İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

5G MOBİL TEKNOLOJİSİNİN GETİRDİĞİ YENİLİKLER VE UYGULAMALAR

Rızvan YILMAZ

114691012

Prof. Dr. Şule IŞINSU ÖZMEN

İSTANBUL

2019

5G Mobil Teknolojisinin Getirdiği Yenilikler ve Uygulamalar

5G Mobile Technology's Innovations and Applications

Rıdvan YILMAZ

114691012

Tez Danışmanı : **Prof. Dr. Şule IŞINSU ÖZMEN** **(İmza)** .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : **Prof. Dr. Cem Sefa SÜTCÜ** **(İmza)** .....
Marmara Üniversitesi

Dr. Öğr. Üyesi Mehmet Bedii KAYA (İmza) .....
İstanbul Bilgi Üniversitesi

Tezin Onaylandığı Tarih : 13 Haziran 2019
Toplam Sayfa Sayısı : 127

Anahtar Kelimeler (Türkçe)
1) 5G
2) Nesnelerin İnterneti
3) Büyük Veri
4) Güvenlik
5) Mobil Haberleşme

Anahtar Kelimeler (İngilizce)
1) 5G
2) Internet of Things
3) Big Data
4) Security
5) Mobile Communications

ÖNSÖZ

Tez çalışmam sırasında kıymetli bilgi, birikim ve tecrübeleri ile bana yol gösteren değerli danışman hocam Prof. Dr. Şule IŞINSU ÖZMEN' e, yüksek lisans eğitimim boyunca yardımlarını esirgemeyen Doç. Dr. Leyla BERBER'e ve Dr. Öğr. Üyesi Mehmet Bedii KAYA' ya, Mobil haberleşme dersini bizlere sevdiren Dr. öğr. Üyesi Tayfun ACARER'e teşekkür ve saygılarımı sunarım.

Ve çalışmalarım boyunca maddi ve manevi destekleriyle her zaman yanımda olan kıymetli eşim Hasibe Yılmaz ve Oğlum Ali Eymen'e sonsuz teşekkürler ederim.

Rıdvan YILMAZ

İstanbul

İÇİNDEKİLER

KISALTMALAR

1N/1G	: Birinci Nesil Haberleşeme
2N/2G	: İkinci Nesil Haberleşeme
3N/3G	: Üçüncü Nesil Haberleşeme
4N/4G	: Dördüncü Nesil Haberleşme
4.5G	:4.5 Nesil Haberleşme
3GPP	: 3rd Generation Partnership Project
AMPS	: Advanced Mobile Phone System
BSC	: Base Station Controller
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
BTS	: Base Transceiver Sytem
CDMA	: Code Dvision Multiple Acess
CEPT	: Conferenceof European Post Telecommunications
CRM	: Customer Relationship Management
D-AMPS	: Digital-Advanced Mobile Phone System
EDGE	: Enhanced Data rates for Global Evolution
ERP	: Enterprise Resource Planning
FDMA	: Freguency Division Multiple Access
GPRS	: General Packet Radio Service
GSM	: Global System for Mobile
HSCSD	: High-Speed Circuit-Switched Data
HSDPA	: High Speed Downlink Packet Access
HSUPA	: High Speed Uplink Packet Access
IMT-2000	: International Mobile Telecommunications

IP	: Internet Protocol :
ITU	: International Telecommunications Unıon
LTE	: Long Time Evolution
LTE-A	: Long Term Evolution -Advanced)
M2M	: Machine to Machine
METIS	: Mobile and wireless communications Enablers for Twenty-twenty(2020) information Society
MS	: Mobile Station
N-ISDN	: Narrow band Integrated Sytem Digital Network
NMT	: Nordic Mobile Telephone
PDC	: Pacific Digital Cellular
SMS	: Short Message Service
TACS	: Toplam Erişim İletişim Sistemi
TDMA	: Zamana Bölümlü Çoklu Erişim
TI	: Standards Committee
TIA	: Telekomünikasyon Endüstri Birliği
TK	: Telekomünikasyon Kurumu
UMTS	: Short Message Service
VOIP	: Voice over İnternet Protocol
WAP	: Wireless Application Protocol

ŞEKİL LİSTESİ

TABLO LİSTESİ

ABSTRACT

In the world there are many changes and developments in the field of technology. These developments directly affect the education, science, health, work and social life of mankind. Changes in the field of technology are described as the Fourth Industrial Revolution. This revolution has emerged from the Internet of Things (IOT-Internet of Things), technologies such as M2Machine to Machine, and applications. The main reason for the development of these technology developments is the developments in their infrastructure in mobile communication networks. The development in this mobile communication sector has made it possible for human beings to have access to information on the internet from mobile computers to mobile phones. People have access to the requested information from anywhere they want independent of time.

The wireless mobile communication system has evolved to this day. It is expected that the Fifth Generation and beyond technologies will start in 2020 starting with the First Generation communication system. The first generation (1G) technology includes the analog system and the possibility of voice communication. Second Generation (2G) technology has been introduced to the digital system as well as voice transmission as well as data transmission (GPRS and EDGE). The third generation (3G) technology has been the result of the fast speed of the data speed level with the transition from Kb \ s to Mb \ s, resulting in an increase in mobile devices and applications. These developments have changed the habits and expectations of the users and the need to reach more data at higher speed has emerged. These needs were improved in the Fourth Generation (4G) by increasing the speed level to compare the data transmission trend rather than the tendency to transmit the sound. In parallel with the development of the Fourth Generation technologies, the studies of the Fifth Generation (5G) technology and the standard studies have been initiated.

The Fourth Generation Technology (5G) is a platform that provides and stores a large data communication that connects everything with each other, while using the Fourth Generation (4G) technologies with mobile devices to connect people through data transmission. Studies on the Fifth Generation (5G) standardization are planned to be completed by 2020 and brought into the product. In the year 2020, the Fifth Generation (5G) technologies, which will collect the same platform for society and society in the world, will shape the countries' industry, technology and science policies and are expected to be used within a few years.

ithin the scope of this thesis study, the technological innovations of the Fifth Generation communication system to the automotive, health, energy, agriculture, smart cities, transportation and logistics sectors and the circulation of the new risky data that may occur from these sectors from the fifth generation communication system and in-network and non-network data security have been examined. . As a result of these investigations, the technological structure of the Fifth Generation communication system and the security vulnerabilities of the data coming from the smart devices and the possible threats of the attack were presented.

ÖZET

Dünyada teknoloji alanında çok büyük değişim ve ilerlemeler kaydedilmektedir. Bu gelişmeler insanoğlunun eğitim, bilim, sağlık, çalışma ve sosyal hayatını doğrudan etkilemektedir. Teknoloji alanında değişimler Dördüncü Sanayi devrimi olarak nitelendirilmektedir. Bu devrim nesnelerin interneti (IOT-Internet of Things), makinelerin birbirleriyle haberleşmesi (M2Machine to Machine) gibi teknolojiler düşünceleri ve uygulamaları ortaya çıkmıştır. Bu teknoloji gelişimlerin ortaya çıkmasının asıl nedeni mobil haberleşme şebekelerinde alt yapılarındaki gelişmelerdir. Bu mobil haberleşme sektöründeki gelişim insanoğlunun internet üzerindeki bilgiye ulaşımını sabit bilgisayarlardan hareketli akıllı telefonlar yani mobil olmasını sağlamıştır. İnsanlar zaman ve mekândan bağımsız olarak istedikleri her yerden istenilen bilgiye ulaşım sağlamaktadır.

Kablosuz mobil haberleşme sistemi günümüze kadar evrim geçirmiştir. Birinci Nesil haberleşme sisteminden başlayıp 2020 yılında Beşinci Nesil ve ötesi teknolojilerin kullanıma girmesi beklenmektedir. Birinci Nesil (1G) teknolojisi analog sistemi içerisin de ses iletişimi imkânı tanınmıştır. İkinci Nesil (2G) teknolojisi analog sistemden sayısal sisteme dönüşmesi ile beraber ses iletiminin yanında veri iletimi (GPRS ve EDGE) gerçekleştirerek görüntülü konuşma, video izleme, müzik dinleme gibi özelliklerle kullanıcılar tanışmıştır. Üçüncü Nesil (3G) teknolojisi veri hızı seviyesi Kb\s den Mb\s geçişi ile hızlı olma özelliği sayesinde kullanıcıların mobil cihazların ve uygulamaların artışına neden olmuştur. Bu gelişmeler kullanıcıların alışkanlıklarını ve beklentilerini değiştirerek daha yüksel hızda daha çok veriye ulaşma ihtiyaçları ortaya çıkarmıştır. Bu ihtiyaçlar ses iletimi eğiliminin yerine veri iletim eğilimini karşılaştırmak üzere hız seviyesi artırılarak Dördüncü Nesil (4G) geliştirildi. Dördüncü Nesil teknolojilerin gelişimi devam ederken paralelinde Beşinci Nesil (5G) teknolojisinin araştırmaları gereksinimleri ve standart çalışmaları başlatılarak devam etmektedir.

Dördüncü Nesil (4G) teknolojiler mobil cihazlarla kullanılarak veri iletimi üzerinden, insanları birbirine bağlarken, Beşinci Nesil Teknoloji (5G) ise her şeyi birbirine bağlayan birçok altyapıyı kullanacak büyük bir veri iletişimi sağlayacak ve depolayacak platform dur. Beşinci Nesil (5G) standardizasyon ile ilgili yapılan çalışmaların 2020 yılına kadar sonlandırılması ve ürün haline getirilmesi planlanmaktadır. 2020 yılında dünyada toplumu ve toplumun kullandığı her bir nesneyi aynı platform toplayacak. Beşinci Nesil (5G) teknolojileri ülkelerin sanayi, teknoloji, bilim politika alanınd şekillendireceği ve birkaç yıl içine kullanılması öngörülmektedir.

Bu tez çalışmasının kapsamı, Beşinci Nesil haberleşme sisteminin Otomotiv, sağlık, Enerji, Tarım, Akıllı şehirler, Ulaşım ve lojistik sektörlerine getireceği teknolojik yenilikleri ve bu sektörlerden oluşabilecek yeni riskli verilerinin Beşinci nesil haberleşme sisteminden dolaşımı ve şebeke içi, şebeke dışı veri güvenliği konusunda incelemeler yapılmıştır. Bu incelemeler sonucunda Beşinci Nesil haberleşme sisteminin teknolojik yapısı ve akıllı cihazlardan şebeke içerisine gelecek verilerin güvenlik zafiyetleri ve olası saldırı tehditleri ilgili çalışma ve öneriler ortaya konulmuştur.

1.GİRİŞ

Dünyada Telekomünikasyon teknolojisinde yaşanan hızlı gelişmeler toplumları birbirlerini yakınlaştırarak sosyal hayatta, ticari ve iktisadi hayatta yeni talepler ve ihtiyaçlar oluşturmaktadır. Bu ihtiyaçlar teknoloji üreticilerinin üzerinde baskı oluşturmasına yol açmış, teknolojilerin gelişmesini hızlandırmıştır.

1970'li yılların sonunda mobil haberleşme sistemlerinin ilk olarak Birinci Nesil (1N) hücresel analog mobil haberleşme sistemi sadece ses temelli hizmetler sunmasıyla hayatımıza girmeye başlamıştır. 1991 yıllında İkinci Nesil (2N) gelişimiyle analog yapıdan sayısal teknolojisine dönüşümü başlayarak haberleşme teknolojisinde ses hizmetinin yanında düşük hızlarda veri iletimi hizmetleri tüketicilere sunulmuştur. İkinci Nesil (2N) sistemin düşük hızda yapılan veri iletiminin tüketicilerin talepleri karşısında yetersiz kalmıştır. Bu nedenle yapılan yeni teknoloji çalışmaları neticesinde 2000'li yılların başlarında Üçüncü Nesil (3N) teknolojisi ortaya çıkmış ve lisanslar verilmeye başlanmıştır. Üçüncü Nesil (3N) ile ses hizmetinin yanında veri iletişimi yüksek hızlara ulaşmış internet ve görüntülü görüşmeler kullanıcılar arasında yaygınlaşmaya başlamıştır. Günümüzde Dördüncü Nesil (4N) LTE olarak adlandırılan, tüketicinin istediği zaman, mekândan bağımsız olarak GSM şebekelerini kullanarak bilgiye erişmektedir.

Dördüncü Nesil (4N) teknolojisi haberleşme sektöründe iki ayrı piyasada faaliyet gösteren mobil ve sabit işletmelerin yeni yatırımları ile telefon alt yapısından internet hizmetleri, kablo televizyon şebekeleri üzerinden ses ve internet hizmetleri, mobil telefonlar üzerinden veri iletişimi her şebekede sunulmaya başlamıştır. Buna paralel olarak akıllı telefon pazarı çok hızla gelişmekte, kullanıcılar üzerinden sunulan yeni hizmetler ve mobil uygulamalar günlük hayatta tüketicilerin ve işletmecilerin hayatlarını kolaylaştıracak şekilde yoğun kullanılmaktadır.

Beşinci nesil mobil teknoloji (5G), 2020 ve ötesindeki talepleri ve iş bağlamlarını ele alacak şekilde konumlandırılmıştır. Tamamen mobil ve bağlantılı bir topluma olanak sağlaması ve sosyal, ekonomik dönüşümleri günümüzde

çoğunun üretkenliği, sürdürülebilirliği ve refahı da dahil olmak üzere birçok yönden güçlendirmesi beklenmektedir. Tamamen mobil ve bağlantılı bir toplumun talepleri, bağlantı, trafik ve veri yoğunluğu / hacmindeki muazzam büyüme, bunu mümkün kılmak için gerekli çok katmanlı yoğunlaştırma, geniş kullanım alanı örnekleri ve yeni uygulamalar beraberinde büyük veriler beklenmektedir.

Beşinci nesil mobil teknoloji (5G), insanlar arasında veri iletişiminin ötesinde bir teknoloji sunmaktadır. Makinelerin kendi aralarında (Machine to Machine-M2M) iletişim halinde olduğu, Nesnelerin İnterneti (Internet of Things-IoT) özellikleri ile insanların makineler arasında akıllı cihazlarla üzerinden etkileşim halinde olduğu tüm hayatı ve tüm dünyayı birbirine bağlayan platformdur. Bu etkileşimler bu platformun üzerinde çok büyük bir veri oluşturacaktır.

Tezimizin ikinci bölümünde, Beşinci Nesil önceki mobil haberleşme sisteminin veri güvenliği, gizlilik sorunları ve saldırı türleri üzerinde araştırmalar yapılmıştır. Üçüncü bölümde, Beşinci nesil teknolojisinin haberleşme sistemine getireceği yeni mimari alt yapı yenilikleri, standardizasyonlar, Dünyada yapılan Beşinci nesil teknolojik çalışmalar incelenmiştir. Dördüncü bölümde, Otomotiv, Enerji, Lojistik, Tarım, Sağlık sektörlerinde gelişen teknolojileri incelenerek ortaya çıkan yeni riskli verilerin Beşinci nesil mobil haberleşme şebekesindeki dolaşımı incelemesi yapılmıştır. Beşinci bölümde, diğer bölümlerde yapılan incelemeler sonucunda şebeke içi ve şebeke dışından gelecek veri güvenlik zafiyetleri ve olası saldırı türlerinin ortaya konulmuştur. Sonuç bölümünde ise Beşinci nesil haberleşme sisteminin güvenlik sorunların ve saldırı tehditleri yaşayabileceği ve bu sorunların giderilmesi konularında değerlendirmeler yapılmıştır.

.

BİRİNCİ BÖLÜM

BEŞİNCİ NESİL ÖNCESİ MOBİL İLETİŞİM TEKNOLOJİLERİ VERİ GÜVENLİK SALDIRILARI

1.1 GİRİŞ

İletişim, *"Duygu, düşünce veya bilgilerin akla gelebilecek her türlü yolla başkalarına aktarılması, bildirişim, haberleşme, komünikasyon."* Olarak tanımlanmaktadır.[1] Buradan yola çıkarak iletişimi üretilmiş ya da edinilmiş her türlü verinin aktarım çabası olarak tanımlamak yanlış olmayacaktır.

Mobilete kavramı, bir yerden bir yere veya bir durumdan bir duruma geçişi yani hareketliliği tanımlamaktadır. Bu kavram insanın varoluşuna kadar gitmekle birlikte günümüzde sürekli hareket halinde olan ve aynı zaman sürekli iletişim kurma ve veri alışverişi ihtiyacı duyan insanların her an bağlantıda kalmasını ifade etmektedir.[2]

Mobilete harekete müsaade eden hemen her şeyi ve durumu kapsamaktadır. Günümüz yaşamın şeklinde insan sürekli yer değiştirme ihtiyacı duymakla birlikte buna ek olarak sürekli bağlı kalma ve iletişim kurma ihtiyacı da hissetmektedir. Anlaşılacağı üzere iletişim telekomünikasyonu da kapsamakta ve günümüz insan ihtiyaçları daimî olarak her yerden internete bağlı kalma arzusu duymaktadır.

Bu bağlamda birinci nesil hücresel teknolojiler olarak bilinen 1G, artan taleplerdeki beklentilerin karşılanmasında 2G, 3G, 4G ve 5G teknolojilerinin, gelişmesine önderlik etmiştir.

---

[1] Türk Dil Kurumu, Büyük Türkçe Sözlük

[2] http://www.karel.com.tr/sites/default/files/belge/doc/ucap/karel_makale_mobilite.pdf E.T.: 18.11.2018

Bu gelişmeler sonucunda ses iletişiminden veri iletişimine mobil cihazların ve mobil uygulamaların artmasına neden olmuştur. İnsanlar artık büyük çoğunluğunu mobil cihazlar üzerinde kullanılan uygulamalar ile vakit geçirmektedir. Bu da kullanıcıların mobil cihazlar üzerinde tutukları kişiye özgü verilerin ele geçirilmesi için saldırganların açık tehdit haline gelmiştir. Tezimizin ikinci bölümünde 5G öncesi mobil haberleşme sistemlerinin getirdiği yenilikleri ve bu yeniliklerle insanoğlunun dijital sistemlere dönüşümü sırasında oluşabilecek veri güvenlik saldırılarını neler olabileceğini incelemesi yapılmıştır.

1.2 Birinci Nesil Mobil iletişim Teknoloji

İnsanoğlunun hayatında gelişen teknoloji ve ihtiyaçları ortaya çıkması ile 1970'li yılların başlangıcında Kablosuz Mobil İletişim sistemleri alanlarında bilim adamlarını çalışmalar başlatılmıştır. Çalışmalar neticesinde hücresel haberleşme sistemlerinin geliştirilmesi Kablosuz Mobil Sistemleri teknolojisi en önemli atılımlar olmuştur.

Birinci Nesil haberleşme sistemin en önemli özelliği hücresel alt yapısına sahip olması, bu özellik sayesinde kullanıcılar sistemi kullanmaya başladığında hücreler arasında dolaşarak etkili bir şekilde kullanmaktadırlar. Bu teknolojinin temel mimarisinde radyo sinyallerinin analog sinyallere aktarı oluşturmaktadır. Analog sistemlerde sinyalleri biçimleri değiştirmeden sonsuz ve sürekli şekilde havadan gönderilmektedir. Telsiz haberleşmesi kullanılmaya başladığından beri bu teknoloji kullanılmaktadır.[3]

Birinci nesil sistemlerde haberleşme tamamen analog şebekeler üzerinden ses trafiği oluşturmaktadır. Ses verisi şebekeler arasında dolaşım yaparak telefon değiştirmeden yurt içinde ve yurt dışı seyahatlerde kullanımına olanak sağlamaktadır.

[3] ERTUNÇ Engin,3N Mobil Haberleşme Sistemlerinde Kapsama Alanı ve Hizmet Kalitesi Denetimlerine İlişkin Ölçüm ve analiz Yöntemleri: Dünya Uygulamaları ve Türkiye Önerileri, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, Kasım 2011, s.7.

Birinci Nesil Teknolojisi evre anahtarlamalı sistemler, analog iletişim teknikleri alt yapısı ile düşük kaliteli ses veri trafiğini taşıyacak şekilde tasarlanmıştı. Bu neden dolayı radyo sinyallerinin analog sinyallere aktarılmasından dolayı sadece arama yapma imkânı tanımaktadır.

1.2.1 Birinci Nesil Veri Güvenliğindeki Sıkıntılar

Kanallar içersin de dolaşan ses verisinin kalitesi çok düşük olmaktadır. Ses verisinin transfer hızı ortalama 9 Kbit/s 'dir. Bu neden dolayı veri (data) imkânı sağlanamamıştır. Ses verisinin analog sinyaller üzerinden kullanılması, elektromanyetik girişime (enterferans) karşı koruma zayıflığına neden olmaktadır Böylelikle hem üçüncü kişiler tarafından haberleşmenin çözülmesini ve dinlenmesini kolaylaştırmakta hem de haberleşme bağlantıların kolay kopmasını sebep olmuştur.[4]

Birinci Nesil alt yapı sisteminde yasal olmayan kullanıcılar, veri hattını kolayca ele geçirerek görüşmeler yaparak yasal kullanıcılara ücretlendirme yansımasına neden olmaktadır. Diğer önemli sorun ise yasal kullanıcılar arasında gerçekleşen konuşmaların şifreli yapılmaması nedeniyle ses veri hattında yasal olmayan kişiler tarafından dinlemeler yapılmaktadır. Analog sistemlere verinin güvensiz oluğu ortaya çıkmıştır. Bu sıkıntıların çözümü için İkinci Nesil Teknolojinin geliştirilmesine neden olmuştur.[5]

1.3 İkinci Nesil Mobil iletişim Teknoloji

Birinci Nesil analog sistemlerinde sadece ses verisi üzerinden hizmet sunabilmesi, hizmet kalitesinde ve ses veri güvenliğindeki yaşanan sıkıntılar oluşması, bu teknoloji hizmet çeşitliliğinin sağlanmaması nedeniyle sayısal haberleşeme sistemlerinin araştırmalarına ve gelişimine sağlanarak Birinci Nesil

[4] ERTUNÇ Engin,3N Mobil Haberleşme Sistemlerinde Kapsama Alanı ve Hizmet Kalitesi Denetimlerine İlişkin Ölçüm ve analiz Yöntemleri: Dünya Uygulamaları ve Türkiye Önerileri, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, Kasım 2011, s.8.
[5] DARICI Ahmet, 3.Nesil Mobil Haberleşme Sistemleri, Telekomünikasyon Kurumu, Ankara 2002, s.7

haberleşme sistemlerinin kullanımı azalmaya başlayarak, sayısal sistem olan İkinci Nesil haberleşme sisteminin yaygın bir şekilde kullanım başlamıştır.

İkinci nesil Hücresel ağ sitemi alt yapısını kullanan kablosuz telefon teknolojidir. Birinci Neslinin İkinci Nesil'e göre avantajı haberleşme iletişimin analog sisteminden sayısal sisteme dönüşmesidir. Sayısal sistemin en önemli özelliklerinde bir tanesi cep telefonlar üzerinden gerçekleştirilen bağlantıları, gönderilen ve alınan verilerin Birinci Nesil sisteminde olduğu gibi iki adet kalana ihtiyaç duymadan tek bir kanal üzerinden sağlanmasıdır. Bu özelliği kısa örneklendirmek gerekir ise cep telefonları gerçekleşince ses ve veri tek bir kanal üzerinden gönderilir ve alınır. Bu zaman zarfında görüşme devam ettiği sürece bu kanala başka kullanıcılar tarafından giriş yapılması mümkün değildir. Birinci Nesil sayısal haberleşme verinin şifrelemesiyle güvenilir bir alt yapı ile ses ve verinin yüksek kalitede ve kapasitede iletimini sağlar.

İkinci Nesil Sistemlerinin GSM alt yapısı geliştirilirken en öncelikli temel prensibi Ülkeler arasında dolaşımı sağlayacak sistemlerini desteklemesi, ses ve verinin iletiminde yüksek kapasite de özelliklerini sahip dijital haberleşme sistemi 'dir. Kuzey Amerika kıtasında Digital AMPS (D-AMPS), CDMAONE, Avrupa Kıtasında GSM sistemleri, Japonya'da ise PDC (Pacific Digital Cellular) birbirine yakın sistemler kullanılmaya başlanmıştı.

2G ve 2.5G sistemlerinde HSCSD (High Speed Circuit Switched Data), GPRS (General Packet Radio Service) ve EDGE (Enhanced Data Rates for GSM Evolution) bu teknolojiyi kullanan sistemlerdir.[6]

GPRS ile Noktadan Noktaya ve Noktadan çok noktaya veri iletimi yapılabilmektedir. Bu sistemin ana özelliği olan kullanılan paket aktarım alt yapısı ile verinin gönderim ve verinin alımı için IP teknoloji haberleşme sistemlerini ilham vermiştir. Dünyada kullanıcıların kullandıkları HSPA, UMTS, EDGE teknolojilerin alt yapısında GPRS sistemlerinin alt yapısı üzerine inşa edilmiştir.

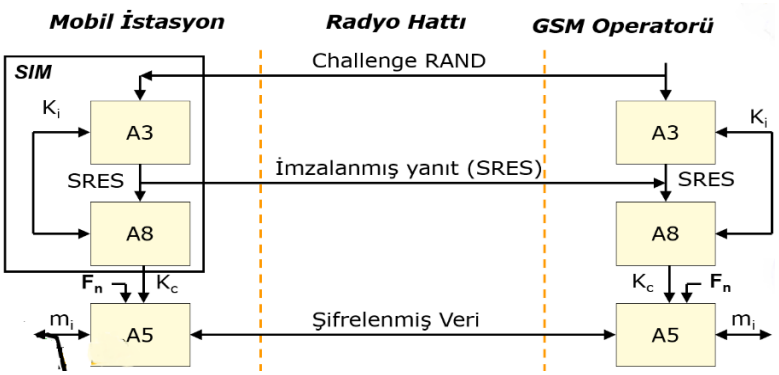
[6] Soy, Hakkı, Özdemir, Özgür ve Bayrak, Mehmet, G*elecek Nesil Mobil Haberleşme Sistemleri: 3G, 4G ve Ötesi.* Uşak Üniversitesi, Uşak, 2012,s.4

GPRS sistemi geliştirilmiş alt yapı ile düşük ve yüksek hızlı verinin işaretlenip GSM ağları üzerinden daha etkin taşınması için bir iletişim imkân sunmaktadır. GPRS sisteminin standartlarında verinin depolama alt yapısı bulunmamaktır.

1.3.1 İkinci Nesil Veri Güvenliğindeki Sıkıntılar

İkinci Nesil Teknolojindeki gelişmeler neticesinde İnternet kullanımı, İşletmeciler için kurumsal mail hizmetleri, web sitelerinin içeriklerinin yaygınlaşması, internet üzerine müzik yayınlarının başlaması, sohbet uygulamalar, haber içerikli yayınlar, Mobil ticaret uygulamaları geliştirildi ve yaygınlaştı.

Bu uygulamalar gelişmesiyle ve yaygınlaşması çeşitli veri güvenliğini tehdit eden saldırı türleri ortaya çıkmıştır. Bu saldırılar SIM karta yönelik saldırılar, baz istasyonları, kablolu ve kablosuz hatlardan gelen tehditler, Mobil ortam virüsleri, solucan tehditleri, kontrol edilmemiş mesajlaşma suiistimal teknikleri olarak sınıflandırılabilmektedir.



Şekil 1 İkinci Nesil Veri Şifreleme Mimarisi

İkinci Nesil Teknolojindeki veri iletişimin sayısal alt yapı kullanıldığı için şifreleme algoritmaları kullanılmıştır. A3 şifreleme algoritması kimlik tanımlama, A8 şifreleme algoritmasında da kullanılan şifreleme üretimi yapılmıştır. Bazı bölgelerde A3/A8 yerine COMP128 algoritması ile ses/verinin şifrelenmesi için A5 algoritması kullanılmıştır. Bu algoritmalar veri güvenliğinin sağlanmasında yetersiz kalmış aşağıda belirteceğimiz tehditler ortaya çıkmaktadır.

1.3.1.1 SIM Kart Tehdit

SIM kartların üzerine **Ki** denilen abonenin oturum açmasını ve doğrulama yapabilmesini sağlayan gizli anahtar değeri vardır. Bu **Ki** değeri SIM kartında ve GSM ağ birimi olan tüm kullanıcıların bilgilerini ve konumlarının sağlandığı HLR biriminde saklanır. Bu **Ki** değeri hiçbir zaman havadan gönderilmemektedir. A3 ve A8 şifreleme algoritmalarıyla **Ki** değeri şifrelenmiştir. Saldırgan Ki değerini eriştiği zaman kullanıcının ses verisini ve hat üzerinden giden veriyi ele geçirebilmektedir. Saldırgan **Ki** değerine SIM kart saldırı veya SIM klonlama yöntemleriyle ele geçirmektedir.

1.3.1.2. Kablolu Hatlardan Gelen Tehditler

GSM şebekesinde verilerin taşındığı iletişim kanalları vardır. Bu kanallar Sho Mesaj Servisi (SMS), Supplementa Servis Verileri (USSD), Kablosuz Uygulama Protokolü (WAP) dir. GSM güncellemelerinde Geliştirilmiş Mesajlaşma Servisi (EMS) ve Multimedya Mesajlaşma servisi (MMS) gibi servislerde bulunmaktadır. GSM sevişlerindeki sorunlar ve güvenlik zafiyetleri nedeniyle bu servisler üzerinden saldıran kullanıcının internet üzerinden saldırı yöntemleri ile verileri elle geçirmeleri yapılmaktadır.[7]

1.3.1.3. Sahte Baz İstasyon Tehditleri

GSM alt yapısı kullanıcılara veri aktarımı baz istasyonları üzerinden yapılmaktadır. Baz istasyonları arasında kimlik doğrulama yapılmadığından saldırıyı yapanlar tarafından sahte baz istasyonları kurularak veriler ele geçirilmektedir.[8]

---

[7] Sağıroğlu, Şeref, Mohammed, Murad A, Mobil ortamlara yapılan saldırılar üzerine bir inceleme TUBAV Bilim Dergisi, Ankara, 2009,Sayı:2

8 Samet, Refik, Çelik Ömer Faruk, Sahte GSM Baz İstasyonu Saldırı Tespit Algoritması, Gazi Üniversitesi, Ankara, 2015

1.3.1.4. Tek Taraflı Kimlik Doğrulaması ve Man-in-The-Middle Saldırısı

Bu saldırı Kullanıcının kimlik doğrulama ağı üzerinden yapılmaktadır. Saldırgan abone olarak mobil ağ koduyla Bas istasyonu ile kullanıcı arasına girerek saldırı işlemini başlatır. Saldırgan Bas istasyonu gibi davranarak kullanıcıya kimlik doğrulaması yaptırmaz. Böylelikle saldırgan kullanıcı ile baz istasyonu arasına girerek gerekli bilgileri değiştirerek veya üreterek verilere ulaşabilmektedir.[9]

1.3.1.5. Şifreleme Algoritmalarına Yapılan Saldırılar

Kimlik Tanımlama A3 şifreleme, şifreleme üretiminde A8 algoritmaları kullanılmıştır. Bazı bölgelerde COMP128 veri şifreleme algoritması kullanılmıştır. 1998 yılına Wagner ve Golberg COMP128 veri şifreleme algoritmasının kırdıklarının açıklaması yapmışlardır. Yaptıkları saldırılarda iki dakika içersin de veriler toplamışlardır.

1.3.1.6. Dos Yöntemi ile Yapılan Saldırılar

Saldırgan GSM servisinin Dos saldırı yöntemiyle devre dışı bırakabilmektedir. Saldırgan erişim kanalı talep mesajı - CHANNEL REQUEST mesajını baz istasyonuna sürekli gönderdiğinde bas istasyonu cevap veremez hale getirmektedir. Bu saldırı yöntemi ile şebeke içersinde kullanıcı verilerinin güvenliği teklike altındadır.

1.4 Üçüncü Nesil Mobil iletişim Teknoloji

İkinci Nesil haberleşme sistemleri gelişiminde ortaya ses veri iletiminin yanı sıra mesajlaşma servisi, faks servisler gibi hizmetler geliştirilmiştir. Bu hizmetlerinin kullanıcılar tarafından kullanılmaya başlaması yeni taleplerin ve ihtiyaçlarının ortaya çıkmasına neden olmuştur. Kullanıcıların çoklu mobil uygulamalarına olan ilginin ve taleplerin giderek artması, bu eğilimin mevcut

9 Meyer, Ulrike, A Man-in the Middle Attack on UMTS, Darmstadt University of Technology Department of Computer Science Hochschulstrasse 10 D-64283 Darmstadt Germany

kullanılan sistemlerde karşılanamaması ve Dünya ülkelerinde haberleşme sistemlerinde bir bütünlük olmaması gibi nedenlerle yeni sistemlerin geliştirilmesi için arayışa girilmiş yapılan çalışmalar sonucunda Üçüncü Nesil haberleşme sistemi geliştirilmiştir.

Üçüncü nesil telekomünikasyon sisteminin çerçevesi 17 Mayıs 1865 yılında kurulan ve Türkiye'nin de kurucu üyeleri arasında yer aldığı Uluslararası Telekomünikasyon Birliği (International Telecommunications Unıon -ITU) tarafından belirlenmiştir. Üçüncü Nesil standartların teknolojisi sistemleri WiMAX, DECT, CDMA2000, UMTS, GSM, EDGE teknolojilerinden oluşmaktadır.

Üçüncü Nesil Teknolojisinde yapılan alt yapı gelişmeleri dünyada teknoloji dönüşümünün başlamasına neden olmuştur. Mobil cihaz ve mobil uygulamaların artmasına neden olmuştur. Kullanıcı mobil video konferansı, görüntülü arama, Mobil Tv, Mobil e-ticaret uygulamalarıyla bilgiye anlık ulaşımı sağlandı. 3dk bir MP3 müzik dosyasını 11 sn-15 dk arasında indirme olanağı sunmaktadır.

Kullanıcı tarafından üçüncü nesil baktığımızda teknolojisini gelişmesiyle Mobil Kullanıcı kavramları 1990 yıllarında ortaya çıkmıştır. Yapı olarak Mobil çalışanlar ve Mobil son kullanıcılar diye alt kola ayrılmıştır. Mobil Çalışanlar ve Mobil son kullanıcılar sunulan uygulamalarda iki ana kategoriye ayrılmak mümkündür.

Kurumsal Uygulamalar; Bilgi akışını mobil ortama taşıyarak, yönetici ve elemanların daha verimli çalışmalarına olanak tanımaktadır. Bu uygulamalar en basit örneği kurumsal bilgi aktarımı, E-posta, Satış Pazarlama on-line onay mekanizmalarıdır.

Bireysel Uygulamalar; Genel anlamda şahısların hayatını kolaylaştıran ve eğlence amaçlıdır. E-devlet, Facebook, Whats App, Instagram, gibi hizmetler olarak gruplandırılabilir. Mobil uygulamalar sayesinde kullanıcıların her türlü bilgilerin bu sistemler üzerinde dolaşmaya başlamıştır. Bazı riskleri ve veri güvenlik sıkıntılarını ortaya çıkarmaya başlamıştır.

1.4.1 Üçüncü Nesil Veri Güvenliğindeki Sıkıntılar

UMTS (3G) Saldırı Türleri	Kimlik Doğrulama (Authentication)	Gizlilik (Confidentiality)	Veri Bütünlüğü (Data Integrity)	Risk
Replay Attack	Evet	Hayır	Hayır	Düşük
Man-In-the-Middle (MiM) Attack	Evet	Evet	Evet	Yüksek
Brute Force Attack	Evet	Hayır	Evet	Orta
Eavesdropping Attack	Hayır	Evet	Hayır	Düşük
Impersonation of The User Attack	Evet	Hayır	Hayır	Düşük
Dictionary Attack	Evet	Hayır	Hayır	Düşük
Impersonation of The Network Attack	Evet	Hayır	Hayır	Düşük
Compromising AV In The Network Attack	Evet	Hayır	Hayır	Düşük
Denial of Service (DoS) Attack	Evet	Evet	Evet	Yüksek
Identity Catching Attack	Evet	Evet	Evet	Yüksek
Redirection Attack	Evet	Evet	Evet	Yüksek
Sequence Number Depletion Attack	Evet	Hayır	Hayır	Düşük
Roaming Attack	Evet	Evet	Evet	Yüksek
Bidding Down Attack	Hayır	Evet	Evet	Orta
Guessing Attack	Evet	Evet	Hayır	Orta
Substitution Attack	Evet	Evet	Evet	Yüksek
Disclosure Of User Identity(IMSI) Attack	Evet	Hayır	Hayır	Düşük
Packets Injection Attack	Hayır	Hayır	Evet	Düşük
Content Modification Attack	Hayır	Hayır	Evet	Düşük
Secret Key Exposure Attack	Evet	Evet	Evet	Yüksek

Tablo 1 Üçüncü Nesil Haberleşme Saldırı Atakları

Üçüncü Nesil haberleşme sistemlerinde veri güvenliğini, 128 bit şifreleme ve AKA (Authentication and Key Agreement) protokolleri kullanarak kimlik doğrulama yöntemleri ile sağlanmaya çalışılmıştır. GSM teknolojisine kullanılan güvenlik metotları kullanarak AKA protokolü geliştirilmiştir. GSM teknolojisine kullanılan A5 şifreleme algoritmasının kırılması nedeniyle kullanıcıların verilerinin korunması amacıyla KASUMI adı verilen 128 bitlik algoritma kullanılmıştır. Bu algoritma yeniden gönderim saldırı (Replay attack) tekniğine karşı koru yapmak ve sahte erişimlere izin vermemektedir.

Haberleşme sistemlerindeki gelişmeler beraberinde verinin korunması ve güvenlik algoritmaları da gelişmeler olmuştur. Bu algoritmalar beraberinde veriye ulaşma konusunda saldırı tipleri de değişmektedir. 2012 yılında Üçüncü Nesil Haberleşme sistemlerinde üç güvenlik veri faktörü olan kimlik doğrulama, gizlilik,

veri bütünlüğü konusunda analiz yapılmıştır. Kullanıcıların mobil üzerinden veriye ulaşma talepleri artmasıyla veriye yönelik saldırı atakları değişiklik göstermektedir. En riskli veri saldırıları aşağıda açıklanmıştır.

1.4.1.1 Man-In-the-Middle Saldırısı

Saldırgan abone olarak mobil ağ koduyla Baz istasyonu ile kullanıcı arasına girerek saldırı işlemini başlatır. Saldırgan kullanıcı ile Baz istasyonları arasındaki verileri iki tarafından farkında olmadan ulaşabilmektedir. Saldırgan kullanıcının MS ağındaki iletişimini dinleme, silme veya kullanıcı bilgilerini ele geçirebilir, değiştirebilir.

MiM saldırı yöntemi en çok kullanılan ve tehlikeli bir saldırı türüdür. GSM, GPRS ve Özellikle UMTS alt yapılarında saldırıları algılamak için büyük bütçeli analiz yöntemleri geliştirilmiştir.

1.4.1.2 Hizmet Yavaşlatma (Denial of Service) Saldırısı

Saldırgan GSM üzerinden gerçekleşen hizmet servislerin ulaşımını engellemek, yavaşlatmak için yapılan saldırı tipidir. Kullanıcı GSM şebekesine kimlik doğrulama yapmadan gerçekleşmektedir. GSM ağ yapısında sahte ve gerçek trafiği sistemler ayırt edememektedir. Bu yöntem GSM altyapısındaki servislere sürekli istek göndererek hizmet sunucularının veya veri ağının kaynaklarını tüketerek çalışmaz hale gelmektedir. Servislerin çalışmaz hala getirilmesi ile diğer saldırı yöntemleri ile kullanıcıların verileri saldırılar yapılmaktadır.

1.4.1.3 Yönlendirme (Redirection) Saldırısı

Çoklu mobil ağlarına yapılan saldırı yöntemidir. Bu saldırıda saldırgan Baz istasyon sistemlerini taklit edebilecek cihazlar kullanarak mobil istasyonları ile Baz istasyonları arasındaki veri bağlantı ve trafiğini ele geçirmektedir. Sahte kurulan mobil istasyon Bas istasyonlarından gelen trafiği yönlendirerek kullanıcıların verilerini ele geçirmektedir.

1.4.1.4 Kimlik Yakalama (Identity Catching) Saldırı

Üçüncü Nesil Haberleşme sisteminde kimlik yakalama saldırılarına karşı az koruma sağlamaktadır. Bu sistemde IMSI mobil sistemlerinden kullanılan 15 karakterli temel numaradır. Haberleşme isteminde ilk olarak IMSI gönderilir ve ilk bağlantı isteğinden sonra geçici abone kimliği bölümünde (TMSI Temporary Mobile Subscriber Identity) değiştirilir. Sistemin içersin de abonelerin bilgilerinin geçici saklandığı (VLR Visitor Location Register) veri tabanında çökme olduğunda bilgiler geçici abone kimliği bölümüne TMSI tanımlanır.[10]

Saldırgan bilgilerin geçici sağlandığı (VLR Visitor Location Register) / mobil cihazlar arasındaki veri trafiğini şifrelenmesi yapan SGSN (Serving GPRS Support Node) taklit etmeye başlar TMSI den kimlik bilgileri göndermeye başlarlar bu esnada veriler sahte cihazlara girer kimlik bilgi verileri ele geçirilmektedir.

1.5 Dördüncü Nesil Mobil iletişim Teknoloji

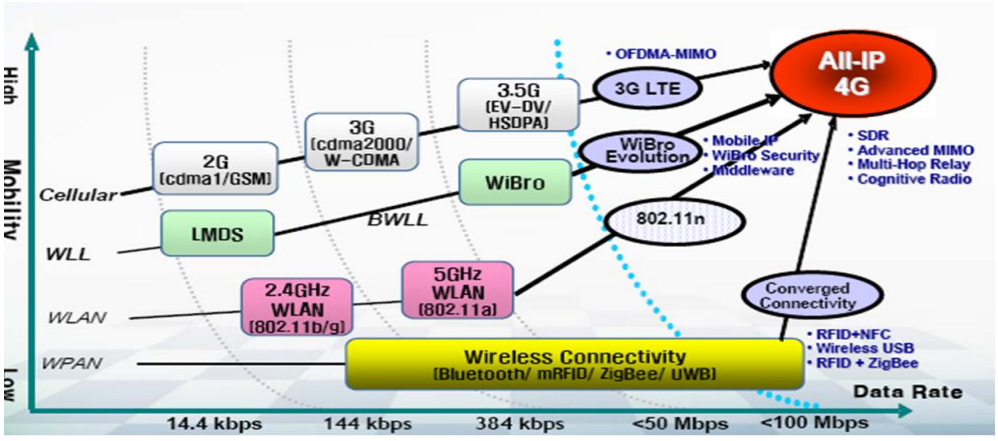
Dördüncü nesil ITU tarafından IMT-Advanced olarak tanımlanan standart dünya çağında kabul görmüş LTE (Long Time Evolution-Uzun Dönemli Dönüşüm) olarak adlandırılmaktadır. Avrupa ülkelerinde kullanılmaktadır. 3GPP Üçüncü Nesil standartlarında LTE'nin sekizinci ve dokunucu versiyonuna denk gelmektedir.

Wimax 802.16m, IEEE, LTE-Advanced, 3GPP teknolojileri ITU aday olarak IMT Advanced isminde adlandırılarak Kabul edilmiştir.

Dördüncü Nesil haberleşme sistemlerinden en önemli özelliği kullanıcıların veya abonelerin yer, mekân, zaman fark etmeksizin mobil akıllı cihazlar üzerinde çalışan mobil uygulamalar vasıtasıyla ve geniş bant alt yapısı kullanarak istenilen bilgi, Müzik, TV, video gerçek zamanlı şekilde ulaşma imkânı tanımaktadır.

[10] Mobarhan, Mojtaba Ayoubi, Evaluation of Security Attack on Umts Authentication Mechanism, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012

Dördüncü nesil haberleşmede önemli bir nokta, istenilen yer ve zamanda kesintisiz haberleşmeyle, bilgi ve servislere geniş bant ile bağlanıp yüksek kalitede bilgi, veri, resim ve video gibi hizmetleri alabilmektedir.



Şekil 2 Dördüncü Nesil Evrim Süreci

Dördüncü Nesil haberleşme sistemi, IP alt yapısı ile bilgisayarlar ve akıllı telefonlar üzerinden, bölgesel alan fark etmeksizin, ağ sistemleri üzerinden noktaları birleştirerek uygun fiyat politikası ile tüketiciler uygulamaların ve servislerin kullanması için geliştirilen sistemdir. Dördüncü Nesil maksimum veri aktarım hızı ve kapasitesi 100 Mbit/s,1 Gbit/s olarak hedeflenmektedir.

2N	3N	4N
Sayısal tabanlı	Sayısal tabanlı	IP tabanlı
Ses odaklı	Ses ve veri odaklı	Veri odaklı
Ayrı işaretleme şebekesi var.	Ayrı işaretleme şebekesi var.	Ayrı işaretleme şebekesi yok.
Dikey şebeke mimarisi	Dikey şebeke mimarisi	Basitleştirilmiş yatay şebeke mimarisi
Devre anahtarlamalı	Devre anahtarlamalı+paket anahtarlamalı	Paket anahtarlamalı+mesaj anahtarlamalı
Veri hızı 9,6 Kbps-14,4Kbps	100 Mbps	1 Gbps
TDMA, FDMA	WCDMA, CDMA2000	OFDM, OFDMA

Tablo 2 1N-2N-3N ve 4N Sistemlerin Benzerlikleri Ve Farklılıklar

Dördüncü Nesil sistemlerin gelişmesi ile beraber gelişen IPV6 sayısal adresleme sisteminin güvenli alt yapısı, yüksek veri hız ile birlikte ortaya çeşitli

sayıda uygulamalar gelişmektedir. İnsanoğlunun etrafında bulunan tüm araçlar, makineleri mobil uygulamalar ile istenilen her yerden yönetilebilmektedir. Buna örnek verirsek evlerde bulunan çamaşır makinesini ve ısınma sistemlerinin işyerlerinden eve gitmeden mobil uygulamalar üzerinden yönetilebilmektedir

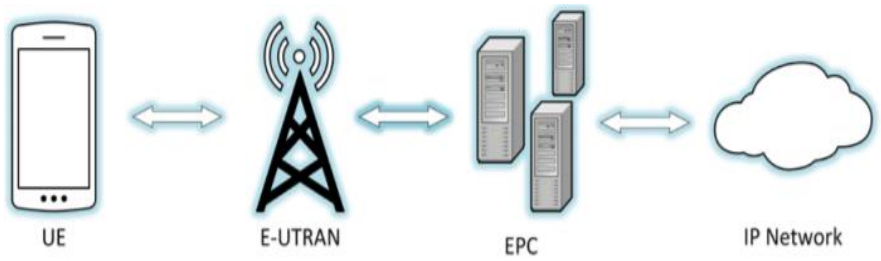
Dördüncü nesil teknolojilerin getireceği hizmetler aşağıda sıralanmıştır.

i. MIMO ile çok daha fazla kullanıcıya, daha hızlı veri hizmeti
ii. Mobil TV, IPTV, HDTV,3D TV servisleri
iii. Esnek Spektrum Kullanımı
iv. Yüksek çözünürlüklü (HD/High Definition) ses görüşmeleri
v. Gerçek zamanlı ses hizmetleri, VOIP hizmetleri
vi. P2P11 uygulamaları ve çok ortamlı mesajlaşma, video sohbet
vii. M2M (Machine to Machine)
viii. İnternet üzerinde çoklu kullanıcılı mobil oyunlar
ix. Mevcut kablosuz standartlarla birlikte işlerlik
x. Kameraları için kablo döşemeye gerek kalmayacaktır.

1.5.1 Dördüncü Nesil (4G) Veri Güvenliğindeki Sıkıntılar

İkinci Nesil ve Üçüncü Nesil haberleşme sistemlerinde yaşanan sıkıntılar nedeni ile Dördüncü Nesil haberleşme sistemlerinde sinyalleşme bölümlerinde daha gelişmiş yetkilendirme sistemleri ve daha güçlü veri şifreleme algoritmaları kullanılmıştır. Dördüncü Nesil haberleşme sistemi, hücresel ağ teknolojisinin aksine veri için ses ve paket anahtarlama teknolojisi kullanmaktadır. VoLTe ve VoIP protokollerini kullanarak ses trafiği verilerin ağ üzerinden geçirmektedir.

[11] P2P (per-to-per): Noktadan-noktaya iletim. İki uç bilgisayarın herhangi bir sunucu (server) ihtiyaç olmadan birbiri ile doğrudan iletişim kurması.



Şekil 3 Dördüncü Nesil Mimari

Dördüncü Nesil Mimari incelediğimizde veriler Mobil cihazlar (UE-User Equipment), E-ULTRAN, EPC sistemleri üzerinde gerçekleşmektedir.

Kullanıcı Cihazı (EU): Dördüncü Nesil haberleşme sisteminin uç noktada kullanılan tabletler, akıllı telefonlar, modemlerden oluşmaktadır. Bu cihazlar ile radyo sinyalleri ile veri alma ve gönderme yapmaktadır. Bu cihazların içersin de SIM kartlardan daha gelişmiş ilave güvenlik imkânları sağlayan USIM (Universal Subscriber Identity Mode). USIM içersin de şifreleme anahtarı ve mobil cihazlarını tanımlayıcı IMSI bilgisi içermektedir. Bu özellik mobil cihazlar ile Baz istasyonları arasındaki veri iletiminde kullanılmaktadır.

E-ULTRAN: Şebekenin yüksek hız seviyesine ulaşımı sağlamak ve ses verisinin dışında veri taşıma özelliği olan Baz istasyonlarından oluşan Radio Access Network dur.

Evrimleşmiş Paket Çekirdek Şebekesi (EPC): Dördüncü Nesil haberleşme sistemi için geliştirilen tüm IP ağ servislerini içeren bir katmandır. Katmanın içersin de bulunan MME (Mobility Management Entity) veri iletişimi için yetkilendirme, şifreleme ve kaynak organizasyonunu yapmaktadır.

Evrimleşmiş Baz İstasyonu (eNodeB): Dördüncü Nesil haberleşme sistemi için E-ULTRAN alanı içersin yer alan Baz istasyonudur. Her bir eNodeB cihazları EPC sistemine bağlanmaktır. Sistemdeki radyo fonksiyonlarını organize eden birimdir.

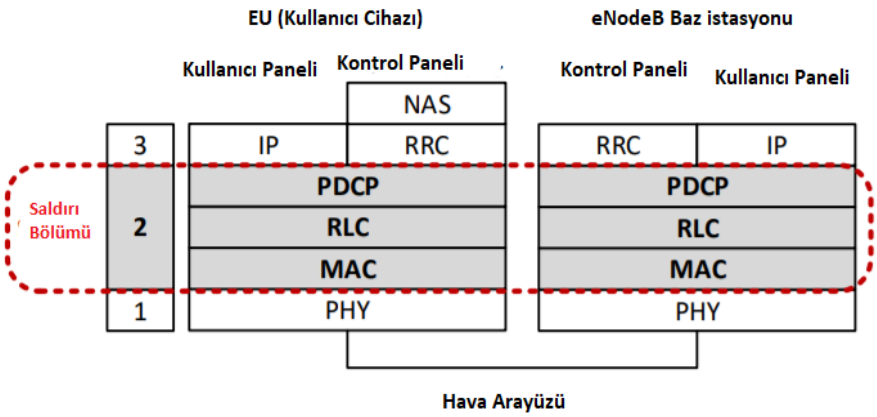
Dördüncü Nesil haberleşme sisteminin bir önceki nesillerin veri güvenlik sıkıntılarını gidermek için şifreleme ve yeni servisler geliştirilerek gidermeye

çalışılmıştır. Haberleşme sisteminde mobil cihazlarda yüksel hız ile veri ulaşımını sağlanmasıyla dünyada mobil cihazların artmasına neden olmuştur. Bu gelişmeyle beraber veriye hızlı ulaşım sağlanmasıyla ulaşılan bilgiler ile mobil haberleşme sistemlerinde güvenlik sıkıntıları evrimleşmiştir.

Haberleşme sistemlerine SIM veya Baz istasyonlarına saldırının yanı sıra mobil cihazlara yönelik saldırılar ortaya çıkmıştır. Saldırı yapılanacak açık kaynak kodlu yazılımlar geliştirilmiştir. Haberleşme şebekelerine yönelik saldırıları ve mobil cihazlara yönelik saldırıları aşağıdaki incelenecektir.

1.5.1.1 Radyo Kaynak Kontrolü (RRC) Protokol Saldırıları

Haberleşme sistemine yönelik protokol saldırı tipidir. Dördüncü nesil iletişim ağlarında cihaz ile Evrimleşmiş Baz istasyonu (eNodeB), Baz istasyonları arasında sinyalleşmeyi ve yönetimi sağlamaktadır. Saldırılar RRC protokolü kullandığı kullanıcıların ağa gönderdiği ölçüm raporu (UE measurement reports) ve ağ yayın bilgileri (Broadcast information) üzerinden saldırılar yapılmaktadır. RRC kullandığı bu iki sistem şifreleme metotlarını kullanmadığı için saldırılara olanak vermektedir.



Şekil 4 LTE Protokol Saldırı Bölümü

Ağ Yayın Bilgisi (Broadcast information) Saldırısı: UE son kullanıcı cihazların ile ilgili geçici kimliklerin ağ yayın kalanı yöntemi (Broadcast) ile gönderilen sistem bilgisi bloğu (System information Block) dur. Evrimleşmiş Baz

istasyonu (eNodeB) düzenli olarak SIB mesajı yayınlar. Bu tür yayın mesajları kimlik ve şifreleme yapılmadığından sahte Baz istasyonları (eNodeB) kurularak bu bilgiler saldırganlar tarafından kolayca öğrenilmektedir.

Cihaz Ölçüm Raporları (UE Measurement Reports) Saldırısı: eNodeB Baz istasyonu hizmet alan UE cihazlarına istenilen ölçüm sonuçları istekleri bildirilir isteği alan UE cihazları ilgili rapor mesajlarını gönderir. Bu tip ölçüm raporları şebeke operatörlerin sinyal sorunlarını çözmek çök önemlidir. Saldırgan bu tip ölçüm raporlarını şifreleme olmadığı için basit kod çözücülerle veri bilgisine kolayca ulaşabilmektedir.

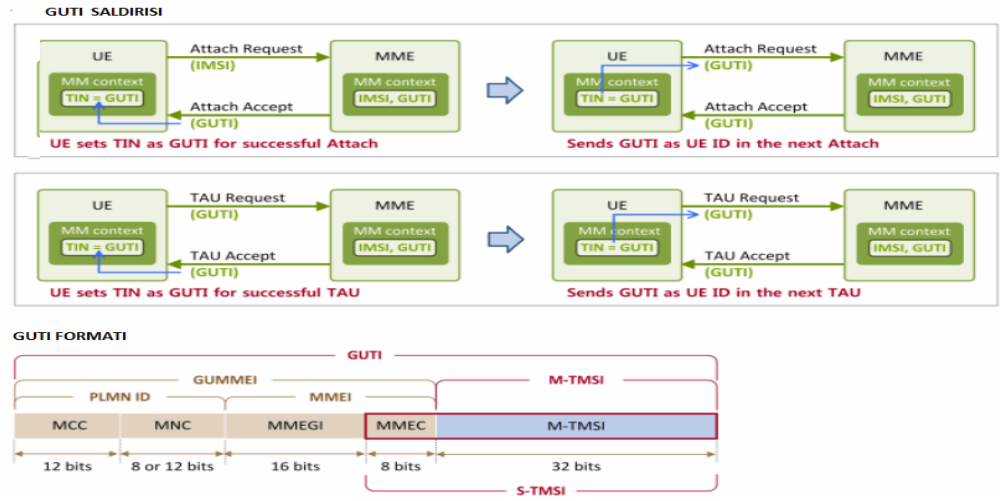
UE cihazlarının gönderdiği ölçüm raporlarında kullanıcı cihazlarının GPS koordinatları bulunmaktadır. Bu kullanıcıların GPRS bilgisini saldırgan tarafından ele geçirilerek konum takibi yapılabilmektedir.[12]

1.5.1.2 Küresel Benzersiz Geçici Tanımlayıcı (GUTI) Saldırısı

Haberleşme sistemine yönelik protokol saldırı tipidir. Dördüncü nesil ağlardaki UE kullanıcı cihazları tanımlanmasında kullanılan parametredir. UE kullanıcı cihazına GUTI değeri şebeke operatör tarafından verilmektedir. Haberleşme şebekesi kesinti olduğu zaman UE kullanıcı cihazı tekrar bağlandığı zaman bir önceki GUTI değeri tekrar atanmaktadır. EU kullanıcı cihazı aynı şebekede bağlantı kesilmeden üç gün boyunca aynı GUTI değerini almaktadır.

GUTI değerinin belli sürelerde değişmemesi veya değişip olduğu zaman bir önceki GUTI değerlerine benzemesi saldırganın EU kullanıcı bilgilerini erişebilmekte ve şebeke içeresinde takibi gerçekleşmektedir.

[12] Rupprech, David, Kohls Katharina, Breaking LTE on Layer Two, https://alter-attack.net/media/breaking_lte_on_layer_two.pdf , Erişim Tarihi:22.12.2018



Şekil 5 GUTI Formatı ve Saldırı Senaryosu

1.5.1.3 Yarı Pasif Atak -Haritalama Alanı Saldırısı

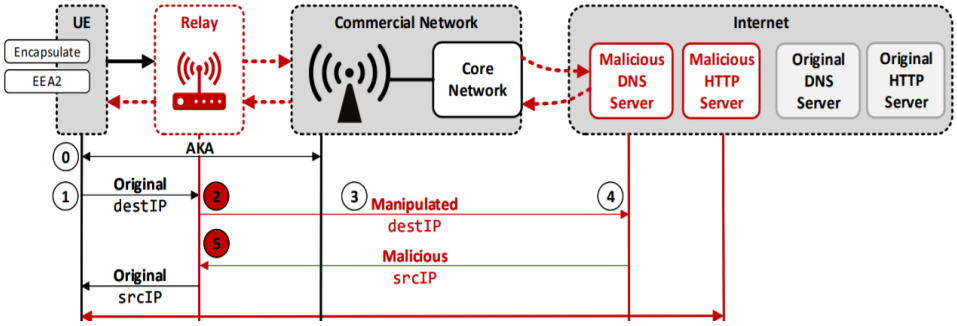
Dördüncü nesil sistemin veri güvenliğini konusunda testler yapılmaktadır. Bu testler bir tanesi CELL ID değerini öğrenebilmek olmuştur. EU kullanıcı mobil cihazların bağlandığı eNodB Baz istasyonun hücre numarasına CELL ID denmektedir. Her bir CELL ID farklı bir anteni ifade etmektedir. Yapılan bu test çalışmasında bisiklet ile şehir içersin de Andorid cellmapper uygulaması kullanarak CELL ID, evrimleşmiş Baz istasyonu eNodeB değerleri toplanarak şekil 6 deki harita çıkarılmıştır.

Şekil 6 LTE izleme Alanı ve Büyük Bir Operatörün Hücreleri

Kullanıcıya VoLTE çağrısı ile broadcast pasif atak yaparak hangi eNodeB Baz istasyonu üzerinden olduğu tespit işlemi yapılmıştır. Bu test incelemesinde 1-3 saniye arasında hedeflenen kişi mobil cihazından bildirim almadan ve gözükmeden VoLTE çağrısı süresi boyunca veriler dineleme yapılabilmiştir. [13]

1.5.1.4 DNS Yönlendirme Saldırısı

UE kullanılan cihazların mobil akıllı telefon olması ve IP teknoloji ile bağlantılar gerçekleştirdiği için kullanıcıların verilerine ulaşmak için değişik saldırı yöntemleri ortaya çıkmaktadır. DNS yönlendirme EU kullanıcı cihazları web sitesine erişimi yapıldığında araya kullanılan yazılımlarla saldırganın istediği yere yönlenmesine neden olmuştur.



Şekil 7 DNS Saldırı Yöntemi

EU Kullanıcı mobil cihazını açar açmaz güvenli bağlantı için şebeke ağından kimlik doğrulama yapmaktadır. Kullanıcı web sitesi ziyaret etmek istediğinde veya uygulama ile sunucuya bağlantı kurduğunda DNS isteği ilk önce UDP ve IP paketinde AES kullanarak şifreleme yaparak kullanıcıya iletir. Bu durumda DNS

[13] Ravishankar Borgaonkar, Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems, Aalto University ,7 Aug 2017, https://arxiv.org/pdf/1510.07563.pdf, Erişim Tarihi: 22.12.2018

sunucunun kullandığı orijinal IP adresi saldırı yazılımları ile durdurulur. Saldırganın istediği IP adresini yönlendirerek kullanıcıyı saldırı işlemi başarılı olmuş olmaktadır.

1.5.1.5 Distributed-Denial-of-Service (DDOS) Saldırısı

Bu saldırı yöntemi saldırgan hedeflediği cihaza veya servise sürekli veri paketi göndererek cihazı veya cihazları çalışmaz hale getirmeyi hedeflemektedir. Dördüncü nesil teknolojinin gelişmesi ile EU mobil cihazların sayısı 2018 yılı itibariyle 5.135 milyar[14] olmuştur.

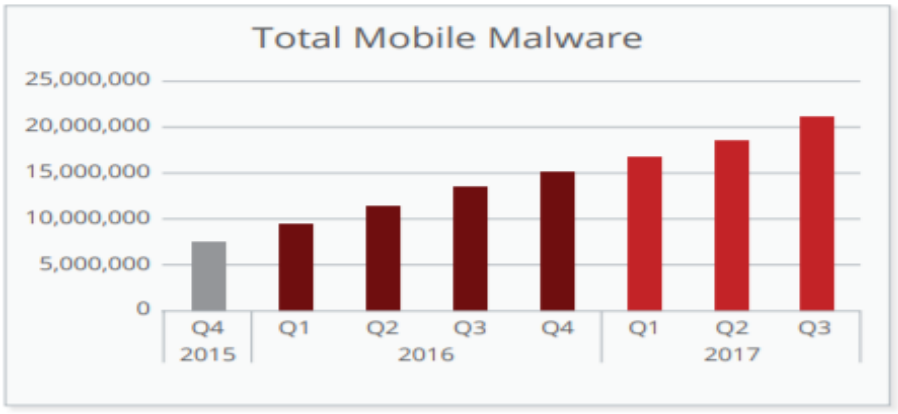
Bu cihazlar mobil işletim sisteminin (IOS, Android, Windows phone, ubuntu) güvenlik açıklarından veya uygulama mağazalarından indirilen uygulamalardan yararlanarak mobil cihazları DDOS saldırıları için tehlikeli hale gelmektedir. Bu tehlikeli mobil cihazlar Dördüncü nesil çekirdek ağına, Baz istasyonlarına saldırı yaparak işlevsiz hale getirmektedir.

1.5.1.6 EU Mobil Cihazlarına Yapılan Saldırı

Mobil haberleşme sistemlerinin evrimleşerek gelişmesiyle mobil cihazlar bilgisayar gibi teknolojileri geçerek her geçen yıl kullanımı artmaktadır. Mobil cihazlar ses verisi iletiminin yerine veri iletimi sağlamak için kullanılmaktadır. Yer ve mekân bağımsız veriye mobil cihazlarla çok rahat ulaşılmaktadır. 2018 yılı itibariyle 5 milyar dünyada mobil cihaz kullanımı ulaşılmıştır. Kullanıcıların veri güvenliği tehlikede olan 5 milyar cihaz var demektir. Mobil cihazlara üzerinde IOS, Android, Ubuntu, Windows Phone gibi işletim sistemleri yer almaktadır. Mobil cihazlara yapılan saldırı türleri aşağıdaki gibidir;

[14] We are Social tarafından 2018 yılında Digital raporundan alınmıştır. 29.01.2018, https://digitalreport.wearesocial.com/ Erişim Tarihi: 22.12.2018

Kötücül Yazılımlar (Malware): Virüs, solucan(worm) trojan, casus yazılımları (Spyware) olarak adlandırılan zararlı yazılımlara verilen isimdir[15]. Kötücül yazılımların hedefi kullanıcı mobil cihazların işletim sistemlerine sızarak kullanıcı verilerine ulaşmak, bilgileri şifrelemek, cihazı işletim sistemini bozarak çalışmaz hale getirmeyi hedeflemektedir. Bu zararlı yazılımlar mobil cihazlara işletim sisteminin uygulama mağazalarından indirilen ücretsiz uygulamalarla, gönderilen sms linkleri ile yöntemler kullanarak sızmaktadır.



Şekil 8 2015 -2017 arası Toplam Kötü Amaçlı Yazılım Örnekleri [16]

Doğrudan Saldırı (Direct Ataks): Mobil cihazların indirilen uygulama zafiyetlerinden veya işletim sistemlerinin zafiyetlerinden yararlanarak yetkisiz erişim yaparak veriye elde etmeyi hedefleyen doğrudan direk saldırıdır. Kötücül yazılımdan farklı olarak yazılım kurulumu yapılmadan zafiyetlerden yararlanarak yapılan saldırı yöntemidir.

Veri İletişimi Dinleme (Data Interception): Mobil cihazlarda tehdit eden saldırı yöntemlerinden biride veri iletimi sırasında araya girerek saldırma

[15] UKŞAL Mesut, Mobile Forensics, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Pogramı, 2015, sayfa 35

[16]https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf,Erişim Tatihi:23.12.2018

yöntemidir.[17] Bu yöntem haberleşme ağ üzerindeki veri paketlerini toplanarak haberleşme ağına sızarak veri bilgileri ele geçirilmiş olmaktadır. Tüm mobil cihazlar 3G ve 4G mobil ağları, Wifi, bluetooth gibi teknolojileri kullanarak veri alışverişi yapmaktadır. Mobil cihazlar haberleşme ağında olduğu müddetçe bu tehditler altında olmaya devam edecektir.

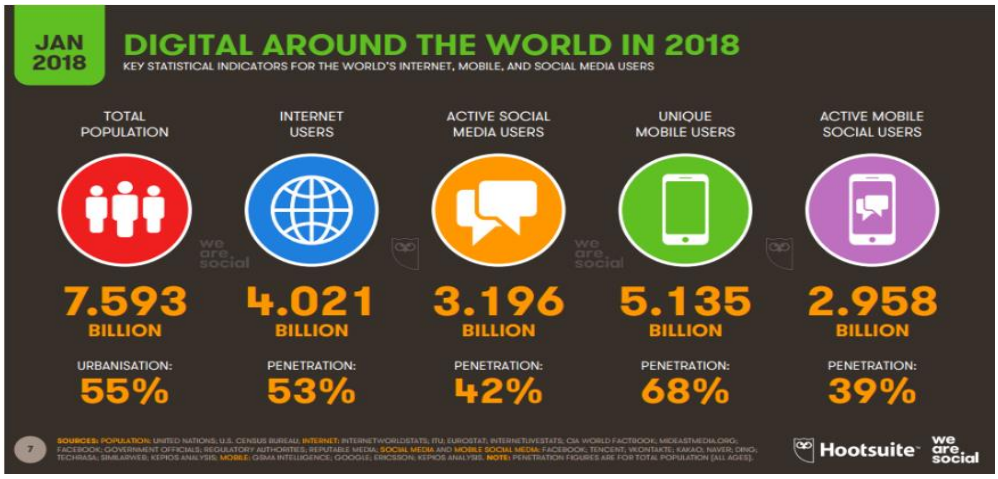
Sosyal Mühendislik Saldırıları (Social Engineering): Mobil cihazların gelişmesiyle mobil uygulamalar ve mobil platforlarda gelişmiştir. Bu platformlar üzerinden mobil cihazların zafiyetlerinden yararlanarak sosyal mühendislik uygulamaları kullanarak oltalama (phishing) saldırı tekniğiyle kişisel ve gizli verileri ele geçirilmektedir.

[17] SAĞIROĞLU, Şeref; BULUT, Hülya. Mobil Ortamlarda Bilgi Ve Haberleşme Güvenliği Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 2009, 24.3 s:501-505

İKİNCİ BÖLÜM

BEŞİNCİ NESİL MOBİL İLETİŞİM TEKNOLOJİLERİ

Birinci Nesil 'den İkinci Nesil'e ve Üçüncü Nesilden Dördüncü Nesil'e kadar mobil haberleşme alanının ortaya çıkan yeniliklerle evrimleşmiştir. Dördüncü Nesil ile beraber dünya 2018 yılı itibariyle dünya nüfusu mobil kullanıcı sayısı 5 milyar kullanıcıya ulaştığı, sosyal medya kullanıcısının 3 milyar ve internet kullanımının 4 milyar kullanıcı olduğu rapor edilmiştir. Böylelikle dünya analog sistemden Dijital dönüşümü evrimleşmeye devam etmemektedir.



Şekil 9 2018 Yılı Dünya İnternet, Sosyal Medya ve Mobil Kullanıcı İstatistikleri[18]

Ses sistemlerinden mobil geniş bantlı multimedya sistemlerine kadar dijital dönüşüm yeniliklerle beraber günlük yaşam tarzımı değiştirmeye, toplumun ilerlemesine ve ekonomilerin gelişmesine katkı sağlamıştır. Mobil haberleşme sistemi geleceğe damga vuracak yenilikler ve gelişmeler yapılmaktadır. Bunların en önemlisi ITU tarafından 2016 yılında standartlaşma çalışmalarına başlanmış

[18] We are Social tarafından 2018 yılında Digital raporundan alınmıştır. 29.01.2018, https://digitalreport.wearesocial.com/ Erişim Tarihi: 22.12.2018

2020 yılında standartların belirleneceği beşinci nesil ve ötesi diye adlandırılan teknolojilerdir. Beşinci nesil ve ötesi teknoloji yenilikleri beraberinde insanoğlu tüm hayatıyla birlikte mobil bağlantılı toplum haline gelmesi beklenmektedir.

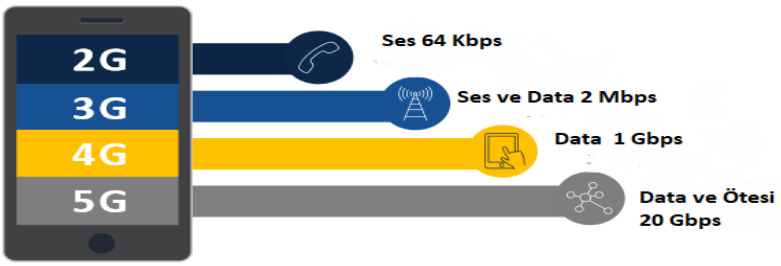
Beşinci nesil teknolojisinin, mevcut kullanılan dördüncü nesil' e göre en büyük farklı yükse veri hızı, bir milisaniyelere varan düşük gecikme süreleri, yüksek veri kapasitesi ve haberleşme sisteminin yazılım tabanlı olmasıdır. Yüksek bant genişliği yeniliği ile aynı anda milyarlarca cihaz ile bağlantı sağlama imkânı tanınacaktır. Bu yüksek alt yapı teknolojisi otomotiv, enerji, tarım, eğlence, sağlık, akıllı şehirler ve kentleşmeler alanlarında devrim niteliği gibi değişimler beklenmektedir.

Beşinci nesil teknolojisi dünyanın neresinde olursanız olun tüm mobil aygıtlara ve cihazları ulaşım imkânı sağlayacaktır. Çin'den Almaya' mobil telefon ile iletişim kurabilir veya akıllı ev sisteminize bağlanılabilinecektir. Mobil iletişiminde ortaya çıkan bu yeni teknoloji uydu, sabit, mobil gibi tüm iletişim alt yapılarında yazılım tabanlı ağ sistemlerine teknolojik dönüşüm sağlayacaktır.

Dördüncü Nesil haberleşme teknolojisi kullanıcıları birbirinin iletişimi hedeflerken beşinci nesil teknolojisi ise her şeyin birbirine bağlanmasını hedeflemektedir. İnsanoğlunun hayatında olan tüm sektörlerin, ekonomilerin, eğlencelerin ve diğer alanların birbirine bağlamayı hedefleyen büyük bir platforma dönüşecektir.

Bu değişimler büyük veri ağını ortaya çıkması ve veri güvenliği konularını önemli olacağını anlamına gelmektedir. Bu teknolojilerin güvenli şekilde kullanmak ve kullanıcı gizliliği nasıl sağlanması gerektiği gelecekte yeni bir sorun olarak karşımıza çıkacaktır.

2.1 Beşinci Nesil (5G) Mobil iletişim Teknoloji



Şekil 10 Haberleşme Teknolojilerin Veri hızlarının Gelişimi

Beşinci Nesil mobil haberleşme sistemi gelecekte dünyanın pek çok ülkesinde dördüncü nesil haberleşme sisteminin yerini alacaktır. Yeni nesil haberleşme sistemleri bulut teknolojileri, yazılım tabanlı ağ mimarisi, sanallaştırma gibi kablosuz ve ağ teknolojilerini yapılan çalışmalar üzerinden geliştirilmektedir. Beşinci nesil teknolojisi dördüncü nesil teknolojisine göre 10 Gbps yüksek hızlarının yanı sıra Nesnelerin interneti (IOT) teknolojisi ile milyarlarca nesnelerin birbirine bağlanması fazla kapasite ve çok düşük gecikme süresi hedeflenmektedir. Nesnelerin interneti (IoT) ile mobil sistemleri, araba-araba iletişimi, akıllı şebeke, akıllı park, blok zincirli tabanlı servisler gibi yeni ağ hizmetleri ve teknolojileri oluşturarak mobil sistemlerine bağlı bir toplum hedeflenmektedir. Telekomünikasyon şirketleri beşinci nesil teknolojilerin 2020 yılında ticari hale geleceği öngörmektedir. Dünyaca telekomünikasyon şirketleri beşinci nesil hücresel şebekelerle ilgili projeler yapmıştır.

Şekil 11 Beşinci Nesil Yenilikleri

Beşinci nesil haberleşme sisteminin dünyada yaygınlaşması beraberinde mobil veri trafiğinde önemli bir artışın olabileceği ön görülmektedir. Bununla birlikte beşinci nesil önceki nesil haberleşme sistemlerinden önemli farklılık göstermektedir. Gelişmiş mobil geniş bant sağlamak için mevcut mobil geniş bant hizmetlerinde yapılan iyileştirmeler beşinci nesil sisteminin kısa vadedeki yenilikleri olacaktır. Uzun vadede beşinci nesil in dikey olarak etkileyeceği sektörlerin ve farklı kullanıcı gurupların talepleri karşılamak için özel sistemler veya bağlantılar beklenmektedir. Bu yeni teknoloji şebeke operatörlerinin Nesnelerin interneti (IoT) uygulamaları ve cihazlar arası bağlantı uyumu gibi yenilikleri ile işletmeler için bir dizi yenilikçi hizmet sunabilecek alt yapı geliştirerek yeni gelir kaynaklarından yararlanma fırsatları doğacaktır.

Beşinci nesil haberleşme sisteminde farklı endüstrilerin değişen ihtiyaçlarını yönelik mobil iletişim verisi (MTC) ile büyük makineleri birbirine bağlanacak şekilde tasarlanmasına yönelik çalışmalar yapılmaktadır. Daha fazla cihaz ve nesnenin otomatik ve uzaktan bağlanması, izlenmesi gerekliliğinden sistemlerin makinelerin altyapılarının uçtan uca makineyle iletişime geçmesine izin verilecektir. Böylelikle çok sayıda sektör kablosuz ağ çözümlerine giderek daha

fazla şebekeye bağımlı hale gelebilir.[19] Beşinci Nesil ağların özellikleri aşağıdaki gibidir.

- Beşinci nesil ağların 10 Gbps varan yüksek hızlar
- Ultra güvenilir ve düşük gecikme
- Masif Nesnelerin interneti
- Diğer sektörleri birbirine bağlayan bir platform olması
- Mesajlaşma, fotoğraf galerisi, multimedya uygulamaları, telefon, kamera, mp3 oynatıcı gibi özellikleri özellikler sağlanacak
- Yüksek hız, yüksek kapasite ve bit başına düşük maliyet
- Ses, video akışı, multimedya etkileşimi, İnternet ve diğer geniş bant hizmetlerini çift yönlü ve doğru trafik istatistiklerini desteklemesi
- Her mobil cihaz kullandığı yere ve şebekeye göre IPv6 adresi sahip olması
- Beşinci nesil teknoloji gelişmesiyle dünya çapında mobil aygıt kullanılabilir
- Mobil iletişim içinde sınırsız veri yayınını bir araya getirme kabiliyeti
- Şebeke içinde kullanılan yönlendirici ve anahtar teknolojisi ile yüksek bağlantı sağlar
- Yazılım ve Danışmanlığı destekleme konusunda yüksek kabiliyet

Beşinci nesil sistemi ortamında IP tabanlı bir çekirdek ağı paylaşan farklı kablosuz teknolojilerin ve servis sağlayıcıların harmanlanması, yüksek hizmet kalitesi, seviyesini korumak için mobil cihazlar için sağlayıcılar ve teknolojiler arasında geçiş yapma imkânı verilecektir.

Gelecekte hayatımızın en önemli bir parçası olacak beşinci nesil haberleşme sisteminin hızlı dikey geçiş ve ağın genel açıklığı, cihazların erişim kontrolü, iletişim güvenliği, veri gizliliği ve mahremiyet gibi birçok güvenlik zafiyeti ortaya

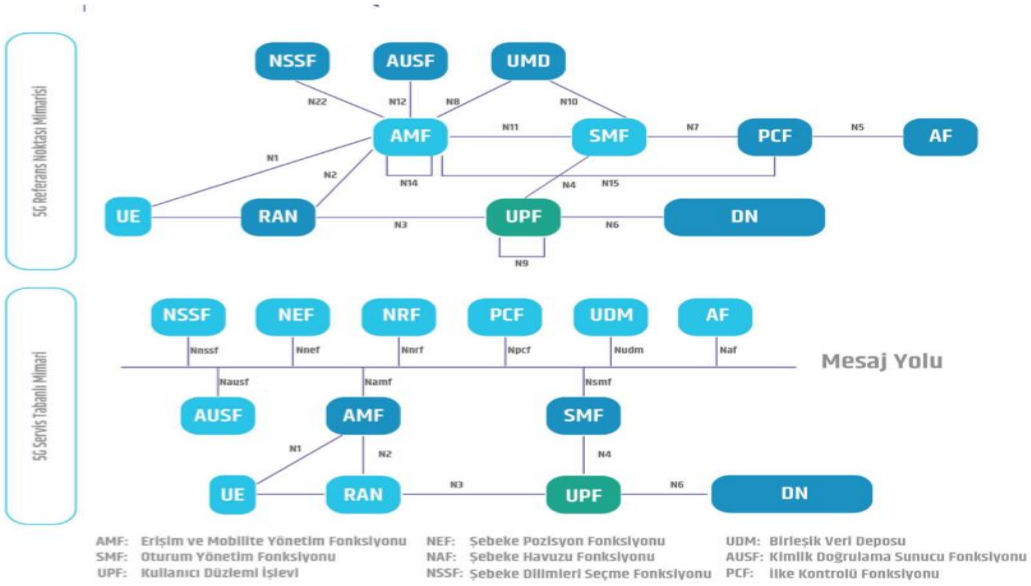
[19] A report by DotEcon Ltd and Axon Partners Group, Study on Implications of 5G Deployment on Future Business Models, 14 March 2018

çıkabilir. Beşinci nesil haberleşme sisteminin IP tabanlı olduğundan, IP adresine özgü güvenlik açıkları üzerinden tehditler oluşabilir.

Beşinci nesil haberleşme sistemlerinin gelecekte başarılı bir şekilde geçiş yapılabilmesi için yüksek düzeyde güvenlik ve gizliliğin güvence altına alınmasının önemli unsurlardan biri olacaktır.

2.2 Beşinci Nesil (5G) Mimari Yapısı

2.2.1 Servis Tabanlı Mimari (SBA)



Şekil 12 Beşinci Nesil Sistem Mimarisi

Önceki nesillere kıyasla 3GPP beşinci nesil sistem mimarisi hizmet tabanlıdır. Bu uygun olan her yerde mimari elemanların tanımlandığı anlamına gelir. Şebeke ağının ortak bir arabirim aracılığıyla bunlardan yararlanmalarına izin verilen şebeke ağı içersin de kullanılan hizmetlerdir. Bu mimaride 3GPP olmayan

bağlantıların merkezi ağ tarafından doğrudan desteklenme özelliği olduğu görülmektedir.[20]

Bu katmanda bulunan farklı servislerin birbiriyle bağlantılarını bu mimaride servis veri yolu şekilde tanımlanmıştır. Bu servislerin arasındaki veriler HTTP REST ve JSON formatında ara yüzleri taşınmaktadır.

Beşinci nesil şebeke içersin de kullanıcı cihazların EU iletişime geçen, bilgilerini bulunduran, depolayan, konumlarını belirleyen servisler bulunmaktadır. Bunların bazılarını aşağıda değinilmiştir.

Erişim ve Mobilete Yönetim (Access and Mobility Management Function- AMF): Kullanıcı mobil cihazların EU şebeke içeresinde hareketliliğini, erişimi ve bağlantılarını yönetmektedir. Kullanıcı mobil cihazların erişim kimlik doğrulamalarını, yetki doğrulamaları, dinleme yönetimi, mobilete yönetimi, mobil cihazın şebekeye katılımı gibi temel görevleri bulunmaktadır.

Oturum Yönetimi (Session Management Function -SMF): Paket veri geçişi (PGW) tarafından gerçekleştirilen oturumları yönetmektedir. Kullanıcı cihazların EU IP adresi atamasını gerçekleştirir. Trafiğin yönlendirilmesini, veri indirim ile ilgili verilerin bildirimini yönetir. Bu hizmetler için politikanın ve ücretlendirmenin nasıl uygulanacağını belirler. Kullanıcı oturumlarını yasal dinlemelerini sağlar.

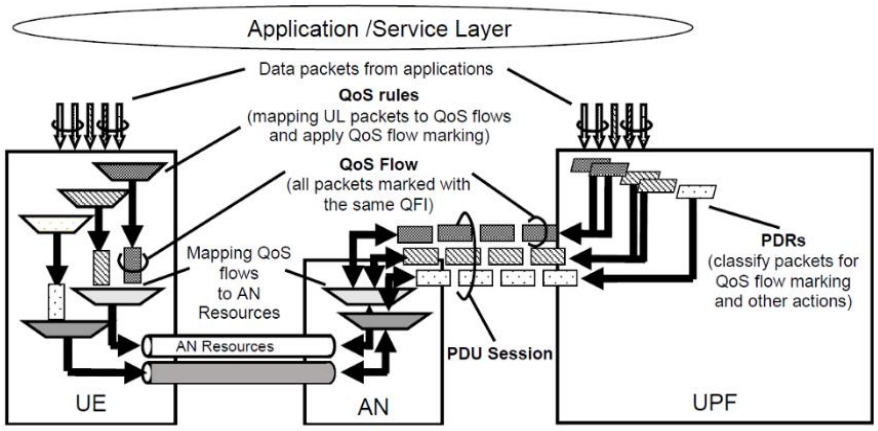
Birleşik Veri Yönetimi (Unified Data management -UDM): Kullanıcı mobil cihazların EU şebeke ağını kullanması için yapılan kimlik doğrulama üretimi ve anahtar sözleşme (AKA) kimlik bilgilerini yönetir. Kullanıcıların alacağı hizmetlere göre erişim izinlerini yönetir. Kullanıcı oturumlarını yasal dinlemelerini sağlar. Kısa mesaj servisini dağıtımını yönetir.

[20] Mademann Frank, The 5G System Architecture, Chairman of 3GPP SA2 , Huawei Technologies, 28 April 2018, Germany

Konum Yönetimi (Location Management-LMF): Kullanıcı mobil cihazların EU konumunu belirleme ve veri indirme trafiğini ölçümü yönetimini sağlamaktadır.

Ekipman Kimlik Kaydı (Equipment identification registration 5G EIR): Kullanıcı mobil cihazların EU kayıtlı cihaz olup olmadığını kontrolünü yönetir.

Kullanıcı Düzlemi Fonksiyonu (User Plane Function -UPF): Şebeke veri yönetim ağı ile kullanıcı mobil cihaz UE arasındaki veri iletişimini yönetmektedir. Veri paketlerin yönetilmesi, veri haberleşmelerin kalitesini, kullanıcı verilerin dinlenmesi için iletişim sağlar. Kullanıcıların şebeke ağındaki trafiklerini ve veri kullanımının raporlamasını yönetir.



Şekil 13 Kullanıcı cihazı ile UPF servisi iletişimi[21]

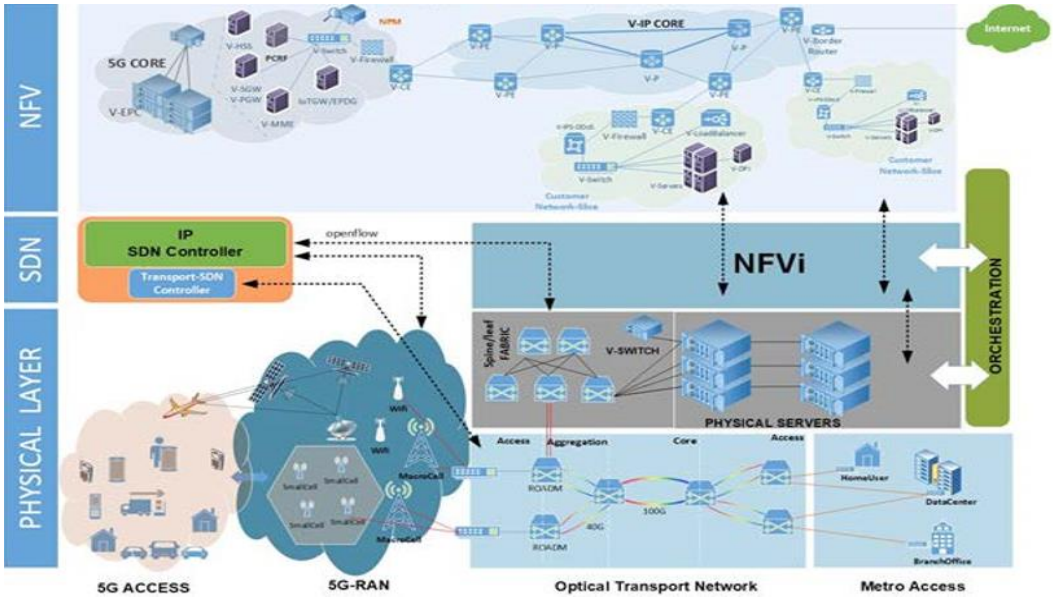
2.2.2 Yazılım Tabanlı Mimari (Software-Defined Network SDN)

Beşin Nesil iletişim teknolojisinin temel yapısını oluşturmaktadır. İletişim ağındaki kontrol ve yönetimi mantıksal bir şekilde yazılım tabanında programlayarak ağ yönetimini kolaylaştırmaktadır. İletişim ağında veri alışverişini yazılımlarla programlayabilmesi gelecekte ağların alt yapısında önemli bir

[21] https://medium.com/5g-nr/5g-service-based-architecture-sba-47900b0ded0a E.Ti:30.12.2018

teknoloji olacaktır. Yazılım tabanlı iletişim (SDN) ve Ağ işlev sanallaştırma (NFV) Beşinci nesil giden yolda anahtar sürücüler olarak kabul edilmektedir.

Beşinci nesil haberleşme sistemler en önemli özelliklerinden olan düşük gecikme süresi ve yüksek hız verimli bir şekilde uygulanabilmesi yazılım tabanlı programların ağ trafiğinin durumunu gözlemleyerek yönetmesinden geçmektedir.



Şekil 14 Yazılım Tabanlı Şebeke Mimarisi

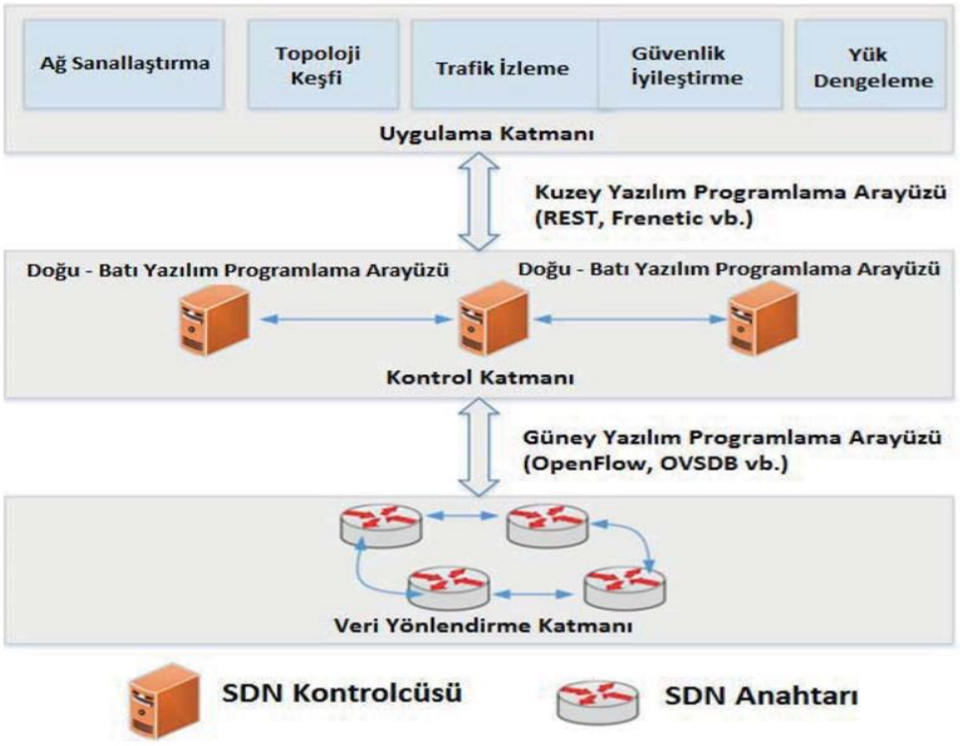
Yazılım tabanlı ağ iletişimi(SDN) heterojen farklı bölümleri arasındaki bölümlerin erişim yetersizliğini çözüm getirebilecek mimari yapıya sahiptir. SDN yaklaşımı, ağ iletişimi donanımının gelen paketlere ve akışlara nasıl tepki vereceğine ilişkin tepki verme tablolarını yapılandırmasına izin veren, hizmet odaklı bir API kullanarak, temel ağ veri düzlemini yöneten denetleyici olarak adlandırılan mantıksal bir merkezi bir yapıya sahiptir.

Bu yeni haberleşme beşinci nesil sisteminin kullanıcılara yüksek hız sağlaması, şebekeye bağlanılacak cihaz sayılarının artma öngörüsü şebeke ağının üzerinden geçen veri trafiği artması şebeke ağının yönetiminde ortaya çıkacak problemleri yazılım tabanlı mimari ile kolaylıkla giderilmesi öngörülmektedir.

SDN yazılım tabanlı ağ programlamaları ile nokta dan noktaya (Network Slicing) kurulan sanal ağlar üzerinden fiziksel altyapı kullanılarak farklı müşteri ihtiyaçlarına özgü özel mobil ağlar oluşturma özelliğine sahip olmayı hedeflemektedir.

Yazılım tabanı programlanabilen alt yapının sayesinde farklı ağ oluşturma mekanizmaları yönlendirme, erişim kontrolü ağdaki denetleyici tarafından kolaylıkla yapılandırabilmektedir. Bu karmaşık donanım prosedürlerinin uyum ihtiyaçlarını azaltmaktadır. Böylelikle farklı altyapıları yazılımlarla kolaylıkla birleştirilmekte ve Bulut bilişim (Cloud Cloud Computing) nesnelerin interneti gibi yeni ağ oluşturma mekanizmalarına adapte olabilmektedir.

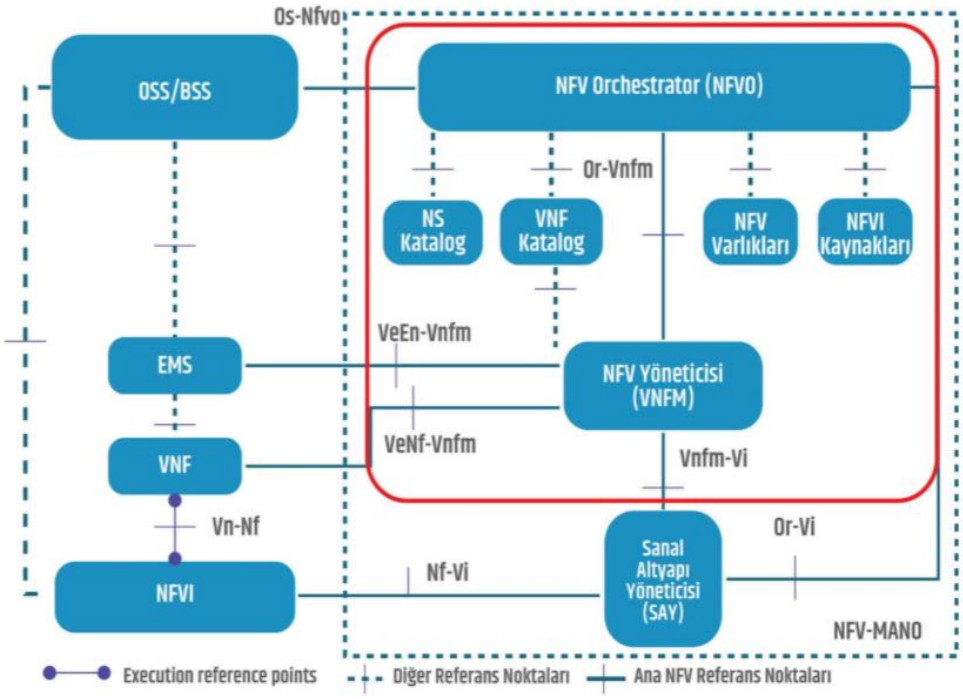
Yazılım tabanlı şebeke ağının üzerinden Nesnelerin interneti (Iot), cihazların iletimimi (C2C), Makinelerin iletişimi (M2M) gibi teknolojiler ile şebekeye bağlanan cihazların ağ üzerinde verilerin güvenlik zafiyetleri oluşturmasına neden olabilecektir.



Şekil 15 Yazılım Tabanlı Şebeke Mimarisi Örnek

2.2.3 Şebeke Fonksiyonları Sanallaştırma (Network Function Virtualisation)

Standart çalışmalarıyla geliştirilmekte olunan Beşinci nesil şebeke sistemlerinde kullanılan üreticiye özgü özel donanımsal cihazlar ihtiyacı ortadan kalkmış tüm alt yapı şebekesinde tek tip standart cihaz belirlenerek yatırım maliyetlerinde avantaj sağlanmayı hedeflenmektedir. Şebeke Fonksiyonları sanallaştırma standartları ETSI bünyesindeki Endüstri grubu tarafından belirlenmiştir.



Şekil 16 Şebeke Fonksiyonları Sanallaşma NFV Mimari

NFV şebeke ağ oluşturma işlevlerinin sunucu donanımından bağımsız olarak yazılım tabında çalışmasına izin verilmektedir. NFV, ağ şebekesi üzerinden fiziksel kaynak katmanındaki bellek kaynaklarını kullanır. Bu katmanda kaynakları hesaplama ve ağ oluşturma yapılarak ara yüzlerle kullanılarak donanımlar sanallaştırılır. Operatör tarafından sağlanan çekirdek donanım hem ağ hem de işletme açısından farklı servis ve fonksiyonların sanallaşabileceği mantıksal bir yapıda sanallaştırılabilir. Bu şekilde gerçek ağ operasyon birimleri çok sürümlü ve

çok fazla sanallaştırma yapılabilmektedir. Böylelikle özel donanımlarla ilgili engellerin aşılması yeni ağ hizmetlerinin kolay bir şekilde yaygınlaşmasına neden olabilecektir.

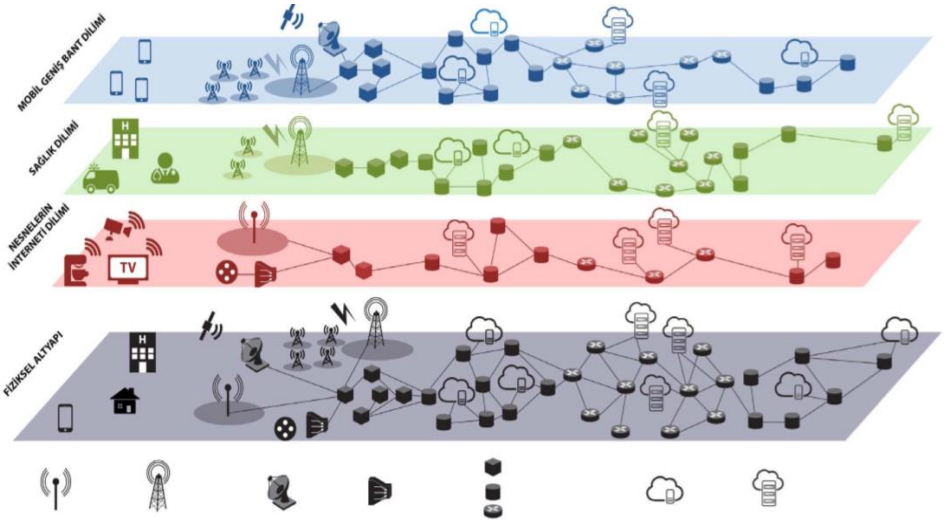
NFV standartlarını düzenleyen ETSI NFV Endüstri spesifikasyon Grubu çalışmalarında NFV dağıtımlarındaki SDN mekanizmalarının destekleyici rolü farklı tipteki anahtarlama ağlarının uyumunu kolaylaştırmak ve yazılım tarafından yönlendirme işlemlerin kontrol etmek olarak ifade edilmiştir. Mobil operatörler mimarisinde yapılan çalışmalarda NFV yapısı benimsenmiştir. Bilişim teknolojisi ve Telekom sektörleri arasında daha fazla iş birliğine dönüşebilecektir.

2.2.4 Şebeke Fiziksel Ağ Yapısı (Network Slicing)

Gelişmiş ağ performansı, daha iyi enerji tüketimi, daha düşük altyapı maliyeti ve etkili kaynak kullanımı için verimli esneklik ve daha yüksek sistem ölçeklenebilirliği için bir mimari optimizasyon ve mevcut hücresel ağın yeniden inşası gerekmektedir. Ağ dilimleme, anahtar sağlayıcılardan biri 2020 yılında beşinci nesil haberleşme ve sonraki iletişim sisteminin mimari bir cevabı olarak kabul edilir. Geleneksel mobil operatörler, tek bir ağ üzerinden çeşitli türlerdeki müşterilere her türden hizmet sunmaktadır. Ancak Şebeke ağ dilimleme operatörlerinin kullanımı artık tüm yapılandırmayı kendi yapılandırması ve özel hizmet Kalitesi gereklilikleriyle tüm ağları farklı dilimler arasında bölüştürmektedir. Dilim tabanlı bir ağda, her dilim ayrı bir mantıksal ağ olarak kabul edilecektir. Bu şekilde, altyapı kullanımı ve kaynak tahsisi geleneksel ağlara göre daha fazla enerji ve maliyet açısından verimli olacaktır.

Beşinci Nesil iletişim sisteminin, 2020'nin ötesindeki hizmetleri, tüketicileri ve iş taleplerini karşılaması beklenmektedir. Çok sayıda kullanıcı ekipmanının desteklenmesi yanında artan ağ trafiği miktarı telefon ve veri hizmetlerinin gelişmiş hizmet gereklilikleri dışında Beşinci nesil çeşitli sağlık, imalat, otomotiv, lojistik, enerji, çevre, inşaat vb. gibi dikey endüstrilerin farklı kullanım durumları ve çeşitli hizmet gereklilikleri için talepler ortaya çıkmaktadır. Bu talepler mevcut haberleşme sistemlerin çözümlenmesi mümkün olmamaktadır. Beşinci nesil

haberleşme sisteminde kullanılması düşünülen ağ şebeke dilimleme özelliği ile operatörün yapısal, elastik mimari yapısı ile bu talepleri çözümlenmesi öngörülmektedir.



Şekil 17 Şebeke Ağ Dilimleri

Şebeke -Ağ dilimleme en basit tanımıyla işlevi, hizmetlerin çeşitliliğini sağlamak amacıyla fiziksel bir altyapının iletişimini ve hesaplama kaynaklarını çok mantıksal ağlarda tasarlamak, bölümlemek, düzenlemek ve optimize etmek için Şebeke Fonksiyonları Sanallaşma (NFV) veya Yazılım Tabanlı Mimari (SDN) kullanmaktır. Şebeke-Ağ dilimlemenin konuşlandırılmasıyla tek bir fiziksel ağ altyapısı Ağ dilimi adı verilen birden fazla sanal ağa dilimlenir diğer bir ifade ile bölümlenir.

Her dilim kendi mimarisine, uygulamalarına, paket ve sinyal işleme kapasitesine sahip olabilir ve belirli son kullanıcılara belirli uygulamaların ve hizmetlerin sağlanmasından sorumludur. Şebeke-Ağ dilimleri kısmen paylaşılan bir altyapı üzerinde çalışmaktadır. Bu alt yapı, Radyo Erişim Mimari (RAN)'deki ağ ögeleri ve paylaşılan Ağ işlevleri Sanallaştırma Altyapısı (NFVI) kaynaklardan oluşmaktadır. Paylaşılan kaynaklarda çalışan ağ işlevleri genellikle her dilim için özelleştirilmiş bir biçimde başlatılmaktadır.

İletişim ağlarında şebeke-ağ dilimlemenin kullanımı hizmet amacı için dilimleme ve altyapı paylaşımı amacıyla dilimleme için iki farkı senaryo bulunmaktadır.

- **Ağ İletişimi Hizmet Kalitesi için Dilimleme:** Son kullanıcılara farklı türde hizmetler sunmak ve belirli dilim içindeki belirli hizmet kalite gereksinim türlerini sağlamak için çeşitli dilimler oluşturmaktadır. Canlı video yayını, tıbbı acil durum müdahale işlemlerine geniş bant bağlantısı gibi hizmet gerekliliklerine özgü dilimlemelerine örnek gösterilebilir.
- **Altyapı Paylaşımı için Dilimleme:** Bu ağ dilimleme senaryosunun temel noktası bir kablosuz ağın Radyo Erişim Mimari (RAN) alanının sanallaştırma ve çeşitli operatörler arasında daha fazla paylaşım yapmaktadır.

Beşinci Nesil iletişim şebeke-ağ dilimlemeni, operatörlerin birbirlerini alt ve alt yapılarını esnek ve dinamik bir şekilde paylaşmalarını sağlamak ve artan sayıdaki cihaz sayısını ve büyük miktarda kullanıcı trafiğini göz önünde bulundurarak kaynakları verimli bir şekilde yönetme yapabilmektedir. Şebeke operatörlerinin oluşturulmasını, yapılandırılmasını ve işletilmesini kolaylaştırmak için mobil operatörlere kolaylık sağlamaktadır. Bu son kullanıcıya şebeke operatörlerin değişik hizmetler sunmanın yolunu açmıştır.

Veri hızının çok üst düzey olduğu dikey sektörlere özgü aynı fiziksel şebeke altyapısında farklı nitelikli yapılar sunulabilmektedir. Sağlık sektöründe uzaktan ameliyat yapılmasında diğer sektörlere göre veri hızı üst düzeyde olacaktır. Sağlık sektörüne özgü hizmetler sunulabilecektir.

Şebeke- ağ dilimleme standardizasyon süreci hala başlangıç aşamasındadır. NGMN, 5G NORMA, Ortak Fonlu çerçeve, WWRF, 3GPP ve 5GPPP olmak üzere çeşitli araştırma projeleriyle ağ dilimleme üzerine birçok çalışma yürütülmektedir. Tüm bu projelerde ağ iletişimi, Beşinci Nesil iletişim sisteminin en temel gereksinimlerinden biri olarak kabul edilir. Şebeke-Ağ gelişimi sistem mimarisi, farklı ağ alt bölümlerindeki gereksinimler ve dilimlemenin ağ mimarisine etkisi ile

ilgilidir. Her şeyden önce, bu çeşitli ağ dilimleme araştırma yönleri için, ortaya çıkan Beşinci Nesil sisteminde görev almak için kapsamlı bir küresel standardizasyon gerekmektedir. Şebeke dilimlemede tam standardizasyon sürecinin 3G'nin 15 ve sonrası sürümlerinde tamamlanması beklenmektedir.

Şebeke-Ağ diliminde önerilen bazı programlanabilir ara yüzler ile programlanmış ağlara yeni potansiyel saldırı yöntemleri ortaya çıkacaktır. Bu veri güvenliğindeki olabilecek zafiyetleri konusunda araştırmalar ve geliştirilmeler çalışılması gerekmektedir.

2.2.5 Bulut Radyo Erişim Ağı (CLOUD-RAN)

Teknoloji sürekli gelişmesi kullanıcılar ve uygulamalardan gelen talebi karşılamak için yeni nesil kablosuz iletişim sistemlerinde sürekli geliştirmeler ve standart çalışmalar yapılmaktadır. Beşinci Nesil ve ilerisi 2020 yıllarında ticari olarak piyasaya sürülmesi, yüksek kullanıcı veri oranlarını düşük gecikme süresi ve küresel sayıda bağlı cihazların artması programlanmıştır. Bu hedef doğrultusunda Beşinci nesil sürekli geliştirmeler ve özellikler geliştirilmektedir. Bunlardan biri Bulut Radyo Erişim Ağı (CLOUD-RAN) teknolojisidir.

Bulut Radyo Erişim Ağı (CLOUD-RAN), Şebeke içersin de farklı konumlarda bulunan Baz istasyonlarını merkezi yerden kontrol edilmesini sağlamaktadır. Böylelikle Baz istasyonlar arasındaki veri iletişimini güçlendirilmesini sağlamaktadır. Bu özellik sayesinde Baz istasyonları arasındaki veri iletişimi güçlendirmesi ile iletişim içersin deki frekans karışmalarını azaltarak mobil kullanıcıların gecikme sürelerini düşülerek yüksek bağlantı hızına ulaşabilmektedir.

Bulut Radyo Erişim Ağı, Baz istasyonlarındaki bazı modüler yapıların bir kısmını bulut mimarisine aktırılarak ihtiyacın olduğu yerlerde Baz kapasiteleri kullanarak veri hızını daha optimize kullanmasına olanak sağlamaktadır. Basit anlamda kamu hizmetleri olan sokak lambaları ve trafik lambaları Bulut Radyo Erişim ağı kullanarak bulut taşınarak az maliyetle yüksek hızlarla hizmet verilebilmektedir.

Bulut Radyo Erişim Ağının bazı faydaları;

- Kullanıcılara ve sektörlere özgü şebeke topolojisi sunar,
- Şebeke ağına merkezi ve sınırlı erişim nedeniyle ağ güvenliğini artırır,
- Şebeke operatörlerin sermaye ve operasyon giderlerini optimize eder,
- SDN /NFV kullanarak yazılım araçları ile kendi kendini yapılandırılabilir ve yönetilebilir.
- Az Enerji tüketimi nedeniyle işletme maliyetlerini ve daha az sayıda ekipman kullanılması ile lira maliyetlerini azaltmaktadır
- Hücre girişimini azalmasına kullanıcı deneyiminin geliştirmesine yol açar.

2.3 Beşinci Nesil Standardizasyonu

Standart kavramı, belli bir konu üzerinden ilgili tarafların bir araya gelerek konu üzerinde çalışmalar yaparak çalışılan konu üzerinde belirli kuralların oluşturulması ve kuralların uygulanması olarak tanımlanmaktadır. Küresel dünyada yaşanan teknolojik gelişmeler sonucunda ortaya çıkan ihtiyaçları belirlemek, bu ihtiyaçları çözüm bulmak ve oluşabilecek rekabet ortamını düzenlemek için ilgili tarafların bir ayara geldiği yerdir.

Uluslararası Telekomünikasyon Birliği Telekomünikasyon Sektörü (International Telecommunications Union Telecommunication Standardization Sector -ITU), Uluslararası Standartlar Teşkilatı (International Organization for Standardization-ISO), Uluslararası Elektroteknik Komisyonu (International Electrtechnical Commission -IEC) Uluslararası standartları organizasyon örgütleridir. Haberleşme alanında uluslararası otoritesi ITU teşkilatıdır.

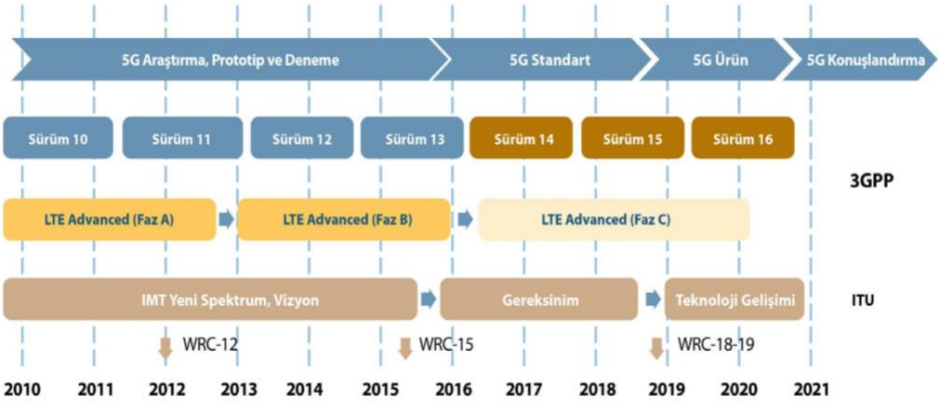
Avrupa Elektroteknik Standartlaştırma Komitesi (Comite Europeen Normalisation-CEN), Avrupa Elektroteknik Standartlaştırma Komitesi (Comite Europeen Normalisation-CENELEC), Avrupa Telekomünikasyon standartları Enstitüsü (European Telecommunications Standard Institute -ETSI) Örgütleri Avrupa bölgesinde standardizasyon alanlarında çalışmalar yapmaktadır.

Beşinci Nesil haberleşme sistemi önceki haberleşme sistemlerine göre küresel tarafların bir araya gelerek geliştirdikleri sistemdir. Geliştirilecek sistem dünya çapında kullanıma geçme olasılığı yüksek olmaktadır. Dünyayı bağlayan haberleşme sistemi olarak ta düşünülmesi doğru olmaktadır. Beşinci Nesil haberleşme sistemi 2020 yılında ticarileşerek tamamlanması beklenmektedir.

Uluslararası Telekomünikasyon Birliği Radyo Telekomünikasyon Standardizasyon Sektörü (ITU-R) Beşinci nesil mobil ağları ve ötesi 2020'ye doğru evrimleşmesi, daha uzun vadeli bir geniş görüşlülük geliştirilmektedir. 2012 yılının başlarında ITU-R gurubu Beşinci nesil haberleşme araştırmalarına dünyada ''2020 ve Sonrası için IMT'' adında geliştirme programı başlatıldı. 2015 yılında ITU-R gurubu IMT' nin gelecekteki büyümesini desteklemek için ilave spektrumdaki müzakerelerin gerçekleştirileceği yer olan 2019 Dünya Radyo Haberleşme Konferansı için mobil geniş bant bağlantılı toplumun vizyonu geliştirildi.

Mobil endüstri liderleri 5GNR yapılandırma sürecini hızlandırmak için Şubat 2017 yılında Barselona da destek açıklamaları yapıldı. Bu destek açıklamasından sonra Mart 2017 tarihinde 3GPP RAN toplantısı Hırvatistan'da yapılarak süreci hızlandırma kararı alındır. 3GPP sürüm 15 parçası olarak belirlendi.

Aralık 2017 tarihinde Lizbon şehrinde ilk 3GPP TSG RAN toplantısında ilk uygulanabilir 5G NR tanımlanması belirlendi. Sektörün önde gelene kuruluşları ve şirketleri 5GNR standardının tamamlanması sonucunda testlerin yapılıp 2019 yılında ticari dağıtımın yapılabileceğini ön görmektedirler.



Şekil 18 Beşinci Nesil Standartlaşma Yol Haritası

Haziran 2018 tarihinde 3GPP'nin teknik şartnameler gurubu Beşinci Nesil Yeni Radyo teknik ayrıntıları tamamlanmıştır. Bu belirlenen standart en önemli özelliği mobil şebeke ağının noktadan noktaya yeni mimari oluşturmaktır. Şebeke operatörleri tarafından nokta dan noktaya yeni iş modelleri gelişmeleri ortaya çıkmasında kolaylık sağlayacaktır. Ortaya çıkartılan bu standart dünya çapında mobil şirketler ve dikey sektörlere yeni iş modellerini geliştirilmesini sağlayacak teknoloji seçenekleri sunmaktadır.

2018-2010 Yılları arasında standartların büyük ölçekli benzetim çalışmaları ve testlerin yapılarak tamamlanması öngörülmektedir. 2019 yılının sonunda ITU IMT-2020 tarafından 3GPP sürüm 16 6GHZ üzerindeki yüksek frekansların uygulamaları gelişmelerinin tamamlanarak 2020 yılında Japonya da yapılacak olimpiyat yaz oyunlarında hizmet verilmesi öngörülmektedir. 2020 Tokyo olimpiyatlarında stadyum içeresinde 1Gbit üzerinde bant genişliği bağlantı gerçekleştirilecektir.

2020 yılı ve sonrası telekomünikasyon operatörlerinden ilk tekliflerin alınması ve teknik maliyet anlamımda minimum düzeye getirilen standarttın kullanıma sunulması hedeflenmektedir.[22]

[22] ETSI, 5G;pocedures for the 5G Sytem Release 15, Referance DTS/TSGS-0223502vf20, 2018 FRANCE

ITU tarafından Beşinci Nesil IMT-2020 belirtilen yükse kapasite ve heterojen yapısı sayesinde mobil akıllı telefonların dışında trilyonlarca makine bağlantısı olacağı, otonom araçlar, uzaktan ameliyat ve sanayi otomasyonları gibi uygulamaların artacağı öngörülmektedir. Bu gelişmeler dijital dünyaya dönüşümü başlangıcı sayılmaktadır. Ağlar üzerinden çok çeşitli verilerin dolaşması anlamına gelmektedir.

2.4 Beşinci Nesil Dünyadaki Çalışmalar

2.4.1 Avrupa

Avrupa'daki Beşinci Nesil önceki haberleşme sistemlerinden yapılan çalışmalar mobil iletişim yapılan gelişmeye öncelik sağlamıştır. Avrupa da geliştirilen İkinci Nesil GSM standardı ve Üçüncü Nesil UMTS ve Dördüncü Nesil LTE standartları dünyanın mobil ağlarının %80 tarafından kullanılmaktadır.

Beşinci Nesil teknolojinin geliştirilmesi Avrupa'nın ekonomiyi yönlendirmesi, endüstrinin rekabetçiliğini güçlendirmesi ve yeni iş olanakları oluşturulması Avrupa için büyük önem taşımaktadır. Avrupa Birliği Bilişim sektörüne yıllık 660 milyar Euro kaynak ayırmaktadır. Beşinci Nesil Avrupa'nın küresel mobil endüstrisindeki liderliğini sağlamada kilit rol oynayacaktır. Avrupa Telekom endüstrisi GSM teknolojisinin ilk günlerinde UMTS ve LTE teknolojilerine kadar küresel rekabetin ön saflarında yer almışlardır. 2012 yılında ağ altyapısı dünya Telekom pazarının yaklaşık %40 200 milyar Avro temsil etmektedir. Avrupa gelecek teknolojilerini araştırma yapmak için 'Çevre Programları (Framework Programmes-FP) finansal araç olarak kullanmaktalar. Üçüncü Nesil UMTS ve Dördüncü Nesil LTE standartlarını geliştirerek bu modeli başarıyla uygulandı. Bu modelli Beşinci Nesil geliştirilmesinde aynı modeli kullanmaktadır.

Project	Small cell	Virtualisation	mmWave	MTC
METIS	✓	–	–	✓
MCN	–	✓	–	–
COMBO	–	✓	–	–
iJOIN	–	✓	✓	–
TROPIC	✓	✓	–	–
E3NETWORK	–	–	✓	–
MOTO	–	–	–	✓
MiWEBA	✓	–	✓	–

Tablo 3 2013 yılında FP7 nin Beşinci Nesil Geliştirilmesinde Finanse Edilen Projeler

Avrupa Birliği FP7 çerçevesinde enerji verimli teknikleri kullanarak ultra yüksek hızlı geniş bant ve MTC gibi konular üzerinde Beşinci Nesil geliştirilmesinde önemli çalışmalar yapılmıştır. FP7 yoluyla yapılan Avrupa Birliği 10 yıl boyunca beşinci nesil teknolojilerinde kablolu ve telsiz haberleşme çalışmaları yapan COMBO, METIS,5GNOW, iJOIN, TROPIC, Mobil Bulut Ağı, PHYLAWS, CROWD ve MOTO projeler desteklenmiştir.

2.4.1.1 5G Altyapısı PPP (5G Infrastructure PPP)

Avrupa Birliğinde Beşinci Nesil standart çalışmaları yapan diğer organizasyon 5G Altyapısı PPP (5G Infrastructure PPP) dir. 5G Altyapısı PPP, 2020'nin ötesindeki yeni nesil mobil iletişim alt yapılarını geliştirmek, araştırmak için halka açık özel bir organizasyondur. 5G Altyapısı PPP sektörleri, operatörler, düzenleyici standardizasyon kuruluşları tüm değer zincirinden paydaşları bir araya getirmektedir. 5G Altyapısı PPP amacı 2020 yılına kadar yıllık stratejik yol haritasını belirlemek, araştırma yapılarak Beşinci Nesil hücresel sistemin ortak vizyonunu oluşturmaktır. 5G Altyapısı PPP, önümüzdeki 10 yıl boyunca her yerde bulunan yeni nesil iletişim altyapıları için çözümler, mimariler, teknolojiler ve standartlar sunacak çalışmalar yapılacaktır.

2.4.1.2 METIS

METIS Beşinci nesil haberleşme geliştirmek için FP7 tarafından desteklenen projedir. Ericsson tarafından koordine edilen Telekom üreticileri ve şebeke operatörlerinden otomotiv endüstrisi ve akademi dâhil 29 ortaktan oluşan bir konsorsiyumudur. METIS projesi, Beşinci Nesil teknoloji çalışmaların gerekli verimliliği, çok yönlülüğü ve ölçümlenme birliği sağlayan bir sistem kavram geliştirmeyi, sistemi desteklemek için kilit teknoloji bileşenlerini araştırmayı, değerlendirmeyi amaçlamaktadır.

METIS genel sistem kavramını oluşturmak için teknoloji bileşenleriyle bütünleşmiş yatay konular belirlemiştir.

- Büyük Makine İletişimi (MMC)
- Doğrudan Cihazdan Cihaza Haberleşme (D2D)
- Hareketli Ağlar (MNs)
- Ultra Yoğun Ağlar (UDNs)
- Ultra Güvenilir iletişim (URC)

2.4.1.3 Diğer Çalışmalar

Avrupa da Ericsson firması Beşinci Nesil çalışmalar yapmaktadır. Ericsson Beşinci Nesil sürdürülebilir bir ‘’Ağa Dayalı toplum’’ u her yerde, her zaman, herhangi birine, her şeye bilgi ve veri paylaşımını sınırsız erişim sağlamak vizyonunu hedeflemektedir. Bu vizyon HSPA, LTE ve WİFİ dahil olmak üzere gelişmiş Radyo Erişim Teknolojilerin bir kombinasyonunun ve belirli kullanım durumları için tamamlayıcı yeni Radyo Erişim Teknolojilerin kombinasyonunun sorunsuz bir şekilde bütünleştirilmesiyle sağlayarak mevcut Radyo Erişim Teknolojilerin değiştirmeden uygulamayı sağlamayı hedeflemektedirler. METIS projesiyle birlikte Beşinci nesil sistemimin temel kavramlarını geliştirerek standardizasyon oluşturmayı hedeflemektedir.

Şekil 19 Beşinci Nesil Ericsson'un 15 GHz'lik MU-MIMO Deneyi

Ericsson and SoftBank 2016 yılında 15 Ghz ve 4.5 Ghz spektrumunda Beşinci Nesil denemelerini tamamladı. Ericsson ve Telefónica 2016 yılında gelecekteki İnternet Kamu-Özel Ortaklığı (5G PPP) için Gelişmiş 5G Ağ Altyapısına ve İletişim Ağları ve Hizmetleri için Avrupa Teknoloji Platformu'na (ETP Networld 2020) projesine odaklandı.[23] Ericsson beşinci nesil ana şebeke, radyo, transmisyon ağları için geliştirilen ilk beşinci nesil yazılım 2018 kullanılmaya başlanacak.

2.4.2 Kuzey Amerika

Kuzey Amerika'daki Beşinci Nesil haberleşme sisteminde yapılan araştırmalar daha fazla akademi ve sanayi merkezli eğilimde olduğundan Avrupa'daki araştırmalardan farklıdır. ABD ve Kanada' da araştırmaları Avrupa'daki gibi koordine eden bir kamu fonu bulunmamaktadır. Amerika Birleşik Devlerinde üniversitelerdeki araştırma finansmanını, Ulusal Bilim Vakfı (NSF) ve Savunma Gelişmiş Araştırma Projeleri ajansı (DARPA) gibi sektörlerden gelmektedir. Beşinci Nesil çalışmalarında üniversiteler ve özel sektörler otak potansiyel teknolojilerin bazılarında birlikte çalışmaktadır. New York Üniversitesi

[23] Policy Department A: Economic and Scientific Policy, European Parliament, Brussels ,2016

Politeknik Enstitüsü (NYU) Beşinci nesil mmWave çözümlerini incelemek ve geliştirmek için Samsung firması ile birlikte çalışmaktadır.

2.4.2.1 Diğer Çalışmaları

New York Üniversitesi, Beşinci Nesil projesi daha az mmWave spektrumunda çalışan yönlü ışın formuna sahip daha küçük, daha hafif antenlerle daha akıllı ve çok daha ucuz bir kablosuz altyapı geliştirmeyi amaçlamaktadır.

Carleton Üniversitesi, Beşinci nesil projeyi Ontaio Ekonomik kalkınma ve Yenilik Bakanlığı tarafından yürütmektedir. Endüstriyel ortaklar Huawei Kanada, Huawei Çin, Apple ABD, Telus, Blackberry (RIM), Samsung Kore, Nortel ve İletişim Araştırma Merkezi Kanada'dır.

Qualcom firması, Beşinci Nesil teknolojide 1000x kapasite zorluğunu gidermek için hücresel sistemleri geliştirme yollarında önemli miktarda araştırma yürütmektedir. 3GPP'ye önerilen Proximity Services adı verilen doğrudan doğuya cihazdan cihaza D2D iletişim modları üzerinde aktif çalışmalar yapmaktadır.

İntel firması, Yeni nesil hücresel sistemlerde mmWave kablosuz teknolojisini kullanmak için araştırmalar yürütmektedir. Küçük hücreli baz istasyonları için taşıyıcı bağlantı 60 Ghz'lik teknoloji üzerinde çalışmaktadır. Ayrıca en az 200 metrelik mesafelerde 1 Gbps ve mobil cihazlara erişim bağlantıları 28 Ghz üzerinde araştırmalar devam etmektedir.

Agilent firması, Beşinci Nesil haberleşme sisteminde yeni nesil kablosuz iletişim sistemleri için test ve ölçüm çözümleri için China Mobile araştırma bölümü ile mutabakat zaptı imzalandı.

2.4.3 Asya

Beşinci Nesil haberleşme yönelik yol haritası oluşturulmasında Avrupa'ya benzer bir yol izlemektedir. Çin IMT 2020 programının organizasyonunda sorumludur. Güney Kore'de Beşinci Nesil için 5G forumu oluşturmuştur. Çin, Japonya, Güney Kore Asya'daki Beşinci Nesil konusunda araştırma yapan başlıca

ülke ülkelerdir. Çin'de yapılan araştırmalar hükümet tarafından başlatılmış ve sanayi sektör, akademi ortaklıkları ile çalışmalar devam etmektedir. Japonya ve Güney Kore endüstri akademi ortaklıklar ile çalışmalar başlatıldı.

2.4.3.1 Çin

Çin'deki Beşinci Nesil mobil iletişimin IMT2020 Promosyon Grubunun kurulmasını destekleyen Çin Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT) ve Ulusal Kalkınma ve Reform Komisyonu ve Bilim ve Teknoloji Bakanlığı (EN) yer almaktadır. Şubat 2013 tarihinde Pekin'de araştırma ve standart tanıtım platformu olarak IMT-2020 tanıtım gurubu kuruldu. IMT-2020 sanayi, akademi ortaklıkları ve uluslararası iş birliği yoluyla Beşinci Nesil küresel standartları desteklemeyi amaçlamaktadır. IMT-2020 çekirdek teknolojisinde 10 guruba ayrılmıştır.

- Yoğun Ağ
- Terminaller Arasında Doğrudan İletişim
- Wifi ile Ortak Ağ Kurma
- Yeni Ağ Mimarisi
- Yeni Çoklu anten Dağınık iletim
- Dördüncü Nesil ve Beşinci Nesil Sinyal İşleme
- Modülasyon ve kodlama tekniklerinin uygulanması
- Yüksek Bant İletişimi
- Frekans Paylaşımı
- Ağ Zekâsı

Beşinci Nesil faaliyetlerine Huawei, Datang Telecom, China Mobile ve ZTE şirketler katılmıştır. Huawei, 2009'dan beri Harvard Üniversitesi, California Berkley Üniversitesi ve Cambridge Üniversitesi gibi yabancı üniversitelerle Beşinci Nesil teknolojileri üzerine, daha geniş radyo frekansı teknikleri ve

hücrelerin dinamik sanallaştırılmasını destekleyen teknikler gibi ortak araştırmalar yapılmaktadır. Huawei firması AB'nin METIS projesine katıldı.[24]

Çin Mobil Akademisi, Beşinci Nesil haberleşme alanında Merkezileştirilmiş Radyo Erişim Şebekesi (C-RAN) mimari önermesi yapıldı. C-RAN gerçek zamanlı bulut altyapısından oluşan merkezi bir ana bant işleme ünitesine dayanan uzak uçtaki radyo frekansı üniteleri ve antenlerden oluşan kablosuz ağ yapısıdır. Bu ağ yapısı ile Maliyetler ve enerji tüketimi etkili bir şekilde azaltılabilir, kullanıcıların bant genişliğini artırabilir birden fazla standardı destekleyebilir ve son kullanıcıya daha kolay, sorunsuz internet hizmetleri verebilme özelliğini sahiptir. C-RAN yabancı operatör ve donanım üreticisinin ilgi odağı olmuştur. Çin Mobil, Microsoft ve HP firmalarıyla C-RAN işbirliğini yapılmaktadır.

2.4.3.2 Güney Kore

Güney Kore Beşinci Nesil haberleşme teknolojileri çalışmalarını, Güney Kore Elektronik İletişim Akademisi, Samsung, LG ve Ericsson- LG gibi bazı mobil iletişim üreticileri ile Güney Kore Yaratma ve Bilim Bakanlığı ve Telekom operatörleri birlikte yürütmektedir.28 Haziran 2013 tarihinde Güney Kore'nin Gelecek Yatarım ve Bilim Bakanlığı ve Çin devleti, Çin deki IMT-2020 gurubu ile Güney Kore 5G Formu Beşinci nesil gelişimi için ikili anlaşmalar yapıldı. Ayrıca Çin Ulusal Bilgisayar Ağı Acil Müdahale (CNCERT) ve Kore Bilgisayar Acil Müdahale Ekibi (KRCERT) iki kuruluş iş birliği ağı güvenlik anlaşmaları imzaladı. Çin ve Kore'den ilgili uzmanlar, Beşinci Nesil uluslararası standartları geliştirme ve belirleme konularında çalışmalar yapıldı.

Samsung, LG ve Elektronik İletişim Akademisi, Güney Koreli şirketler tarafından ortaklaşa yeni Beşinci Nesil ağ mimarisini ortaklaşa belirlediler. Ağ mimarisi sunucu ağ geçidi, dış hücreler ve iç hücreler olmak üzere üç katmandan oluşturulmuştur. İç hücresel veri ana hücreye dış taşıyıcıya iletir daha sonra dış hücresel paket sunucu ağ geçidi ile birlikte optik fiberler üzerinden anahtarlamayı

[24] 5G Americas,Global Organizations Forge New Frontier of 5G, July 2016

gerçekleştirir. Hücresel ağdaki bas istasyonları ortak kanal girişimimi azaltmak için kapsama alanını almak için dar ışın yönlü antenler kullanılmaktadır.

30 Mayıs 2013 tarihinde Güney Kore de Samsung, LG ve Ericsson şirketlerin kurduğu 5G formunun genel kurulu seul şehrinde yapıldı. 2015 yılında Beşinci Nesil standardizasyon soruları ve 2020'de ticarileştirme konularında görüşmeler yapıldı. Beşinci Nesil yalnızca hayatı kolaylık sağlamayacağı aynı zamanda işletmelere ve ülke ekonomik büyümelere yardımcı olabileceği düşünülmektedir. 1000 kat daha yüksek verim ve daha az güç tüketen akıllı makinelerin piyasaya sürülmesi beklenmektedir.

Güney Kore de 5G formu mizyonu ve vizyonu aşağıda maddelemiştir.

- Ulusal Politika oluşturulması
- 5G Ar-Ge'nin teşvik edilmesi
- 5G ekosistemine destek sağlanması
- Global iş birliği sağlamak

2.4.3.3 Japonya

Güney Kore'ye benzer şekilde Japonya da Beşinci nesil iletişim teknolojisi gelişimi için endüstri akademi ortaklığı destelenmektedir. Japonya'nın Yokosuka Araştırma Parkı (YRP) Ar-Ge Promosyon Derneği, Güney Kore'nin Beşinci Nesil Formu, Tayvan'ın Kablosuz ve Bilgi Teknolojiler İletişim Liderleri Birleşmiş Kurulu (WIT CLUB), Çin'in Geleceği Formu gibi organizasyon bölgenin kuruluşları tarafından desteklenmiştir. AB'nin METIS proje ekibi ve China Mobile Gelecekteki bilgi ve İletişim Teknolojileri Zirvesi Pekin de yapıldı. Bu zirvede hükümet temsilcileri, uzmanlar, Telekom operatörleri, Avrupa, Çin, Japonya, Güney Kore, diğer ülkeler ve bölgelerin önde gelen yazılım, donanım üreticileri Beşinci nesil teknolojisi için gelişim stratejisi ve AR-GE planına ilişkin çalışmalar yapıldı. Beşinci Nesil üzerine araştırma, standardizasyon gereklilikleri üzerine araştırma, Beşinci Nesil spektrum planlanması, Pazarlama analizi ve vizyonları,

Beşinci nesil yenilikçi hizmet uygulamaları ve gereksinimleri, Kablosuz iletim ve ağ teknolojileri, gelecekteki ağ gelişimi için stratejiler ve yakınsama uluslararası iş birliği tartışıldı.

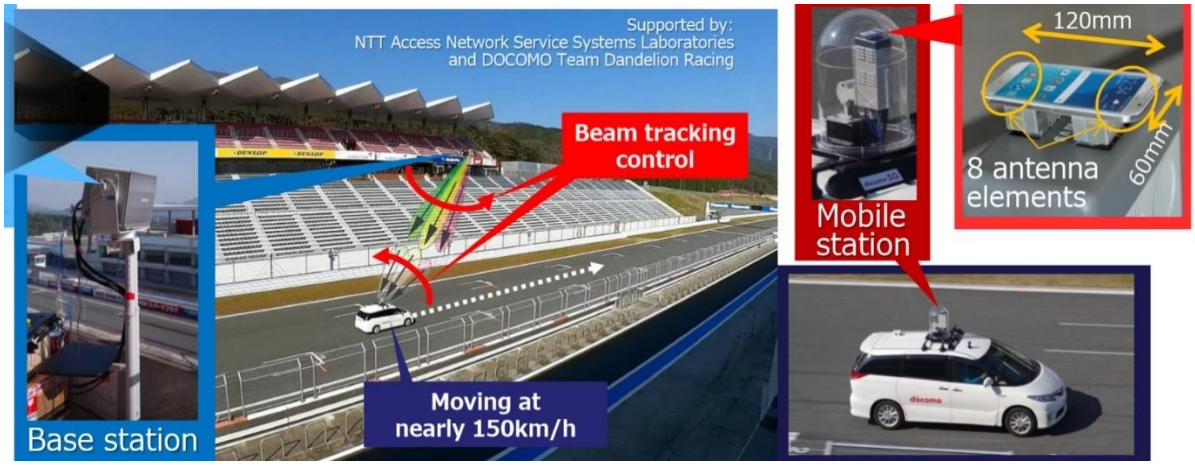
2013 yılının şubat ayında Japon Telekom operatörü NTT DoCoMo şirketi, Japon Tokya Teknoloji Enstitüsü'nün teknik desteğiyle Ishigaki Adasında 11 GHz frekans bandında 10 Gbps veri iletimi konusunda başarılı bir dış deney gerçekleştirildi.

2013 yılının Ekim ayında NTT DoCoMo, iletişimde ultra yüksek hız ve düşük gecikme özelliğine sahip donanımlarını Japonya Birleşik Teknoloji Gelişmiş Sergisi'nde (CEATEC) teknolojisi sergisinde tanıtımı yapıldı. NTT DoCoMo 5 Gbps üzerinde standart haline getirilmesi konusunda çalışmalar yapmaktadır. Artırılmış gerçeklilik, yüz tanıma, kelime tanımlama, çeviri vb. dâhil olmak üzere kullanıcıların çeşitli işlemleri kolayca kullanabilmeleri için giyilebilir donanımlar Beşinci Nesil teknoloji içeresinde kullanmayı hedeflenmektedir.[25]

2.4.3.4 Diğer Çalışmaları

Samsung, Beşinci Nesil Teknolojisi için çalışma yapan teknoloji şirketlerinden olmuştur. 2013 yılında mayıs ayında mmWave Beşinci Nesil teknolojisini duyurdu. Samsung'un Advanced Communications Lab'ın dış mekân deneyleri ve Güney Kore'nin Suwon kentinden 64 anten elemanı kullanan bir ilk örnek verici test edildi. 28 GHz taşıyıcı frekansında 1.056 Gbps hıza ulaşabilmektedir. Diğer bir test ise Japonya Fuji pistinde yaklaşık 150 km/s hızında maksimumum 2.59 Gbps hız elde edilmiştir.

[25] 5G Americas, Global Organizations Forge New Frontier of 5G, July 2016



Şekil 20 Samsung Beşinci Nesil 28GHz Beam İzleme Deneyi

Samsung firması, 120mm x 60 mm boyutunda bir kutuya monte edilmiş akıllı telefon kullanarak, 8 anten elemanlı mobil istasyon ile MIMO çoğullaşması hem Baz istasyon da hem de mobil istasyonlarda ışın biçimlendirme kullanarak 3.77 Gbps hız elde edilmişti. [26]

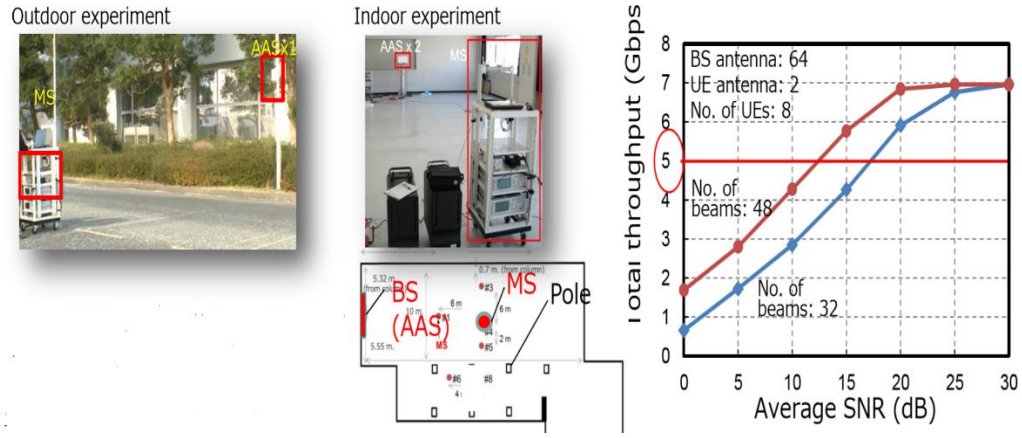
Samsung 2018 yılının ikinci yarısında Samsung ve Verizon arasında yapılan anlaşma ile ABD'de kullanıcılar ticari Beşinci Nesil hizmetlerinin ilk deneyimin yaşayacaklar Samsung ABD deki en büyük mobil şebeke operatörüne Yapılan anlaşma Beşinci Nesil teknolojisi Sabit Kablosuz Erişim (FWA) tabanlı ağ çözümleri tedarikini ana hatlarıyla içermektedir Beşinci Nesil hizmetlerinin başlamasının sektörün öngördüğünden iki yıl önce başlamasını sağlamıştır. Beşinci Nesi FWA, bakır ve optik fiber ağların konuşlandırılması gerektirmen, bağlantı hizmetlerinin Gigabit hızlarında radyo spektrumundan sağlanmasına olanak sağlayan kilit bir teknoloji olarak öne çıkmaktadır. samsung ve Verizon 2019 yılın ikinci yarısında Sacramento'da hizmet vermeyi hedeflemektedir. Şirketler önümüzdeki yıllarda FWA hizmetinin kullanan hane sayısı 30 milyona çıkması beklenmektedir.[27]

[26] https://www.nttdocomo.co.jp/english/info/media_center/event/mwc2017/pdf/about_5g.pdf ET:20.01.2019

[27] https://news.samsung.com/global/5g-is-now-part-1-2018-the-year-of-5g Et:20.01.2019

NEC Coporation, 23 Mayıs 2018 yılında Tokyo şehrinde iki Baz istasyonu arasında ışın formunu kullanarak sekiz mobil istasyonda 4.5 GhZ bandında dünyanın ilk 5.5 Gbps hız veri gönderim denemeleri başarılı gerçekleştiği duyurdu.

NEC ve NTT DOCOMO dijital sinyal işleme yoluyla sinyal işlemciler ve büyük elemanlı antenlerden oluşan iki Baz istasyonu arasında koordineli bir ışın biçiminde uygulama yapıldı. 9 ile 11 Mayıs 2018 tarihleri arasında Kawasaki şehrinde sekiz kullanıcı mobil istasyonlar arasında eş zamanlı bir veri iletim denemesi yapıldı. Bu denemede sekiz mobil istasyonda optik fiber üzerinden sinyal işleme ile antenleri toplam 128 elemente bağlayan optik besleyici yapısının küçük Baz istasyonları vasıtasıyla ışın biçimlendirmesi kullanılarak sekiz mobil istasyonda 5.5 Gbps kablosuz iletişim sağlandı. Bu yapı özelliği ile yüksek nüfus yoğunluğuna sahip kentsel alanlarda bile daha yüksek kapasiteli iletişim sağlanması hedeflenmektedir.



Şekil 21 NEC Beşinci Nesil 5.2 GHz Denemeleri

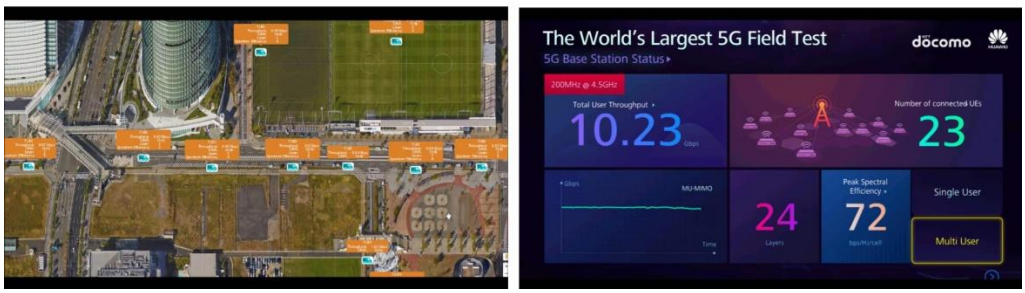
Fujitsu, NTT DOCOMO firması Beşinci Nesil haberleşme sisteminin ticari hizmetleri sorunsuz bir şekilde sunmak için mevcut donanım kullanarak bir Beşinci nesil ağını gerçekleştirmeyi amaçlamaktadır. Fujitsu Üçüncü nesil LTE ve LTE-Advanced ağlarıyla aynı anda çalışma esnekliğine sahip alanları geliştirilerek

Beşinci nesil ağlarında kullanılması hedeflenmektedir. Üçüncü nesil LTE-LTE-Advanced radyo erişim teknolojileri için mevcut Baz istasyonlarında minimum donanım değişikliği ve yazılım değişiklikleri gerçekleştirerek Beşinci nesilde kullanılması öngörülmektedir.

Şekil 22 Fujitsu 4.6GHz Dış Mekân Deneyi

Fujitsu 4.6 GHz dış mekân da sekiz kullanıcı cihazı, bir kullanıcı anten ve 4 dağıtılmış anten, 16 yerleştirilmiş anten ile gerçek zamanlı dağıtılmış anten ile yerleşik anten karşılaştırmalı denemeler gerçekleştirildi.

Huawei, 16 Kasım 2016 Tarihinde Japonya da 3GPP Beşinci Nesil anlaşmalarına uygun alt yapı kullanarak 4.5 GHz bandında dünyanın ilk geniş saha ölçekli denemesini gerçekleştirdi. Japonya'nın Yokohama kentinde gerçek bir kentsel uygulama senaryosunun makro hücre kapsamında 11.29 Gbps/sn kullanıcı verimi 0.5 milisaniyeden daha az tek yönlü kullanıcı düzlemi sağlandı. Bu deneme Beşinci nesil teknolojisinin en önemli çalışması olmuştur.



Şekil 23 Huawei 4.6GHz Büyük Ölçekli Beşinci Nesil Test Çalışması

Huawei, 23 Mayıs 2018 Tarihinde Japonya da 39GHz milimetre dalga (mmWave) bandını kullanarak başarılı bir Integrated Access Backhaul (IAB) teknoloji denemesi yaparak Beşinci nesil denemelerinde önemli bir dönük noktası olmuştur. Japonya'nın Minato Mirai 21 sahil bölgesi Yokohama'da gerçekleştirilen saha deneyi, IAB bulunduğu yerden 39 GHz sinyalleri kullanana Beşinci nesil Baz istasyonu ile Beşinci nesil röle bağlantısı arasında kablosuz veri iletimini içermektedir. Mobil kullanıcı 29GHz sinyalleri üzerinden kablosuz erişim sağladı.

YIL	ŞİRKET	PROJE ADI
2016	Huawei and Vodafone Group plc	Huawei ile olan Vodafone Group, Newbury'de (İngiltere) 70GHz'de çalışan bir deneme sisteminin özelliklerini gösteren bir 5G alan testini tamamladı.
2017	Huawei and China Mobile Ltd.	Huawei ve China Mobile, 5G 3.5GHz prototipini ve Ka-Band milimetre dalga prototipini sergiledi
2017	Huawei and Deutsche Telekom	Huawei ve Deutsche Telekom, tüm Cloud 5G ağ dilimlemesini çalışmaları yapıldı.

Tablo 4 HUAWE Beşinci Nesil Diğer Projeleri

2.4.4 Türkiye

Türkiye'de Beşinci Nesil ve ileri teknolojileri incelemek, ürün, hizmet geliştirmek amacıyla endüstri, üniversite, sivil toplum örgütleri, akademi bir araya geleceği ve iş birliği yapabileceği yapılan çalışmaların tek bir merkezden yönetilmesi amacıyla 2016 yılında Yeni Nesil Mobil Haberleşme Teknolojileri Türkiye Forumu (5GTR) Kurulmuştur. Uluslararası organizasyonlara üye katılımı gerçekleştirmek, ürün, servis geliştirerek dünya pazarına açılabilmek, endüstri sektörünün ihtiyaçlarını karşılayacak ürünler çıkarması forumun amaçlarındandır. 2017 Tarihinde 5GTR faaliyetleri başlamıştır. Çalışmanın ilk bölümünde Çekirdek ağ ağ Çalışma grubu, Fiziksel Ağ grubu, Hizmet ve uygulama grubu, Standardizasyon grubu ve alt grupları kurulma karar alınıştır.

2017 yılında BTK önderliğinde Avea, TURKCELL, Vodafone, Hacetepe, Bilkent, ODTU, üniversitesiler ile Beşinci Nesil Açık Test Saha İş birliği protokolü imzalandı. Bu protokol ile Akademisyenlerin, doktora öğrencilerin, diğer kuruluşların Beşinci nesil geliştirmelerinin yapılması için test şebeke alt yapılarının kurulması öngörülmüştür.

Güney Kore de Beşinci nesil çalışmaları yürüten 5G Forum ile 5GTR Forumu ve Japonya 5GMF Forumu arasında 2017 yılında karşılıklı anlaşmalar yapıldı.

Telekomünikasyon şirketlerinden olan TURKCELL ve HUAWEI ortak yürüttükleri çalışmalar çerçevesinde Beşinci Nesil mmWave olarak kabul edilen 71.5-73.5 GHz band aralığın da 70 Gbps hıza ulaşılmıştır.

2.5 Beşinci Nesil Teknolojinin Etkileşimdeki Teknolojiler

2.5.1 Cihazdan Cihaza İletişim (D2D)

Beşinci Nesil önceki haberleşme sisteminin şebeke içerisindeki tüm cihazlar, merkezi Baz istasyonları ile iletişime geçerek veri iletimini sağlayacaktır. Baz istasyonları devreden çıkararak şebeke ağının kapsama alanını genişletmek için çalışmalar yapılmıştır. Dördüncü Nesil standardında Cihazdan Cihaza iletişim

(D2D) teknolojisi geliştirildi. D2D iletişimi, bir ağda Baz istasyonu veya ara cihazlar olmadan birden fazla D2D cihazı veya kullanıcı arasındaki iletişimi sağlayan teknolojiyi ifade etmektedir. Bu teknoloji Beşinci Nesil ve ileri teknolojisi ile yaygınlaşmaya başlanmadı hedeflenmektedir.

Cihazdan Cihaza iletişimin kullanım bakıldığında operatör şebeke merkezi yönetiminde kullanıcı cihazı EU Baz istasyonu gibi kullanarak kapsama alanını genişletmektedir. Diğer bir kullanım şebeke operatör olmadan birden fazla cihazlar kendi aralarında iletişime geçerek ağ kurabilmektedir.

Beşinci Nesil teknolojisinin yaygınlaşmasıyla Cihazdan Cihaza (D2D) iletişimin yaygınlaşması verilerin tüm cihazlar üzerinden dolaşması anlamına gelmektedir. Bu cihazlar taşıdığı verilerin önem durumuna göre saldırı tehditleri oluşabilecektir. Bu hem cihazın kullanıcıları hem de operatörlerin verilerinde zafiyet gösterebilir.

2.5.2 Görünür Işıkla İletişim (VLC)

Geleneksel Radyo Frekans (RF) tabanlı kablosuz iletişim ihtiyaçlarını karşılamada sıkıntıları çözüm oluşturmak ve alternatif oluşturmak için yapılan çalışmalar üzerine Görünür Işıkla İletişim (VLC) teknolojisi geliştirmek için çalışmalar başlatılmıştır. LED ışık frekanslarını kullanarak veri iletiminde 500 Mbps hızına ulaşabilmektedir. Bu LED ışık frekanslarını yanıp sönmesi ile veriyi mesaj haline getirebilmekte kullanıcının akıllı telefonların üzerinde bulunan kamera aracılıyla ışık mesaja dönüştürülmektedir. Böylelikle mekânda veya alanda ışık ekranları üzerinden veri iletişimi sağlanabilmektedir.

Beşinci Nesil yayılması ve kullanılması beklenen VLC iletişimi LED ışıklarının olduğu hava alanları, dükkânlar, sokak lambaları, LED reklam panoları gibi geniş alanlarda veri iletişimi sağlanır hale gelecektir. Akıllı şehirler ve Otomotiv sektörlerinde bu teknolojinin yoğun kullanımı beklenmektedir. Bu teknoloji kullanımında zafiyetler gösterme konusunda açık gözükmektedir. Her türlü cihaza istenilen yerden cihazlara, otonom araçlara ulaşabilmektedir. Bu da

taklit etme, dinleme, saldırı yöntemleri ile veri güvenliği konusunda güvenlik açıkları verebilmektedir.[28]

2.5.3 Makine Tipi İletişim (MTC)

Beşinci Nesil standart çalışmalarını yürüten METIS grubunun 3GPP' de Makine Tipi İletişim (MTC) terimi kabul edildi. Mobil Tipi İletişim mobil makineleri birbirine bağlanmaktadır. MTC İletişimi bir sunucu arasında olabileceği gibi doğrudan iki MTC cihazı arasında da olmaktadır. Sağlık, lojistik, üretim otomasyon, enerji gibi endüstri alanlarında potansiyel olarak kullanılması öngörülmektedir. Beşinci Nesil en önemli ultra güvenilir ve düşük gecikme özelliği ile makineler arasındaki iletişimin yaygınlaşmaması hedeflenmektedir.

MTC, Beşinci Nesil Şebeke ağına iki ana zorluk getirmektedir. Bunlardan biri bağlanması gereken cihazların sayısının çok fazla oluşudur. Gelecek ağ yapısında toplam 50 milyar cihazın bağlanması gerektiği öngörülmektedir. İkinci zorluk ise ağ üzerinden çok fazla bağlı olan cihazların gerçek zamanlı uzaktan kontrol edilme ihtiyacı getirmektedir. Bu ihtiyaç milisaniyeden daha düşük gecikme süresi gerektirmektedir.

MTC uygulamaları farklı trafik özelliğine sahiptir. Genellikle küçük ve nadir veriler uplink üzerinde daha yüksek trafik hacmi ortaya çıkarmaktadır. Bu şebeke ağın veya iletişiminde sorunlara neden olabilir.[29]

[28] WU Shaoen, WANG Honggang, Visible Light Communications for 5G Wireless Networking Systems: From Fixed to Mobile Communications, IEEE Network, December 2014, 0890-8044

[29] Machine-type communications: current status and future perspectives toward 5G systems, Aolto University,2015

ÜÇÜNCÜ BÖLÜM

BEŞİNCİ NESİL (5G) MOBİL İLETİŞİM TEKNOLOJİLERİ UYGULAMA ALANLARI VE YENİ RİSKLİ VERİLER

Beşinci Nesil Kablosuz haberleşme sistemleri dünyayla iletişim kurması ve daha verimli sanayi daha akıllı teknoloji geliştirilmesinde yenilikçi yolların başlangıcı anlamına gelmektedir. 2020 Yılında ticarileşmesi beklenen Beşinci Nesil haberleşme sistemi klasik mobil geniş bant uygulamaların internet, ses iletişimin ötesinde ultra gecikme süresi, yüksek hız özellikleri ile dikey sektörleri ihtiyaçlarını gidererek tüm sektörleri birbirine bağlayan iletişimin ötesindeki teknolojinin başlangıcı olarak nitelendirebiliriz. Bu bölümde Beşinci Nesil haberleşme sistemlerinin bazı sektörlerde getirdiği yenikleri ve şebeke ağına veri dolaşımı yapabilecek yeni verilerin analizleri yapılmıştır.

3.1 Otomotiv Sektörü

Diğer sektörlerin en önemlisi otomotiv sektöründe Beşinci nesil haberleşme sistemi ile yakınsama olmaktadır. Otomotiv Endüstrisi bağlı cihaz teknolojisi kullanımı erken olarak başlayan sektör olmuştur. Otomobil üreticileri tarafından bağlantılı hazır otomobillerin geliştirilmesinde önemli uygulamalar yapılmıştır. Araç içi deneyimin iyileştirilmesi, trafik akışının ve karayolunun genel güvenliğinin sağlanmasına yardımcı olmak, araçların performansı hakkında bilgi edinmek ve bakıma yardımcı olmak gibi uygulamalar otomotiv sektörünün konusu olmuştur.

Otomotiv endüstrisindeki hizmetlere bakıldığında araç içi bilgi-eğlence iyileştirilmesi, otonom sürüşün doğru evrimleşmesi, araçtan her şeye haberleşme Beşinci nesil haberleşmenin getirdiği fırsatlar olarak değerlendirilmektedir.

3.1.1 Akıllı Hareketlilik (V2X)

Otomotiv Sektörü uzun yıllar boyunca araçlar arasında iletişim kurulması ve bilinçli araçlar üretilmesi konusu çalışmalar yapılmaktadır. Araçlar arasında iletişim (V2V), araçların yakınındaki ağlarla iletişim (V2I), araçların internet ağlarıyla (V2N) aynı anda iletişim kurulması hedeflenmektedir. Elektronik, Bilgisayar, algılama teknolojileri ve makine öğrenme konularındaki gelişmeler endüstri sektöründeki makineler arasındaki iletişimi uygulamaya geçilmesini hızlandırmıştır.

Beşinci nesil sistemlerinde birden fazla hizmetten gelen verimlilik, gecikme, güvenilirlik, kapasite ve mobilite yüksek performans sağlayan hizmetler ve özellikleri araçların ve akıllı şehirlerin oluşmasında büyük adım haline gelmesi düşünülmektedir.

Akıllı hareket (V2X) teknolojisi, Araçların birbirleriyle ve tüm her şey ile iletişime geçerek trafik kazaların azalmasını, sürücülerin güvenilir ve rahat kullanımı sağlamak amacıyla akıllı şehirlerde kullanıldığı teknolojidir. 2016 yılında yapılan araştırmalarda V2X sistemlerinin uygulamaya geçilmesiyle oluşan kazaların %80 oranında düşüş göstereceği öngörülmektedir. 2019 yılında üretilecek araçların Akılı Hareketlilik (V2X) teknolojisinin standart donanım halinde piyasaya sürülmesi konusunda çalışmalar yapılmaktadır.[30]

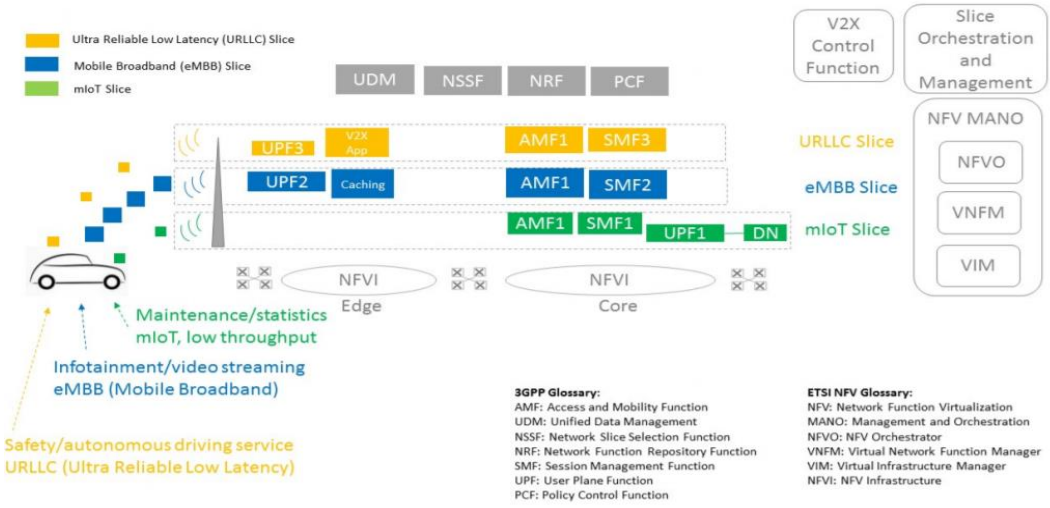
Akıllı hareket (V2X), araçlar arasında iletişimi sağlayarak altyapıyı mobilete yapısına dönüştürerek karayolları arasında gerçek zamanlı bilgilerin otomatik olarak Beşinci nesil haberleşme ve diğer teknolojiler aracılığıyla merkezi bir yapıya aktarılarak, bu bilgilerin yapay zekâ programları ile analiz ederek karayolların ve diğer ulaşım altyapıların verimli kullanımını üst düzeye çıkabilecektir. Araçların sürücüleri ve yolcuları trafik sinyal aşamalarını, çalışma alanlarını, yol tehlikelerini

[30] Visiongain. Automotive Vehicle To Everything V2X Communications Market 2016 Visionagain, Report 2016.

Beşinci nesil ve ötesi teknolojileri kullanarak mobil uygulamalar kullanarak kullanıcıya ulaşabilme bu teknolojiye bir örnek gösterilebilir.

Gelecek teknolojisi Beşinci nesil teknolojisi yazılım tabanlı (SDN), Kontrol-Kullanıcı Düzlem Ayrımı (CUPS), Şebeke sanallaştırması (NFV), Şebeke ağ dilimleme özellikleri ile veri akışlarının anlık oluşması, merkezi kontrol düzleminde yönetilmesi sağlayarak akıllı hareket (V2X) ve akıllı şehirlerin oluşturulmasın temel taşı niteliğindedir.

Akıllı hareket (V2X), araçların üzerindeki geliştirilmiş algılayıcılar ile aracın dışındaki çevreye veya diğer araçlarla konuşup aracın etrafındaki tüm veri bilgilerini dinleyerek toplanmaktadır. Bu da verilerin güvenliği konusunda zafiyet gösterebilir.



Şekil 24 Akıllı Hareketlilik(V2X) Beşinci Nesil Şebeke Ağı Örneği

Akıllı Hareketlilik (V2X) 3GPP TS 22.1853 standart sürüm14 çalışmalarında aşağıdaki servisler kullanıma sunulmuştur.

- İleri Çarpışma Uyarı Sistemi
- Acil Araç Uyarı Sistemi
- Yol Güvenliği Servisleri
- Otomatik Park Sistemi

- Yanlış Yol Sürüş Uyarı Sistemi
- Çarpışma Öncesi Algılama Uyarısı Sistemi
- Trafik Akışı Sistemi
- Hassas Yol Kullanıcı Güvenliği

Akıllı Hareketlilik (V2X) 3GPP TS 22.1853 standart sürüm15 ve sonrası çalışmalarında aşağıdaki servisler kullanıma sunulmuştur.

- Algılayıcı Durum Harita Paylaşımı
- Uzaktan Kontrol Araçlar
- Çevreye karşı Ortak Algılama Sistemi
- Dinamik Sürüş Paylaşımı
- Şehir İçi Sürüş Kavşak güvenlik bilgi Sağlama[31]

3.1.2 Navigasyon Bağlantı

Araçların seyir halinde navigasyon uygulamalarına bağlanarak sürücülere yararlı bilgiler vermektedir. Temel Kavram radyo yayın standartlarına göre veya mobil iletişim için hücresel ağlar aracılığıyla kullanıcılara trafik raporları sağlamaktadır. Böylelikle sürücülerin bulunduğu alanda trafik koşulları hakkında, trafik yoğunluğunu kaçınarak uygun konum üzerinden yolculuğa devam etmektedir. Bu bilgilendirmeler Beşinci nesil haberleşme sistemleri üzerinden anlık şekilde araca veri gönderilecektir. Gerçek zamanlı trafik yoğunluğu verilerini artırılmış navigazyon hizmet uygulamaları ile trafik akışını en düzeye çıkararak akıllı hız, şerit modülleri dahil ederek kullanıcıya üst düzey hizmet sunmaktadır.

[31] 3GPP TR 22.886, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on enhancement of 3GPP support for 5G V2X services

3.1.3 Otomotiv Sektörü Yeni Riski Veriler

Akıllı hareketlilik (V2X) sisteminin veri aktarımını sağlayan 3GPP'de geliştirilen tamamlayıcı aktarım modulü aşağıdaki gibidir.

Direk iletişim (Direct Communications), Araçların herhangi bir ağa bağlanmadan direk araçlar arası iletişim olarak tanımlayabiliriz. V2X teknolojisinin getirdiği yenilikle araçların kendi aralarında iletişim kurarak yol çalışma uyarısı, kavşak hareketlilik yardımcısı, kör nokta asistanı, sola dönüş yardımı gibi hizmetlerin sayesinde birbirleriyle veri dolaşımı sağlanmış olacaktır. 3GPP sürüm 12/13 cihazdan cihaza (D2D) ara yüzünü ve teknolojisini temel almaktadır. Düşük gecikmeli iletişimin sağlanmasında ve büyük miktarlarda verilerin diğer araçlarla verilerin aktarımını yapılmasında yardımcı olmaktadır.

Ağ iletişim (Network Communications), Beşinci Nesil haberleşme mimarisi vasıtasıyla verilerin cihazdan ağa bulut servislerine uçtan uca çözüm sağlamak için V2X için kullanılan sistemdir. Trafik akış kontrolü, Bulut tabanlı paylaşımlar, 1 km ilerde yol tehlikesi, Uzaktan kontrol gibi hizmetleri kapsamaktadır. [32]

Akıllı hareketlilik (V2X) sisteminin ve Beşinci Nesil haberleşme sisteminin gelişiminde otomotiv sektörü ile bilişim sektörünün birlikte çalışmalar yapmaktadır. Bu çalışmalar araçların sensör ve işlemcilerle akıllı olmasına neden olmuştur. Araçların veri alışverişini sağlamak için kullanılacak akıllı bağlantı cihazları şu şekildedir.

Heterojen Bağlantı; Araçların her şey ile iletişimi, Bilgi ve Eğlence bağlantıları, Gerçek zamanlı bağlantı, Bluetooth, Kablosuz bağlantı noktası, Hücresel Şebeke Dördüncü ve Beşinci Nesil, Ethernet, Radar, Kamera, 3D HD harita, hassas konumlandırma servis bağlantı cihazlarıdır.

[32] https://www.qualcomm.com/media/documents/files/accelerating-c-v2x-commercialization.pdf Erişim Tarihi:11.02.2019

Cihaz İçi Zekâ; Bilgisayarlı görüş, Sezgisel güvenlik, Makine öğrenme, Artırılmış gerçeklik, sezgisel bağlantılar, Cihaz açık algılama sistemleridir.

2018 Yılında yayınlanan rapora göre internet kullanımının büyük çoğunluğu mobil cihazlardan oluşmaktadır. Beşinci Nesil ve Nesnelerin interneti teknolojilerin hayata girmesi ile bu internete bağlantı sağlayacak cihazların sayıların büyük bir artış sağlanacağı görülmektedir. Beşinci Nesil haberleşme teknolojisi ile internete veriler artık anlık yüklenecektir.

Otomotiv sektörüne baktığımızda bu riskli veriler aşağıdaki şekilde gruplanmıştır.

Anlık Kişisel Veriler, Araç kullanıcısının kullanım alışkanlık verileri, anlık yer ve konum bilgisi, Kullanıcının araca özgü verileri (Aracın Modeli, Markası, Teknik özellikleri gibi), Araç içersin de bulunan kameranın görüntü verileri, Araç içersin de kullanılan eğlence cihazlardan alınabilecek ses verileri gibi kişi belirleyecek verilerdir.

Anlık Cihazın Toplayacağı Veriler, Araç içersin de kullanılan işlemci, algılayıcılar, Bluetooth, Kablosuz bağlantı noktası, Kamera cihazların diğer cihazlarla iletişime geçtiği anda ulaştığı ve kısa zamanlı üzerinde tuttuğu verilerdir. Cihazdan Cihaza iletişim halinde olunan cihazların başka kullanıcılara ait verilere ulaşabilecektir.

Araç kullanım halinde iken araç da bulunan cihazların dış ortam bulunan görüntüleri veya sesleri araç sahibinin bilgili olmadan ulaşabilir ve bu bilgileri kendi üzerinden tutabilir. Ulaşılan bu bilgiler anlık başka platformlardan izinsiz aktarılabilinir.

Anlık Cihaza Özgü Veriler, Araç içersin de kullanılan cihazların üreticiler tarafından cihazı belirleyecek kimlik numaraları bulunmaktadır. Araç üreticileri araç içerinde hangi cihazları kullandığını kimlik numaralarını takip etmektedir.

Araç içersin de kullanılan cihazların marka ve modellerini veya hangi tip cihazlar kullanıldığını anlık platformlar aracılığı ile öğrenilebilme risk ortaya

çıkmaktadır. Bir dünya markalı otomotiv şirketinin x markalı bir cihaz kullanıldığı öğrenildiğinde o cihazla alakalı zafiyetler üzerinden tüm araçları veya araç kullanıcıları tehdit altında olabilmektedir.

Mal ve Can Güvenliğini Tehdit Eden Riski Olan Veriler, Cihazlar ve nesneler arası veri iletiminde verinin değişmesi, bozulması sonucunda ortaya çıkan can ve mal güvenliğini tehdit eden veri tipleridir. Kullanıcının Araç içeresinde kullanım durumunda iken araç bluetooth, wifi veya diğer cihazlar üzerinden aracın işlemci sistemleri ele geçirilerek yön değiştirilmesi ile can güvenliğine bir örnektir. 2013 Tarihinde yapılan bir deneme de Porsche markalı lüks aracın uzaktan işlemcisi ele geçirilerek kullanıcı içeresinde olmadan araç çalıştırılması ve yön verilmesi başarılmıştır.[33]

3.2 Enerji Sektörü

Enerji Sistemleri yıllar boyunca gelişen teknolojilerle ve ihtiyaç talepleri ile sürekli gelişmiştir. Dökme yağ, gaz, kömür, petrol gibi yakıtlar ile dünya nüfusunun ihtiyaçları karşılanmaktadır. Yeni enerji sisteminde artık yenilebilir rüzgâr, güneş gibi enerji sistemleri üzerinde çalışmalar yapılmaktadır. 2017 yılı itibariyle Avrupa da kömür enerji kullanımı azalarak yerini güneş, rüzgâr gibi yenilebilir kaynaklardan enerji üretimine yönelmiştir.[34]

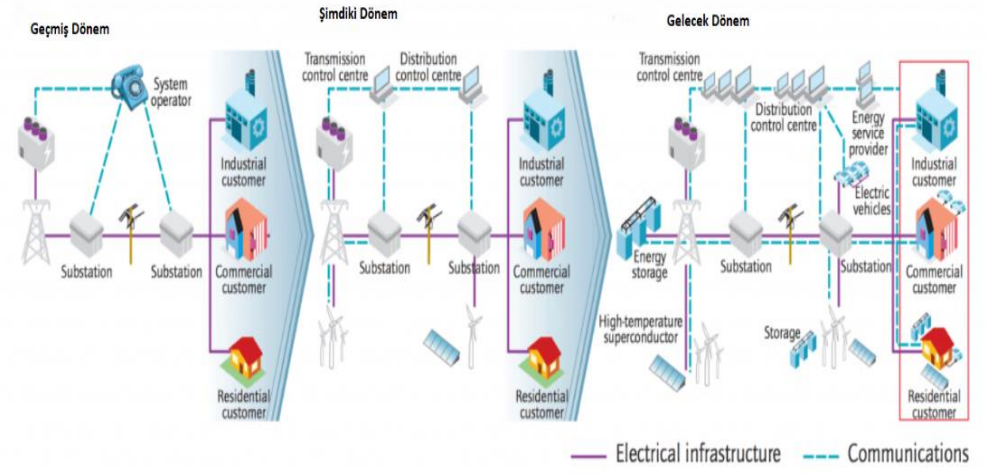
Enerjinin üretiminde ve geliştirilmesinde son kullanıcıların enerji kullanım çeşitliliğin analiz yapılması ve buna uygun enerji üretim seviyelerinin karşılanması uygun planlamaların yapılması gerekmektedir. Enerji sektörü bu planlamaları doğru yapabilmesi için Akıllı şebekeler geliştirerek kullanım analizleri, ihtiyaç analizleri, dağıtım analizleri, tedarik analizleri gibi verileri elde etmiş olacaktır. Beşinci Nesil Haberleşme sistemleri ile bu verilerin anlık izlenebilmesi sağlanmış olacaktır.

[33] https://www.youtube.com/watch?v=3nJQYLdE878 Erişim Tarihi:11.03.2019
[34] https://www.dunyaenerji.org.tr/bp-enerji-gorunumu-2018/ Erişim Tarihi:11.03.2019

Beşinci Nesil haberleşme sistemi ile Enerji Sektöründe Smart grid, Akıllı şebeke, Akıllı sayaç okuma, Gerçek zamanlı kontrol, Akıllı aydınlatmalar, Akıllı enerji ölçüm algılayıcı cihaz ve teknolojiler ile verimli enerji kullanımını sağlanması hedeflenmektedir.

Birçok bağlantısız cihazların Akıllı enerji şebekesine entegre edilmesi ile bu bağımsız cihazların Beşinci nesil haberleşme veri iletişim alt yapısını kullanarak birbirleriyle iletişim sağlaması ile enerji ihtiyaçların daha iyi analiz edilmesini ve doğru bir şekilde izlenmesine sağlayacaktır.

Beşinci Nesil haberleşme sistemleri bağlantıları aracılığıyla verileri toplamak, enerji altyapısını daha verimli bir şekilde planlamak ve kesinti süresini azaltmak için önlemler almasını yardımcı olacaktır. ABD Chattanooga TN orta ölçekli kasabada şiddetli bir rüzgâr fırtınasında elektrik kesintilerinin süresini smart grid teknolojisi kullanılarak %50 den fazla azaltarak bir fırtına için operasyon maliyetinde 1.4m dolar fayda sağlamıştır.[35]



Şekil 25 Akıllı Enerji İletişim Örneği

[35] https://www.accenture.com/t20170222T202102__w__/us-en/_acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf Erişim Tarihi:11.03.2019

Akıllı yol ve sokak aydınlatmaları ile kamu alanda enerji tasarrufuna neden olabilmektedir. Akıllı aydınlatma San Deigo ve Barselona şehirlerinde kullanıma başlandı. Sistem sayesinde yılda yaklaşık 1.9 m dolar tasarruf elde edilmiştir.

Beşinci Nesil haberleşme sistemlerinin yenilebilir rüzgâr enerji çiftliği alanında çok büyük faydalar ötesine geçmektedir. Bu alanda AB H2020 VirtuWind projesi üzerinde çalışmalar yapılmaktadır. Bu proje Beşinci Nesil haberleşme mimarisi olan yazılım tabanlı ağ (SDN) ve ağ fonksiyonu sanallaştırma (NFV) rüzgâr çiftliklerinde sanallaştırılmış bir ağ yapısı kurulması hedeflenmiştir. Rüzgâr çiftliklerin güvenli ve verimli çalışma sağlamaktadır. Bu tür kontrol ağ yapıları kurulumu, işletilmesi ve bakımı gibi yüksek maliyetlerin yerine yazılım tabanlı ağ (SDN) ve ağ fonksiyonu sanallaştırma (NFV) teknolojilerini kullanarak bu süreçleri daha hızlı ve daha basit getirmektedir.

3.2.1 Enerji Sektörü Yeni Riski Veriler

Beşinci Nesil haberleşme sistemi Enerji Sektöründe bağlantısız tüm cihazları birbirine bağlayarak haberleşme şebekesinde ve internet ortamında enerji sektörüne ait verileri ulaşılabilir ve uzaktan kontrol edilebilir olacaktır.

Enerji sektörüne baktığımızda bu yeni riskli veriler aşağıdaki şekilde gruplanmıştır.

Anlık Kişisel Veriler, Akıllı sayaç okuma cihazları ile anlık kullanıcıların enerji tüketim okumalarından oluşan analiz edilebilen verilerdir. Kullanıcıların enerji kullanımı konusundaki alışkanlıkları ve kullandıkları verileri anlık takip edilebilecektir. Bu veriler kişiyi niteleyen kişinin can ve mal güvenliğini tehdit eden veri kapsamına girmektedir.

Anlık Ticari Veriler, Tüzel kuruluşların işlettikleri fabrikaların, depoların, merkezi binaların akıllı sayaç okuma cihazları ile işletmelerin enerji kullanım eğilimleri, alışkanlıkları belirleyen verilerdir. Uzaktan kontrol edilebilen verilerdir. Bu veriler, işletmenin yaptığı işi belirleyen, işletmeyi niteleyen özel veriler olarak

görebiliriz. Bu veriler öğrenildiğinde işletmenin üretimine veya yaptığı işlemlere çok büyük can ve mal kaybına neden olabilecektir.

Anlık Kamusal Veriler, Ülkenin, şehrin veya bölgenin sanal enerji ağları ile akıllı şebekeler ile anlık uzaktan yönetim sağlanabilmektedir. Bu akıllı enerji ağları ve şebekeleri sayesinde bölgenin önemli enerji analizlerini anlık elde edebilmektedir. Bu bilgiler kamu alanında çok önemli bilgiler olarak görebilmekteyiz. Bu şebeke ağının verileri ele geçirilmesi veya değiştirilmesi bölgenin enerji ihtiyacında kesintiler ve arızalara neden olabilmektedir. Bu bölgesel veya ulusal karışıklığa neden olabilecektir.

3.3 Lojistik Sektörü

Lojistik ve Tedarik Zinciri Yönetimi, genellikle üreticiden dağıtım merkezine, dağıtım merkezinden perakendeciye ve üreticiden perakendeciden tüketiciye, dağıtım zincirinin çeşitli noktaları arasındaki ürünlerin ve bilgilerin akışıyla ilgilidir.

Nesnelerin internet teknolojisi şirketlerin lojistik yaklaşımlarında büyük etkisi olması beklenmektedir. Beşinci Nesil Teknolojisi gelişmeleri lojistik sektörü üzerinde önemli bir etkiye sahip olacağı düşünülmektedir. Beşinci Nesil Teknolojilerin getireceği yüksek hızlı Internet özelliği sayesinde gelişmiş tedarik zinciri sektöründe şeffaflığı, güvenirliği ve verimli kaynakların planlamasını yapılabilecektir.

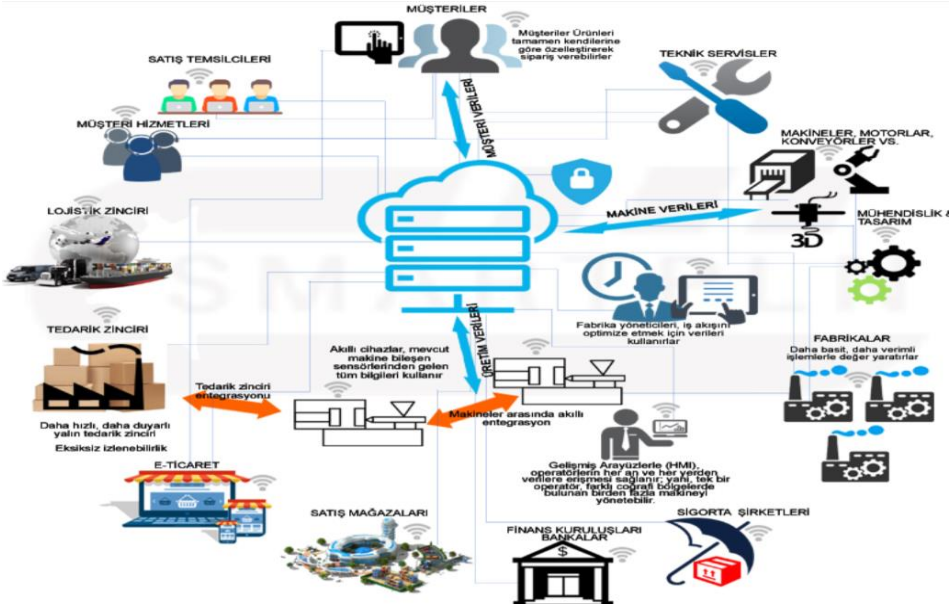
Nesnelerin odaklı akıllı envanter yönetimi ile hasar tespitlerinin gerçek zamanlı takip edilmesi ve kamera, algılayıcılar cihazlarıyla palet içi kontrol sağlayarak doğru envanter sonuçlarına ulaşması mümkün olabilmektedir. Bu da depo verimliliğini artması kaliteli hizmet sağlayacaktır.

Lojistik alanında optimum varlık kullanımı, tüm varlıkları gerçek zamanlı izlemek ve makine ve araçları cihazlarla merkezi bir sisteme bağlayarak hataların azaltılmasına işgücü verimliliğin artmasına neden olacaktır.

Lojistik alanının en önemli konularından Filo ve varlık yönetimi alanında kablosuz bağlantılar ve algılayıcılar cihazları kullanarak diğer nesne cihazları ile haberleşerek optimize edilmiş yollar kullanılmasına, daha iyi yakıt ekonomisine neden olabilecektir.

Lojistik sektöründe düşük nüfuslu bölgelerde İnsansız hava araçları kullanarak paket teslimatı yapılarak sektör yüksek hızlı teslimat sağlayacaktır.

Beşinci Nesil haberleşme sistemi yukarıda bahis edilen kullanım durumları teknolojisi ile destekleyecek ve gerçek zamanlı bilgi ve teslimat tahminlerinin doğruluğu lojistik sektöründe büyük evrimleşmeyi sağlayacaktır.



Şekil 26 Akıllı Lojistik Yönetim Süreci

3.3.1 Lojistik Sektörü Yeni Riski Veriler

Beşinci Nesil haberleşme sistemi lojistik sektöründe bağlantısız tüm cihazları birbirine bağlayarak haberleşme şebekesinde ve internet ortamında lojistik sektörüne ait verileri ulaşılabilir ve uzaktan kontrol edilebilir olacaktır.

Lojistik sektörüne baktığımızda bu yeni riskli veriler aşağıdaki şekilde gruplanmıştır.

Anlık Kişisel Veriler, Kişilere ait olan emtianı taşınması aşamasında bilgilerinin ilgili sistemlere kayıt edilmesi veya takip edilmesi sonucunda oluşan verilerdir. Amazon ve Google firmaları insansız hava araçları ile taşıma işlemleri üzerinde çalışmaktadır. Bu taşımada kişiye özgü emtianın takip edilmesi, izlenebilmesi kişiye özgü veri olarak düşünebilmekteyiz.

Anlık Ticari Veriler, Ticari işletmelerin ürettikleri veya pazarladıkları ürünlerin, üreticiden tüketiciye dağıtım sürecince izlenebilirliği olan verilerdir.

Bir noktadan diğer bir noktaya gidecek ürünlerin miktarı, ürünlerin cinsi, ürünlerin barkod numarası, ürünlerin fiyatları, ürünün sıcaklık, ürünün nem bilgisi, bulunma şartları gibi bilgisi, ticari işletmeyi niteleyen veri tipleridir. Bu veriler depolardan tüketiciye kadar izlenebilir olması ticari işletmeler için riskli veri niteliğindedir.

3.4 Tarım Sektörü

Birleşmiş milletler Gıda ve Tarım Örgütünün yaptığı açıklamada dünya nüfus artışındaki hız beslenmek için çiftçilerin 2050'de 2006'da olduğundan %70 daha fazla gıda yetiştirmeleri gerekmektedir. Bu açıklama çevremizde sürekli değişen iklim ve doğanın göz onunda bulundurulduğunda imkânsız bir göre gelebilir. İklim değişikliği, toprak bozulmadı ve su kıtlığı, yıllar içinde giderek etkisini artırmaya devam etmektedir. Bu sıkıntılarla mücadelelerde yardımcı olacak insanoğlunun geliştirdiği teknolojiler olacaktır. Endüstriyel nesnelerin interneti ve Akıllı Tarım nesnelerin interneti olarak adlandırdığımız teknolojiler tarım alanında büyük bir avantaj sağlayabilecektir.

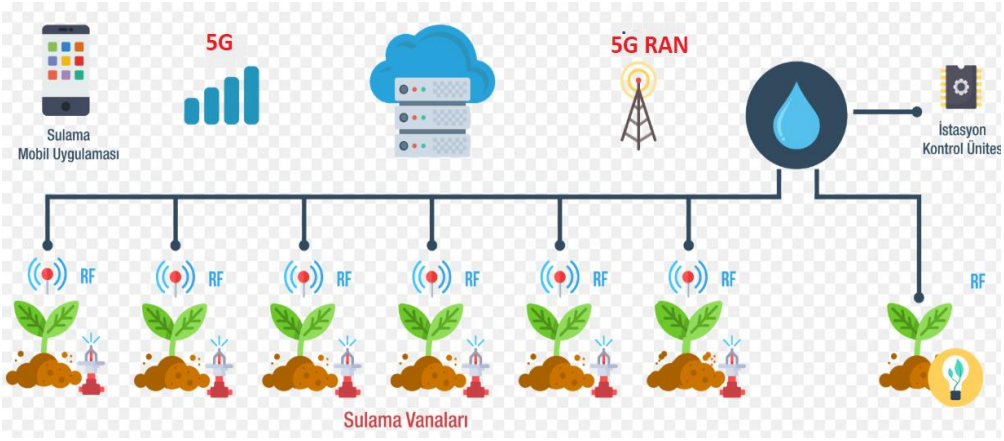
Akıllı Tarım, Çiftçinin yaptığı tarımsal operasyonları ve işlemleri geliştirmek, takip etmek, otonom haline dönüştürmek veya iyileştirmek için bilgi ve iletişim teknolojilerin geliştirdiği teknolojilerdir. Algılayıcılar toprak yapısını, gübreleme, hava durumu gibi bilgileri toplama işlemi yaparak Beşinci Nesil hücresel kablosuz

ağlar üzerinden bir ağ geçici cihazıyla merkezi bir sunucuya veya bulut teknolojisine iletir ve çiftçilerin arazileri, mahsulleri, çiftlik hayvanları, makinde durumları hakkında bilgi veri analizleri gerçekleştirir. Bu algılayıcılardan toplanan veriler analiz edildiğinde çiftçiler bu verilerle verimliliği artırmak için çalışmalar yapabilecektir.

Beşinci Nesil haberleşme sisteminin yüksek hızları ve bant genişliği ile nesnelerin İnternet'inin tarımda çok fazla kullanılmasına ve daha çok uygulamaların ortaya çıkmasına neden olabilecektir.

3.4.1 Akıllı Sulama Yöntemi

Tarım alanında sulama yöntemi, çiftçilerin en çok kullandıkları yöntemlerinden biridir. Sulama yöntemlerinin verimli bir şekilde fayda sağlaması için, Nesnelerin interneti ve Beşinci Nesil haberleşme teknolojileri kullanarak uzak algılayıcılardan toplanan veri sonucunda su kaynağının nereye yönlendirilmesi gerektiğini ne türlü bir hacimde ve ne kadar sürede kullanacağını anlık olarak akıllı cihazlardan izleyerek analiz yapılabilmektedir.



Şekil 27 Akıllı Sulama Sistemi Örneği

3.4.2 Akıllı Gübreleme Yöntemi

Gübreleme, toprağın üzerinde bitkinin daha verimli beslenmesi için toprağa verilen kimyasal elementlerden oluşturmaktadır. Nesnelerin ve Beşinci Nesil haberleşme teknolojilerin getireceği çözüm uygulamaları ile çiftçinin ne kadar ve hangi hacimde gübrenin toprağa vereceği uzaktan kontrol edilebilmektedir.

3.4.3 Akıllı Hayvancılık Yöntemi

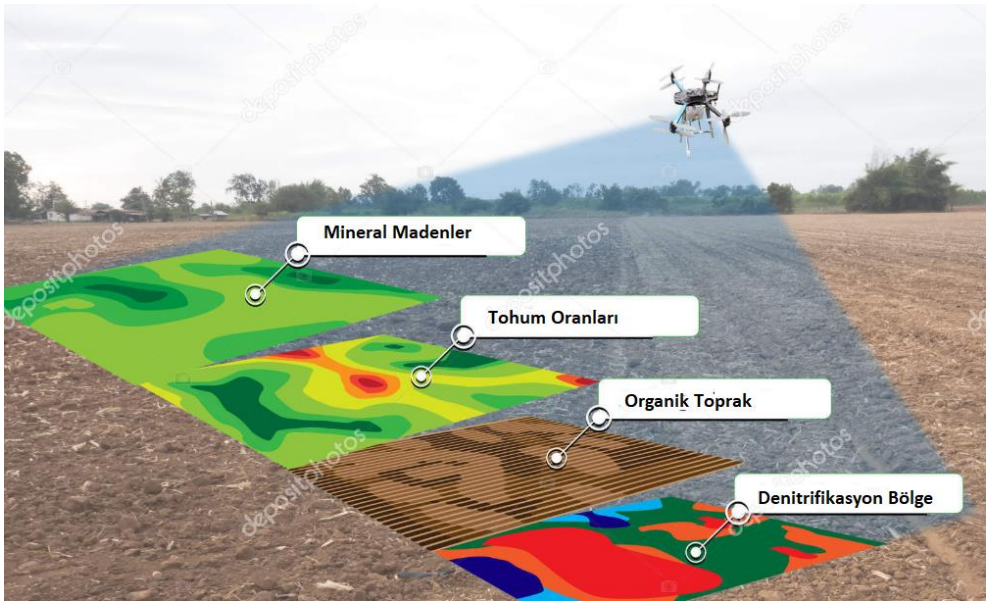
Beşinci Nesil haberleşme sistemleri kullanarak hayvanların üzerine yerleştirilen algılayıcılar ile hayvanların dolaşımını, vücut ısısı, nabız, doku direnci gibi biyomedikal verileri gerçek zamanlı takip edilebilecektir ve geliştirilebilecektir.

3.4.4 Akıllı Ürün İletişimi

Dünya nüfusunda ki artış ürünlerin daha çok fazla yetiştirilmeye neden olmuştur. Ürün üretimini artırmak, atıkları ve maliyetleri aza indirmek ve kaynak tüketimini artırmak için teknolojilerden yararlanılabilecektir. Beşinci Nesil haberleşme sistemleri ve algılayıcılar sayesinde gerçek zamanlı ürünün durumunu, toprağın durumunu gerçek zamanlı izlenebilmektedir.

3.4.5 Akıllı Hava Ürün Takip

Toprağın değişimi, mantar ve sulama ile ilgili tarımsal sorunların ortaya çıkarmak için geniş tarım alanının sürekli izlenmesi gerekmektedir. Bu işlem yapılması çok zor ve maliyetlidir. İnsansız hava araçlarına monte edilen algılayıcıların ve tarım alanlar da bulunan algılayıcılar ile veri iletişimine geçerek geniş tarımsal alanlar düşük maliyetlerle hassas şekilde merkezi sistemden izlenebilir hale gelecektir.



Şekil 28 İnsansız Hava Araçları İle Akıllı Tarım Örneği

3.4.6 Tarım Sektörü Yeni Riski Veriler

Beşinci Nesil haberleşme sistemi Tarım alanında bağlantısız tüm cihazları birbirine bağlayarak haberleşme şebekesinde ve internet ortamında tarım alına ait verileri ulaşılabilir ve uzaktan kontrol edilebilir olacaktır.

Tarım Alanında baktığımızda bu yeni riskli veriler aşağıdaki şekilde gruplanmıştır.

Anlık Kişisel Veriler, Tarım alanlarını bireysel çiftçilerin Akıllı tarım cihazların kullanarak kendi ürünlerini veya tarım alanlarını, hayvanları, bitkileri izleme yaparken oluşturdukları veri tipleridir. Bu veri tipleri çiftçiye ait ürün veya çiftçiye ait tarım alanlarının analizlerini yapabilecek nem, sıcaklık, miktar, kimyasal değerler vb bilgilerdir. Ayrıca tarım alanlarının sürekli izlenebiliyor olması, konum gibi bilgiler çiftçinin ait özel bilgilerdir.

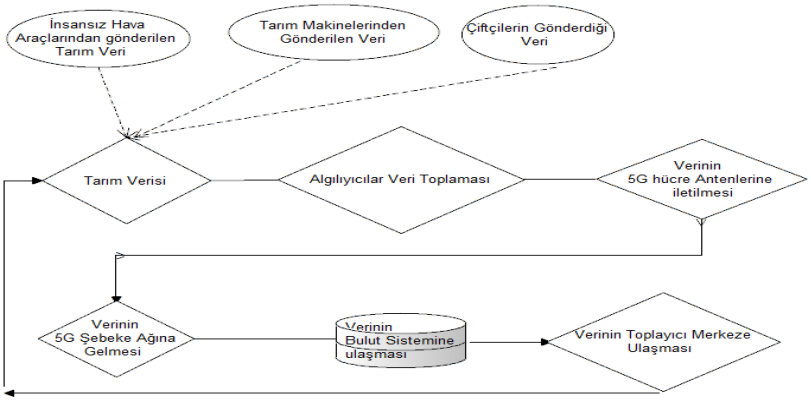
Anlık Ticari Veriler, Tüzel işletmelerin tarım alanında faaliyet göstermeleriyle akıllı tarım teknolojisinin kullanılmasıyla tarım alanlarından, bitkilerden, hayvan izleme bölümlerinden ticari işletmelere özgü verilerdir.

İşlemenin ne kadar süt üretim kapasitesi olduğu, ne kadar hayvan olduğu kaç hayvanın sağlıklı olduğu gibi ticari işletmelere özgü verilerdir. Bu veriler işletmenin rakiplerinde olduğu takdirde işletmenin rekabet konusunda sıkıntıya gireceği verilerdir.

Anlık Cihaz Toplayacağı Veriler, Tarım alanları üzerine yerleştirilen akıllı cihazların veya kullandıkları akıllı cihazların veri işlemciler tarafından toplanan verilerdir. Akıllı cihazların üzerinden topladığı veriler gerçek zamanlı ilgili şebeke üzerinden bulut sistemine aktarılmaktadır. Cihaz üzerindeki bu veriler şebekeye aktarılmadan önce geçici süre veriyi üzerinde tutma işlemi verinin güvenliğini risk altına olabilecektir.

Anlık Toplumu Etkileyen Veriler, Akıllı Tarım uygulamaları, nesnelerin internet cihazları ve Beşinci Nesil haberleşme sistemlerinin kullanarak bir ülkeyi, bir bölgenin toplumunun tarım yapısını anlık izlenebilmektedir. Bu toplumun tarım alanındaki özel durumunu analizini yaparak iyileştirme yapılması konusunda çok önemlidir. Ancak bu veriler ışığında toplumun tarım problemlerini verisi anlık izlenmesi toplum zafiyetleri verisi ortaya çıkmaktadır. Bu veri analizi yapılarak toplum üzerinde algı yönetimi, toplumu yönlendirme gibi toplum mühendisliğini operasyonlarına neden olabilecek anlık riskli verilerdir.

3.4.7 Tarım Verisini Beşinci Nesil Haberleşme Şebekesinde Dolaşımı



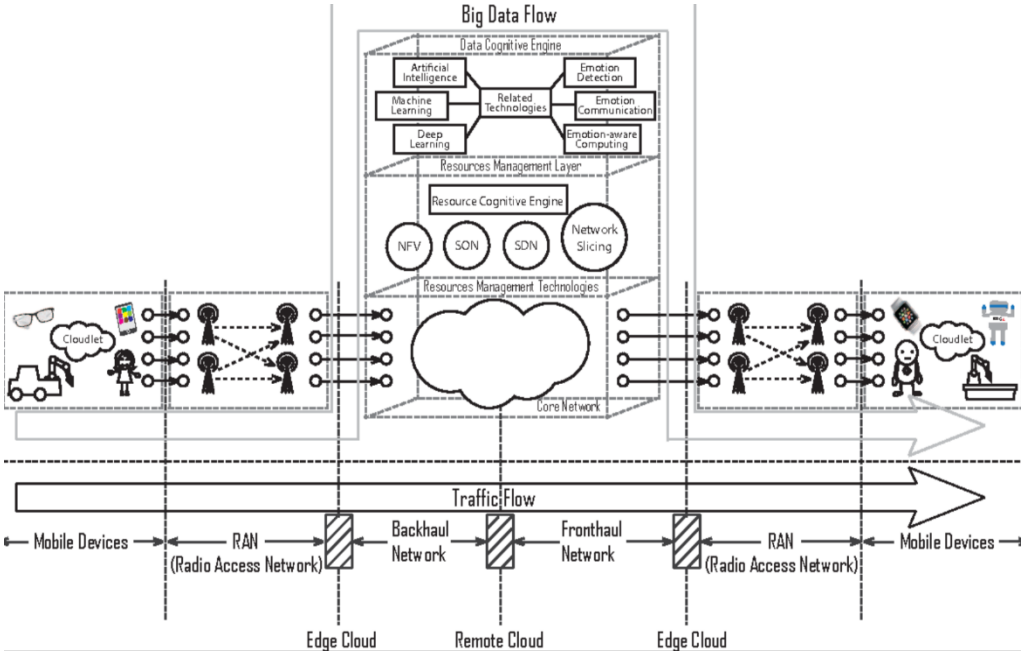
Şekil 29 Tarım Verisinin Beşinci Nesil Haberleşme Sistemi Dolaşımı

Akıllı Tarım sistemlerinde tarım alanlarına yönelik uygulamaların sonucunda oluşana özel ve nitelikli verilerin insansız hava araçlarından, çiftçilerden veya algılayıcı cihazlar ile toplanması, algılayıcılara en yakın kablosuz Beşinci nesil Kablosuz radyo erişim antenleri ile Beşinci Nesil şebeke ağına iletilmektedir. Veri şebeke ağından geçerek bulut ortamında bulunan tarım servislerin veri tabanlarına kayıt edilmektedir. İlgili tarım merkezleri tarafından bulut ortamındaki veri toplanır gerekli analizler yapılarak kullanıcılara veya ilgili yerlere iletilir. Tarım alanın ile ilgili hassa veriler şebeke ağı içersin de dolaşım yapmaktadır.

Bu hassas veriler algılayıcılar ile şebeke ağı arasında, Şebeke ağı ile bulut sistemleri arasındaki veri iletim arasında güvenlik riskleri ve saldırganların ataklarına uğraya bilmektedir. Bu bölümlerde oluşabilecek veri zafiyetleri sonucunda veri değişebilir, dinlenebilir, verinin gizliliği oluşmamış olmaktadır.

3.5 Sağlık Sektörü

Sağlık sistemleri, büyüyen ve yaşlanan nüfus nedeniyle sürekli artan sağlık talebinden kaynaklanan önemli zorluklarla karşı karşıya kalmaktadır. Gayri Safi yurt içi hasılanın bir yüzdesi olarak sağlık bakımı maliyeti, ortalama ekonomik büyümeden daha hızlı büyümeye devam etmektedir. Verimliliği arttırma ve maliyetleri düşürme fırsatları, daha fazla sağlık izleme, akıllı tıp ve uzaktan tanı ve cerrahi gibi daha fazla veri ve verinin toplanmasına ve yönetilmesine olanak sağlayan teknolojik uygulamalardan doğacağı öngörülmektedir. Nesnelerin interneti cihazları ile Beşinci nesil haberleşme sistemleri üzerinden gelecek büyük veri yönetimi, analizi sayesinde hastalıkların ve tıbbı kararların alınmasına yardımcı olabilecektir.



Şekil 30 Beşinci Nesil Haberleşme Sistemi ile Akılı Sağlık Mimarisi

Sağlık hizmetlerinde uzaktan sağlık hizmetleri, uzaktan ameliyat, süreli izleme merkezi yönetim sağlayarak özellikle avantaj sağlayarak maliyetlerin azalmasına etki edecektir. Beşinci nesil haberleşme sisteminin en büyük özelliği yüksek hız ve düşük gecikme süre akıllı sağlık hizmetlerinin önemli gelişimde bulunması beklenmektedir.

Sağlık hizmetlerinde eş zamanlı anlık cihaz iletişimi, uzaktan izleme, ev de bakım ve hastalık yönetimi yoluyla hasta bakımının iyileştirilmesi hedeflenmektedir. Bu sistemler kan basıncı, kalp atış hızı, vücut ısısı ve diğer vücut fonksiyonel parametreler gibi hayati belirtileri geniş bir alan ağı üzerinden izlemek, hastaların vücutlarına uygulanan algılayıcılar ve cihazlar kullanılmaktadır. Bu cihazlardan elde edilen veriler ağ üzerinden merkezi sağlık hizmet sağlayıcılarına iletilir. Hayati belirtilerin izlenmesi, kalp ritmindeki değişiklikler uzaktan anlık izlenebilir gerekli müdahaleler anlık yapılabilmektedir.

3.5.1 Akıllı Sağlık Görüntüleme Sistemi

Akıllı Sağlık sisteminin en büyük teknoloji gelişimi sağlık ile ilgili görüntü verilerin coğrafi bölge mesafesi, zaman kavramı olmaksızın uzaktan erişilebilmesi

ve hızlı paylaşımının gerçekleştiriliyor olmasıdır. Nesnelerin interneti ve Beşinci nesil haberleşme sisteminin yüksek hız düşük zaman kaybı özellikleri akıllı sağlık gelişimine büyük gelişmeler getirecektir. Dünyanın herhangi bir bölgesinden tıbbı görüntüleri, fotoğrafları veya test sonuçlarını ihtiyaç duyulan başka bir doktorun uzmanlığına erişmeleri sağlanır ve kaliteli sağlık hizmeti geçekleşmektedir. Böylelikle dünyanın değişik bölgelerinde tıbbı uzmanlık olmayan yerleşim yerlerin yüksek hız ve düşük gecik özelliği ile uzmanlık seviyesinde yardım alabileceklerdir. Böylelikle yüksek seviyede ağır hasta olan hastaların fiziksel olarak seyahat etmeden üst düzey tıbbı yardım alabilecekler.

3.5.2 Akıllı Sağlık Giyim Sistemi

Akıllı sağlık giyim sistemleri, çoklu mikro fizyolojik sinyal verilerini bir raya getirerek çoklu fizyolojik sinyal verilerinden oluşmaktadır. Tıbbı teşhis için insan vücudunun en temel gereksinimi biyoelektrik sinyalidir. Tekstil sektöründe yapılan sağlık giysileri insan vücudunun biyoelektrik sinyal verileri toplayacak ve izleyecek şekilde tasarlanmaktadır. Yapılan giysilerle insan vücudunun kan oksijen seviyesini, kalp ritimleri, bunun gibi vücut veri sinyalleri online sürekli bir şekilde merkezi bir yapıda takip edilebilmektedir. Bu giysilerin içersin de nesnelerin interneti algılayıcılar ile veriler toplanarak Beşinci nesil haberleşme sistemi üzerinden bulut ortamına veya ilgili bulut sağlık hizmetlerine aktarılmaktadır. Giyilebilir akıllı sağlık giysileri algılayıcı cihazlarının üzerinden veriler gelerek analizler yapılarak kronik sağlık hastalıklarının teşhisi ve takibinde anlık sürekli kullanılabilecektir.

Şekil 31 Akıllı Sağlık Giysisi

3.5.3 Kırsal Alanlarda Akıllı Sağlık Hizmeti

Beşinci haberleşme ve ötesi sistemlerin gelişmesiyle kırsal alanlarda yaşayan insanların yüksek hız internetin gelmesiyle teknolojinin getirdiği uygulamalardan fazla yaralanabilecekler. Bunlardan bir tanesi akıllı sağlık hizmetleridir. Kırsal alanda yaşayanlar tıbbı teşhis hizmeti istedikleri zaman anlık sağlık hizmeti alabilecektir. Akıllı sağlık hizmetlerinin izlenmesi, hasta sağlığı durumuna ilişkin herhangi bir zamanda kırsal kliniğinde teknoloji imkânlarıyla sağlanacaktır. Kırsal alan kliniği ile kentsel il hastaneleri arasında teknoloji bağlantıları ile anlık sürekli sağlık hizmeti verilebilecektir. Kırsal alanda yaşayanların sağlık hizmetlerinin kalitesi artıracak ve kronik hastalıkları olan bir hastanın durumunu iyileştirmesinde yardımcı olacaktır.

3.5.4 Robot Destekli Tedavi ve Cerrahi

Akıllı Sağlık sisteminde, Beşinci Nesil haberleşme sistemlerinin yüksek veri hızı, düşük gecikme süresi özellikleri ile robotların cerrahide uzaktan kullanılması önü açılmıştır. Özellikle düşük gecikme süresi robotların sıfır seviyesinde algılamaların olması çok öneli hale gelmektedir. Bununla birlikte, birçok uzaktan cerrahi vakası, muhtemelen çok özel durumlar için istisna olan kablosuz Beşinci Nesil haberleşme ile sabit ağlara dayanacaktır. Beşinci Nesil ve ötesi teknolojilerin bu alanda kullanılmasında destekleyebileceği gelişmiş özellikleri mevcut olması, uzaktan tanı ve cerrahi operasyonların dokunsal geri bildirimi bulunmadığından cerrahi operasyonlar görsel veri üzerinden yapılabilmektedir. Uzman doktor uzaktan ameliyat yaptığında robot elleri dokunsal olarak hissedememektedir. Sistem görsel veri üzerine dayanabilmektedir.

Buna rağmen önemli hastalıkların tıbbı cerrahi operasyonların mekân ve konum gözetmeksizin istenilen dünyanın herhangi bir yerinde en üst düzeyde uzmanlık alarak cerrahi operasyon gerçekleştirilme seviyesine gelmiştir.

2019 yılında Çin de doktorlar Beşinci Nesil haberleşme sistemiyle ilk uzaktan ameliyatı yapılmıştır. Huawei ve China Unicom Fujian Şubesi, Fujian Tıp

Üniversitesi Mengchao Hepatobiliary Hastanesinde cerrahlar, yaklaşık 30 mil uzaklıktaki laboratuvarda hayvan ameliyatı yapıldı. İnternet bağlantı gecikme süresi 100 milisaniye yani 0,1 saniye olmuştur. Hayvanın karaciğeri çıkarılması bu uzaktan ameliyat ile başarılı olmuştur.[36]

Şekil 32 Beşinci Nesil Haberleşme Sistemi ile yapılan Uzaktan Ameliyat

Uzaktan ameliyat için Beşinci nesil haberleşme şebekesinin kullanımının en büyük avantajı sunduğu düşük gecikme süresidir. Gecikme ne kadar düşük olursa ameliyat robotu cerrahın eylemlerine on veya yüzlerce mil öteden daha fazla tepki verebilecek. Bu da yapılan hata olasılığının azaltır ve cerrahın aynı odadaymış gibi çalışma izni vermektedir.

Uzak ameliyat gibi özel ve hassas veri Beşinci Nesil haberleşme sisteminin içinde dolaşmış olacaktır. Haberleşme sisteminin güvenliği ve sürdürülebilmesi artık çok önem taşımaktadır.

3.5.5 Uzaktan İzleme Sağlık Sistemi

Modern hareketsiz yaşam tarzları be büyük yaşlanma popülasyonuyla birleşmiş beslenme alışkanlıkları, kalp hastalığı, aşırı kilo, diyabet ve astım gibi kronik hastalıkların artmasına neden olmuştur. Dünya sağlık örgütüne göre bu tip hastalıklar şu anda dünyadaki ölümlerin çoğunda yaşanmaktadır. Diyabet sorunu giderek artış göstermektedir. 2030'da yedinci önde gelen ölüm nedeni olarak

[36] https://www.huawei.com/en/industry-insights/outlook/mobile-broadband/wireless-for-sustainability/cases/worlds-first-remote-operation-using-5g-surgery, Erişim Tarihi:16.03.2019

beklenmektedir. Endüstriyel ve büyük şehirlerde düşük dış hava kalitesi, kanser, astım ve kalp hastalıkları, akciğer hastalıklarına yol açmaktadır. Kronik hastalıklar en yaygın ve masraflı sağlık sorunları arasında olsa da uzun süreli izleme yoluyla erken teşhis ile önlenebilir veya uygun tedavi yöntemi etkin şekilde kontrol edilebilir.

Nesnelerin interneti kullanılan küçültülmüş algılayıcılar, gömülü bilgisayar cihazları kablosuz Beşinci nesil ağ teknolojilerin gelişimi uzaktan sürekli sağlık izleme sistemlerinin önünü açmıştır. Uzaktan sağlık izleme, bireylerin günlük faaliyetlerini kesintiye uğramadan her yerden ve gerçek zamanlı fizyolojik belirtilerin izlenmesini sağlamıştır. Bireyler istedikleri ortamlarda farklı vücut algılayıcılar tarafından toplanan fizyolojik verileri anlık ve gerçek zamanlı uzak bir tesisten analiz edilebilmektedir. Sistem uzun vadeli sağlık analizleri yapabilir ve anormal durumları tespit ederek acil durum alarm sinyalleri üretebilir. Akıllı sandalyeler ve akıllı yataklar gibi akıllı sağlık mobilyaları bireyin fizyolojik durumunu ölçülmesinde kullanılabilecektir.

Bu tip uygulamalar ve akıllı cihazlar sayesinde bireye özgü hassas veriler kablosuz Beşinci nesil haberleşme şebekesinde dolaşımı gerçekleşecektir.

3.5.6 Akıllı Hastane Yönetimi

Teknolojiye bağlı olarak gelişen akıllı sağlık sisteminde hastanelerin organizasyonlarında kolaylıklar getirmektedir. Nesnelerin interneti ile hastane içinde bulunan algılayıcı cihazların yardımıyla hastane gerçek zamanlı izlenebilir ve yönetilebilir. Akıllı algılayıcılar ile hastanenin içinde bulunana demirbaşların veya ilaçların anlık durumlarını alınabilmektedir. Hastane içinde hastanın konum bilgileri alınabilmektedir.

Ülkedeki veya bölgedeki hastanelerin yatak durumlarını, acil hasta sayılarını, hasta kabul veya hasta çıkış verilerini, doktor sayılarını, hastanede bulunan sağlık cihazlarını merkezi bir yapıdan gerçek zamanlı izleme yapılma olanağını sağlamaktadır. Bu bilgiler ile hastane içinde iyileştirmeler veya iş akışlarını düzenleyebilmesini sağlamaktadır.

3.5.7 Sağlık Sektörü Yeni Riski Veriler

Beşinci Nesil haberleşme sistemi Sağlık alanında bağlantısız tüm cihazları birbirine bağlayarak haberleşme şebekesinde ve internet ortamında Sağlık alına ait verileri ulaşılabilir ve uzaktan kontrol edilebilir olacaktır.

Sağlık Alanında baktığımızda bu yeni riskli veriler aşağıdaki şekilde gruplanmıştır.

Anlık Kişisel Veriler, Bireylerin kullandıkları akıllı sağlık cihazlarının üzerinden gelen bireye ait özel verileridir. Bu veriler bireylerin üzerine takılan vücut algılayıcılar tarafından toplanan fizyolojik verileri anlık ve gerçek zamanlı izlenebilmektedir. Bu verilerin akıllı cihazlar üzerinden bulut tutularak verilerin analizi yapılabilmektedir.

Anlık Cihaz Toplayacağı Veriler, Bireyleri üzerine yerleştirilen akıllı cihazların veya kullandıkları akıllı sandalye, akıllı yataklar gibi cihazların veri işlemciler tarafından toplanan verilerdir. Akıllı cihazların işlemciler üzerinden topladığı veriler gerçek zamanlı ilgili şebeke üzerinden bulut sistemine aktarılmaktadır. Cihaz üzerindeki bu veriler şebekeye aktarılmadan önce geçici süre veriyi üzerinde tutma işlemi verinin güvenliğini risk altına alabilecektir.

Anlık Cihaz Özgü Veriler, Akıllı sağlık sistemlerinde veriyi toplayan akıllı cihazların içersin de kullanılan cihazların üreticiler tarafından cihazı belirleyecek kimlik numaraları, üreticiye ait bilgiler bulunmaktadır. Üreticileri cihazların içerinde hangi cihazları kullandığını kimlik numaralarını takip etmektedir.

Bu cihazların içersin de kullanılan cihazların marka ve modellerini veya hangi tip cihazlar kullanıldığını on-line platformlar aracılığı ile öğrenilebilme risk ortaya çıkmaktadır. Bireyin vücudunda x markalı bir cihaz kullanıldığı öğrenildiğinde o cihazla alakalı zafiyetler üzerinden tüm araçları veya araç kullanıcıları tehdit altında olabilmektedir.

Anlık Ticari Veriler, Sağlık sektöründe faaliyet gösteren işletmelerinin Hastane, poliklinik, sağlık merkezlerinin oluşturduğu işletmelere özgü verilerdir. Sağlık merkezlerinde bulunan hasta sayıları, sağlık cihazları sayıları, ilaç sayıları işletmelere ait veriler tek bir merkezden izlenebilir veya yönetilebilir.

Sigorta şirketleri, sağlık poliçelerinde verdikleri hizmetleri anlık kontrol edebileceklerdir. Böylelikle uygun ve doğru ödemelere yapılabilecektir. Sağlık sektöründeki sigorta şirketlerinin ödeme riskleri doğru yapılacak sigorta şirketlerinin dolandırılma seçeneği azalacaktır.

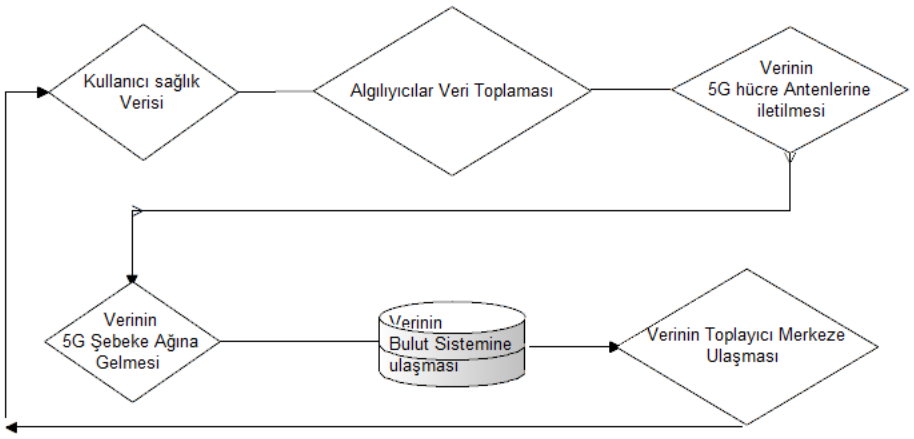
Anlık Toplumu Etkileyen Veriler, Akıllı sağlık uygulamaları, nesnelerin internet cihazları ve Beşinci Nesil haberleşme sistemlerinin kullanarak bir ülkeyi, bir bölgenin toplumunun sağlık yapısını, kronolojik hastalıklarını anlık izlenebilmektedir. Bu toplumun sağlık durumunu analizini yaparak iyileştirme yapılması konusunda çok önemlidir. Ancak bu veriler ışığında toplumun genetik sağlık problemlerini verisi anlık izlenmesi toplum zafiyetleri verisi ortaya çıkmaktadır. Bu veri analizi yapılarak toplum üzerinde algı yönetimi, toplumu yönlendirme gibi toplum mühendisliğini operasyonlarına neden olabilecek anlık riskli verilerdir.

Akıllı sağlık sektörlerindeki uygulamalar doğrudan tüketicileri yani hastaları ilgilendirmektedir. Akıllı sağlık uygulamaları geliştirmeden önce bu uygulamaların veya akıllı cihazların test edilmesi ve onaylanması sağlık sektörü ile ilgili tüm yasal gerekliklerini yerine getirerek sağlık sektöründe kullanılmalıdır. Sağlık sektöründe kullanılacak akıllı cihazların ilgili teknoloji standardizasyon konularında sağlık verilerinin güvenliği, gizlilik gibi şartları sağlamak zorunda olmalıdırlar. Bu akıllı cihazların haberleşme şebeke içersin de cihaz kimlik numaraları çok önemli olmaktadır. Bu cihazların birinde veri güvenlik zafiyeti gösterildiği zaman hangi kimlik numaralı ve parti numaralı cihazlarda olduğu hızlı ve bir şekilde müdahale edilebilme olanağı sağlayacaktır.

Sağlık Sektöründe anlık veri toplayan bağlı cihazlar veya robotlara güvenmek bazı şeylerin yanlış gittiği durumlarda yükümlülük belirlemek açısından önemli

sorunlar doğuracaktır. Bu güvenlik ve sorumluluk sorunlarını çözümlenmesi gerekmektedir.

3.5.8 Sağlık Verisini Beşinci Nesil Haberleşme Şebekesinde Dolaşımı



Şekil 33 Sağlık Verisinin Beşinci Nesil Haberleşme Sistemi Dolaşımı

Akıllı Sağlık sistemlerinde tüketiciye yani hastalara yönelik uygulamaların sonucunda oluşana özel ve nitelikli verilerin algılayıcı cihazlar ile toplanması, algılayıcılara en yakın kablosuz Beşinci nesil Kablosuz radyo erişim antenleri ile Beşinci Nesil şebeke ağına iletilmektedir. Veri şebeke ağından geçerek bulut ortamında bulunan sağlık servislerin veri tabanlarına kayıt edilmektedir. İlgili hastaneler veya sağlık merkezleri tarafından bulut ortamındaki veri toplanır gerekli analizler yapılarak kullanıcılara veya ilgili yerlere iletilir. Sağlık ile ilgili hassa veriler şebeke ağı içersin de dolaşım yapmaktadır.

Bu hassas veriler kullanıcı ile algılayıcılar veya algılayıcılar ile şebeke ağı arasında, Şebeke ağı ile bulut sistemleri arasındaki veri iletim arasında güvenlik riskleri ve saldırganların ataklarına uğraya bilmektedir. Bu bölümlerde oluşabilecek veri zafiyetleri sonucunda veri değişebilir, dinlenebilir, verinin gizliliği oluşmamış olmaktadır.

DÖRDÜNCÜ BÖLÜM

BÜYÜK VERİ VE BEŞİNCİ NESİL (5G) MOBİL İLETİŞİM ŞEBEKESİNİN VERİ GÜVENLİK ZAFİYETLERİ

4.1 Büyük Veri

Büyük Veri, artan hacimlerde ve daha yüksek hızda gelen daha fazla çeşitliliği içeren verilerdir. Büyük veriler, özellikle yeni veri kaynaklarından daha büyük, daha karmaşık veri kümeleridir. Büyük veri, bilgi toplama ve makine öğrenimi projelerinde ve diğer ileri analitik uygulamalarında kullanılma potansiyeline sahip, büyük miktarda yapılandırılmış, yarı yapılandırılmamış ve yapılandırılmamış veriler olarak tanımlanmaktadır.

Büyük veri hacimli veriler, ticari işlem sistemleri, müşteri veri tabanları, tıbbı kayıtlar, internet verileri, mobil uygulamalar, sosyal ağlar, bilimsel deneylerin toplanan sonuçları, mobil şebeke ağında oluşan veriler, kullanılan makine verileri ve kullanılan gerçek zamanlı veri algılayıcıları gibi sayısız farklı kaynaktan gelebilmektedir. Nesnelerin interneti ortamlarında veriler ham şekilde bırakılabilir veya analiz edilmeden önce veri madenciliği araçları veya veri hazırlama yazılımları ile kullanılarak önceden işlenebilir.

4.1.1 Büyük Veri Sınıfları

Büyük veri büyük değer, yüksek hız ve genişletilebilir veri çeşitliliği içermektedir. Bunlar üç sınıfta yapılandırılmış veri, yarı yapılandırılmış veri, yapılandırılmamış veri şeklindedir.

4.1.1.1 Yapılandırılmış Veri

Yapılandırılmış büyük veri, Verinin analiz kolaylıkla yapılabilen, saklanabilen ve işlenebilen verilerdir. Bu veriler genellikle biçimlendirilerek veri tabanlarında tutulmaktadır. Veri tabanlarında tüm satırları ve sütunları içeren saklanabilecek yapılandırılmış sorgu dili SQL denilen ilişkisel verilerdir. Google

gibi arama motorlarında verilerin web ortamında kolayca bulunabilmesi için yapılandırılmış veri kullanmaktadır. Bu tip veriler oluşturduğu ortam en güzel örnek SQL veri tabanı olarak verilebilir. Örneğin bir işletmenin kullandığı sistemlerinde tutuğu müşterinin adı, vergi numarası, adresi, satılan ürün adetleri, Fatura Tarihi, ürün bilgileri, gibi düzenli, kolayca erişilebilen ilişkisel verilerdir.

Results | Messages

	FATURA_TARIHI	FATURA_NO	STOK_ADI1	MUSTERI_ADI	MARKA	GRUP1	BOLGE	BIRIM_FIYAT_KDVSIZ	D
10	2013-06-27 00:00:00	110552	LANSMAN KARTLARI	KUT ECZA DEPOSU LTD.STI	ELLARO	POP	TURKEY	0.2698080000	1
11	2013-07-04 00:00:00	110557	ELLARO PLAJ ÇANTASI	STERN TEK KOZMETIK SAN.VE TIC.A.S	ELLARO	POP	TURKEY	7.0893200000	1
12	2014-05-15 00:00:00	110742	MY KATALOG	ARIAN CHIMIA TECH CO.	MY	POP	IRAN	5.6249820000	1
13	2014-06-27 00:00:00	3401	SCHON KARTON STAND 12Lİ	ARAZRENK DISTRIBUTION CO.	SCHON	STAND	ASIA	3.1938000000	1
14	2014-07-17 00:00:00	3411	MY KATALOG	PRIVATE ENTREPRENEUR GRIDCHIN SERGEY IVANOVICH	MY	POP	NULL	5.4328050000	1
15	2014-09-09 00:00:00	3461	NOTE ENGLISH CATALOG	UNAT YAĞ GIDA SAN. VE TİC.A.Ş.	NOTE	POP	MENA	0.0216270000	1
16	2014-09-09 00:00:00	3461	NOTE ARABIC CATALOG	UNAT YAĞ GIDA SAN. VE TİC.A.Ş.	NOTE	POP	MENA	0.0216270000	1

Şekil 34 SQL Veri Tabanında Saklanan Yapılandırılmış Veri Örneği

4.1.1.2 Yarı Yapılandırılmış Veri

Yarı Yapılandırılmış veri, rasyonel veri tabanında bulunmayan ancak analiz edilmesi kolaylaştıran, verinin yönetilebilmesini organize edilmesine sahip verilerdir. Bu veriler ilişkisel veri tabanlarına uygun olmayan verilerdir. Çeşitli web sayfalarından üretilen, şemaya dayalı olmayan, bir den fazla özelliği gibi özellikleri vardır. Yarı Yapılandırılmış verilere e-postalar, XML ve JSON örnek verilebilir.

```
{Row:{Musteri_id:" 12345",Emp_name:"Leyla"},
Row:{ Musteri_id:" 56786",Emp_name:"Bedi"},
Row:{ Musteri_id:" 67858",Emp_name:"Tayfun"},
Row:{ Musteri_id:" 90890",Emp_name:"Şule"}, }
```

Şekil 35 JSON Yarı Yapılandırılmış Veri Örneği

4.1.1.3 Yapılandırılmamış Veri

Yapılandırılmamış veriler, önceden tanımlanmış bir şekilde organize edilmemiş veya önceden tanımlanmış bir veri modeline sahip olmayan bir veridir. Dünyanın Dijital dönüşümünde verilerin yüzde doksanı yapılandırılmamış

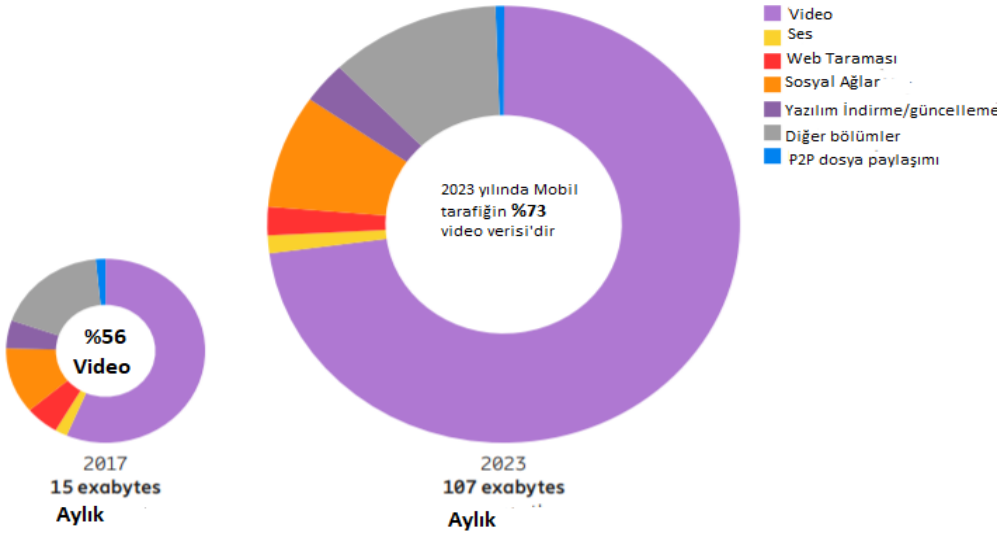
verilerdir. Şemaya dayalı olmayan, ilişkisel veri tabanına uygun olmayan, video, müzik, PDF, Word, görüntüler gibi verilere yapılandırılmamış veriler denilmektedir.

4.1.2 Büyük Veri Özellikleri

Büyük veri bilim adamların yaptığı araştırmalar neticesinde beş boyuttan değerlendirmişlerdir. Hacim, Hız, Çeşitlilik, Doğruluk ve Değer boyuttan incelenmiştir.

4.1.2.1 Büyük Veri Hacmi

Toplam veri miktarını gigabayt, terabayt, petabayts, exabayt, zetabayt veri ölçü biriminden değeri ifade etmektedir. 2020 yılından sonra Nesnelerin interneti ve Beşinci nesil ileriki sistemler ticarileşerek yaygınlaşmasıyla büyük verinin hacminde artışlara meydana gelecektir. 2018 yılı Ericsson raporuna 2023 yılında aylık veri trafiği 107 exabytes olarak öngörülmektedir. Bu trafiğin %73'ü video olarak öngörülmektedir.



Şekil 36 Ericsson 2018 Aylık Uygulama Kategorisine Göre Mobil Veri Trafiği

4.1.2.2 Büyük Veri Hızı

Hem verilerin oluşturma hızı, yakalama hızı ve veri akış hızını ifade etmektedir. Beşinci Nesil haberleşme sisteminin getirdiği teknoloji özelliği ile artık veriler çok yüksek hızla iletişim halinde olacaktır. Akıllı cihazların ve algılayıcılar gibi dijital cihazların gerçek zamanlı veri hızlı şekilde oluşacaktır. Geleneksel veri yönetim sistemleri büyük veri işlemlerini anında gerçekleştirme özelliklerine sahip değillerdir.

4.1.2.3 Büyük Veri Çeşitliliği

Üretilen veriler yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış olarak üç bölümden oluşmaktadır. Yapılandırılmış büyük veri, Verinin analiz kolaylıkla yapılabilen, saklanabilen ve işlenebilen verilerdir. Bu tip veriler oluşturduğu ortam en güzel örnek SQL veri tabanı olarak verilebilir. Yarı Yapılandırılmış büyük veri, rasyonel veri tabanında bulunmayan ancak analiz edilmesi kolaylaştıran, verinin yönetilebilmesini organize edilmesine sahip verilerdir. Yarı Yapılandırılmış verilere e-postalar, XML ve JSON örnek verilebilir. Yapılandırılmamış veriler, önceden tanımlanmış bir şekilde organize edilmemiş veya önceden tanımlanmış bir veri modeline sahip olmayan bir veridir. Video, müzik, PDF, Word yapılandırılmamış büyük veri örnektir.

4.1.2.4 Büyük Veri Geçerliliği

2020 yılında ticarileşmesi beklenen Beşinci nesil haberleşme sistemiyle 2023 yılında aylık mobil trafiği 107 exabytes gibi büyük veri oluşması öngörülmektedir. Bu da büyük verinin doğrulu konusunda çalışmalar yapılması gerekmektedir. Nesnelerin interneti ile akıllı cihazlarda sürekli veri iletişimi olacaktır. Şebekenin güvenliği veya akıllı cihazların veri güvenliği sağlanmaz ise büyük verilerden doğru analizler oluşmayacaktır.

4.1.2.5 Büyük Veri Değeri

Büyük verinin en önemli boyutu değer oluşturmasıdır. Büyük verinin saklanması, analiz edilmesi sonucunda kuruluşlara önemli katma değer sağlaması gerekmektedir. Örneğin, Kozmetik firmasının müşterinin alışkanlıklarını doğru olarak analiz edilmesi, kuruluşun yapacağı yatırımların ve yenilikleri doğru ve az maliyetle yapılarak kuruluşa fayda sağlamaktadır.

4.2 Beşinci Nesil Haberleşme Şebekesinde Dolaşan Anlık Büyük Veri Tipleri

Akıllı Tarım, Akıllı Şehirler, Akıllı ulaşım, Akıllı sağlık gibi endüstriyel dikey sektörlerde değişik teknolojiye dayalı yatırımlar ve gelişme çalışmaları yapılmaya devam edilmektedir. Dikey endüstriyi ve diğer akıllı cihazları birbirine dünya da birbirine bağlayacak olan teknoloji Beşinci nesil haberleşme teknolojisindeki gelişmeler olacaktır. Beşinci Nesil haberleşme sistemi büyük verinin oluşmasında büyük etkili olacaktır. Değişik nesnelerin veya cihazların tüm bilgileri Beşinci nesil kablosuz şebekenin içinde geçerek büyük veri oluşturacaktır. Ericsson firmasının 2018 yılında yayınladığı raporda 2023 yılında 3,5 milyar akıllı cihazı bağlı olacağı bildirmiştir.[37] Bu da kablosuz haberleşme sisteminde çok büyük sayıda akıllı cihaz ve büyük veri dolaşımı olacaktır. Şebeke içeresinde dolaşacak bu verilerin güvenliği çok önemli olmaktadır.

4.2.1 Anlık Web Verileri

Kullanıcının akıllı cihazdan Beşinci Nesil kablosuz ağ şebekesine üzerinden anlık web sayfalarının görüntülenmesi, aramaları, okuma gibi kullanıcı düzeyinde web davranış verilerdi. Kullanıcılar mobil cihazlar üzerinden Google, YANDEX, INFO, gibi arama motorları kullanarak e-ticaret, alış-veriş siteleri, tatil siteleri gibi ihtiyaçlara yönelik aramaların yapıldığı bu tip veriler kablosuz haberleşme şebekesi içeresinde takip edilebilen anlık web verilerine örnek gösterilebilir.

---

[37] https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf,Erişim Tarihi:23.02.2019

4.2.2 Anlık Metin Verileri

Mobil cihazların yaygınlaşması ve internet hızlanması ile kullanıcılar mobil cihazlar üzerinden değişik hizmetlerde uygulamalar geliştirilmiştir. Bu geliştirilmiş uygulamalar içersin de metin verilerin olduğu haberler, sosyal iletişim uygulamaları, internet üzerinden bulunan belgelerdir. E-posta, haber siteleri, FACEBOOK, TWITER, Linkedln, uygulamalar anlık metin verilerine örnek verilmektedir.

4.2.3 Anlık Zaman ve Konum Verileri

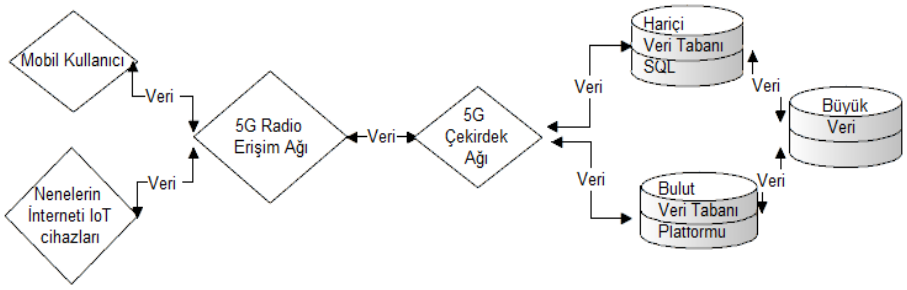
GPS, Mobil telefonların Beşinci nesil şebeke ağına bağlanarak zaman ve konum bilgisini anlık izlenildiği ve kayıt edilebildiği verilerdir. Ticari kuruluşların müşterilerini veya bireysel olarak arkadaşlarının konum bilgilerinin mobil şebekeler üzerinden anlık izlenebilmektedir. YANDEX Harita, Google Harita, Apple Harita, Here Harita, Aile konum bulucu uygulamalar konum izniyle anlık konum bilgileri şebeke ağına göndermektedir.

4.2.4 Anlık Sosyal Ağ Verileri

Kullanıcıların kendi aralarında etkileşim yapabilmesi için geliştirilen uygulamalardır. Mobil cihazların artışı işe mobil uygulamalar kullanarak kullanıcılar anlık sosyal ağ üzerinden iletişim kurmaktadırlar. Facebook, Linkedln, Myspace, Twiter gibi uygulamalar günümüzde en çok kullanılan sosyal ağlara örnek verilebilmektedir. Kullanıcılar bu sosyal ağ uygulamalarına mobil cihazlardan ve kablosuz ağlardan anlık kullanılmaktadır. Böylelikle kullanıcıların alışkanlıkları, beğendikleri, ilgi alanları anlar izlenebilmektedir. Beşinci Nesil haberleşme sistemiyle beraber gelen yüksek hız ile bu uygulamaların farklı alanlara kayabileceği görülmektedir.

4.2.5 Anlık Algılayıcıların Verileri

Algılayıcı verileri, Fiziksel ortamdan bir tür girdiyi algılayan ve yanıt verebilen akıllı cihaz çıktısıdır. Akıllı cihazlardan başka bir sisteme bilgi veya veri girdisini sağlamak ve veriyi yönlendirmek için kullanılmaktadır. Nesnelerin interneti ortamının ayrılmaz bir bileşenidir. Akla gelebilecek hemen hemen her türlü varlık benzersiz bir tanımlayıcı ve bir kablosuz ağ üzerinden verileri aktarmasıdır. Radyo Frekans Kimliği (RFID) veya bluetooth cihazları algılayıcılardan veriyi toplayan cihazlardır. Beşinci nesil ve ileriki kablosuz haberleşme sisteminin devreye girmesiyle algılayıcılar büyük veriler şebekeye iletecektir. Bunun yönetimi ve güvenliği konusunda zorluklarla karşılaşılabilir.



Şekil 37 Algılayıcıların 5G Şebekesinde Veri Dolaşım Örneği

4.2.6 Anlık Operatör Verileri

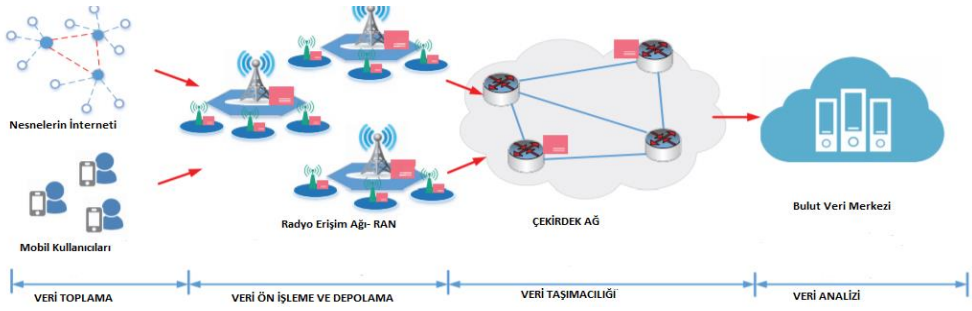
Operatörler tarafından şebeke içersin de bulunan Radyo Erişim Ağı (RAN) ve çekirdek ağ (CN) üzerinden toplanan verilerdir. Çekirdek ağ üzerinden şebeke performans bilgileri, başarılı aramalar ve uygulama başına kullanım endeks verileri örnek gösterilebilir. Radyo Erişim Ağı üzerinden radyo sinyali ölçümleri, çağrı bırakma oranı, hata durumu, devir teslim raporları kaynak durum bilgileri örnek gösterilebilir. Mobil şebeke ağları üzerinden toplanan ham veri toplama büyük veri analizi için ilk adımdır.

4.2.7 Anlık Endüstriyel Veriler

Gelecek Yıllara baktığımızda Endüstriyel, Tarım, Akıllı şehirler, Lojistik, Sağlık, Enerji, Otomotiv alanlarında teknolojik gelişmeler devam etmektedir. Bu gelişmeler teknoloji cihazlarla, akıllı cihazlarla Beşinci Nesil şebeke ağı ile direk ilişki içeresindedir. Bu ilişki içersin de Endüstriye özgü veriler algılı cihazlar bağlantı yoluyla anlık Kablosuz şebeke ağına büyük veri olarak dolaşımı öngörülmektedir. Bir ülkenin ulaşım ağından enerji ağına kadar, sağlık ağından lojistik ağına kadar bir şebeke üzerinde anlık veri alış-verişi gerçekleştirmiş olacaktır. Bu tip şebeke üzerinde oluşacak büyük verilerin dolaşması, yönetilmesi ve güvenlik riskleri doğacaktır.

4.3 Beşinci Nesil Haberleşme Şebeke Ağı İçersin de Büyük Veri iletişimi

Beşinci nesil haberleşme ve ileri sistemleri heterojen kaynakları kullanarak her yerde kablosuz ağların kullanımını sağlayacaktır. Bu şebeke ağında veri kaynakları ve veri merkezleri arasında iletişim köprü kurarak verinin toplanmasında taşınmasında aracılık yapmaktadır.



Şekil 38 Büyük Veri Beşinci Nesil Şebeke Ağında Veri İletişimi

4.3.1 Veri Toplama

Nesnelerin cihazların fiziksel nesnelerin veri alışverişinde akıllı sayaçlar, insansız uçaklar, otomobil gibi bağlı cihazlarla verimli bir şekilde yönetilmelerini sağlamaktadır. Örneğin, Nem algılayıcıları, ışık algılayıcıları ve sıcaklık

algılayıcıları gibi akıllı bağlı cihazlar büyük veri üretebilir veya büyük miktarda veri toplayabilmektedir. Akıllı Cep telefonları da çeşitli gömülü algılayıcılar sayesinde farklı büyük veri toplama potansiyeline sahiptir.

4.3.2 Veri Ön İşleme

Veri ön işleme, büyük Verinin sıkıştırma veya şifreleme gibi ham verilerden gerçekleştirilen işlemleri ifade etmektedir. Veri ön işleme bölümünde verileri analiz edilmemektedir yalnıza sıralama işlemi yapılmaktadır. Veriler rahat ve programlanabilir bir şekilde analiz için hazırlanmaktadır. Nesnelerin cihazlardan gelen şebekeye ağına gelen verinin ilk aşamada Radyo Erişim Ağ karşılamaktadır. Bu bölümde veri çekirdek ağa ulaştırılır.

4.3.3 Veri Taşımacılığı

Beşinci nesi kablosuz ağlarda kullanılan Radyo Erişim Ağ (RAN) ve Çekirdek Ağ (CN) yapısında analizlerin yapılabilmesi için veri merkezlerine doğru veriyi taşıyabilmektedir. Radyo Erişim Ağında ve Çekirdek Ağ üzerinden veri taşınacak sonunda veri merkeze ulaşacaktır. İlişkili farklı büyük veri kümeleri sağlık, enerji ulaşım gibi veriler şebeke üzerinden geçiş yapacaktır. Gerçek zamanlı işleme, güvenilir iletişim sağlamak ve taşıma sırasında veri bütünlüğü, gizliliği korumak gerekmektedir.

4.3.4 Veri Analizi

Verilerin analiz etmek ve algoritmalar geliştirmek veya daha fazla kullanım için yeni potansiyelleri ortaya çıkarmak için kullanabilecek faydalı verileri çıkarmak için çeşitli araç ve yöntemlerin kullanıldığı ana süreçtir. Beşinci nesil şebeke ağına gelen verinin veri taşıma yöntemi ile veri merkezlerine ulaştıktan sonra faydalı veri elde etmek için kullanılan veridir.

4.4 Beşinci Nesil Haberleşme Veri Güvenlik Zafiyetleri

Mobil Kablosuz iletişim sistemlerinin tarihine baktığımızda başlangıcından itibaren verinin güvenliği konusunda sorunlar, verinin korunamama problemleri sürekli olmuştur.

Birinci Nesil mobil kablosuz ağ iletişim sistemlerinde yasadışı kopyalamak, maskelenme veri güvenliği zafiyetleri yöntemleri ile cep telefonların ve kablosuz şebeke kanallarını tehdit etmiştir.

İkinci Nesil mobil kablosuz ağ iletişim sistemlerinde sistem üzerinde gerçekleşen mesaj servislerine saldırılar yapılarak veriyi ele geçirme, değiştirme yoluyla tehditler gerçekleşmiştir.

Üçüncü Nesil mobil kablosuz ağ iletişim sistemindeki gelişmeler ile IP tabanlı iletişim geçilmiştir. Mobil cihazların artışı ve kablosuz ağların etki alanlarındaki internet veri güvenlikleri yoluyla veri ele geçirilmesi, değiştirilmesi ile tehdit edilmiştir.

IP tabanlı iletişim gereksiniminin artmasıyla Dördüncü Nesil mobil ağları geliştirildi. Bu mobil kablosuz ağ iletişiminde akıllı cihazların, multimedya gibi özelliklerle yeni alanların mobil alanların içerisinde artmıştır. Bu gelişmeler daha karmaşık ve dinamik veri güvenliğini tehdit edecek ortamlar oluşmuştur.

2020 yılında ticarileşerek Beşinci Nesil haberleşme sistemleri yayılması beklenmektedir. Bu yeni nesil haberleşme sistemiyle birlikte milyarlarca cihazların şebeke içerisinde girmesiyle veri güvenliği konusunda tehditler daha büyük ve geniş olacaktır. Bu nedenle, Mobil ağların kablosuz yapısı içerisindeki güvenlik sıkıntılarını ile birlikte Beşinci nesil haberleşme sistemini kullanacak diğer cihazlarında oluşturacağı veri güvenlik problemlerin de sıkıntılar olacaktır.

Bu bölümde Beşinci nesil kablosuz ağ yapısındaki veri güvenlik zafiyetlerini ve diğer teknolojilerin şebeke içerisine taşıyacağı veri güvenlik riskleri incelemesi yapıldı.

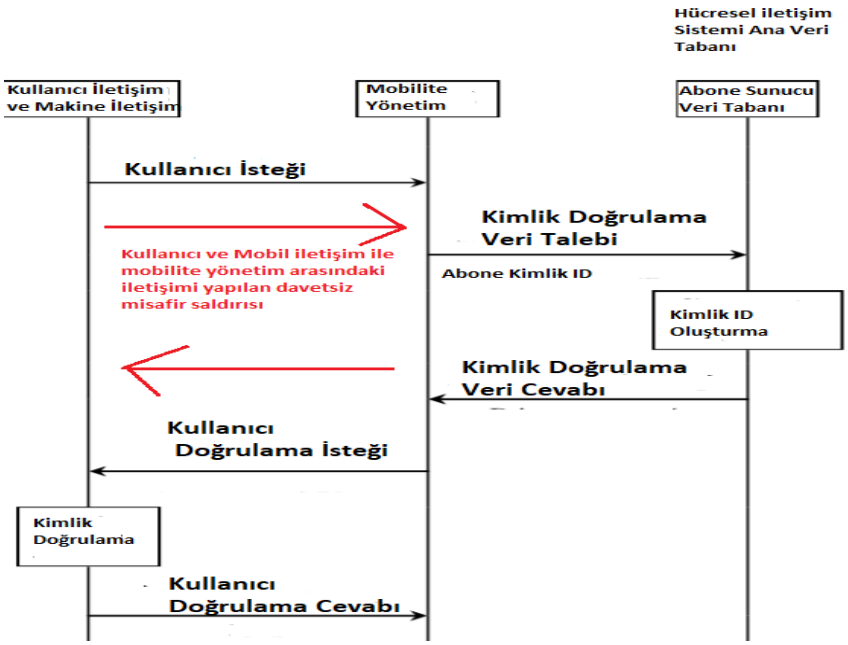
4.4.1 Beşinci Nesil Haberleşme Sistemi Şebeke İçi Veri Zafiyetleri

4.4.1.1 Grup Temelli Kimlik Doğrulama Zafiyetleri

Beşinci nesil kablosuz sistemin çok sayıda heterojen bağlı cihazı kullanması ve Kimlik Doğrulama ve Anahtar Anlaşması (AKA) protokolü dahil olmak üzere çağdaş kablosuz standartlar tarafından sağlanan aynı güvenlik seviyesinde olması beklenmektedir. Mevcut AKA protokolü, çok fazla sayıda cihazı destekleyecek seviyede tasarlanmamıştır. Bu nedenle AKA protokolü Beşinci nesil kablosuz güvenlik standartlarında geliştirilmesi beklenen protokoldür. Beşinci nesil kablosuz sistem yeni nesil mobil ağlarda, kullanıcı deneyiminin sürekliliğinin ve nesnelerin internet bağlantılarının destelemede yardımcı olacaktır. Çok sayıda heterojen cihazı desteklemesi nesnelerin internet cihazlarının bağlanmasında ve güveli olmasında zorluklara neden olmaktadır.

Beşinci nesil teknolojide nesnelerin internet cihazları aynı anda milyarlarca cihazın bağlanması beklenmektedir. Buda Beşinci nesil şebeke içersin de ağ erişimi isteyen milyarlarca cihaz grubunun kimlik doğrulama ve veri güvenliği gibi sorunlar ortaya çıkarmaktadır.

Mevcut AKA şartnamesine göre, her cihaz hem servis ağını hem de cihazın ev ağını içeren tam bir doğrulama prosedürü gerçekleştirmelidir. Birçok cihazın eşzamanlı olarak erişmesi gerektiğinde nesnelerin internet cihaz senaryosunun belirlediği bir durum olduğunda, servis ve ev ağı arasındaki sinyal, Beşinci nesil teknolojisinin yüksek hız anlayışına etki etmektedir. Grup tabanlı AKA protokolünün amacı, birçok cihazın bir grubunun aynı anda erişmesi gerektiğinde servis ve ev ağı arasındaki sinyalleşmeyi azaltmaktadır.



Şekil 39 Kimlik Doğrulama Mesaj Dizi Şeması

AKA protokolünde güvenlik zafiyetleri, abonenin kimliğinin ele geçirilmesi veya Makine Tipi iletişim (MTC) ile Mobilete Yönetim Varlık (MME) arasındaki oturum ana anahtarının davetsiz misafir saldırgan tarafından türetilmesidir.

AKA protokolünün en çok bilinen zafiyeti ise, Kullanıcı UE'nin ağa ilk bağlanmasının Uluslararası Mobil Abone Kimlik (IMSI)'nin açık metinle iletilmesini gerekmektedir. IMSI her abonen için benzersiz olduğundan saldırı izleme yöntemi ile ele geçirilmesine neden olmaktadır. Ancak Üçüncü nesil ile geliştirilen AKA protokolünde geçici kimlik talep edildiğinde abone kimliği pasif saldırılarına önlem olabilmektedir.

Grup Temelli Kimlik Doğrulama (AKA) protokolüne özgü zafiyetler aşağıda belirtilmiştir.

Davetsiz Misafirin, Hizmet Veren Ağ Üzerinden Makine Tipinin iletişimin Doğrulanması; Bu Tehdit Makine Tipi iletişimin hizmet veren ağ tarafından tanımlanması ile ilgilidir. Kimlik Doğrulama protokolüne AKA özgü bir tehdit modelidir. Davetsiz misafir, ağa erişmek için başka bir makine tipi iletişim taklit etmeye çalışmaktadır. Hizmet veren şebeke ağı ağ erişiminin yalnızca doğru

şekilde tanımlanmış makine tipi iletişim verilmesini sağlayarak tehdit meydana gelecektir.

Davetsiz Misafirin, Bir Makine Tipi İletişim ile Servis Ağı Arasında Kararlaştırılan Oturum Yönetici Anahtarı Üretir: Bu tehdit yalnızca makine tipi iletişim ve yalnızca servis ağı tarafından bilinmesi gereken oturum yöneticisi anahtarının gizliliği ile ilgilidir. Ayrıca Kimlik Doğrulama protokolüne AKA özgü bir tehdit modelidir.

Davetsiz Misafir Makine Tipi İletişim İzlemesi; Davetsiz misafirin Uluslararası Mobil Abone Kimlik (IMSI) öğrenmesini ve devir teslim sinyalleri yoluyla Makine Tipi İletişimi izlemek için kullanılmasını sağlayan gizlilik tehdididir.

Davetsiz Misafir, Hizmet Veren Ağ Tarafından Grubun bir Üyesi Olarak Onaylanır: Bu grup yaklaşımı tarafından ortaya konan yeni bir tehdittir. Davetsiz misafir başka bir Makine Tipi İletişim taklit etmesi gerekmemektedir. Hizmet ağını grubu üye olmaya, şebeke ağa erişmeye ikna etmesiyle olmaktadır.

Grubun Bozuk Bir Üyesi, Hizmet Veren Ağ Tarafından Grubun Başka Bir Üyesi Olarak Doğrulanır: Şimdiye kadar davetsiz misafir dışarıdan sızmaya çalışan bir tehdit olarak görüldü. Bu yeni tehdit ise, aynı zamanda grubun bir üyesi olan veya Makine Tipi İletişim kontrolünü bozan ve tamamen kontrol eden davetsiz misafir tehdittir. Grubun bir parçası olmaktan kaynaklanan ek bilgilerle daha güçlü bir davetsiz misafir olarak gördüğü belirtilmektedir. Davetsiz misafir grubun başka bir üyesini taklit etmeye çalışabileceğinden hizmet veren şebeke ağ, erişim ağına erişimden önce Makine Tipi iletişime doğru bir şekilde tanımlanmalıdır.

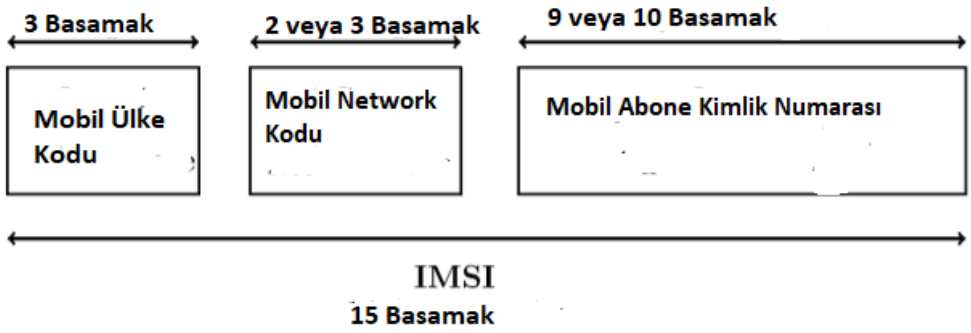
Grubun Bozuk Bir Üyesi, Grubun Başka Bir Üyesi Tarafından Servis Ağı Olarak Doğrulanır: Bu tehdit aynı zamanda grubun bir parçası olan bir davetsiz misafir içermektedir. Davetsiz misafirin amacı, grubun bir üyesi olan bir Makine Tipi İletişim ağ erişimini aradığında servis ağını taklit etmektedir.

Grubun Bozuk Üyeleri Sıralamak, Üçüncü Bir Grup Üyesi İle Servis Ağı Arasında Kararlaştırılan Oturum Ana Anahtarını Türetir: Bu tehdit grubun

üyesi olan birden fazla Makine Tipi İletişim bozma kabiliyeti ile davetsiz misafir kabiliyetlerini daha da genişletmektedir. Davetsiz misafirin amacı, servis sağlayıcı ağ ile davetsiz misafir tarafından kontrol edilmeyen üçüncü bir Makine Tipik İletişim arasında kararlaştırılan oturum ana anahtarını öğrenmektedir.

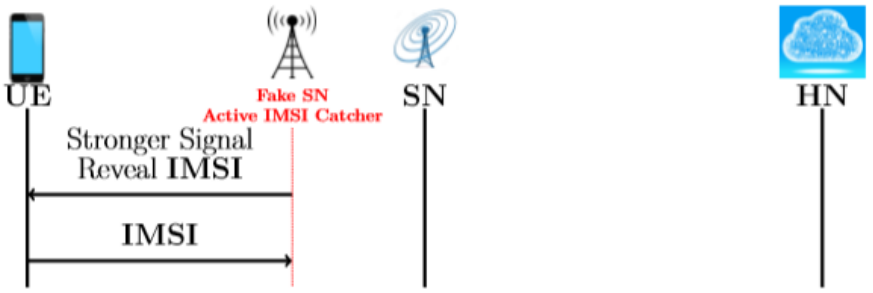
Beşinci Nesil haberleşme sistemlerinde kullanılan Kimlik Doğrulama ve Anahtar Anlaşması protokolünün hem eski haberleşme versiyonlarından gelen güvenlik zafiyetlerini olduğu tespit edilmiştir. Saldırganlar bu protokollerin zafiyetleri bildiği ve geliştirdikleri için Beşinci Nesil haberleşme sisteminde geliştirilmesi beklenmektedir.

4.4.1.2 Uluslararası Mobil Abone Kimlik Numarası Güvenlik Zafiyetleri



Şekil 40 Uluslararası Mobil Abone Kimliği

Uluslararası mobil abone kimliği, Mobil İletişim Global Sistemi ve Evrensel Mobil Telekomünikasyon Sistemi şebekesi cep telefonu kullanıcıları ile ilişkilendirilen, genellikle on beş rakam olan benzersiz sayıdır. Mobil ağlardaki en önemli konulardan biri Mobil Abone kimliğinin gizliliğidir. Dördüncü ve Beşinci nesil haberleşme sisteminde Kullanıcı Doğrulama protokolünde kullanılmaktadır. Kullanıcı şebeke içersin de servis ağına bağlanıldığında kullanıcı mobil kimliği bilgisi şebekeye iletmektedir. Bu Bölümde saldırganlar Mobil Abone Kimliği yakalayıcı tekniğiyle bilgileri ele geçirmektedir. Mobil Abone Kimliği yakalayıcıları mobil ağ abonelerini gizlemek ve takip etmek için kullanılan cihazlara verilen genel addır.



Şekil 41 Mobil Şebeke İçinde Mobil Abone Kimlik Yakalayıcı örneği

Beşinci Nesil haberleşeme sisteminin Kimlik Doğrulama ve Anahtar Anlaşma protokolünde ETH Zürih ve Berlin'deki teknik üniversitesi yapılan güvenlik araştırmaları sonucunda protokolün tüm değişkenlerine karşı yeni bir gizlilik saldırısına izin verildiğini keşfedildi. Bu yeni keşfedilen güvenlik açığı, bölgedeki mobil trafiği engelleyebilecek bir saldırganın belirli bir sürede gönderilen aramaların veya SMS'lerin sayısı gibi bireysel abone faaliyetlerini izleyebilmesi için yazılım tanımlı bir radyoya sahip olması saldırganın aramalar veya metinler gönderilirken saldırganın yanında olmasa bile, kullanıcının kaç çağrı veya kısa mesaj gönderdiğini bilgisi ulaşabilmektedir. Kullanıcı bir ilk defa saldırı yapanın alanına girer ve daha sonra bölgeyi terk ederler geçmiş çağrı, metin etkinlikleri saldırı yapanın etki alanına girer savunmasız kalmaktadır.

Beşinci Nesil standartlarında yer alan kullanıcılara geçici kimlik numarası kullansa bile pasif bir saldırgan aralarında ilişki bularak gerekli Facebook, Twitter gibi sosyal medya kimlikleri veya telefon numaralarına ulaşabilmektedir. Nesnelerin internet cihazlarının Beşinci nesil şebeke ağına büyük veri oluşturduğunda güvenlik zafiyeti olma olasılığı çok düşük olmalıdır. Binde Bir ihtimal bile güvenlik zafiyeti verildiğinde verilerin değiştirme ve dinlenme olasılığı doğmaktadır. Büyük verilerin doğrulu ve doğru şekilde depolanması sıkıntıya girecektir.

4.4.1.3 Yazılım Tabanlı Ağ Güvenlik Zafiyetleri

Beşin Nesil iletişim teknolojisinin temel yapısını oluşturmaktadır. İletişim ağındaki kontrol ve yönetimi mantıksal bir şekilde yazılım tabanında

programlayarak ağ yönetimini kolaylaştırmaktadır. İletişim ağında veri alışverişini yazılımlarla programlayabilmesi gelecekte ağların alt yapısında önemli bir teknoloji olacaktır. Bu avantajlarına rağmen Yazılım Tabanlı Network tabanlı Beşinci nesil ağı güvenlik konularında zafiyetle nedeniyle oluşturulmasında zorluklar olacaktır.

Yazılım Tabanlı Ağ güvenlik üzerine yapılan araştırma çalışmaları, Yazılım Tabanlı Ağ kontrolörü üzerine inşa edilen güvenlik uygulamaları üzerine olmuştur. Geleneksel bir ağ mimarisinde, uygulamaların bazı cihazlarla iletişim kurarken ağ donanım cihazlarını programlaması gerekmektedir. Yeni bir üretici tarafından üretilen donanım cihazları değiştirilirse, bu cihazlar genellikle farklı bir Uygulama Programlama Arabirimi kullandığından, şebeke ağının programlanmasını ve zafiyetler vermesine neden olmaktadır. Bu sorunları çözümlenmesi için Beşinci nesil teknolojisinde çözülmesi için Yazılım Tabanlı Ağ mimarisi geliştirildi. Bu mimari uygulama katmanı, kontrol katmanı, veri katmanı şeklinde üç bileşenden oluşmaktadır. Geleneksel ağ mimarisine karşılaştırıldığında şebekeye gelen verileri ayırır ve hepsinin üst uygulama düzlemine maruz bırakmadan iki düzlemde kontrol etmektedir. Kontrol düzlemi şebeke ağının donanım cihazlarını otomatik olarak yöneteceğinden, ağı kontrol düzlemi tarafından verilen bir birim ara yüzle doğrudan kontrol etmesine yardımcı olarak ağa belirtilen donanım değişikliğinde yazılım tabanlı ağ dikkate almamaktadır. Bu işlevi yerine getirerek bu mimari merkezi kontrol ve programlanarak aynı özellikleri ağ güvenliği zorlukları ve zafiyetleri ortaya çıkarmaktadır. Yazılım Tabanlı ağ iletişim kanalının aşağıdaki nedenlerle savunmasız kalabilmektedir.

1. Uygulamalar ve denetleyici arasında güvenlik düzeyi düşük kimlik doğrulaması ile şebeke içerisine Uygulama Programlama Arabirimi iletilerini üzerinde zafiyetlere neden olmaktadır.
2. Yazılım Tabanlı Ağ üzerinde uygunsuz yetkilendirme, uygulama yapıldığında kötü amaçlı erişime neden olabilmektedir.

3. Şebeke içersin de kontrolör ve anahtarlama arasındaki trafiğin şifrelenmemesi gizli aramalara ve yanıltıcı haberleşmeye neden olabilmektedir.
4. Bu düzeyde güvenli olmayan zayıf kimlik doğrulamasının olmaması ortadaki adam saldırılarına neden olabilmektedir. Bu tür saldırıların ile şebeke içerisinde iletişim akışının kullanımda olduğunu ve hangi trafiğe izin verildiğini gömesini ve dinlenmesini kolaylaştırılır.

Yazılım Tabanlı Ağ mimarisinde bulunan güvenlik açıkları birçok veri güveliği değiştirilmesine, dinlenmesine yol açacaktır. Kötü niyetli bir saldırganın Yazılım Tabanlı Ağa saldırmak için bu güvenlik açıklarını gösteren üç klasik saldırı tipi aşağıda belirtilmiştir.

IP Sahteciliği: Bu mimaride ilk tip IP sahteciliğidir. Yazılım Tabanlı Ağlarına sahte paketleri ağa entegre etmek için sahte IP adresleri kullanmaktadır. Bir Dağıtılmış Ağ saldırısında (DDOS), saldırgan IP sahteciliğini üzerinden bulunabilecek IP adreslerini kullanarak TCP SYN mesajlarını, UDP SYN mesajlarını veya ICMP mesajlarını hedef cihaza saldırı gerçekleştirmektedir. Bu saldırı ile mimarinin yönetilme, karar alma engellemekte ve performansını düşürülmesine neden olmaktadır.

Ortadaki Adam Saldırısı: Bu tip saldırıda, şebeke ağ içersin de saldırgan gizlice kendilerine güvenen iki taraf arasındaki veri iletişimi sırasında araya girerek veriyi iki tarafa değiştirerek iletmektedir. Yazılım Tabanlı Ağda iletişim kanalları arasında doğrulama yeterliliği olmadığı için Otadaki Adam Saldırısıyla verileri gizlice dinleyerek şebeke içindeki tüm ayrıntıları öğrenebilmektedir.

Tekrarlama Saldırıları: Orta Adam Saldırısına benzer şekilde saldırgan şebeke ağının veri kanallarına sızarak gizlice dinlemeye başlamaktadır. Saldırgan geçerli veri iletimini sürekli tekrarlar ve geciktirir, böylelikle şebeke içindeki hedef kullanıcılar veri iletişimini başarıyla tamamladıklarını düşünmeyi sağlayarak hedef kullanıcıları kandırmaktadır.

4.4.1.4 Şebeke Fonksiyonları Sanallaştırma Güvenlik Zafiyetleri

Beşinci Nesil teknolojisi geliştirme gruplarından 3GPP çalışma grubu, güvenlik ve gizlilik gereksinimlerinin belirlenmesinde ve Beşinci Nesil güvenlik mimarilerinin ve protokollerinin belirlenmesinde aktif olarak yer almaktadır. Şebeke Fonksiyonları Sanallaştırma gelecekteki iletişim ağları için çok önemli olacak bir teknolojidir. Ancak gizlilik, bütünlük, özgünlük ve reddedilme gibi güvenlik zafiyetleri bulunmaktadır.

Mobil ağlarda Kullanımı açısından bakıldığında Mevcut Şebeke Fonksiyonları Sanallaştırma platformlarının sanallaştırılmış telekomünikasyon servislerine uygun güvenlik sağlanmadığı görülmektedir. Mobil ağlarda kullanımına devam eden temel zorluklarsan biri, yapılandırma hataları ve dolayısıyla güvenlik kesintilerine yol açan Sanal Ağ İşlevlerinin dinamik doğasıdır.[38]

		Etkilenen 5G Teknolojileri				Gizlilik
Saldırı Tipleri	**Hedef Nokta /5G Şebeke Ağ Elamanı**	**SDN**	**NFV**	**Kanallar**	**Bulut**	
DOS Saldırısı,	Merkezi kontrol elemanları	Evet	Evet		Evet	
Kaçırma Saldırıları	SDN kontrolör, hipervizör	Evet	Evet			
Sinyal Fırtınaları	5G çekirdekli ağ elemanları			Evet	Evet	
Kaynak (Dilim) Hırsızlığı	Hiper Yönetici, paylaşılan bulut kaynakları		Evet		Evet	
Yapılandırma Saldırıları	SDN (sanal) anahtarlar, yönlendiriciler	Evet	Evet			
Doygunluk Saldırıları	SDN kontrolör ve anahtarları	Evet				
Penetrasyon Saldırıları	Sanal kaynaklar, bulutlar		Evet		Evet	
Kullanıcı Kimliği Hırsızlığı	Kullanıcı bilgi veri tabanları				Evet	Evet
TCP Seviyesi Saldırıları	SDN kontrolör-anahtar iletişimi	Evet		Evet		
Ortadaki Adam Saldırısı	SDN kontrolör iletişimi	Evet		Evet		Evet
Sıfırla ve IP Taraması	Kontrol kanalları			Evet		
Tarama Saldırıları	Açık hava arayüzleri			Evet		Evet
Güvenlik Anahtarlarına Maruz Kalma	Şifrelenmemiş kanallar			Evet		
Anlamsal Bilgi Saldırısı	Abone konumu			Evet		Evet
Zamanlama Saldırıları	Abone konumu				Evet	Evet
Sınır Saldırıları	Abone konumu					Evet
IMSI saldırıları Yakalamak	Abone konumu			Evet		Evet

Tablo 5 Beşinci Nesil Güvenlik Sorunları

Saldırgan hedef Beşinci Nesil şebekesinin Şebeke Fonksiyonları Sanallaştırma ve Yazılım Tabanlı ağ yapısına DOS saldırısı, Kaçırma saldırısı,

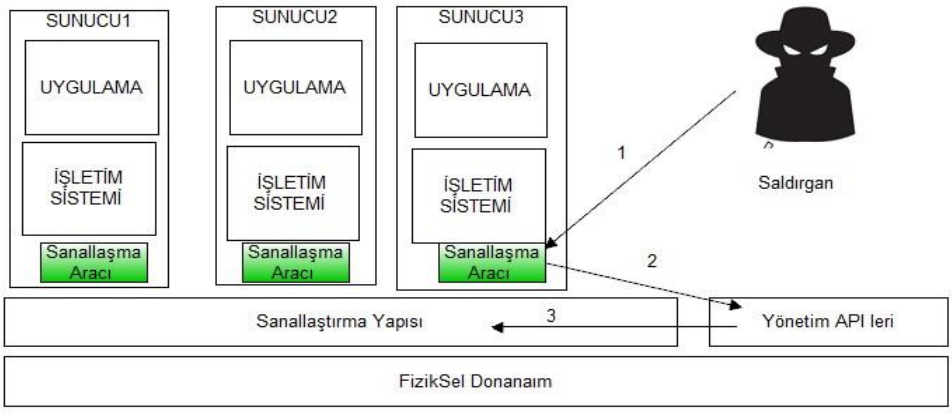
[38] A. van Cleeff, W. Pieters, and R. J. Wieringa, "Security Implications of Virtualization: A Literature Study," in 2009 International Conference on Computational Science and Engineering, vol. 3, Aug 2009, pp. 353–358

Yapılandırma Saldırıları yapılarak saldırgan tarafından ele geçirildiğinde tüm şebeke ağı tehlikeye girmiş olacaktır.

Şebeke Fonksiyonları Sanallaştırma yöntemi fiziksel donanım üzerinden çalışan kaynakların sanallaştırılarak çalışmaktadır. Şebeke Fonksiyonları Sanallaştırma güvenlik zafiyetleri fiziksel ağ üzerinde iki tehdit kümesi birbiriyle kesiştiğinde güvenlik zafiyetleri ortaya çıkmaktadır.

Saldırgan şebeke ağ üzerinde fiziksel donanıma üzerinde sanallaştırma programına saldırıldığındaki senaryoyu incelediğimizde saldırının başarılı olması durumunda tüm şebeke ağ için büyük risk doğurmaktadır. Bu yönteme Sanal kaçış saldırısı adlandırılmaktadır.

Bu saldırıda senaryosunda saldırgan ilk olarak fiziksel sunucunun işletim sistemine erişerek Şebeke Fonksiyonları Sanallaştırma yazılımına taviz işlemleri başlamaktadır. Şebeke ağı bağlantıları ve bulut yönetim ağı araçlarını kullanarak sanallaşma yazılımının uygulama programlama ara yüzüne erişim kazanması ardından saldırgan büyük etkiye neden olması için sanallaşma yazılımına girmektedir. Bu saldırılar sanallaştırma yazılımı ile Şebeke Fonksiyonları Sanallaştırma arasındaki izolasyon neden olmaktadır.



Şekil 42 Şebeke Fonksiyonları Sanallaştırma Kaçış Saldırı Senaryosu

4.4.1.5 Mobil Bulutlarda Güvenlik Zafiyetleri

Bulut bilgi işlem sistemleri, kullanıcılar arasında paylaşılan çeşitli kaynakları içerdiğinden bir kullanıcının tüm sistemin performansını düşürmek daha fazla kaynak tüketmek veya diğer kullanıcıların gizlice erişim kaynağını tüketmek için kötü niyetli trafiği yayması mümkün olmaktadır. Mobil bulut bilişimi Beşinci Nesil eko sistemi ile iç içedir. Bu nedenle kablosuz ağ şebekesi alt yapısında veri güvenliği açıkları oluşturmaktadır.

Mobil bulut bilişimini tehditlerini hedeflenen bulut seğmenlerine göre ön uç, arka uç ve ağ tabanlı güvenlik tehditlerine göre sınıflandırılmaktadır. Mobil bulut bilişim mimarisinin ön ucu, bulut tesislerin erişmek için gereken uygulamaların birimlerin çalıştığı mobil terminalden oluşan istemci platformudur.

Tehdit çevre düzenlemesi fiziksel tehditlerden farklı olabilmektedir. Gerçek mobil cihaz ve diğer donanım bileşenlerinin uygulama tabanlı tehditlere karşı birincil hedefler olmaktadır. Casus yazılım ve diğer kötü huylu yazılım ile saldırgan uygulamalarını bozmak veya hassas kullanıcı bilgileri toplamak için kullanılmaktadır.

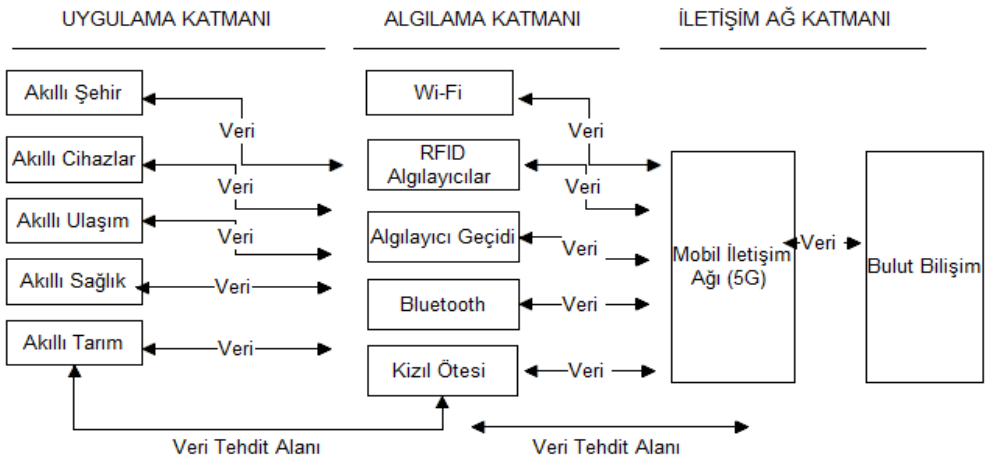
Arka uç platform, bulut sunucuları, veri depolama sistemleri, sanal makineler, sanallaştırma yazılımları ve bulut hizmetleri sunmak için gerekli protokollerinde oluşmaktadır. Bu platformda tehditler bakıldığında HTTP ve XML DOS saldırıları gibi türleri vardır. Ağ tabanlı mobil güvenlik tehditleri, mobil cihazları buluta bağlayan Radyo Erişim Teknolojilerine yöneliktir. Wİ-Fİ taraması, DOS saldırıları, adres kimliğine bürünme ve oturum ele geçirme gibi tehditlerle Bulut Radyosu Ağı Beşinci nesil mobil bulutlardaki güvenlik zorluklarına neden olmaktadır.

Beşinci Nesil mobil iletişimin gelişmesiyle Bulut Radyo Erişim Ağı mobilete kapasitesi artışına neden olmaktadır. Bulut Radyo Erişim Ağı sanal sistemler, bulut bilişim teknolojisi ile ilgili doğal güvenlik sorunlarına eğimlidir. Örneğin Bulut Radyosu Erişim Ağı merkezileşmiş mimarisine tek bir başarısızlık noktası tehdidinde bulunmaktadır. Bakıldığında bu tip teknolojilerin gelişmesiyle

faydalarının yanı sıra veri güvenliğin giderilmesi konusunda çalışmalar yetersiz kalmaktadır.

4.4.2 Beşinci Nesil Haberleşme Sistemi Şebeke Dışı Veri Zafiyetleri

Beşinci Nesil haberleşme sistemlerinin kullanılmaya başlamasıyla birçok sektörü ve teknolojiyi iletişimini nesnelerin interneti donanımlarıyla bir araya getirerek birleştirmektedir. Birçok cihaz ve teknoloji yeni teknoloji şebeke dışından mobil kablosuz şebeke ağına veri taşıması yapacaktır. Bu bölümde kablosuz mobil ağa dışardan gelebilecek ver güvenlik zafiyetleri incelemesi yapılacaktır.



Şekil 43 Beşinci Nesil Sistemine Dışardan Gelen Veri iletişim Şeması

4.4.2.1 Uygulama Katmanındaki Veri Zafiyetleri

Beşinci nesil haberleşme sistemi iletişim ağına veri başlangıç noktası uygulama alanıdır. Bu alanda nesnelerin internetin sağladığı çeşitli uygulama ve servislerden oluşmaktadır. Bu uygulamalar akıllı şehirler, akıllı ev, akıllı ulaşım, akıllı enerji, akıllı sağlık, akıllı tarım hizmetleridir. Bu katmandaki kötü amaçlı saldırılar uygulamayı hatalı çalışmasını tetikleyerek geliştirilen teknolojilerin uygulama program kodunda zafiyetlere neden olarak verilerin ele geçirilmesine neden olmaktadır. Bu dikey sektörlerin gelişmeleriyle nesnelerin interneti ile

Beşinci nesil haberleşme sistemleri sayesinde milyarlarca uygulamalar ve cihazlar şebeke içinde tehlikeye neden olacaktır. Uygulama katmanına yönelik ortak tehditler aşağıdaki gibidir.

Kötü Amaçlı Kod Saldırıları: Bu tür bir saldırıda uygulamanın çalıştırıldığı işletim sistemi için ayrı bir işletim sistemi çalıştıran internet saldırısı yerleşik cihazlarına yayılan kötü amaçlı bir solucan örnek verilebilir. Bu Solucan saldırılarında akıllı şehirlerin cihazlarında, ev kullanıcı cihazlarında internete etkin aygıtlara etki etmektedir. Bu tür kod saldırılarında bir arabanın Wi-Fi, internete bağlı multimedya araçları ile aracın kontrol bölümüne saldırı yapılarak aracın hâkimiyetini ele geçirmektedir.

Nesnelerin interneti ile ve Beşinci Nesil iletişim sistemlerinin hayata geçmesiyle akıllı araçların şebeke içersin den dünyanın herhangi bir yerinden kötü amaçlı kod saldırıları ile akıllı araçların direk kontrol edebilecek, yön verebilecek veya aracı veri dineleme aracı haline getirebilecektir. Bu senaryonun tam tersine bakıldığında araca sızan bir saldırgan Mobil kablosuz şebeke ağına saldırı tehditleri gönderebilir.

Düğüm Tabanlı Uygulama Kurcalama; Bilgisayar korsanları cihaz güvenlik noktalarından yararlanarak kötü niyetli kök uygulama kurulmaktadır. Bu tehdit anlayışında aygıtın çalışmamasına, ortamın ısınmasına veya donmasına neden olmak için kendi ortamını değiştirmektedir. Kurcalanmış bir sıcaklık algılayıcısı sabit bir sıcaklık değerini gösterebilir veya akıllı evdeki kurcalanan kamera ortamın resimleri çekerek merkezi bir alana aktarılabilmektedir. Saldırgan hedef ortamdaki cihazları kurcalayarak verileri ele geçirebilir veya değiştirebilir bu şekilde verilerle kurcalanmış şekilde Beşinci nesil şebekeye gönderilmektedir.

Akıllı Sayaç/ Şebeke saldırıları: Bu tip saldırılarda, kullanım verilerini hizmet operatörüne faturalandırmak için göndermekten sorumlu olan akıllı sayaçlara yapılan saldırılardır. Akıllı sayaçların faturalandırma için gönderilen veriyi saldırgan ele geçirdiğinde mekânın boş olduğu ortaya çıkıp hırsızlığa neden olabilir. Bu örnekten yola çıktığımızda Nesnelerin interneti ve Beşinci Nesnelerin

haberleşme sistemi içerisinde milyarlarca cihaz veri alışverişi yapabilecek dünyanın herhangi bir yerinden yapılacak saldırılarda bölgenin veya ülkende çok büyük felaketlere, ekonomiye milyarlarca dolar zarar verecektir.

4.4.2.2 Algılama Katmanındaki Veri Zafiyetleri

Algıla katmanındaki güvenlik tehditleri düğüm düzeyinde değildir. Düğümler algılayıcılardan oluştuğu için, cihaz yazılımını kullanan cihazla değiştirmek için onlardan yararlanmak isteyen bilgisayar korsanlarının temel hedefidir. Algılama katmanında zafiyetlerin çoğu algılayıcıların veri toplama araçların dışardan gelen tehditlerinden gelmektedir. Algılama katmanındaki ortak tehditler aşağıdaki gibidir.

Veri Dinleme Saldırısı: Nesnelerin interneti ile Beşinci nesil haberleşme teknolojilerin gelişmesiyle cihazlar arasındaki iletişim internet üzerinden olacağından cihazlar yapılan saldırılar ile cihaz üzerine yerleşen kötü amaçlı uygulamalar sayesinden veri dinleme veya değiştirme olanağı sunacaktır. Cihazlar internet ortamından gelecek saldırılara karşı savunmasız olacaktır. Bu saldırı senaryosunda akıllı cihazlar üzerindeki algılayıcı ileteceği veriler dinleme yöntemiyle verileri toplamaya çalışır.

Atakları Koklama: Saldırganlar, cihazdan bilgi edinmek için kötü niyetli algılayıcılar veya akıllı cihazları normal cihazların yakınına koyarak bilgileri ele geçirebilmektedir. Akıllı ortamlarda nesnelerin interneti ile akıllı cihazların insan hayatına girmesi ile kullanıcıların izni olmadan ortamdan verileri saldırganlar taraftan izlenebileceği, değiştirilebileceği anlamına gelmektedir.

Beşinci nesil mobil kablosuz ağ sisteminde insandan insana, insandan cihaza veya cihazdan cihaza paylaşılan veriler saldırganlar tarafından izlenebilir ve ele geçirilme riskleri olmaktadır.

4.4.2.3 Radyo Frekans Tanımlama Veri Güvenlik Tehditleri

Nesnelerin internet kavramı ile birçok akıllı cihazların Beşinci nesil haberleşme cihazlarına veri taşıma işlemi gerçekleştirecektir. Bunlardan bir tanesi Radyo Frekans Tanımlama cihazlarıdır. Bu cihazlar değişik sektör uygulamalarında kullanım sağlamaktadır. Algılama katmanından alınan verileri Radyo Frekans üzerinden Beşinci nesil iletişim şebeke ağına iletmektedir. Radyo Frekans Tanımlama etiketlerinin gizlilik ve güvenlik sorunları oluşması durumunda verilerin güvenli iletilmesi konusunda büyük sorunlar yaratacaktır. Uygun şekilde korunmayan Radyo Frekans Tanımlama etiketleri her zaman veriyi gizli dinleme, veriyi yetkisiz şekilde ele geçirmesine neden olacaktır. Yetkisiz okuyucular etiketlere erişim kontrolü olmadan erişerek gizliliği veriyi ihlal etmektedir. Radyo Frekans Tanımına tehdit eden saldırılar aşağıdaki gibidir.

Koklama: Radyo Frekans Tanım okuyucuları her zaman etiketlere kimlik bilgilerini geri göndermeleri için istek gönderir. Okuyucu etiketler tarafından gönderilen bilgileri okuduğunda bir arka uç sunucusunda depolanan verilerle doğrulanır. Radyo Frekans Tanımlama etiketlerinin çoğu gerçek okuyucuları ile sahte okuyucuları ayrımını yapamamaktadır. Saldırgan etiket okumaları hedef verilere ulaşmak için kullanabilecektir.

Takip: Saldırgan Radyo Frekans Tanım etiketlerden alınan bilgilerle bir nesnenin, bir kişinin veya kurumun yerini ve hareketlerini izleyebilmektedir. Bir nesneye etiket eklendiğinde ve nesne okuyucusunun alınana girdiğinde saldırgan nesneyi tanımlayabilir ve yerini bulabilir.

Hizmet Reddi: Okuyucu etiketten bilgi istediğinde kimlik verisini veri tabanı sunucusunda depolanan kimlik ile karşılaştırır. Hem okuyucu hem de arka uç sunucu hizmet reddi saldırılarına karşı savunmasızdır.

Radyo Frekans Tanımlama cihazlarına dünyanın herhangi bir yerinden Beşinci nesil iletişim ile ilgili saldırı metotları ile saldırı yapabilir veriyi takip edebilir veya ele geçirebilmektedir.

4.4.2.4 Akıllı Röle İletişimindeki Veri Güvenlik Tehditleri

Beşinci Nesil haberleşme paralelinde nesnelerin interneti teknolojilerin gelişmesiyle cihazların birbirleriyle olan iletişimi çok önemli hale gelmiştir. Cihazlar arasında iletişim yöntemlerinden biri akıllı rölelerdir. Akıllı rölelerin mantığı iletişim şemasında röle dijital mesaj güvenliği sağlamak görevlidir. Bir röle den diğer röleye dijital mesajı her bir baytın sekiz veri biti içerdiği ikili bayttan oluşmaktadır. Merkezi iletişim baz istasyonundan geçerek her bir iletişimi içerecektir. Dağıtılmış iletişim ise, iletişimin doğrudan veya ara yarı akıllı röleler aracılığıyla yapılabileceği anlamına gelmektedir.

Beşinci nesil geçişinde çok sayıda cihazı ve uygulamayı desteklemeyi amaçladığı için akıllı röle uygulama bazında uygulanması beklenmektedir. Akıllı röle kullanımında yaşanacak güvenli zafiyetleri aşağıda belirtilmiştir.

Tekrar Saldırı: Geçerli verilerin kötü amaçlı olarak tekrarlandığı bir tür saldırıdır.

DOS Saldırısı veya Hizmet Reddi Saldırısı: Geçerli bir kaynağın kullanılmadığı bir saldırı türüdür.

Orta Saldırıdaki Adam: Saldırganın kendisinin kötü niyetli olarak yerleştirdiği ve iki taraf arasındaki iletişim sık sık değiştirdiği saldırı türüdür.

Serpiştirme Saldırısı: Devam eden iletişimden gelen iletişimin ve iletişimden kimlik doğrulama elde edeceği bir saldırı türüdür.

Önemli olan diğer güvenlik sorunu ise, araya girme saldırısında neden olacak çok taraflı kimlik doğrulamasıdır. Serpiştirme saldırısında iki cihaz arasında ii cihaz arasında iki farklı oturum kullanır. Birincisi bas istasyonu ve Röle, İkincisi aktarma ve aktarma arasında ve tüm hizmetleri yerine getirme bu saldırı başarılı olursa tüm veri kaybına neden olacak ve yanlış verilerin analizinde yanlış karar verilmesine neden olmaktadır.

4.4.2.5 Kablosuz Algılayıcı Veri Güvenlik Tehditleri

Beşinci nesil ve ötesi teknolojilerin gelişiminde etkileyeceği heterojen yapılarda gerçek zamanlı veri toplamak ve yönetmek için kullanılan teknolojiler den en önemlisi kablosuz algılayıcılardır. Kablosuz algılayıcılar çok küçük olması, düşük maliyetlerde olması, az enerji harcamasıyla yaygınlaşmıştır. Kablosuz algılayıcılar iletişim ağlar içindeki baz istasyonunu üzerinden ilgili bilgileri toplamaktadır.

Kablosuz algılayıcılarda güvenlik birçok saldırı türünden etkilenen tüm sistemleri ve geleneksel kablosuz algılayıcı ağların temel özelliklerinden biridir. Güvenlik saldırıları ağdaki algılayıcı cihazların fiziksel olarak erişebilir olması ve ağda minimum kapasitesinin kullanılması nedeniyle güvenlik zafiyetler olmaktadır.

Sinyal Sıkışma Saldırısı: Kablosuz algılayıcı ağındaki alıcı anten tarafından yayılan radyo sinyallerini aynı vericiye iletmesiyle olmaktadır. Bu saldırılar radyo parazit ve kaynak tükenmesi üzerinde etkilidir.

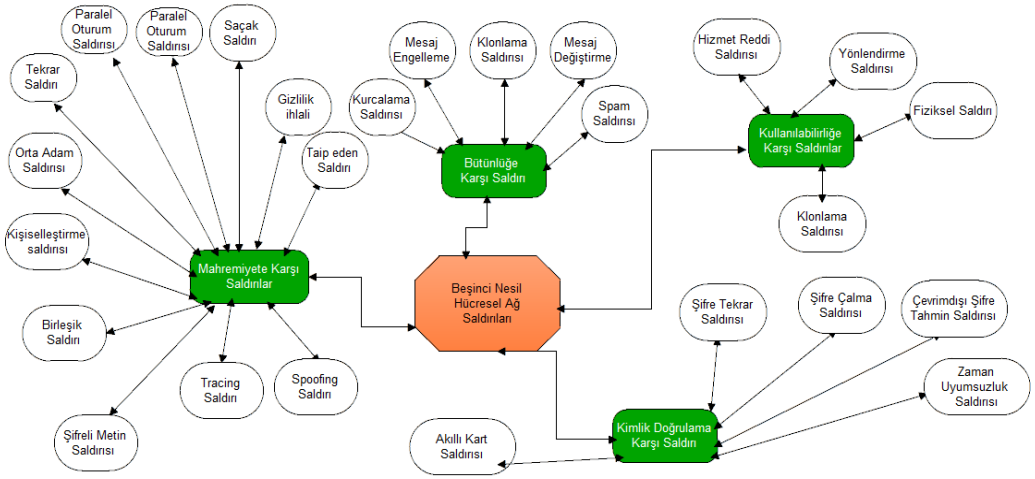
Düğüm Kesinti Saldırısı: Kablosuz algılayıcıların bileşenlerinin işlevselliğini duruyor ve saldırılar ağda fiziksel ya da mantıksal olarak uygulanmaktadır. Bu saldırıların etkileri veriyi okuma, toplama ve işlevleri başlatma gibi düğüm hizmetlerini durdurmaktadır.

Yakalama Saldırısı: Kablosuz algılayıcıların ağında saldırgan algılayıcıların fiziksel olarak ele geçirerek algılayıcıların alt yapısı kötü niyete kullanılmaya başlandı. Bu saldırının etkilerine bakıldığında hizmetleri durduruyor ve ağı kontrolünü sağlamaktadır.

Dinleme Saldırısı: Kablosuz algılayıcıların verileri aktarım iletişimi içersin de gizli dinleme yapılan saldırıdır. Kulak misafiri de gizlilik olarak adlandırılmaktadır. Bu saldırının etkileri hassas kablosuz algılayıcıların veri bilgilerini ayıklamakta ve düğümlerin gizliliğini silmektedir.

4.4.3 Beşinci Nesil Haberleşme Sistemi Genel Saldırı Tehdit Türleri

Beşinci Nesil haberleşme sisteminin hücresel ağı yapılabilecek saldırı tehditleri dört bölümde sınıflandırılması yapıldı. Birincisi mahremiyete karşı saldırılar, ikincisi bütünlüğe karşı saldırılar, üçüncüsü kullanılabilirliğe karşı saldırılar, dördüncüsü ise kimlik doğrulaması saldırıları şeklinde kategori yapılmıştır.



Şekil 44 Beşinci Nesil Hücresel Ağ Tehditlerin Türleri

4.4.3.1 Mahremiyete Karşı Saldırı Tehdit

Bu kategoride gizli dinlenme saldırısı, paralel oturum saldırısı, tekrarlama saldırısı, ortadaki adam saldırısı, kimliğe bürünme saldırısı, orta saldırı, izleme saldırısı, göz kamaştırıcı saldırısı, gizlilik ihlali, uyarlama seçilen şifre metni olarak kategori edilmektedir. Aralarında en ciddi saldırı tipi ortadaki adam saldırısıdır.

Hücresel ağlardaki ortadaki adam saldırısı, kötü niyetli üçüncü tarafların baz alıcı verici baz istasyonunu arasında yerleşerek iki taraflı iletişime dinlemeye değiştirmeye bağlamaktadır.

4.4.3.2 Bütünlüğe Karşı Saldırı Tehdit

Bu kategorideki ileti engelleme saldırısı, klonlama saldırısı, ileti değiştirme saldırısı, ileti ekleme saldırısı ve istenmeyen saldırılar yer almaktadır. Bütünlüğe karşı yapılan saldırı Beşinci nesil erişim noktaları ve mobil kullanıcılar arasındaki verinin değiştirilme temeline dayanmaktadır.

Beşinci nesil hücresel ağlar için kimlik doğrulama ve gizlilik koruma şemaları iletilen verilerin bütünlüğünü sağlamak için şifreleme algoritmaları kullanılmaktadır.

4.4.3.3 Kullanılabilirliğe Karşı Saldırı Tehdit

Bu kategoride ilk giren ilk çıkar saldırısı, yeniden yönlendirme saldırısı, fiziksel saldırı, kopya alma saldırısı ve serbest saldırı türleri yer almaktadır. Bu saldırının amacı bir hizmeti örneğin veri yönlendirme servisini kullanılmaz hale getirmektir. İlk giren ilk çıkar saldırısı saldırgan tarafından girme ve toplama zaman aralık verilerini toplamaktadır.

Yönlendirme saldırısı, saldırganın yönlendirme yapabilmesi için sinyal gücünü arttırarak hücresel ağlarında bir baz istasyonunu taklit ederek kullanıcı verileri kolayca almak mümkün olacaktır.

4.4.3.3 Kimlik Doğrulama Karşı Saldırı Tehdit

Bu kategoride parola yeniden kullanma saldırısı, parola çalma saldırısı, sözlük saldırısı, aba kuvvet saldırısı, zaman uyumsuzluk saldırısı, sahtecilik saldırısı, doğrulama saldırısı, akıllı kart saldırısı, kısmi ileti çarpışma saldırısı türlerinden yer almaktadır.

Kimlik doğrulama karşı bir saldırının amacı, istemciden sunucuya kimlik doğrulaması ve sunucudan istemciye kimlik doğrulamasını saldırı düzenleyerek

işlevsiz hale getirmektir. Parola yeniden kullanma saldırısı ve parola çalma saldırısı, saldırganın yasal kullanıcı olduğunu iddia ettiği ile sözlükten parola farklı sözlükler tahmin ederek oturum açmaya çalıştığı parola tabanlı kimlik doğrulama sisteminin işlevsiz hale getirir.

4.4.4 Dünyadaki Veri Güvenlik Saldırıları

4.4.4.1 Mobil Cihazlardaki Saldırılar

Symantec firmasının 2019 yılında yayınladığı 2019 İnternet Güvenliği Tehdit raporuna göre mobil cihazlarda fidye kötü yazılım saldırısı sayısı 2017 yılına göre üçte bir oranında artış yaşanmıştır. Mobil fidye kötü yazılımlarının en çok etkilenen yüzde altmış üç ile ABD olmuştur. Çin yüzde on üç ve Almanya yüzde on olarak takip etmiştir. Mobil cihaz güvenliğini yönetmek organizasyonlar için zorluk yaratmaya devam etmektedir.

Symantec 2018 raporuna göre mobil uygulama kategorilerinde günde ortalama 10 kötü amaçlı mobil uygulama engellendi. Mobil araçlar uygulamasından %39, yaşam biçimi uygulaması ise %7 kötü amaçlı yazılım rastlanmıştır. Mobil uygulamaların yüksek riskli verilere ulaşımı 2018 yılında %7 olarak belirlenmiştir. Sağlık verilere erişimi %2 olarak rapora yansımıştır. [39]

4.4.4.2 Nesnelerin İnternet Saldırılar

2017 de Nesnelerin interneti saldırılarındaki büyük artış yaşanmaktadır. Symantec ürünlerine ayda ortalama 5200 saldırı engellemiştir. Bu saldırıların çoğunluğu yönlendiriciler ve bağlı kameralardan, diğer bağlı cihazlardan gerçeklemiştir. Saldırılarda kullanılan virüslü kameraların oranı 2018 yılında önemli ölçüde artığı görülmektedir. Bağlı cihazların saldırıların %15'nin virüslü kameralar, %75 yönlendiriciler, %5 Multi medya cihazlarından oluşturmaktadır.

[39] Symantec, 2019 İnternet Güvenliği Tehdit Raporu, Volume 24

Diğer bir saldırı türü de Telnet'dir. 2018'de yapılan saldırıların %90 dan fazlasını oluşturmaktadır. Nesnelerin internet cihazlarına yoğun şekilde saldırılar düzenlenmektedir. Bunların %32'i Lightaidra , %31 Kaiten hizmet reddi dağıtım virüslerinden oluşmaktadır.

4.4.4.3 Bulut Sistemleri Saldırılar

Beşinci Nesil hücresel ağ sistemi bir parçası olan bulut sistemlerinde yanlış yapılandırmalar oluşması nedeniyle 2018 yılında çok çeşitli güvenlik açıkları ortaya çıkmıştır. Bulut bileşimlerinin yapılan saldırılarda 70 milyondan fazla kayıt çalındığı ortaya çıkmıştır. 2017 yılında MongoDB gibi açık veri tabanlarına karşı yapılan fidye kötü yazılım saldırıları saldırganın içerikleri sildiğini ve geri yüklemek için ödeme istediği görülmüştür.

Potansiyel Saldırganların internette yanlış yapılandırılmış bulur kaynaklarının tanımlamasını sağlayan çok sayıda araç bulunmaktadır. Bu araçlarla kolaylıkla bulut teknolojilerine saldırılar yapılması kolay haline gelmiştir. Bulut bileşimlerinde kullanılan donanım yongalarındaki birçok güvenlik açığının ortaya çıkmıştır. Meltdown, Spectre gibi kötü yazılımlar güvenlik uygulamalarından yararlanarak saldırılarda bulunmaktadır.

4.4.4.4 Dünyada Gerçekleşen Saldırılar

Haberleşme alanlarındaki teknolojilerin gelişmesiyle veriye ulaşma çok hızlı olmaya başlamıştır. Beşinci nesil hücresel ağ teknolojisinin yürürlüğe girmesiyle milyarlarca cihaz anlık bir ağ üzerinde olması planlamaktadır. Bu ağ üzerinde dolaşacak verilerin değişmediğini veya dinlenmediğini anlamak giderecek zorlaşacaktır. Son yapılan araştırmalarda verilerin korunmasında yetersiz önlemler alındığı ortaya çıkmıştır.

Beşinci nesil haberleşme öncesi dünyada yaşanan başarılı olan veri saldırıları mevcut durumu analiz etmek için aşağıda incelenmiştir.

1. 2013 yılında Adobe şirketi 2.9 milyon hesabın kişisel bilgilerinin çalındığını açıkladı. Kullanıcıların girişleri, şifreleri, adları, kredi kartı numaraları ve son kullanma tarihleri gibi bilgilerin çalınmıştır. Bu saldırıda adobe firmasının kendi ürünleri ilgili 40GB üzerinde kaynak kodu çalınması saldırının büyüklüğünü göstermektedir.
2. 2016 yılında tüm zamanların en büyük ihlallerinden bir olan 3 milyar YAHOO hesabı saldırıya uğradı.
3. 2016 yılında UBER bilgisayar korsanlarının 57 milyondan fazla sürücünün bilgisinin çalındığını bildirdi.
4. 2017 yılında arkadaş bul sitelerinden 412 milyon kullanıcı hesabı çalındı.
5. 2017 yılında en az150 ülkede 100.00 grup ve 400.000 den fazla makine Wannacry virüs tarafından bulaştırıldı.
6. 2017 yılında Truva atı virüsü olan Ramnit finans sektörünü büyük oranda etkiledi.
7. 2017 Yılında Nesnelerin internet cihazları saldırıları %600 artmış bulunuyor.
8. 2017 yılında endüstriyel kontrol sistemine bağlı güvenlik açıklarında %29 artış olmuştur.
9. 2018 yılında 150 milyon kullanıcıyı etkileyen 'My Fitness Pal' türünde saldırıya uğranıldığı bildirildi.
10. Fidye yazılımı tarafından en fazla saldırı yapılan sektör sağlık alanında olmuştur.2020 yılında bu saldırılar dört kart artacağı öngörülmektedir.

4.4.5 Beşinci Nesil Teknolojisinin Verilerin Hukuk Sistemine İlişkisi

Dünyada bilgisayarların ve internet kullanıcılarının artışı nedeniyle toplumsal, sosyal ve ekonomik hayatının internet üzerine kayması neticesinde verilerin ihlali ve çalınma gibi saldırıların arması nedeniyle kişisel veri koruma kanunları üzerinde çalışmalar başlatılmıştır. Veri koruma yasalarının temel amacı bireylerin, kişisel bilgilerini yanlış kullanımlarına karşı korumaktadır.

Gerçekleştirilen bu yasalar Beşinci Nesil haberleşme ve ötesi teknolojilerinin gelişmesiyle veri koruma konunda çok şeylerin değişebileceği düşünülmektedir.

4.4.5.1 Genel Veri Koruma Yönetmeliği (GDPR)

Genel Veri Koruma Yönetmeliği, 28 Avrupa Birliği ülkesinin tamamında veri koruma yasasının standart hale getirilmiştir. Yönetmelikte kişisel olarak tanımlanana bilgilerin kontrol edilmesi ve işlenmesi konusunda katı kurallar getirmiştir. Genel Veri Koruma Yönetmeliği 2018 tarihinde Avrupa Birliğine yürürlüğe girmiştir. Bu yönetmelikte kuruluşların kişisel olarak tanımlanabilir bilgileri nasıl toplandığını, saklandığını ve kullandığını kapsamaktadır. Bireylere, kişisel verilerinin nasıl toplandığını tutulduğunu ve kullanıldığını ve kim tarafından daha fazla kontrol sağlamayı amaçlamaktadır.

Bu yönetmelik Geniş anlamda kuruluşlardan kişisel verilerin yasal olarak adil ve şeffaf şekilde işlenmesi, belirli, açık ve meşru bir amaçla sadece gerekli olan verilerin toplanması, verilerin doğru ve güncel tutulması, verileri tanımlanabilecek ve gerekenden daha uzun süre saklama yapılmaması, verilerin güvenliği için gerekli teknik kurumsal önlemlerin alınması istenmektedir. Yönetmeliğe uyumsuz olan şirketlerin uyumsuzluk cezaları çok fazla olmaktadır. Bu cezalar 20 milyon Euro ya da şirketlerin toplam küresel gelirlerinin %4'ü kadar değişmektedir. Verilerin işlemek için yeterli müşteri onayına sahip olmamak ya da tasarım kavramıyla gizlilik ihlal edildiğinde para cezaları kademeli bir yaklaşım vardır.

Genel Veri Koruma Yönetmeliğinin maddelerinde kuruluşların aşağıdaki hususlarla ilişkin elektronik olarak yazılmış kayıtların tutulması ve istenildiğinde bu kayıtların vermeye hazır olması gerektiğini söyler:

- Tüm kontrol cihazlarının, işlemcilerin ve veri koruma görevlisinin iletişim bilgileri
- Bilginin toplandığı yöntem ve süreçler
- Toplanan bilgilerin kategorileri
- Verinin Toplanma Amaçları

- Toplanan bilginin nasıl kullanıldığı
- Veri toplama işleminde etkilenen belirli guruplar,
- Verilerin ne kadar süreyle tutulacağına dair tahmin
- Kişisel verilerini korumak için alınan güvenlik önlemleri

Bu yönetmelikte işletmelere çok ağır cezalara verilmektedir. Verinin güvenliğini veriyi kullanacak işletmelere vermektedir. Beşinci nesil haberleşme sistemleri gerçekleştirecek telekomünikasyon şirketleri veya haberleşeme şebekesine veri taşıyacak akıllı cihazların üreticileri veri güvenliğinin üst düzeyde çalışmalar yapması gerekmektedir. Veri güvenlik sorumluluklarını yerine getirilmedikleri takdirde çok büyük cezalara neden olacaktır.

Beşinci nesil öncesi ve sonrası sistemlerinin güvenlik zafiyetlerini incelediğimizi düşünüldüğünde veri güvenliğinin, doğruluğunun sağlanamayacağını gözükmektedir. Genel veri koruma yönetmeliğinin bireysel gizliliği korumak için tasarlanan süreçlerde oluşacak veri tabanları siber saldırı hedefinde olacaktır.

4.4.5.2 Beşinci Nesil Teknolojilerinde Ağ İşlevlerinde Sanallaştırmada Veri Güvenliği ve Gizlilik Sorunları

Beşinci Nesil haberleşme sistemimin en temel özelliklerinden ağ işlevlerinde sanallaştırma özelliğidir. Ağ işlevleri Sanallaştırma, birden fazla ve farklı mantıksal ağı desteklemek için bir fiziki ağ üzerinde kullanılan alt yapıdır. Her mantıksal ağ kullanıcılarına özel protokoller ve işlevler kümesi sağlamaktadır. Ağ sanallaştırmanın önemli bir yönü bu sistemi içersin de üç ana katılımcılardan oluşmaktadır. Bunlar ağ altyapısını sağlayıcıları, Sanal ağ operatörleri ve kullanıcılardır. Bu üç katılımcı bağımsız ve farklı amaçlarla yönlendirilebilmektedir. Bu nedenle sanal ağın tüm yönlerinin doğru ve güvenli bir şekilde çalışmasını sağlamak için her zaman iş birliği yaptıkları varsayılamaz. Sanallaştırılmış ağ mimarilerindeki güvenlik sorunları önemli zorlukla getirmektedir.

Sanallaştırma süreçlerine bakıldığında güvenlik ve gizlilik sorunları örnekler arasında paylaştırılan depolama ve paylaşılan ağların kullanılması ek güvenlik açıkları ortaya çıkarabilir. Sanallaştırılmış uçtan uca mimari birleşenleri arasında ara bağlantı korunmadığı taktirde yeni güvenlik tehditleri oluşturabilecektir. Bu özellikteki veri güvenlik tehditleri verinin ele geçirilmesi, değiştirilmesi veya dinlenmesi konusunda sıkıntılar oluşturacaktır.

4.4.5.3 Beşinci Nesil Teknolojilerinde Yazılım Tabanlı Ağlarda Veri Güvenliği ve Gizlilik Sorunları

Beşinci Nesil haberleşme sisteminin en büyük özelliği yazılım tabanlı iletişimdir. Yazılım Tabanlı ağ iletişimi ağ güvenliği dağıtımları için çok ihtiyaç duyulan esnekliği sunmak için merkezi bir kontrol modeli sağlamaktadır. Bu özelliğin birçok fayda ile birlikte özellikle bulut ve sanallaştırılmış ortamların ortaya çıkmasıyla yeni tehditler ortaya koymaktadır. Farklı düzlemlere ayrılmış ve kontrol işlevselliğinin merkezi bir sistemde toplanması da yeni zorluklar oluşturmaktadır. Arızalı veya kötü amaçlı yazılım kontrol düzlemine verilen erişim olanağı ile tüm ağı tehlikeye atabilmektedir.

4.4.5.4 Nesnelerin İnternetinde Yasal Sorunlar

Beşinci Nesil haberleşme sistemleri tüm teknolojileri birleştiren bir yapı olarak karşımıza çıkmaktadır. Bu yapılarsan bir tanesi Akıllı cihazlardır. Beşinci nesil sistemlerinin gelişmesiyle giderek hayatımızın parçası haline gelmektedir.

Nesnelerin İnterneti akıllı cihazların herhangi bir yasal çerçeve veya düzenleyici kurallar, yasalar olmadan çoğalmaktadır. Beşinci nesil ve ötesi teknolojiler sayesinde şebekeye bağlanarak birbirleriyle iletişim kurabilmektedir. Böylece yasal bir sorumluluk olmadan şebeke ağında solucan kutu haline gelmektedirler. Saldırganları için saldırı araçlarına dönüşmektedir.

Bağlı akıllı cihaza sahip işletmeler, veri ihlali veya saldırı durumunda kim sorumlu olacağı büyük bir soru haline gelmiştir. Akıllı şehir, Akıllı ev, veya Akıllı endüstrilerde birbirleriyle iletişim kurulan bir yapıda cihazların tümü aynı

üreticiden olmayabilir ve farklı yazılım sağlayıcıları içerebilmektedir. Böylelikle verinin korunmasında ciddi sıkıntılar çıkacaktır.

4.4.5.5 Beşinci Nesil Haberleşme Sisteminden Kaynaklanan Yasal Sorunlar

Beşinci nesil haberleşme sisteminin şebeke ağına daha fazla cihazın bağlanmasını sağlamak, siber güvenlik için daha fazla ve daha yüksek risk anlamına gelmektedir. Beşinci Nesil haberleşme sistemine eklentiler sistemin daha fazla dijitalleşmesine ve daha fazla şebekeye kontrolsüz giriş noktası olmasını sağlar. Bu nedenle saldırganlar şebeke içersin de zayıf bağlantı bulma olasılıkları artmaktadır. Şebeke içersin de bulunan tüm endüstriyel sektörler verilerin dinlenmesi, çalınması gibi risklere neden olmaktadır. Bu riskler Şebeke içersin de bulunan otonom araçların veya uzaktan ameliyat yapılması sırasında saldırıla maruz kalınabilir.

Bu tip risklerin ortadan kalması için gerekli uluslararası hukuki çalışmaların yapılması gerekmektedir.

SONUÇ

5.SONUÇ VE DEGERLENDİRMELER

Mobil haberleşme sistemlerinin gelişimi, kullanıcı ihtiyaçların değişmesine paralel olarak öncelikle ses ve veri iletişimi ile başlamış, daha sonra ses, mesaj, internet verileri ile devam etmiş ve nesnelerin interneti ile evrim geçirerek günümüze kadar gelmiştir. Bu gelişme ile birlikte, mobil şebeke üzerinde veri güvenliği ve gizliliğinin önemi artarken sistemin zafiyetleri de farklılaşmaya başlamıştır.

Birinci Nesil mobil haberleşme sisteminde ses verisi iletişimde kolaylık sağlarken, yasadışı klonlama, maskelenme, sahte Baz istasyonları, Dos saldırıları gibi saldırı yöntemleri ile şebeke içerisinde veri dinleme, değiştirme yaparak şebekenin güvenliği tehdit edilmiştir. İkinci Nesil mobil haberleşme sistemlerinde geliştirilen mesaj servis teknolojisinin kullanılmaya başlamasıyla saldırılar bu kez de mesaj servislerini üzerinden yapılmaya başlanmış ve şebekeyi tehdit altına almıştır. Üçüncü Nesil mobil haberleşme sistemlerinde, hem kullanılan teknoloji de hem de kullanıcının kullandığı telefonlarda çok büyük değişikliklere neden olmuştur. Kullanıcıların telefonları akıllı telefonlara dönüşmüş, ses, mesaj servisleri yerine internet kavramı ve mobil uygulamalar ortaya çıkmıştır. Kullanıcılar mobil uygulamalar üzerinden bilgiye ulaşabilmekte ve akıllı mobil cihazların kullanımı artmaktadır. Üçüncü Nesil mobil haberleşme sistemlerindeki gelişim, saldırganların kullanıcı verilerine ulaşma yöntemlerini de değiştirmiştir. Şebeke üzerinden Hizmet yavaşlatma, DDos, kimlik yakalama gibi saldırılarla kullanıcı bilgileri tehdit edilmiştir.

Kullanıcıların mobil uygulamalar ile veriye hızlı ulaşma isteği Dördüncü Nesil mobil ağ sisteminin geliştirilmesine neden olmuştur. Dördüncü Nesil mobil ağ yapısı bir öncekilere göre daha hızlı ve IP tabanlıdır. Bu nedenle kullanıcılar

dünyanın herhangi bir yerinden şebekeye bağlanarak istediği mobil uygulamayı, internet uygulamalarını, multimedya ve video gibi servisleri kullanabilmektedir. Bu uygulamalar aracılığıyla kullanıcının konumu, kişisel verileri şebeke üzerinden ulaşılır olmuştur. Saldırganlar bu bilgilere ulaşmak için şebekeye veya akıllı telefonlara Yarı pasif Atak, DNS yönlendirme gibi saldırılar yaparak verileri ele geçirmeye çalışmışlardır. Mobil haberleşme ağlarındaki bu güvenlik sorunları ve saldırı türleri detaylı şekilde tez çalışmasında açıklanmıştır. Önümüzdeki yıllarda Beşinci Nesil mobil haberleşme sistemlerindeki çeşitli zafiyetler daha önceki sistemlerdeki güvenlik sorunlarına ilave olarak yeni güvenlik sorunlarını gündeme getirecektir.

2020 yılında ticarileşerek Beşinci Nesil mobil haberleşme sistemlerinin kullanımı ve yayılması beklenmektedir. Beşinci Nesil mobil haberleşme sistemlerinin, önceki mobil ağlardan farklı olarak ultra güvenilir, yüksek hız ve düşük gecikme özellikleri ile tüm sektörleri ve teknolojileri birbirine bağlayan iletişim platformu haline gelmesi düşünülmektedir. Bu özellikler nedeniyle, milyarlarca cihaz şebeke içerisine çok büyük anlık veri üretilecek ve bu veriler aynı zamanda şebeke içinde dolaşıma girecektir. Bu büyük veri dolaşımı üzerinden, Beşinci Nesil haberleşme sisteminin güvenlik zafiyetleri kullanılarak, ne yazı ki verinin mahremiyetine, bütünlüğüne, kullanılabilirliğine yönelik saldırılar oluşacaktır.

Beşinci Nesil haberleşeme sistemi standart çalışmaları Uluslararası Telekomünikasyon Birliği Telekomünikasyon -ITU bağlı alt çalışma gurupları tarafından yürütülmektedir. Telekomünikasyon ve internet konularında uluslararası yetkinliğe sahip olduğundan otorite konumundadır. ITU ve ona bağlı kuruluşların yapacağı standart çalışmalar mobil haberleşme sektörünü ve yakınsamada olacak diğer sektörleri bağlayıcı konumda olacaktır. Çalışma guruplarının Beşinci Nesil haberleşme sistemlerinin zafiyetlerinin giderilmesi yönünde üst düzey çalışmalar yapması gerekmektedir. Veri güvenlik zafiyetlerinin giderilmesi konuşunda ITU ve alt çalışma guruplarına önerilerimiz aşağıda sıralanmıştır.

- Şebeke içerisinde dolaşan verilerin risk analizi yapılarak düşük, orta, yüksek, çok yüksek şeklinde risk gurupları oluşturulabilir. Beşinci Nesil sisteminin temel özelliklerinden olan yazılım, sanallaştırma ve şebeke dilimleme özelliklerini kullanarak risk guruplarına göre birbirinden bağımsız şebeke ağlarına ayrılabilir. Böylelikle düşük risk gurubunda olan bir cihaz yüksek risk gurubu şebeke ağı içersin de bulunmayacaktır. Sağlık sektöründe kullanıcıların kullandığı akıllı giysilerin, akıllı ilaçların veya uzaktan yapılan ameliyatların kullanılan akıllı cihazların gerçek zamanlı anlık saldırıya uğraması çok tehlikeli sonuçlar doğuracaktır. Sağlık sektörüne özel şebeke alt yapısı kurularak noktadan noktaya şifreleme ile saldırı yöntemlerine önlem alınabilmektedir.
- Nesnelerin interneti ile şebeke içerisine güvenliliği belli olmayan milyarlarca akıllı cihaz bağlanması öngörülmektedir. Bu tip akıllı cihazlar şebeke ve şebeke dışındaki tüm kullanıcıları, verileri saldırı altında olabilecektir. Uluslararası Telekomünikasyon Birliği Telekomünikasyon teşkilatına bağlı güvenlik sertifikasyon komitesi kurulması gerekmektedir. Kuruluş şebeke içerisine girecek akıllı cihazların güvenlik ve saldırı testlerini yapacaktır. Bu testler sonucunda saldırılara karşı güvenlik sorunu bulunmayan akıllı cihazlara benzersiz güvenlik kod verecektir. Bu kod ile şebeke içerisine bağlantı hakkı elde etmiş olacaktır. Saldırganlar güvenlik zafiyeti olan akıllı cihazlar bulamayacaklar ve saldırılarını gerçekleştiremeyeceklerdir.
- Yapay zekâ ve makine öğrenme teknolojileri kullanarak yapılan saldırıların analizler yapabilen saldırı önleyici yazılımlar geliştirilebilir. Bu yazılımlar sayesinde güvenlik zafiyetleri önceden görülerek gerekli önlemler alınabilmektedir.
- Akıllı cihazların mobil şebekeye verileri gönderimi sırasında WİFİ, RFID, Algılayıcılar, Bluetooth, kızıl ötesi teknolojiler kullanılmaktadır. Bu teknolojilerin kendine özel güvenlik zafiyetleri

bulunmaktadır. Güvenlik açıkları üzerinden saldırılar yapılmaktadır. Bu teknolojileri üreten üreticiler ile ITU bağlı çalışma gurupları tarafından giderilmesi gerekmektedir. Bu güvenlik sorunu giderilmediği takdirde verinin bütünlüğünü, kullanılabilirliğini ve dinlenmesi gerçekleşecektir.

Beşinci Nesil haberleşme sistemi kullanılarak tüm nesneler birbirleriyle etkileşim halinde olacaktır. İnsandan makineye, makineden makineye sürekli anlık etkileşim halinde olunacaktır. Etkileşim hukuki alanda sıkıntılara neden olacaktır. Otonom araçların akıllı şehirlerde kullanımı esnasında saldırı uğradığında kaza neden olacaktır. Bu kaza sonucunda hukuki sorumluluk nasıl olacağı konusunda belirsizlikler yaşanacaktır. Otomobil firması, akıllı cihaz üreticileri, kullanıcılar, mobil haberleşme sistemleri hukuki sorumluluk konusunda belirsizlikler yaşayacak olayın sorumlulukları bulunamayacaktır. Uluslararası yasa koyucuların ve Beşinci Nesil çalışmaları yapan çalışma guruplarının nesnelerin hukuku konu başlıklı altında komisyon kurarak regülasyonları oluşturması gerekmektedir.

Teknoloji üretici firmaları ürettikleri ürünlerin içerisinde veri trafiğini kayıt altına alabilecek Log sisteminin getirilmesi, hukuki açıdan ve veri ihlali sırasında sorumluluğu belirlemesinde faydalı olacaktır. 2020 yılında hayatımıza girecek olan Beşinci Nesil haberleşme sistemi güvenlik ve gizlilik zafiyetleri yüzünden veri ihlali gibi çok büyük sorunlar yaşayacağımızı bu tez çalışmasında ortaya koyulmuştur.

KAYNAKLAR

5G Americas Whitepaper	Cellular V2X Communications Towards 5G 2018
A Medium Corporation US	A Medium Corporation US 2018
Abdullah DEMİR	Femtocell ve Şebeke Entegrasyonunun İncelemesi Bilgi Teknolojileri be İletişim Kurumu İstanbul 2013
Abdurrahman TOKTAŞ	LTE, WİMAX VE WLAN iletişim Sistemleri için Mimo Anten Tasarımları ve Prototiplerinin Gerçekleştirilmesi Elektrik-Elektronik Mühendisliği Ana Bölüm Dalı, Mersin Üniversitesi Mersin 2014
Afşin BÜYÜKBAŞ	CDMA VE UMTS: Üçüncü Nesil Mobil Haberleşme Teknolojilerinin Karşılaştırılması, Türkiye Önerisi Bilgi Teknolojileri ve İletişim Kurumu Ankara 2005
Ahmet DARICI	3. Nesil Mobil Haberleşme Sistemleri Telekomünikasyon Kurumu Ankara 2002
Ahmet ÖZTÜRK	Bilgi Teknolojisi Alt Yapılarının Yönetiminde Yeni Nesil Yaklaşımlar; Bilgi Teknolojileri ve İletişim Kurumu Altyapısına Yönelik Bir Model Önerisi Bilgi Teknolojileri ve İletişim Kurumu Ankara 2013
Ahmet SOBACI	Spektrumun Etkin Kullanılması amacıyla 450-470 MHZ Frekans Bandında Yapılan Düzenlemeler ve Düzenlemelerin Marmara Bölgesine Etkisi ve Öneriler Bilgi Teknolojileri ve İletişim Kurumu Ankara 2012
AKBULUT Akhan, ZAİM Abdül Halim KARATAS Gözde	Mobil Cihazlarda Güvenlik- Tehditler ve Temel Stratejiler 2016
ALAVI MILANI Mir Mohammad Reza FARYAD Vahid	Mobil İletişim Nesillerin Evrimi İncelemesi : 4G'YE kadar Karadeniz Üniversitesi, Bilgisayar Mühendisliği Bölümü
AMAN ULLAH	IoT: Applications of RFID and Issues ISSN: 2367-9115 Pakıstan 2018
Antonella Molinaro, Antonio Iera, Francesco Menichella Claudia Campolo	5G Network Slicing for Vehicle-to-Everything Services University Mediterranea of Reggio Calabria NTT Data Italy 2017
Arş. Gör. Mehmet Fatih GÜRKAN	Düzenleyeici ve Denetleyici Kurum olarak Bilgi Teknolojileri ve İletişim Kurumu (BTK) İnönü Üniversitesi Hukuk Fakültesi Dergisi 2013
Atilla SEÇKİ	Genişband Uygulamaları ve Genişband Pazarında Çok Genişband (UWB) Teknolojisinin Yeri ve Türkiye Düzenlemeleri Bilgi Teknolojileri ve İletişim Kurumu Ankara 2005
Azzet GÜLŞEN	900 ve 1800 MHz Frekans Bandlarının Gelecekteki Kullanımı ve Türkiye Analizi Bilgi Teknolojileri ve İletişim Kurumu Ankara 2013

Bekir ÖZTÜRK	Türkiye'de ve Dünyada Sanal Mobil Şebeke Hizmeti (SMŞH)'nin Uygulama Biçimleri, SMŞH İşletmecilerinin Elektronil Haberleşme Piyasasına Giriş Engelleri ve Türkiye için Çözüm Önerileri Bilgi Teknolojileri ve İletişim Kurumu Ankara 2015
Bilal KOÇ	Mobil Bankacılık ve Türkiye'deki Uygulamaların Değerlendirilmesi Marmara Universitesi Banakacılık ve Sigorta Enstirüsü Bankacılık Anabilim Dalı İstanbul 2015
BORGAONKAR Ravishankar, NIEMI Valteteri SHAIK Altaf	Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems Aalto University
Cemal KOÇAK	Geniş Bant Hücresel İletimde (LMDS) TDMA /FDD Kullanarak Gerçek Zamanlı Çoklu Ortam Uygulaması Dumlupınar Üniversitesi Mühendislik Fakültesi Kütahya
Christos Politis	A New Generation of e-Health Systems Powered by 5G White Paper 2016
CRETU Vladimir BOCAN Valer	Security and Denial of Service Threats in GSM Networks Buletinul Stiintific al Universitatii “Politehnica” din Timisoara, ROMANIA 2004
Darrell M. West	How 5G technology enables the health internet of things Center for Teknology Innovation at Brookings Washington 2016
Doc. DR Askın DEMİRKOL	GSM-Hücre Planlama Yönetimi URSI-Türkiye’2014 VII. Bilimsel Kongresi ,Sakarya Üniversitesi Elaziğ 2014
DOĞRU İbrahim Alper UTKU Anıl	Mobil Kötücül Yazılımlar ve Güvenlik Çözümleri Üzerine Bir inceleme Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Ankara 2016
Dr.Mustafa Murat CANDAN	Üçüncü Nesil Mobil Haberleşme Sistemleri için Türkiye'de Uygulanacak Frekans Bandı,Lisns,Servisler,Uygulamalar ve Ülkemizdeki Durumu Telekomünikasyon Kurumu Ankara 2002
ELHAJJ Imad, CHEHAB, KAYSSI ayman BASSIL Ramzi	Effects of Signaling Attacks on LTE Networks Department of Electrical and Computer Engineering Beirut 2013
Emin ÖZTÜRK	Wlan Kablosuz Yerel Alan Ağları Teknolojisinin İncelemesi,Mevcut Düzenlemelerin Değerlendirilmesi ve Ülkemize Yönelik Düzenleme Önerisi Bilgi Teknolojileri ve İletişim Kurumu Ankara 2004
Engin ERTUNÇ	3N Mobil Haberleşme Sistemlerinde Kapsama Alanı ve Hizmet Kalitesi Denetimlerine İlişkin Ölçüm ve analiz Yöntemleri: Dünya Uygulamaları ve Türkiye Önerileri Bilgi Teknolojileri ve İletişim Kurumu Ankara 2011
Erdem CAN	Mobil Cihazların Çalışma Sistemleri ve Çevre Üzerindeki Etkileri Gazi Eğitim Fakültesi Orta Öğretim Fen ve Matematik Alanları Eğitim bölümü Fizik Eğitim AnaBilim Dalı Ankara 2006
Erol ÇETİN	Yeni Nesil Erişim Şebelerinde Bina İçi Kblo ve Tesislerin Paylaşımı: Avrupa İncelemesi, Türkiye'ye Yönelik Hukuki Durum Değerlendirmesi ve Düzenleme Önerileri Bilgi Teknolojileri ve İletişim Kurumu Ankara 2014

Esra GÖK	IP Tabanlı Şebekeler Üzeriden Ses İletimi (VOIP) Kapsamında Acil Aramalara Erişim ve Konum Verisi: Ülke UYgulamaları ve Türkiye Önerisi Bilgi Teknolojileri ve İletişim Kurumu Ankara 2013
Faruk YAYLA	Frekans İhalelerinin İhale Teorisi Kapsamında Değerlendirilmesi: Dünya Uygulamaları ve Türkiye İçin Model Önerisi Bilgi Teknolojileri ve İletişim Kurumu Ankara 2009
Fatma Belgin ŞAHİNOL	Üçüncü Nesil Mobil Telekomünikasyon Şebekelerinde Erişim: Srounlar ve Türkiye'ye Yönelik Öneriler Bilgi Teknolojileri ve İletişim Kurumu Ankara 2006
Fazlı KAYBAL	700 MHz Bandı İçin Türkiye Önerileri Bilgi Teknolojileri ve İletişim Kurumu Ankara 2014
FİKRİ AĞGÜN	Geçmişten Günümüze Hücresel Haberleşme Teknolojilerinin Gelişimi 2016
FRANKLIN, Joshua, BARTOCK Michael CICHONSKI Jeffrey	Guide to LTE Security U.S. Department of Commerce December 2017
Fredrik Jejdling	Ericsson Mobility Report Ericsson Sweden 2018
Furkan CİVELEK	Yeni Nesil Şebekelerin Telekomünikasyon Sektöründe Düzenlemelere Etkileri Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Ankara 2010
GEZGİN Deniz Mertkan	Kablosuz Ağ Teknolojileri ve şifreleme Trakya Üniversitesi Edirne 2011
Gönül İPEKÇİ	Mobil Haberleşme Cihazları ile İlgili Ulusal Bilgi Bankası Oluşturulması İçin Bir Model Önerisi Telekomünikasyon Kurumu Ankara 2005
Hakkı Soy	Gelecek Nesil Mobil Haberleşme Sistemleri: 3G, 4G ve Ötesi Uşak Üniversitesi Uşak 2012
Hanefi ÇINAR	Geçmişten Günümüze Hücresel Haberleşme Teknolojilerinin Gelişimi 2016
Hilmi YILMAZ	Kapalı Alanlarda 2N ve 3N Mobil Haberleşme Sistemlerinden Kaynaklı Elektromanyetik Alan Şiddetlerinin Karşılaştırılmalı Değerlendirmesi Bilgi Teknolojileri ve İletişim Kurumu İzmir 2013
Hüseyin EKİZ	Geniş Bant Hücresel İletimde (LMDS) TDMA /FDD Kullanarak Gerçek Zamanlı Çoklu Ortam Uygulaması Dumlupınar Üniversitesi Mühendislik Fakültesi Kütahya
İLGAR Hakan	MOBİL UYGULAMALARDA ERİŞİM İZİNLERİ İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı İstanbul 2016
İsmail ERTÜRK	Geniş Bant Hücresel İletimde (LMDS) TDMA /FDD Kullanarak Gerçek Zamanlı Çoklu Ortam Uygulaması Dumlupınar Üniversitesi Mühendislik Fakültesi Kütahya
Jale KÜÇÜKÜNSAL	Metropol Alanalr İçin Kablosuz Erişim Metropolıtan Area Network Kablosuz Metropol Alan Ağları- Wman Uygulamaları ve Düzenleme Önerileri Telekomünikasyon Kurumu Ankara 2006

Jun Yang, Jiehan Zhou,Yixue Hao, Jing Zhang,and Chan-Hyun Youn Min Chen	5G-Smart Diabetes:Toward Personalized Diabetes Diagnosis with Healthcare Big Data Clouds 2018
Jun Yang, Yixue Hao,, Shiwen Mao and Kai Hwang Min Chen	A 5G Cognitive System for Healthcare Huazhong University of Science and Technology Basel, Switzerland 2017
Kadir Kaya PAÇACI	Karasal Sayısal TV Yayıncılıpı ,Genişbant Pazarına Etkisi ve Dğzenleme Prespektifi Telekomünikasyon Ankara 2006
Konstantinos Antonakoglou Maria A. Lema	5G Case Study of Internet of Skills: Slicing the Human Senses King's College London
KUMAR Ashvini TIWARI Girish	Security Review and Study of DoS Attacks on LTE Mobile Network ISSN: 2321-8169 Volume: 5 Issue: 7 693 2017
Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke Mohamed Amine Ferrag	Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes 2017
Mademann Frank	The 5G System Architecture Chairman of 3GPP SA2, Huawei Technologies Germany 28 April 2018
Mehmet ALTINSOY	Genişbant Toptan Erişim Modelleri Arasındaki Geçiş Stratejilerinin Değerlendirilmesi: Yeni Nesil Erişim Şebekelerine Geçiş Odaklı Düzenleyici Yaklaşımlar ve Çözüm Önerileri Bilgi Teknolojileri ve İletişim Kurumu Ankara 2011
Mehmet Bayrak	Gelecek Nesil Mobil Haberleşme Sistemleri: 3G, 4G ve Ötesi Uşak Üniversitesi Uşak 2012
Mehmet EKİN	1400 MHZ Frekans Bandının LTE Hizmetlerinde Kullanılması: Türkiye İçin Düenleyici Öneriler Bilgi Teknolojileri ve İletişim Kurumu Ankara 2014
Mehmet Alper TEKİN	Yakınsamanın Telekomüniksyon Pazarına Etkileri: Dünya Uygulamaları ve Türkiye İçin Öneriler Bilgi Teknolojileri ve İletişim Kurumu Ankara 2009
Mehtap TÜZER	İkinci NesilHaberleşme Sistemlerinin Üçüncü Nesil Haberleşme Sistemlerine Adaptasyonu Gazi Üniversitesi Fen Bilimleri Enstirüsü, Yüksek Lisans Tezi 2010
Metin ACAR	4G Yeni Nesil LTE GSM Baz İstasyonu Anten Tasarımı Uludağ Universitesi Mühendislik-Mimarlık Fakültesi Dergisi Bursa 2010
Mu. Yzb. Hakan YÜCEL	Döndürcü Nesil (4G) Haberleşme Teknolojilerinin İncelenmesi ve Kara Kuvvetleri Taktik Seviye Birliklerinde Muharebe Koşullarında Uygulana birliğinin Analizi KaraHarp Okulu Savunma Bilimleri Enstitüsü Tekkoloji Yönetimi Ana Bilim Dalı Ankara 2014
Muammer ŞEYLAN	Üçünü Nesil Mobil Haberleşme Hizmetlerinin Yetkilendirme Politikaları ve Türkiye'ye Özgü Ulusal Bir Model Yaklaşım Telekomünikasyon Kurumu nkara 2007

Munip GEYLANİ — Geçmişten Günümüze Hücresel Haberleşme Teknolojilerinin Gelişimi 2016

Musa ÇIBUK — Geçmişten Günümüze Hücresel Haberleşme Teknolojilerinin Gelişimi 2016

Mustafa Serdar OSMANCA — 4G Teknolojisinde Kullanılmakta Olan Wimax ve 3GPP LTE Sistemlerinin İncelenmesi ve Karşılaştırılması Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimleri Enstitüsü Kahramanmaraş 2012

Nadide ERİŞ — LTE Yetkilendirmesinde Ortak Altyapı Konusu, Modeller ve Türkiye için Öneriler Bilgi Teknolojileri ve İletişim Kurumu Ankara 2015

Nitin Bange,Monika Kumbhar,Snehal Patil Suraj Shinde — Smart Medication Dispenser Technology Institute, Panhala from Shivaji India 2017

Ogr.Gor. Ahmet KIRDAR — GSM-HÜCRE PLANLAMA YÖNTEMI URSI-TÜRKİYE'2014 VII. Bilimsel Kongresi ,Sakarya Üniversitesi Elaziğ 2014

Özgür Özdemir — Gelecek Nesil Mobil Haberleşme Sistemleri: 3G, 4G ve Ötesi Uşak Üniversitesi Uşak 2012

PATRICIU Valeriu, BICA Ion VINTILA Christina-Elena — Security Analysis of LTE Access Network Computer Science Department Military Technical Academy Bucharest, ROMANIA ISBN:978-1-61208-113-7 2011

Paul Wismer — SMART PILL DISPENSER -A NEW TOOL FOR IMPROVING PATIENT ADHERENCE Balda Healthcare Germany 2016

Policy Department A: Economic and Scientific Policy — European Leadership in 5G European Parliament's Committee Brussels 2016

Qualcomm — accelerating-c-v2x-commercialization 2019

Rami URFALIOĞLU — 4. Nesil Mobil Haberleşmenin Standartlaşma Sürecinde Aday Teknolojiler LTE ve Mobil Wimax'in Karşılaştırılmalı Analizi, Türkiye için Geçiş Stratejisi Önelrileri Bilgi Teknolojileri ve İletişim Kurumu Ankara 2011

Research Scholar, Umesh Chandra, Assistant Professor Shagufta Praveen — Influence of Structured, Semi-Structured, Unstructured data on various data models IJSER 2017 2017

SAĞIROĞLU Şeref, ÇOLAK İlhami YAVANOĞLU Uraz — Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler 2012

SALEHI Seyedmohammad, ESMAILPOUR Amir SOLANKI Mayur — LTE Security: Encrytion Algorithm Enchancements Norwich University ASEE Northeast Section Conference 2013

Smriti Pande — Privacy and Security Challenges of RFID 2013 Proceedings of the Information Systems Educators Conference San Antonio, Texas, USA 2013

T.Uzm.Talat GÜÇLÜ — Teknoloji, Pazar ve Düzenleme Boyutuyla MOBİL TV 2008

T.Uzm.Yrd. Ramazan YILMAZ	Teknoloji, Pazar ve Düzenleme Boyutuyla MOBİL TV 2008
Tiago M. Fernández-Caramés and Paula Fraga-Lamas	Towards The Internet-of-Smart-Clothing: A Review on IoT Wearables and Garments for Creating Intelligent Connected E-Textiles Department Computer Engineering, Faculty of Computer Science, Universidade da Coruña Spain December 2018
Tülay URAN	Yeni Nesil Kablosuz Haberleşme Sistemleriiçin Spektrım Kullanımının Ücretlendirilmesi:Dünya Uygulamaları ve Türkiye'ye Yönelik Öneriler Bilgi Teknolojileri Ve İletim Kurumu Ankara 2011
UĞUR YALÇIN	4G Yeni Nesil LTE GSM Baz İstasyonu Anten Tasarımı Uludağ Universitesi Mühendislik-Mimarlık Fakültesi Dergisi Bursa 2010
Wang Wu Shaoen	Visible Light Communications for 5G Wireless Networking Systems: From Fixed to Mobile Communications IEEE Network December 2014
Waqas Muhammed Haus Michael	Security and Privacy in Device-to-Device (D2D) Communication : A review IEEE Communications Surveys, Tutoraials 2016
Yasir Javed1, 2, J. Abdullah, J.M.Nazim, N.Khan A.S.Khan1	Security issues in 5G device to device communication IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.5, May 2017 Riyadh 2017
ZOLANVARI Maede	SDN for 5G https://www.cse.wustl.edu/~jain/cse570-15/ftp/sdnfor5g.pdf 2015