) teknolojileri ve uygulamaları, olası güvenlik riskleri ve alınması gereken tedbirlere yer verilmiştir.

Anahtar Kelimeler: Makineler arası iletişim, M2M, nesnelere arası internet, hücreli şebekeler, güvenlik

1. GİRİŞ:

Geçtiğimiz son 10 sene içerisinde haberleşme sistemlerinde baş döndürücü gelişmeler yaşanmıştır. Her yerden, her zaman veriye ulaşma ihtiyacı, İnternet protokolü (IP), sensör teknolojileri, mobil haberleşme teknolojileri ve gömülü cihaz teknolojilerindeki gelişmeler gerçek ve dijital dünyanın ihtiyaçlarını karşılarken bir yandan da birbirleri ile olan etkileşimini artırmıştır [1,3].

Teknolojideki gelişmelerle birlikte haberleşme altyapıları IP protokolü üzerinden hizmet verir ve yönetilebilir hale gelmektedir. Bulut bilişim olarak adlandırılan yapılar ile her türlü uygulama, servis olarak kullanıma sunulabilmektedir. Böylece verilen ses, veri ve görüntü tabanlı hizmetler çok büyük miktarlarda artmakta ve çeşitlenmektedir. Sonuç olarak teknolojideki bu gelişim ve yaygınlaşma ile birlikte çok farklı yeni hizmet türleri ortaya çıkmaktadır.

Anılan gelişmeler ile birlikte makineler arası iletişim de yaygınlaşmıştır. İnsan aracılığı olmadan veya sınırlı müdahalesi ile makinelerin birbirleri ile kurdukları iletişim şekline M2M (Makineden Makineye Haberleşme-Machine to Machine Communication) denilmektedir. M2M haberleşmesinde; İnternet, GSM, GPRS, uydu, Wi-Fi, Zigbee, Bluetooth, RFID vb. kablolu ve kablosuz teknolojiler kullanılabilir [2,5,11].

M2M uygulamalarının ve iletişiminin mobil internet ile sağlanması, 2009 yılından itibaren tartışmalara konu olmuştur. M2M uygulamaları bazı bilim adamları tarafından bilgisayar ve internetten sonra büyük bir buluş olarak tanımlanırken bazıları tarafından ise bekle ve gör davranışı şeklinde araştırmalar incelenmektedir. Bununla birlikte M2M uygulamaları aslında yeni bir buluş değildir. Gömülü kontrol uygulamaları ile uğraşanlar için M2M uygulamaları, sadece mevcut işlerinin bir adım ötesindeki yeni bir çalışma olarak ta değerlendirilmektedir [2].

Nesneler arası İnternet farklı yaklaşımları ve teknolojileri bir araya getiren yeni bir kavram olarak yakın zamanda karşımıza çıkmaya başlamıştır. Nesneler arası İnternet (IoT); yaygın olarak çevremizde yer almakta olan cihaz ya da objelerin IP protokolü üzerinden, haberleşme teknolojileri vasıtası ile tekil olarak adreslendirilerek haberleşmesinin sağlanması olarak adlandırılmaktadır [1].

Nesneler arası İnternet'e yönelik ilk çalışmalar 2000'li yıllarda dünya üzerinde herhangi bir lokasyondaki RFID'li cihaza İnternet üzerinden erişebilme amacı ile yapılmıştır. Nesneler arası İnternet, bugün gelinen noktada İnternet üzerinden kontrol edilebilen, herhangi bir lokasyonda yer alan; tekil ID değerine sahip, adreslenebilir, kontrol edilebilir cihazlar kastedilmektedir. Yeni nesil akıllı cihazların gelişimi ile birlikte söz konusu cihazlara sensör, hesaplama, haberleşme yeteneklerin birlikte çalışabilirliği kazandırılmıştır [1,3,17].

Yine yakın gelecekte, IoT vizyonuna sahip cihazların akıllı telefon vb. cihazlardan daha fazla özelliklere sahip olacağı, 2025 yılında yaklaşık olarak büyük çoğunluğu alt yapılara ilişkin çözümlerde kullanılmak üzere 50 milyar akıllı cihazın IoT teknolojileri sayesinde haberleşeceği öngörülmektedir [17,22,25]. Birbirlerine bağlı büyük miktardaki cihazların ve ürettiği verinin Söz konusu rakamlara ulaşan Nesneler arası İnternet ağının ve üreteceği veri miktarının; toplum, çevre, ekonomi ve bireyler üzerinde fayda sağlayacağı aşikârdır.

Araştırmacılar tarafından İnternet ve hücresel şebekelerin birbirine yaklaşması ile birlikte IoT ve M2M haberleşmesinin hızlı bir şekilde geliştiği ve yaygınlaştığı, mevcut araştırmalara göre M2M teknolojilerinin, veri haberleşmesi ya da SMS gelirlerine göre İşletmelere 1000 kat daha fazla gelir bırakacağı ifade edilmektedir [14].

Kuşkusuz Nesneler arası İnternet'in ve M2M uygulamalarının temel amacı günlük yaşantımızda yapılan işlemlerin otomatize edilmesi olmakla birlikte, günlük yaşantımızda kullanılan hemen hemen tüm nesnelerin IoT ya da M2M ile erişilebileceği bir sistemin, İnternet'in şimdiye kadar doğurduğundan çok daha fazla sayıda güvenlik risklerini de beraberinde getireceği düşünülmektedir [2,3,8,9,22]

Bu araştırma kapsamında 2. bölümde literatürde yapılan benzer çalışmalara, 3. bölümde M2M iletişim ve detaylarına, 4. bölümde Hücresel Şebekelerde yer alan olası güvenlik risklerine, 5. bölümde güvenlik önerilerine, 6. bölümde değerlendirmelere ve 7. bölümde sonuçlara yer verilmiştir.

2. LİTERATÜR TARAMASI

M2M iletişim cihazların birbirleri ile haberleşebilmesini sağlayan cihaz ya da sistemlerden oluşmaktadır. Nesneler arası İnternet teknolojileri ise bulut bilişim, akıllı cihazlar, sensörler, ev otomasyonu vd. uygulamalar ile birlikte geniş alanda görülmeye başlanmıştır. IoT paradigması farklı cihaz türlerinin İnternet teknolojilerini kullanarak birbirleri ile haberleşmesini sağlamaktadır. RFID cihazlar ve Wireless Sensör Networks(WSN) IoT teknolojisini yaygınlaştıran iki önemli faktör olarak karşımıza çıkmaktadır. Bu bölümde literatürde son on senede yayımlanmış araştırmalara yer verilmiştir.

Nesneler arası İnternet, özellikleri, uygulama alanları, IoT teknolojilerinde sağlanması gereken temel özellikleri, söz konusu sistemlerin sağlanması gereken ve detaylarına [1,2,3,13,28,37] de yer verilmiştir. IoT sistemlerinin; ölçeklenebilirlik, düşük maliyetli cihaz ve teknolojiler bütünü olması gerekliliği, esneklik, QoS desteği, güvenlik gereksinimlerini karşılaması, yönetilebilir/izlenebilir teknolojiler bütünü sağlanması gerektiği söz konusu makalelerde ifade edilmiştir.

M2M teknolojisi, mimarisi, uygulamaları, trendleri, özellikleri, güvenlik riskleri ve önerileri [2,5,7,11,15,27,31,37] 'de yer verilmiştir.

M2M sistemlerinin standardizasyonuna yönelik çalışmalar [2,15,25,27]'de yer verilmiş, genel olarak bu alanda ETSI, 3GPP ve IEEE'ye yönelik çalışmaların öne çıktığı görülmektedir.

Temel M2M uygulama alanları [2,6,9,10,12,15,21,23,25,31]' de yer verilmiş olup, genel uygulama alanlarının güvenlik, takip, ödeme sistemleri, sağlık, kontrol sistemleri, ölçüm sistemleri (smart grid) ve tesis yönetimi (akıllı şehirler, akıllı yaşamlar) şeklinde önerildiği görülmektedir.

Wu ve arkadaşları tarafından yapılan çalışmanın ise gerek IoT, gerekse M2M teknolojileri için gelecek çalışmalara projeksiyon olacağı düşünülmektedir [2].

3. MAKİNELER ARASI İLETİŞİM (M2M)

3.1. M2M Kavramı

Makineden makineye haberleşme, makineler arası iletişim veya 3GPP'nin kullandığı şekliyle makine tipi iletişim (MTC) gibi isimlendirmeler kullanılsa da en yaygın hali M2M'dir. M2M, iki farklı elektronik sistemin birbirinden bağımsız ve birbirini etkilemeden ve az ya da hiç insan müdahalesi olmadan haberleşmesi olarak tanımlanmaktadır [5,7,11,15,27,31,37]. Bu iki sistemden biri takip, yönetim, kontrol veya ölçme gibi işlemlerin yapılmak istendiği yapıdır. Çoğunlukla bir sensör ve network erişimini sağlayacak erişim biriminden oluşur. Buradan sensörler aracılığıyla elde edilen veriler kablolu veya kablosuz bir ağ üzerinden kontrol merkezlerine veya sistemlerine iletilir [2,5,31,37].

M2M ile ilgili birçok standart ETSI tarafından oluşturulmaktadır ve ETSI'ye göre; "kablolu, kablosuz ya da hibrid hatlar üzerinden farklı protokolleri kullanarak tıbbi görüntüleme sistemlerinden akıllı izleme ile tedarik zincirine, akıllı ölçüm sistemlerinden otomat makinelerin uzaktan kumanda edilmesine kadar hayatımıza dinamizm ve kolaylıklar kazandıran teknolojiler bütünü" olarak tanımlanmaktadır [15].

Modern manasıyla M2M uygulamalarının temeli 1995 yılında Siemens tarafından geliştirilen ve M1 olarak adlandırılan GSM Data Modülü ile atılmıştır. Filo takip sistemleri, POS cihazları ve benzeri alanlarda kullanılan bu uygulamanın hemen ardından 1997 yılında otomotiv ve telematik sistemlerde kullanılan daha gelişmiş M2M uygulamaları yerini almıştır.

Bununla birlikte yaygın manası ile kullanımın 2000'li yıllarda Nesnelere Arası İnternet'in RFID Sensörler ile yapılan çalışmaları ile araştırmacıların dikkatini çektiği görülmüştür. Diğer taraftan 2009 yılında ETSI tarafından M2M çalışma grubu kurulmuş ve standardizasyon çalışmaları başlamıştır [1,15].

3.2. M2M, IoT, WSN ve CPS Teknolojileri Arasındaki İlişki

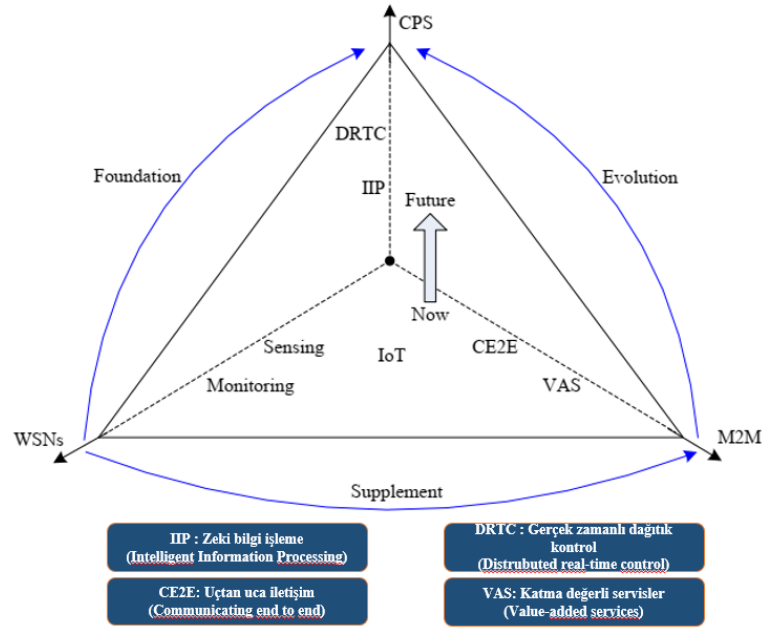
M2M, IoT, WSN ve CPS (CPS: Cyber Physical Systems) kavramları sıklıkla çıkmasına rağmen M2M teknolojileri çok kısıtlı ya da hiç insan müdahalesi olmaksızın birbirleri ile haberleşebilen cihaz ya da bilgisayarları ifade etmektedir.

CPS teknolojilerinde ise belirli amaca yönelik üzerinde sensörleri ve hesaplama yeteneği bulunan toplamış olduğu veriyi belirli hedef cihaz ya da networke gönderebilen cihazlar kastedilmektedir.

WSNs teknolojileri ise farklı fiziksel lokasyonlara dağılmış algılayıcılardan oluştuğu, söz konusu algılayıcıların belirli amaca yönelik olarak verileri toplayarak ana istasyona gönderdiği bir yapı olarak karşımıza çıkmakta olduğu görülmektedir.

IoT ise genel olarak 4 bileşenden oluşur: 1) algılama özelliği 2) heterojen erişim 3) bilgi işleme 4) uygulamalar, güvenlik ve gizlilik vb servisler şeklindedir. Bununla birlikte WSNs, M2M ve CPS'in IoT'un bileşeni olduğu düşünülebilir.

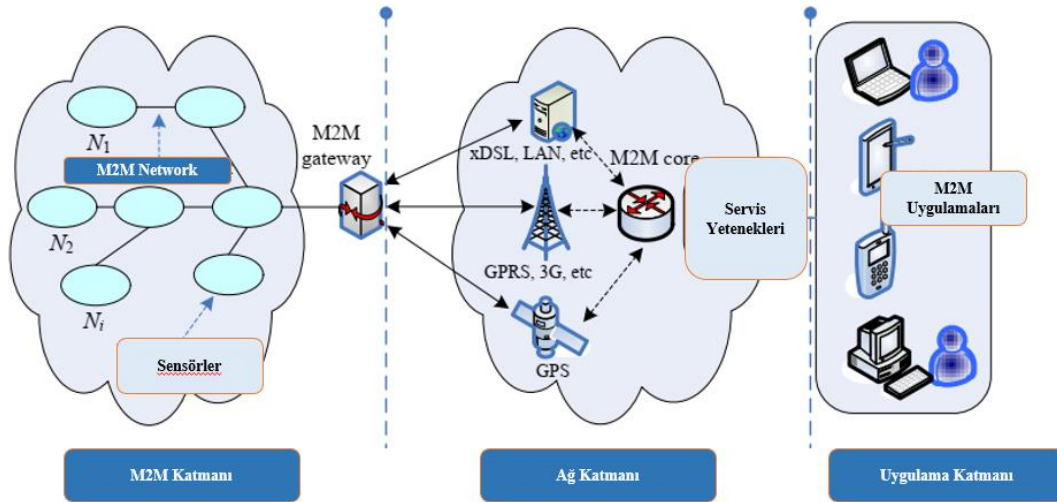
Ancak 4 teknolojinin de hemen hemen aynı bileşenlere sahip olduğu, tasarım aşamasında farklılık gösterebileceği ifade edilmiştir. Diğer yandan RFID ve M2M teknolojisindeki pasif cihazların yerini CPS adı verilen aktif cihazların olduğu teknolojilerin aldığı ifade edilmiştir [32,37]. Söz konusu kavramların birbirleri ile olan ilişkileri Şekil-1’de verilmiştir [32,27].



Şekil-1: M2M, IoT, CPS ve WSNs arasındaki korelasyon [32, 37]

3.3. M2M Mimarisi

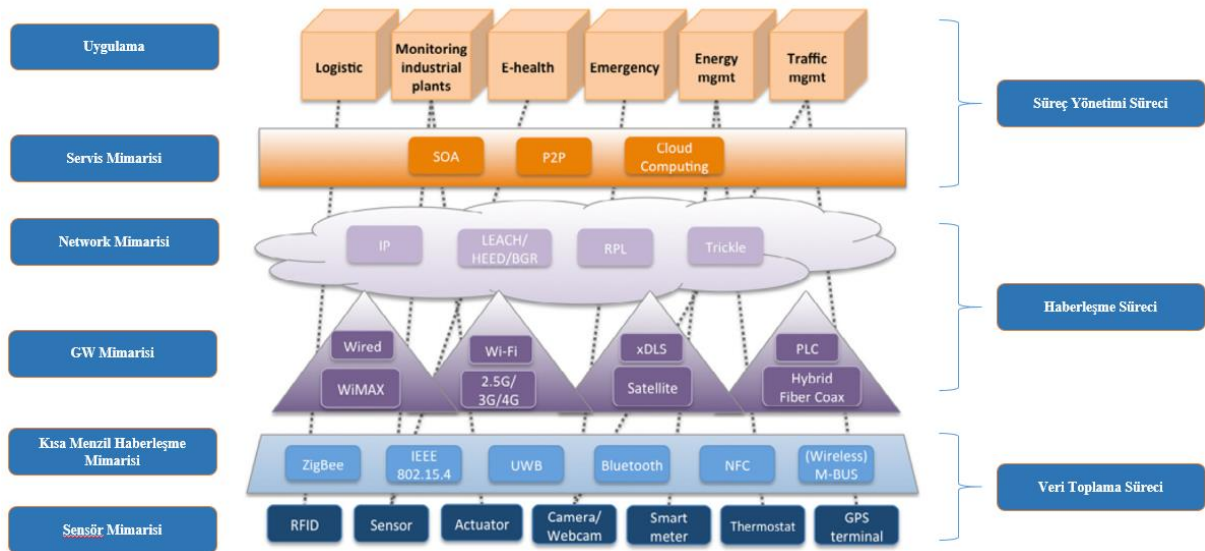
İdeal bir M2M uygulaması dünyanın herhangi bir yerinde yer alan cihaza güvenli bir ağ/Internet bağlantısı sunmalıdır. Buna ek olarak herhangi bir menzil ya da gecikme sorunu yaşatmamalı, mümkün olduğunca az enerji harcamalı ve sınırsız çıktı verebilirken maliyetleri minimumunda tutmayı başarmalıdır. Fonksiyonel açıdansa hem bilgi güvenliği ve gizliliğini temin etmeli hem de bilgiye kolay erişim sağlarken bilgi yönetimini de verimli olarak gerçekleştirmelidir. ETSI tarafından tanımlanan M2M iletişimin en temel yapısı Şekil-2’de görüleceği üzere üç ana katmandan oluşmaktadır [15,25,37]. Bu katmanlardan ilki ve iletişimin başlangıç noktası uygulama katmanıdır. Kullanıcı veya cihazın kendisi uygulama katmanını kullanarak talep edilen hizmeti başlatır. İkinci katman olan ağ katmanı gerekli veriyi uygulama katmanından alarak taşır ve M2M ağ geçidini kullanarak iletişim kurulmak istenen makine veya makinelere iletir. Çoğu işlemin yapıldığı üçüncü katman ise M2M cihaz katmanıdır. Uygulama katmanından gelen verinin işlendiği, değerlendirildiği ve hizmet türüne göre uygulama katmanına geri dönüşümün yapıldığı yerdir.



Şekil-2: ETSI M2M Mimarisi (15,37)

Ağ katmanında mesafe ve konuma göre kablolu, kablosuz veya her ikisinin de beraber kullanıldığı hibrit teknolojiler kullanılabilir. Günümüzde en yaygın kullanılanlarına ise uzak mesafelerde GSM, GPRS ve uydu, kısa mesafelerde ise WiFi, Zigbee, Bluetooth ve RFID sayılabilir.

M2M teknolojilerinde karşımıza çıkacak genel yapı ise Şekil-3'te sunulmuştur [1]:



Şekil-3: M2M uygulamalarında 3 aşamalı genel yapı [1].

3.4. M2M Uygulama Alanları

Temel M2M uygulama alanları aşağıda yer verilmiştir [2,6,9,10,12,15,21,23,25,31]:

- **Güvenlik** : izleme, alarm sistemleri, erişim kontrol, araç/ev/kampüs güvenliği
- **Takip ve İzleme**: Filo yönetimi, talep yönetimi, öde ve kullan sistemleri, varlık izleme, navigasyon, trafik bilgi/yönetim
- **Ödeme sistemleri**: Satış terminali (POS),Otomat makineleri, Oyun makineleri
- **Sağlık**: Hasta izleme sistemleri, yaşlı ya da engelli takibi, web üzerinden tele tıp hizmetleri, uzaktan teşhis desteği,
- **Uzaktan bakım/kontrol sistemleri**: sensörler, ışıklandırma, pompalar, vanalar, asansör kontrol, otomat makine kontrolü, araç teşhisi
- **Ölçüm sistemleri**: güç, gaz, su, ısıtma, grid kontrol vb. endüstriyel ölçümler
- **Üretim**: Üretim zinciri izleme ve otomasyonu
- **Tesis Yönetimi**: Ev/bina/kampüs otomasyonu

3.5. M2M Standardizasyon Çalışmaları

M2M standartları konusunda uluslararası, bölgesel, yerel standart kuruluşları çalışmalarını sürdürmektedirler. Genel olarak M2M standardından beklenenler M2M hizmetlerini “tak ve çalıştır” şeklinde etkinleştirmek, bağlantı, güvenlik, AAA, bakım gibi konularda ortak işleyiş belirlemek ve M2M konusundaki çeşitliliği azaltarak ortak ara yüzler belirlemektir

Çeşitli organizasyonlar tarafından M2M sistemlerinin geliştirilmesine yönelik yapılan çalışmalara [2,15,25,27]’te yer verilmiş olup, Tablo-1’de sunulmuştur [2]:

Tablo-1: M2M Standardizasyon Çalışmaları

Standart Geliştirici Organizasyon	M2M Çalışmalarına Katkıları
3GPP	Release 10: Düşük güç, tıkanıklık ve aşırı yük kontrolü, tanımlayıcılar, adresleme, abonelik kontrolü ve güvenlik gibi özellikler için gereksinimleri tanımlama ve radyo ve ağı optimize edilmesi, Release 11: aygıttan ağıta iletişim için ağ iyileştirmeleri, M2M ağ geçidi, M2M grubu ve ortak konumlandırılmış M2M aygıtları için geliştirmeler, ağ seçimi ve yönlendirme, servis gereksinimleri ve optimizasyonları.
ETSI	M2M ağ mimarisi: uçtan uca bir görünüm sağlamak için her ağ elemanın işlevsel ve davranışsal gereksinimlerini tanımlanması
GSMA	M2M için GSM operasyonu: GSM tabanlı gömülü modül tasarımında radyo arayüzü, uzaktan yönetim, UICC sağlama ve kimlik doğrulama ve temel bileşen maliyetleri gibi operasyonel sorunların gözden geçirilmesi, Dikey pazarlarda sağlık, kamu hizmetleri, otomotiv ve tüketici cihazlarının kullanım durumlarına
IEEE	802.16p (WiMAX): hava arayüzünün optimize edilmesi için düşük güç tüketiminin optimize edilmesi, toplu cihaz aktarımı, cihaz kimlik doğrulaması Gelecek konular: M2M ağ geçidi, kolektif M2M ağları, gelişmiş M2M özellikleri
	802.11 (WiFi): Spektrum yönetiminin sağlanabilmesi amacı ile hava arayüzünün optimize edilmesi,
	802.15.4 (Zig Bee): Smart Grid Networkler için hava arayüzünün optimize edilmesi,
Wimax Forum	Ağ sistemi mimarisi özellikleri: kullanımları, düşük OPEX ile dağıtım modellerini, IEEE 802.16 protokollerine dayalı işlevsel gereksinimleri ve uçtan uca M2M sistemi için performans yönergelerini tanımlanması
WFA	Akıllı şebeke görev grubu: pazarlama girişimleri, hükümet ve endüstri katılımı ve teknik / sertifika programları aracılığıyla akıllı şebeke içinde Wi-Fi'nin benimsenmesini teşvik edilmesi Sağlık hizmetleri görev grubu: Ev ve Hastane Sağlık Hizmetleri pazarı segmenti için Wi-Fi'yi tercih edilen kablosuz erişim teknolojilerinin korunması
OMA	Cihaz yönetilebilirliği: Ağ geçidi tarafından yönetilen cihazlar için gereksinimleri tanımlanması
TIA	M2MSW architecture TR50: Akıllı cihazlar, uygulamalar veya ağlar arasındaki olayların ve bilgilerin izlenmesi amacı ile erişim ortamından bağımsız arayüz standartlarının geliştirilmesi
CCSA NITS	CCSA TC10: genel gereksinimler, uygulamalar, ağ oluşturma, algılama ve ilgili kısa menzilli RF bağlantısı dahil olmak üzere yaygın ağlara odaklanılması,
	NITS WGSN: genel gereksinimler, uygulamalar, ağ oluşturma, algılama ve ilgili kısa menzilli RF bağlantısı dahil olmak üzere yaygın ağlara odaklanılması,

3.6. M2M Sistemlerinde Temel Güvenlik Sorunları

Pek çok M2M uygulamasında M2M cihaz ya da sensörleri tarafından elde edilen veriler hassas ve korunması gereken bilgileri içermektedir. Elde edilecek verilerin gizliğinin korunması, bütünlüğünün sağlanması, verilerin sürekli olarak toplanabilir olması önem arz etmektedir. M2M sistemlerinin maruz kalabileceği güvenlik riskleri aşağıda sıralanmıştır [6,9,10,26,28]:

Fiziksel Saldırıları: Cihaza hasar verilebileceği gibi cihaza doğrudan bağlantı ile üzerindeki yazılıma müdahale edilebilir, eğer Hücresel şebekede çalışan bir M2M sensörü ise SIM kartı klonlanabilir, cihaza ait kimlik bilgileri öğrenilebilir veya değiştirilebilir. Söz konusu saldırıların önlenmesi amacı ile cihazların yazılımlarının, üretilen verilerin bütünlüğünün sağlanması önem arz etmektedir.

Konfigürasyon saldırıları: Cihazın yazılımının ve/veya konfigürasyonlarının değiştirilmesi, cihazın sahibi tarafından yapılan güvenliği tehlikeye düşürebilecek yanlış ayarlar gibi hatalar kullanılarak yapılan saldırılardır.

Protokol saldırıları: Bu saldırılar doğrudan cihaza yapılır. DoS, DDoS (Denial-of-Service) saldırıları örnek olarak verilebilir. DoS saldırılarında sunucular aşırı derecede meşgul edilerek veya anlamsız protokol paketleri göndererek istemciler(M2M cihazlara) hizmet vermesi engellenebilmektedir. Dos saldırıları haberleşme sistemlerinde en çok karşılaşılan ve en kolay gerçekleştirilen saldırılardır. Bu saldırıları gerçekleştirmek için yazılmış hazır programlar bulunmaktadır.

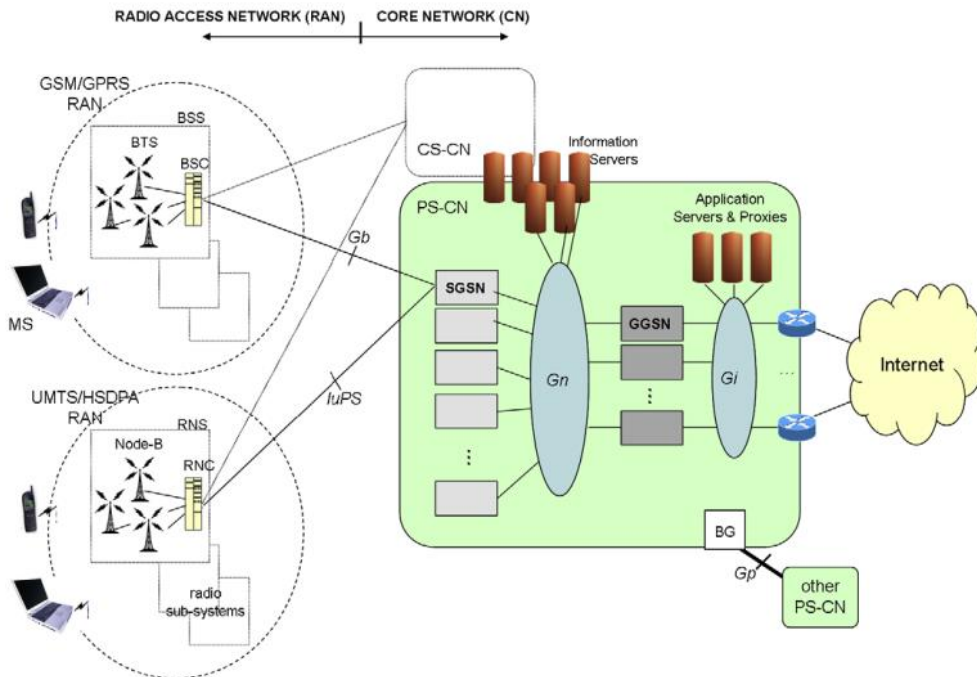
Temel Şebekeye Yönelik Saldırıları: Temel ağ şebekesine yönelik gerçekleştirilebilecek saldırılar ile sistemin işlevsiz hale getirilmesi amaçlanabilir. Bu nedenle cihazlar üzerindeki gerekli yönlendirme, yetkilendirme, saldırı tespiti ve engellenmesine yönelik cihazların gerektiği gibi konumlandırılması önem arz etmektedir.

Kullanıcı Veri ve Kimliğinin Çalınmasına Yönelik Saldırıları: Söz konusu sistem üzerinde gerek sistemi işletenler, gerekse sistem dışından cihaz ya da şebekelerin saldırılara maruz kalması durumunda kişisel bilgi güvenliği ihlalleri olabilecektir. Örnek olarak çocuğunun nerde olduğunu öğrenmek isteyen ebeveynlere yönelik bir uygulama kapsamında; söz konusu konum bilgilerinin yetkisiz ve kötü niyetli kişilerin elde etmesinin engellenmesi son derece önemli bir konudur. Bu nedenle tasarımda gerekli tedbirlere dikkat edilmelidir.

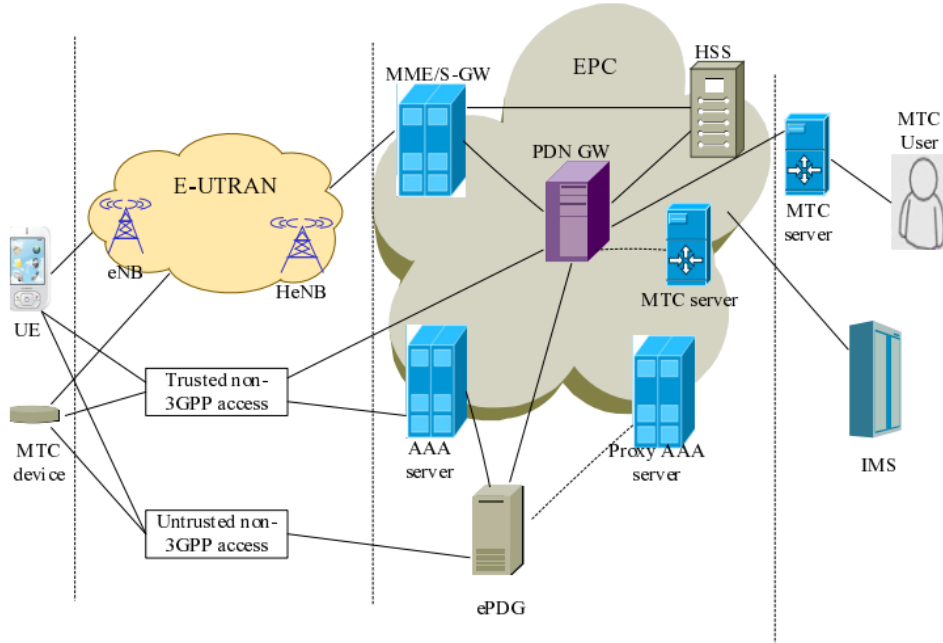
4. HÜCRESEL ŞEBEKELERDE GÜVENLİK SORUNLARI

Mobil ve taşınabilir terminaller için Genişband kablosuz bağlantı; 3G şebekelerin yaygınlaşması ile mümkün olmuştur. 3. nesil hücreli şebekeler (3G) ile birlikte hücreli şebekeler, bilimsel çevreler tarafından yeni konu olmaya başlayan DoS (denial-of-service: Servis kesintisi) ataklarına maruz kalmaya başlamıştır. Saldırı türleri genel olarak; network konfigürasyonu, RNC üzerindeki durum geçişleri, kanal tahsisleri, zaman aşımı süreleri, şebeke kapasitesi vd. birçok parametre göz önünde bulundurularak gerçekleştirilmektedir [4,30,33].

2G network yapısı temel olarak PSTN şebekesine bağlı, devre anahtarlama (circuit switched :CS) core network ve Radio Access Network'ten (RAN) oluşmaktadır. Şekil-4'te 3G şebekesinin genel hücreli şebeke çizimi [4], Şekil-5'te ise LTE şebekesinin genel hücreli şebeke çizimine verilmiştir [30].



Şekil-4: Genel 3G Topolojisi [4]



Şekil-5: Genel LTE Topolojisi [30]

3G şebekelerinde genel olarak karşılaşılabilecek atak türleri; broadcast IP paketi gönderimi ile bir bölgedeki tüm MS'lerin ve şebeke kaynakların meşgul edilmesine yönelik paging saldırıları ve tahsisli kanalların meşgul edilmesine yönelik saldırılar şeklinde belirtilmektedir [4].

LTE şebekelerinin ise 3G şebekelerine göre saldırıya daha açık olduğu; IP address spoofing, DoS attacks, viruses, worms, spam mails ve kontrolsüz çağrılar şeklinde saldırılara maruz kalabileceği belirtilmektedir [30,33]. Bununla birlikte LTE-A'nin beraberinde eski teknolojilere ait güvenlik açıklıklarını barındırdığı, şebekenin IP Multimedia Subsystem (IMS) ve Next Generation Networks (NGN) özelliklerini taşıması ile birlikte IP protokolüne ait riskleri beraberinde getirdiği ifade edilmiştir[30].

Laya ve arkadaşları tarafından yapılan çalışmada ise; hücresel şebekelerde M2M servislerinin yaygınlaşması ile birlikte Random Access channel'a yönelik saldırıların artacağı ve network kaynaklarında çakışmaların yaşanacağı ifade edilmiştir [33].

5. M2M GÜVENLİK ÖNERİLERİ

M2M uygulamalarında M2M cihaz ya da sensörleri tarafından elde edilen veriler hassas ve korunması gereken bilgileri içermektedir. Gelişen ve değişen teknoloji ve haberleşme imkânlarının etkisiyle hayatımızda daha fazla yer edinecek olan M2M uygulamalarının güvenliği tüm güvenli haberleşme uygulamalarına benzer ana esaslar üzerine bina edilmesi gerekmekte olup, aşağıda söz konusu esaslara yer verilmiştir [9,18,28]:

Yetkilendirme ve Kimlik Doğrulama (Authorization and Authentication) : M2M ağında tanımlı her bir cihaz, düğüm noktası ve yönetim birimleri ile ilgili kimlik doğrulama süreçleri yetkisiz erişimi önlemelidir. ETSI tarafından belirlenen yetkilendirme ve kimlik doğrulama standartlarına göre Kmr - M2M Root Key ve Kmc - M2M Connection Key olarak adlandırılan çeşitli anahtarlar kullanılmaktadır. Bu anahtarlar servis sağlayıcı ve düğüm noktası ile uç birimler arasında kullanılan çeşitli anahtarlama mekanizmalarıdır.

Rol temelli erişim kontrolü (RBAC- Role Based Access Control) : M2M ağı üzerindeki her bir cihaz, düğüm noktası, gateway ve kullanıcı modülleri kendilerine atanacak rol ile ancak o ağda yer alabilecektir. Ayrıca SCADA sistemlerinde olduğu gibi uygulama katmanında kullanıcı rollerinin ayarlanması da güvenlik için bir zarurettir.

Veri doğruluğu ve bütünlüğü (Data validation and Integrity) : Özellikle düğüm noktalarına yapılan saldırılarda veya trafiğin bozulması gibi durumlarda uçtan uca doğrulama yapılması verinin doğruluğu ve bütünlüğü açısından önemlidir. Bu doğrulamayı ya da kontrolleri sağlayacak üçüncü parti çok sayıda uygulama, cihaz geliştirilmiş olup mevcut M2M ağ haberleşme protokolleri de kullanılabilir.

Veri Gizliliği (Trusted Environment) : İletilen verinin üçüncü kişilerce ele geçirilemeyecek şekilde başta haberleşme kanallarının güvenliği olmak üzere düğüm noktalarının güvenliği ve cihazlar arası uçtan uca şifreli haberleşme altyapılarının kullanılması gerekmektedir.

Oturum Yönetimi (Session Management) : M2M ağında her bir katman için oturum yönetimi kendi altyapısının özelliklerine göre set edilmelidir. Uygulama ile haberleşme kanalı arasında ya da diğer iki katmanda oturum ilkeleri yönetim modülünde tanımlanacak ilkelere göre ayarlanmalıdır.

Loglama ve İzleme (Auditing and Monitoring) : Ne kadar güvenli bir altyapı kurulursa kurulsun hem mevcut altyapıda işleyişin kontrolü ve olası hatalara güvenlik ihlallerine müdahale açısından hem de anlık saldırı tespiti açısından mutlaka loglama ve izleme yapılmalıdır. Log sonuçları ile özellikle kurumsal büyük M2M altyapılarında işleyiş ile ilgili geriye dönük raporlama imkânı elde edilebileceği gibi bir güvenlik haritası çıkarma imkânı da doğacaktır.

Sistemin genel güvenlik tesisinin ise Şekil-6'da görüldüğü gibi yapılandırılmasının genel bakış olarak doğru olduğu değerlendirilmektedir.

Application Layer	IoT uygulamaları	Lojistik Sistemler Güvenliği	Akıllı Ev Sistemleri Güvenliği	Medikal Sistemler Güvenliği	Akıllı Trafik Sistemleri Güvenliği	Çevre İzleme Sistemleri Güvenliği	...	Diğer Sektörler/Sistemler	
	Uygulama Destek Katmanı								Ara yazılım teknoloji güvenliği
Transportation Layer									
Transportation Layer	Local Area Network	Local Area Network Security							
	Core Network	Internet Security							
	Access Network	Ad Hoc Security	GPRS Security	Wifi Security	3G Security	Other network security			
Perception Layer									
Perception Layer	Perception Network	RFID Security	Protocol Security	WSN Security	Routing Protocol Security	RSN Security	Fusion Security		GPS Security
			Base Station Security		Crypto Algorithms		Sensor+RFID Reader Security	WSNs+RFID Reader Security	
	Tag Counterfeit Security		Key Management		Sensor + Tag Security				
	Tag Encode Security		Node Trust Management		Sensor Tag Security				
Perception Node									

Şekil-6: Genel Güvenlik Mimarisi [18].

6. DEĞERLENDİRME

3G/4G teknolojilerinin gelişmesi ve ucuzlaması, IPv6'nın kullanımının başlaması ile birlikte hızlı bir şekilde, M2M teknolojilerinin hüresel şebekelerde yaygınlaşacağı görülmektedir.

M2M uygulama ve cihazlarının bulut bilişime uygunluğu, minimum yönetim maliyeti ve ölçeklenebilir olması söz konusu teknolojilerin yaygınlaşması açısından gereklilik olarak görülmektedir.

M2M Teknolojilerinin yaygınlaşacağı temel yaşam alanlarının; güvenlik ve kamu güvenliği, akıllı şebekeler (gaz, su, enerji vd.), takip ve iz sürme, ödeme sistemleri, sağlık, endüstriyel otomasyon, aydınlatma, akıllı şehirler şeklinde olacağı anlaşılmaktadır.

M2M teknolojilerinde standartlaşmanın sağlanması, M2M sistemlerinin ölçeklenebilir/yönetilebilir/güvenilir olması temel gereksinim olarak ifade edilmiştir. Bununla birlikte genel olarak M2M Sistemlerinin:

- Ölçeklenebilir, yönetilebilir ve güvenilir bir tasarıma sahip olması,
- Sistemin tamamının izlenebilirliğine,
- Güvenlik ihlallerinin tespitine,
- Büyük miktardaki cihazların yönetilebilirliğine
- Adreslenebilir olmasına,
- Gruplanabilir olmasına,
- Zaman gecikmeli veri iletimine
- Paket kayıplarını fark edebilecek ve önleyebilecek bir yapıda olmasına
- Düşük güç tüketimi ve bandgenişliği kullanımına

Olanak sağlaması önem arz etmektedir.

Hüresel şebekelerde ise 3G, LTE ve IMS ve NGN altyapıları ile birlikte şebekenin hemen hemen tüm noktalarından IP networklerine bağlantı olması nedeni ile İşletmeler tamamen Internet'e açık hale geldiği görülmektedir. Bu kapsamda;

- Haberleşme ve sinyalleşme kanallarına yönelik olabilecek saldırılara yönelik gerekli önlemlerin alınması,
- Şebeke tasarımlarının referans kullanıcı yerine trafik üretebilecek ya da şebekeye IP networklerden erişebilecek yetkisiz erişimlere göre kontrol mekanizmalarının sağlanması,
- Abonelerin kötü niyetli olarak diğer abonelere ya da şebeke ekipmanlarına zarar vermesine engellemeye yönelik tedbirlerin alınması,
- M2M cihaz ve şebeke arasında kriptografiye dayalı yetkilendirme mekanizmalarının sağlanması

Önem arz ettiği düşünülmektedir.

7. SONUÇ

Mobil haberleşme teknolojilerindeki gelişmelere paralel olarak hızla yaygınlaşan M2M uygulamaları devletlerin, yerel yönetimlerin ve bireylerin hayatında birçok kolaylıklar kazandırdığı gibi kişisel verilerin gizliliği, yaşam hakkının ihlali ve ülkeler arası siber saldırılarda önemli bir araç olarak kullanılma potansiyeline sahiptir. Literatürde yer alan araştırmalardan bahsedildiği üzere M2M uygulamaları ile ilgili her bir temel bileşene ait (donanım, yazılım, uygulama ve network gibi) güvenlik önlemlerin ayrı ayrı değerlendirilmesi/uygulanması gerekmektedir.

ETSI, IEEE, 3GPP başta olmak üzere spesifik bileşenlere ait güvenlik standartlarının uygulanması ve bunların kontrolü her bir ülke için yasa yapıcı veya regülasyon kurumları tarafından sıkıca takip edilmesi gereken hususlardır. Ekosisteme çok ciddi katkıları olan bu tür uygulamaların yeni nesil haberleşme altyapıları, modüle cihazlar ve çok fonksiyonlu uygulamalar ile hayatımızın bir parçası olacağı gerçeği kaçınılmaz gözükmektedir. Bu tür uygulamaların çoğunlukla internet altyapılarını kullanacağı düşünülerek başta internet altyapısı ile ilgili güvenlik koşullarının iyileştirilmesi ve kişisel verilerin korunması ile ilkelerin tüm dünyada hayata geçirilmesi önem arz etmektedir. Yeterli güvenlik altyapısına sahip olmayan tüm makineler arası iletişim çözümleri illegal olarak üçüncü taraflarca erişilecek sistemlerden dolayı verilerinin elde edilebildiği, bozulabildiği veya servis engellemesine maruz kalabileceği değerlendirilmektedir.

8. KAYNAKLAR

- 1- Borgia E., The Internet of Things vision: Key features, applications and open issues, *Computer Communications* 54 (2014) 1–31
- 2- Wu G., Talwar S., Johnsson K., M2M: From Mobile to Embedded Internet, *IEEE Communications Magazine* 49 (2011) 36-43
- 3- Atzori L., Iera A., Morabito G., The Internet of Things: A survey, *Computer Networks* 54 (2010) 2787–2805
- 4- Ricciato F., Coluccia A., Alconzo A., A review of DoS attack models for 3G cellular networks from a system-design perspective, *Computer Communications* 33 (2010) 551–558
- 5- Pereira C., Aguiar A., Towards Efficient Mobile M2M Communications: Survey and Open Challenges, *Sensors* 2014, 14, 19582-19608
- 6- Gubbi J. Buyya R., Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems* 29 (2013) 1645–1660
- 7- Fengming Cao F., Zhong Fan Z., Cellular M2M Network Access Congestion: Performance Analysis and Solutions, 1st International Workshop on Internet of Things Communications and Technologies, 2013
- 8- Hongsong C., Security and Trust Research in M2M System, *Vehicular Electronics and Safety (ICVES)*, 2011 IEEE International Conference, 286 – 2901
- 9- Lu R., Xu Li X., Liang X., GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications, *Communications Magazine, IEEE* , 2011, (Volume:49 , Issue: 4), 28-35
- 10- Cha, I., Shah, Y., Schmidt, A. U., Leicher, A., & Meyerstein, M. V. (2009). Trust in M2M communication. *Vehicular Technology Magazine, IEEE*, 4(3), 69-75.
- 11- J. Kim, J. Lee, J. Kim, and J. Yun, “M2M service platforms: Survey, issues, and enabling technologies,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 61–76, 2014.
- 12- Zhang Y., Home M2M Networks: Architectures, Standards, and QoS Improvement, *Communications Magazine, IEEE* ,2011 (Volume:49 , Issue: 4),44-52
- 13- Walczak, D., Wrzos, M., Radziuk, A., Lewandowski, B., & Mazurek, C. (2012, July). Machine-to-Machine communication and data processing approach in Future Internet applications. In *Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on* (pp. 1-5). IEEE.
- 14- Murrnets I., Anomaly Detection in Cellular Machine-to-Machine Communications, *Communications (ICC)*, 2013 IEEE, 2013, 2138-2143
- 15- Pandey, S., Choi, M. J., Kim, M. S., & Hong, J. W. (2011, September). Towards management of machine to machine networks. In *Network Operations and Management Symposium (APNOMS), 2011 13th Asia-Pacific* (pp. 1-7). IEEE.
- 16- Katusic, D., Weber, M., Bojic, I., Jezic, G., & Kusek, M. (2012, September). Market, standardization, and regulation development in machine-to-machine communications. In *Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference on* (pp. 1-7). IEEE.

- 17- Bojic, I., Jezic, G., Katusic, D., Desic, S., Kusek, M., & Huljenic, D. (2012, September). Communication in machine-to-machine environments. In *Proceedings of the Fifth Balkan Conference in Informatics* (pp. 283-286). ACM.
- 18- Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, 20(8), 2481-2501.
- 19- Saied Y., A survey of collaborative services and security-related issues in modern wireless Ad-Hoc communications, *Journal of Network and Computer Applications* 45 (2014) 215–227
- 20- Internet: Probe-IT, ETSI M2M Standarts, http://www.probe-it.eu/wp-content/uploads/2012/06/K1_ETSI-M2M-oneM2M-and-the-need-for-semantic-IoTWeek2012.pdf, Son Erişim: 18/11/2020
- 21- Chen, Kwang-Cheng, and Shao-Yu Lien. "Machine-to-machine communications: Technologies and challenges." *Ad Hoc Networks* 18 (2014): 3-23.
- 22- Luis Barriga, et al. "M2M Remote-Subscription Management", *Ericsson Review* 2011
- 23- M. J. Booyen, J. S. Gilmore, S. Zeadally and G. J. van Rooyen, "Machine-to-machine (M2M) communications in vehicular networks," *KSII Transactions on Internet and Information Systems*, vol. 6, no. 2, pp. 480–497, Feb. 2012.
- 24- Bojic, I., Granjal, J., Monteiro, E., Katusic, D., Skocir, P., Kusek, M., & Jezic, G. Communication and Security in Machine-to-Machine Systems.
- 25- Galetić, Vedran, et al. "Basic principles of Machine-to-Machine communication and its impact on telecommunications industry." *MIPRO, 2011 Proceedings of the 34th International Convention. IEEE*, 2011.
- 26- I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M. Meyerstein, "Security and trust for M2M communications," presented at WWRP Meeting 22, Paris, France, 2009.
- 27- Chen, M.; Wan, J.; Gonzalez, S.; Liao, X.; Leung, V. A Survey of Recent Developments in Home M2M Networks. *IEEE Commun. Surv. Tutor.* 2014, 16, 98–114.
- 28- R. Roman, P. Najera, J. Lopez, Securing the internet of things, *IEEE Computer* 44 (9) (2011) 51–58.
- 29- Taleb, Tarik, and Andreas Kunz. "Machine type communications in 3GPP networks: potential, challenges, and solutions." *Communications Magazine, IEEE* 50.3 (2012): 178-184.
- 30- Cao, J., Ma, M., Li, H., Zhang, Y., & Luo, Z. (2014). A survey on security aspects for LTE and LTE-A networks. *Communications Surveys & Tutorials, IEEE*, 16(1), 283-302.
- 31- Zhang, Y., Yu, R., Nekovee, M., Liu, Y., Xie, S., & Gjessing, S. (2012). Cognitive machine-to-machine communications: visions and potentials for the smart grid. *Network, IEEE*, 26(3), 6-13.
- 32- Wan, J., Chen, M., Xia, F., Di, L., & Zhou, K. (2013). From machine-to-machine communications towards cyber-physical systems. *Computer Science and Information Systems*, 10(3), 1105-1128.
- 33- A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the Random Access Channel of LTE and LTE-A Suitable for M2M Communications? A Survey of Alternatives," *IEEE Surveys and Tutorials on Commun.*, vol. 16, no. 1, Jan. 2014, pp. 4–16.
- 34- C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, "Data mining for Internet of things: A survey," *Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1–21, Nov. 2013.

- 35- Ksentini, Adlen, Yassine Hadjadj-Aoul, and Tarik Taleb. "Cellular-based machine-to-machine: overload control." *Network, IEEE* 26.6 (2012): 54-60.
- 36- S. Mirzadeh, H. Cruickshank, and R. Tafazolli, "Secure device pairing: A survey," *IEEE Commun. Surv.-Tuts.*, vol. 16, no. 1, pp. 1–24, Dec. 2013.
- 37- M. Chen, J. Wan, and F. Li, "Machine-to-Machine Communications: Architectures, Standards and Applications," *KSI Transactions on Internet & Information Systems*, vol. 6, pp. 480-497, 2012.
- 38- Chen, M., Gonzalez, S., Leung, V., Zhang, Q., & Li, M. (2010). A 2G-RFID-based e-healthcare system. *Wireless Communications, IEEE*, 17(1), 37-43.
- 39- Pereira C., Aguiar A., Towards Efficient Mobile M2M Communications: Survey and Open Challenges, *Sensors* 2014, 14, 19582-19608
- 40- Cha, Inhyok, et al. "Trust in M2M communication." *Vehicular Technology Magazine, IEEE* 4.3 (2009): 69-75.
- 41- Internet: beecham research, Towards Smart Cities, <http://m2msummit.pl/wp-content/uploads/sites/6/2014/10/brl-m2m-towards-smart-cities-wp-2014-sep.pdf>, Son Erişim: 18/11/2020
- 42- Internet: Ericsson, M2M: the Internet of 50 billion devices, http://www.ericsson.com/au/res/region_RASO/docs/2010/ericsson_50_billion_paper.pdf, Son Erişim: 18/11/2020
- 43- Internet: Huawei, M2M: the Internet of 50 billion devices, <http://www.huawei.com/en/about-huawei/publications/winwin-magazine/hw-079060.htm>, Son Erişim: 18/11/2020
- 44- Internet: Hunz, Machine-to-machine (M2M) security, http://events.ccc.de/camp/2011/Fahrplan/attachments/1883_m2m.pdf, Son Erişim: 18/11/2020
- 45- Internet: IEEE, M2M Service Architecture: Delivering M2M Services Over Heterogeneous Networks, http://www.ieee-cqr.org/2012/May17/Session%209/Chonggang_Wang_InterDigital.pdf, Son Erişim: 18/11/2020
- 46- Internet: NEC, Standards for Machine-to-Machine communication, <http://www.cambridgewireless.co.uk/presentation/joergswetina010713.pdf>, Son Erişim: 18/11/2020