
GAZİ ÜNİVERSİTESİ
Gazi
1926

5G AĞLARINDA GÜVENLİK SERVİSLERİ YÖNETİMİNİN ADLİ BİLİŞİM BAKIŞ AÇISIYLA İNCELENMESİ VE BİR ADLİ BİLİŞİM SİSTEMİ ÖNERİSİ

Altuğ ÇİL

DOKTORA TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

AĞUSTOS 2023

Altuğ ÇİL tarafından hazırlanan "5G AĞLARINDA GÜVENLİK SERVİSLERİ YÖNETİMİNİN ADLİ BİLİŞİM BAKIŞ AÇISIYLA İNCELENMESİ VE BİR ADLİ BİLİŞİM SİSTEMİ ÖNERİSİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Mehmet DEMİRCİ

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. ...……..……..

Başkan: Prof. Dr. Suat ÖZDEMİR

Yapay Zeka Mühendisliği Ana Bilim Dalı, Hacettepe Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. ……..……

Üye: Prof. Dr. Mustafa ALKAN

Elektrik-Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. ...…….……...

Üye: Prof. Dr. Ali KARA

Elektrik-Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. ...……

Üye: Doç. Dr. Pelin ANGIN

Bilgisayar Mühendisliği Ana Bilim Dalı, Orta Doğu Teknik Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum. ...……

Tez Savunma Tarihi: 03/08/2023

Jüri tarafından kabul edilen bu tezin Doktora Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Altuğ ÇİL
03/08/2023

5G AĞLARINDA GÜVENLİK SERVİSLERİ YÖNETİMİNİN ADLİ BİLİŞİM BAKIŞ AÇISIYLA İNCELENMESİ VE BİR ADLİ BİLİŞİM SİSTEMİ ÖNERİSİ

(Doktora Tezi)

Altuğ ÇİL

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ağustos 2023

ÖZET

İnternet erişimi olan cihazların düşük gecikme, yüksek hız ve bant genişliği gibi gereksinimlerinin karşılanabilmesi yeni nesil haberleşme teknolojisi olan 5G ile mümkün olacaktır. Akıllı sağlık, akıllı şehir, insansız hava araçları yönetimi gibi uygulamalarda da kullanılan 5G teknolojisi anten ve frekans yapılarındaki yeniliklerle yüksek sayılarda bağlantıyı destekleyebilecek bir kablosuz haberleşme mimarisi ve ağ yapısı üzerine tasarlanmıştır. 5G ağlarındaki karmaşık yapının yönetimi, hız ve gecikme gibi gereksinimlerin karşılanabilmesi yazılım tanımlı ağların (Software-Defined Network, SDN) kullanımıyla mümkündür. Ağ adli bilişimi kapsamında mevzuata uyumlu standart bir sürecin bulunmaması çalışmaların zor olmasına sebep olmakta ve güvenilirliğini azaltmaktadır. Artan internet kullanımının 5G ağlarında güvenlik ve adli bilişim süreçlerini mevcut duruma göre daha zor kılacağı düşünülmektedir. Bu tezde mevzuata ve uluslararası standartlara uyumlu bir ağ adli bilişim süreci ve SDN tabanlı 5G ağlarına uyumlu bir ağ adli bilişim sistemi geliştirilmesi amaçlanmaktadır. 5G ve SDN alanında yapılan adli bilişim çalışmaları yetersiz olduğundan tezde öncelikle teknik durumun tespitinin gerçekleştirilmesi amacıyla güvenlik olaylarına karşı farklı kontrolcülerin adli bilişim yetenekleri deneylerle incelenmiştir. Farklı kontrolcü kullanımlarında adli bilişim açısından farklı sonuçlar alındığından standart bir sürecin gerekliliği ispatlanmıştır. Ardından mevzuat ve uluslararası uygulamalar ağ adli bilişimi odağında incelenerek literatürde ilk defa mevzuat uyumlu bir ağ adli bilişim süreci oluşturulmuştur. Ardından bu sürecin otomatik işlemesi için bir ağ adli bilişim sistemi geliştirilmiştir. Gerçek internet erişim verisi kullanılarak test edilen sistemin mevzuatta belirlenen kayıt gereksinimlerini, akan trafiğin sadece %0,87'si boyutundaki bir dosya ile kayıt altına alabildiği görülmüştür. Sistem kayıtların özetleme, şifreleme, elektronik imzalama, yedekleme ve süresi dolan kayıtları yok etme işlemlerini de başarıyla gerçekleştirmektedir. Sistem ayrıca zararlı hedefleri engelleme, saldırılara karşı uyarı üretme ve uluslararası veri sızıntılarını tespit etme yeteneklerine de sahiptir. Geliştirilen sistem SDN tabanlı 5G ağlarında adli bilişim hazırlık düzeyini artırmakta, kişisel verilerin korunmasına katkı sağlamakta, cezai yaptırımların önüne geçmekte, sistem güvenliğini artırmakta ve sınır ötesi adli bilişim çalışmalarına imkân tanımaktadır.

Bilim Kodu : 92401
Anahtar Kelimeler : 5G, yazılım tanımlı ağlar, adli bilişim, siber güvenlik
Sayfa Adedi : 151
Danışman : Doç. Dr. Mehmet DEMİRCİ

INVESTIGATION OF SECURITY SERVICES MANAGEMENT IN 5G NETWORKS FROM THE PERSPECTIVE OF FORENSIC INFORMATION AND A PROPOSAL FOR A FORENSIC SYSTEM

(Ph. D. Thesis)

Altuğ ÇİL

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

August 2023

ABSTRACT

Meeting the needs of devices with internet access such as low latency, high speed and bandwidth will be possible with 5G, which is a new generation communication technology. 5G technology, which is also used in applications such as smart health, smart city, and unmanned aerial vehicle management, is designed on a wireless communication architecture and network structure that can support high numbers of connections with innovations in antenna and frequency structures. The management of the complex structure in 5G networks and meeting the requirements such as speed and delay are possible with the use of software-defined networks (SDN). The absence of a standard process in compliance with the legislation within the scope of network forensics makes the studies difficult and reduces its reliability. It is thought that increasing internet usage will make security and forensic processes in 5G networks more difficult than the current situation. In this thesis, it is aimed to develop a network forensics process in compliance with the legislation and international standards and a network forensics system compatible with SDN-based 5G networks. Since the forensic studies in the field of 5G and SDN are insufficient, the forensic capabilities of different controllers against security incidents were examined with experiments in order to determine the technical situation in the thesis. Since different results are obtained in terms of forensic computing in different controller usage, the necessity of a standard process has been proven. Afterwards, legislation and international applications were examined with the focus of network forensics, and for the first time in the literature, a network forensic process compatible with the legislation was created. A network forensics system was then developed to automate this process. The system was able to record the log requirements determined in the legislation with a file size of only 0.87% of the flowing real internet traffic. The system also successfully performs the hashing, encryption, electronic signature, back-up and wiping of expired records. The system also has the capabilities to block malicious targets, generate alerts for attacks, and detect international data leaks. The developed system improves the forensic readiness in SDN-based 5G networks, contributes to the protection of personal data, prevents criminal sanctions, and enables cross-border forensic studies.

Science Code : 92401
Key Words : 5G, software-defined networking, digital forensics, cyber security
Page Number : 151
Supervisor : Assoc. Prof. Mehmet DEMİRCİ

TEŞEKKÜR

Tez çalışmam boyunca kıymetli görüşlerini esirgemeyerek bana yol gösteren tez danışmanım Doç. Dr. Mehmet DEMİRCİ'ye en içten teşekkürlerimi sunarım. Tez izleme komitesinde yer alarak çalışmalarıma değerli bilgileriyle katkı sağlayan Prof. Dr. Sevil ŞEN AKAGÜNDÜZ'e, Prof. Dr. Mustafa ALKAN'a ve Prof. Dr. Suat ÖZDEMİR'e teşekkürlerimi sunarım.

Akademik izin süreciyle doktora hayatımı kolaylaştıran çalıştığım kurumum TÜBİTAK'a teşekkür ederim. Tez süreci boyunca desteklerini benden esirgemeyen Alperen Zekeriya KARATAŞ'a teşekkür ederim. Bilimsel bakış açısıyla beni aydınlatan Beyin ve Sinir Cerrahisi Uzmanı Doç. Dr. İsmail BOZKURT'a teşekkürlerimi sunarım.

Elimden tutarak ilkokula götürdükleri günlerden beri desteğini ve duasını benden esirgemeyen annem Birsen ÇİL'e, babam Recep ÇİL'e ve ablam Ahu ÇİL'e sonsuz teşekkürlerimi sunarım.

Çalışmalarım süresince desteğini benden hiç esirgemeyen, her zaman motivasyon sağlayarak tezi bitirmeme büyük katkı sunan sevgili eşim Büşra BOZKURT ÇİL'e çok teşekkür ederim.

Doktora serüvenimden sadece bir yaş daha büyük olan, varlığı en büyük şükür sebebim olan canım kızım Sare ÇİL. Bu tezi birlikte geçirebileceğimiz vakitlerden eksilterek bitirdim. Sabrın için çok teşekkür ederim güzel kızım.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ x

ŞEKİLLERİN LİSTESİ xi

RESİMLERİN LİSTESİ xii

SİMGELER VE KISALTMALAR xiii

1. GİRİŞ 1

2. 5G AĞLARI VE GÜVENLİK YAPISI 13

2.1. 5G Ağ Mimarisi 13

2.2. 5G Ağlarında Güvenlik 17

2.3. Yazılım Tanımlı Ağ (SDN) Mimarisi ve Avantajları 21

2.4. SDN Kullanım Alanları 23

2.5. SDN Güvenliği 24

3. 5G AĞLARINDA ADLİ BİLİŞİM 29

3.1. Ağ Adli Bilişimi 29

3.2. 5G Ağlarında Adli Bilişim Çalışmaları 31

3.3. SDN Ortamlarında Adli Bilişim 33

3.4. İdari ve Hukuki Çalışmalar 38

3.5. Tez Çalışmasının Literatürle Karşılaştırılması 39

4. SDN KONTROLCÜLERİNİN ADLİ BİLİŞİM SÜREÇLERİNE ETKİSİNİN İNCELENMESİ 45

4.1. Adli Bilişim Deneyleri 46

4.1.1. Altyapı bilgileri ve genel yöntem 47
4.1.2. ICMP paketleri iletimi 48
4.1.3. Mesajlaşma içeriği elde etme 51
4.1.4. Port tarama 52
4.1.5. Web sunucu taraması 54
4.1.6. Hizmet engelleme saldırıları 55
4.2. Bölüm Değerlendirmesi 58
5. MEVZUAT VE ULUSLARARASI UYGULAMALARA UYUMLU AĞ ADLİ BİLİŞİM SÜRECİ GELİŞTİRİLMESİ 63
5.1. Ağ Adli Bilişimi Odağında Mevzuat İncelemesi 63
5.1.1. 5651 sayılı kanun ve ilgili yönetmelikler 64
5.1.2. 5070 sayılı elektronik imza kanunu 73
5.1.3. 5237 sayılı Türk ceza kanunu 74
5.1.4. 5271 sayılı ceza muhakemeleri kanunu 74
5.2. ISO 27001 Standardı 75
5.3. Bilgi ve İletişim Güvenliği Rehberi 77
5.4. SDN Tabanlı 5G Ağlarında Adli Bilişimin İdari Açıdan İncelemesi 83
5.5. Ağ Adli Bilişiminde Uluslararası Durum Tespiti 84
5.6. SDN Adli Bilişiminde Delil Kaynakları ve Bilirkişilik 86
5.7. Mevzuat ve Uluslararası Uygulamalara Uyumlu Ağ Adli Bilişim Sürecinin İdari ve Teknik Gereksinimleri 89
5.8. Bölüm Değerlendirmesi 91
6. SDN TABANLI 5G AĞLARINA UYUMLU ADLİ BİLİŞİM SİSTEMİ 93
6.1. Sistemin Tasarlanması 94
6.1.1. Logların elde edilmesi 94
6.1.2. Özetleme 97
6.1.3. Şifreleme 97

6.1.4. Elektronik imza 98
6.1.5. Yedekleme 99
6.1.6. Verilerin yok edilmesi 99
6.1.7. URL filtreleme – trafik engelleme 100
6.1.8. Uluslararası veri sızıntısı tespiti 101
6.1.9. Eşik tabanlı uyarı sistemi 102
6.1.10. Sistemin otomatizasyonu 103
6.2. Deneysel Çalışmalar 103
6.2.1. Altyapı bilgileri 105
6.2.2. Deney süreçleri 105
6.2.3. Deney sonuçları 107
6.3. Bölüm Değerlendirmesi 112
7. TARTIŞMA 117
7.1. İdari Açıdan Tartışma 117
7.2. Teknik Açıdan Tartışma 120
7.3. Adli Bilişim ve Delil Elde Edilmesi Açılarından Tartışma 123
8. SONUÇ VE ÖNERİLER 127
8.1. Sonuçlar ve Değerlendirme 127
8.2. Karşılaşılan Zorluklar 131
8.3. Gelecek Çalışma Önerileri 131
KAYNAKLAR 135
ÖZGEÇMİŞ 151

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 4.1. ICMP paketleri iletimi adli bilişim deneyleri paket sayısı ve yüzdesi bilgileri 50

Çizelge 4.2. Mesajlaşma içeriği elde etme deneyleri paket sayısı ve yüzdesi bilgileri . 52

Çizelge 4.3. Port tarama adli bilişim deneyleri paket sayısı ve yüzdesi bilgileri 53

Çizelge 4.4. Uygulanan testlerde güney arayüzünde ilgili adli bilişim tespit durumu .. 59

Çizelge 4.5. Uygulanan test ve atakların genel sonucu 61

Çizelge 6.1. Log elde edilmesi sözde kodu..... 96

Çizelge 6.2. Uluslararası veri sızıntısı tespit sistemi sözde kodu 101

Çizelge 6.3. Eşik tabanlı uyarı sistemi sözde kodu..... 102

Çizelge 6.4. Deney ortamı altyapısı..... 105

Çizelge 6.5. Log dosyaları ve trafik boyutları 109

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 2.1. SDN tabanlı 5G ağları 14

Şekil 2.2. Temel NFV mimarisi 16

Şekil 2.3. SDN mimarisi 22

Şekil 4.1. Deney ortamı 48

Şekil 4.2. ICMP paketleri iletimi adli bilişim deney süreci 49

Şekil 4.3. Mesajlaşma içeriği elde etme adli bilişim deney süreci 51

Şekil 4.4. Port tarama adli bilişim deney süreci 53

Şekil 4.5. Web sunucu adli bilişim deney süreci 54

Şekil 4.6. DoS saldırıları adli bilişim süreci 56

Şekil 4.7. Güney arayüzü paket sayısı yüzdeleri genel görünümü 60

Şekil 4.8. Güney arayüzü paket boyutu yüzdeleri genel görünümü 60

Şekil 6.1. Özetleme, şifreleme ve elektronik imza süreci ve katkıları 98

Şekil 6.2. DoD 5220.22-M yöntemi adımları 100

Şekil 6.3. Sistemin genel tasarımı 103

Şekil 6.4. Deney ortamı topolojisi 104

Şekil 6.5. Farklı dosya uzantılarının boyut kıyaslaması 110

Şekil 7.1. Sistemin OSCAR kriterleri açısından değerlendirmesi 123

Şekil 7.2. Delil kaynaklarının karşılaştırılması 125

RESİMLERİN LİSTESİ

Resim **Sayfa**

Resim 6.1. Saldırı esnasındaki bant genişliği (Mbps)..... 111

Resim 6.2. Saldırı ve akış/sn bilgileri 111

Resim 6.3. Bant genişliği eşiği tabanlı uyarı örneği 111

Resim 6.4. Akış/sn eşiği tabanlı uyarı örneği 112

Resim 6.5. Uluslararası veri sızıntısı tespit örneği 112

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
GB	Gigabyte
Gbps	Gigabits Per Second
Ghz	Gigahertz
MB	Megabyte
Mbps	Megabits Per Second
Mhz	Megahertz
ms	Milisaniye
ns	Nanosaniye
TB	Terabyte

Kısaltmalar	**Açıklamalar**
4G	Fourth Generation (Dördüncü Nesil)
5G	Fifth Generation (Beşinci Nesil)
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
API	Application Programming Interface (Uygulama Programlama Arayüzü)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
BPDU	Bridge Protocol Data Unit (Köprü Protokolü Veri Birimleri)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CBC	Cipher Block Chaining (Şifre Blok Zincirleme)
CBDDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

CDP	Cisco Discovery Protocol (Cisco Keşif Protokolü)
CMK	Ceza Muhakemeleri Kanunu
CPU	Central Processing Unit (Merkezi İşlem Birimi)
D2D	Device to Device (Cihazdan cihaza)
DDoS	Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DHCP	Dynamic Host Configuration Protocol (Dinamik İstemci Yapılandırma Protokolü)
DNS	Domain Name System (Alan Adı Sistemi)
DoS	Denial of Service (Hizmet Engelleme)
EECC	European Electronic Communications Code (Avrupa Elektronik İletişim Kodu)
ENFSI	The European Network of Forensic Science Institutes (Avrupa Adli Bilim Enstitüleri Ağı)
ENISA	The European Union Agency for Cybersecurity (Avrupa Siber Güvenlik Ajansı)
GDPR	General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)
HTTP	Hyper Text Transfer Protokol (Hiper Metin Transfer Protokolü)
ICMP	Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)
IDS	Intrusion Detection System (Saldırı Tespit Sistemi)
IETF	Internet Engineering Task Force (İnternet Mühendisliği Görev Gücü)
IMEI	International Mobile Equipment Identity (Uluslararası Mobil Cihaz Kodu)
IMSI	International Mobile Subscriber Identity (Uluslararası Mobil Abone Kimliği)
IoT	Internet of Things (Nesnelerin İnterneti)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention System (Saldırı Önleme Sistemi)
ISO	International Organization for Standardization (Uluslararası Standardizasyon Teşkilatı)
İSS	İnternet Servis Sağlayıcı
LAN	Local Area Network (Yerel Alan Ağı)
LI	Lawful Interception (Kanuni Müdahale)

LLDP	Link Layer Discovery Protocol (Bağlantı Katmanı Keşif Protokolü)
MAC	Media Access Control (Ortam Erişim Kontrolü)
MANO	Management and Orchestration (Yönetim ve Düzenleme)
MD5	Message Digest Algorithm 5 (Mesaj Özetleme Algoritması 5)
MIMO	Multiple-input / Multiple-output (Çoklu Giriş / Çoklu Çıkış)
mmWave	Milimeter Wave (Milimetre Dalga)
MSISDN	Mobile Station International Subscriber Directory Number (Mobil İstasyon Uluslararası Abonelik Dizin Numarası)
NAS	Non-Access Stratum (Erişimsiz Katman)
NAT	Network Address Translation (Ağ Adresi Dönüştürme)
NFV	Network Functions Virtualization (Ağ Fonksiyonları Sanallaştırma)
NSH	Network Service Header (Ağ Servis Başlığı)
NIST	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
NTP	Network Time Protocol (Ağ Zaman Protokolü)
QoE	Quality of Experience (Deneyim Kalitesi)
QoS	Quality of Service (Servis Kalitesi)
RAM	Random Access Memory (Rastgele Erişimli Bellek)
RAN	Radio Access Network (Radyo Erişim Ağı)
RRM	Radio Resource Management (Radyo Kaynak Yönetimi)
RRU	Remote Radio Unit (Uzak Radyo Ünitesi)
RTT	Round Trip Time (Gidiş Geliş Süresi)
SDN	Software-Defined Network (Yazılım Tanımlı Ağ)
SFC	Service Function Chain (Servis Fonksiyon Zinciri)
SFF	Service Function Forwarder (Servis Fonksiyonu İletici)
SHA	Secure Hash Algorithm (Güvenli Özetleme Algoritması)

SIC	Successive Interference Cancellation (Ardışık Girişim İptali)
SIEM	Security Information and Event Management (Güvenlik Bilgi ve Olay Yönetimi)
SOC	Security Operation Center (Güvenlik Operasyon Merkezi)
SSD	Solid State Drive (Katı Hal Sürücüsü)
SSL	Secure Sockets Layer (Güvenli Soket Katmanı)
STP	Spanning Tree Protocol (Yayılan Ağaç Protokolü)
TCK	Türk Ceza Kanunu
TCP	Transmission Control Protocol (Geçiş Kontrol Protokolü)
TLS	Transport Layer Security (Taşıma Katmanı Güvenliği)
UDN	Ultra-Dense Networking (Ultra Yoğun Ağ)
UDP	User Datagram Protocol (Kullanıcı Veri Bloğu İletişim kuralları)
URL	Uniform Resource Locator (Tekdüzen Kaynak Konumlayıcı)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VPN	Virtual Private Network (Sanal Özel Ağ)
VNF	Virtual Network Function (Sanal Ağ Fonksiyonu)
VNSF	Virtual Network Security Function (Sanal Ağ Güvenliği Fonksiyonu)

1. GİRİŞ

Gelişen teknoloji sonucunda mevcut mobil ağ altyapıları ihtiyaçları karşılayamaz hale geldiğinden dolayı yeni nesil bir haberleşme teknolojisi olarak 5G kullanıma sunulmuştur. 5G teknolojisine geçişin temel amacı kullanıma sunulan her teknolojik nesneye yüksek kabiliyette iletişim yeteneği kazandırmasıdır. Haberleşmeyi insandan insana, makineden insana ve insandan makineye olarak gerçekleştirecek altyapı da 5G sayesinde mümkün kılınacaktır. 5G sistemlerinin 10 Gbps (Gigabits Per Second) seviyesinde hız ve 1 ms (Milisaniye) altında gecikme ile hizmet vermesi hedeflenmektedir. 100 milyarı aşan sayılarda düşük hızlarda bağlantıyı destekleme yeteneği de 5G ile gelmektedir. Yeni nesil enerji yönetim süreçleri, akıllı sağlık ve akıllı ulaşım sistemleri, insansız hava araçları yönetimi, artırılmış ve sanal gerçeklik, endüstri 4.0 gibi alanlarda 5G uygulamaları mevcuttur. 5G'yi günlük yaşantımızın içerisine sokmak için gerekli olan araştırma alanlarının başında kablosuz haberleşme gelir. Frekans tahsisi, milimetre dalga (Milimeter Wave, mmWave), anten teknolojileri gibi kablosuz haberleşme alanlarının yanı sıra yazılım tanımlı ağlar (Software-Defined Network, SDN), ağ fonksiyonları sanallaştırma (Network Functions Virtualization, NFV) ve yapay zeka teknolojileri de 5G'nin gerçek hayata uygulanabilir olması için gerekli diğer alanlardır. Tüm bu teknolojilerin birlikte uygulanmasıyla 5G ağları için beklenen verimlilik, yüksek düzeyde kapsama ve hizmet kalitesi (Quality of Service, QoS) gibi gereksinimler sağlanmış olacaktır [1].

Yaklaşık 40 yıl öncesine dayanan mobil haberleşme serüvenin en büyük gelişim noktası olarak nitelendirilebilecek 5G teknolojisinin 2022 yılında 107 milyar ABD (Amerika Birleşik Devletleri) doları olan pazarının, 2027 yılında küresel boyutta yaklaşık 331 milyar ABD dolarına ulaşması beklenmektedir [2]. 2018 yılında ABD'de kullanımının ardından Güney Kore de 5G ağını kurmayı başarmış olup, Güney Kore'nin ardından Asya ülkelerinde de hızlı bir şekilde 5G hizmeti sunulmaya başlanmıştır. Kullanım oranları günden güne artan 5G teknolojisinin 2027 yılında yaklaşık 4,5 milyar aboneye sahip olması beklenmektedir. 2027 yılında Avrupa'daki mobil aboneliklerin %85'inin de 5G türünde olması beklenmektedir. Ülkemizde 5G frekans ihalesinin 2023 yılı içerisinde gerçekleştirilmesi beklenmektedir [3].

5G'nin getireceği bu yenilikler mobil ağ, baz istasyonu yapısı ve çekirdek ağ tarafında büyük değişiklikler gerektirmektedir. Frekans kullanımı 5G'ye geçişle teknik anlamda büyük değişikliklere uğramış olup, bu frekansların tahsisi hususu 5G operatörleri için büyük bir rekabet oluşturmaktadır. ABD'de Verizon şirketi 1,8 milyar dolara 180 Mhz (Megahertz) genişliğindeki frekansı satın aldıktan sonra 39 Ghz'de (Gigahertz) ve 28 Ghz'de lisansları da alarak bütün ülkeyi kapsama altına alabilmiştir. 5G erişimi sağlayacak olan operatörlerin frekans ihtiyaçlarını karşılamalarından öte baz istasyonu tekniklerini de düşünmeleri ve küçük hücre yönetimi, sabit kablosuz erişim ve yeşil iletişim gibi hususları da göz önünde bulundurmaları gerekir [1]. Ancak en önemli hususlardan birisi de 5G ağ altyapısının kurulabilmesi için SDN ve NFV tabanlı sistemlerin geliştirilmesi ve uygulamaya alınmasıdır. Çok sayıda kullanıcı ve nesnelerin interneti (Internet of Things, IoT) cihazı içerecek olan 5G ağlarının ağ yönetimi için SDN kullanımı zorunluluk içermektedir. 5G çekirdek ağlarının güvenlik mimarisi de SDN üzerine kurgulanmaktadır. SDN'in değiştirilebilir mimarisi sayesinde güvenlik politikaları, kimlik doğrulama, şifreleme gibi güvenlik servisleri 5G ağlarına uygulanabilir [4].

5G ağlarında güvenlik servisleri yönetimi ve adli bilişim süreçleri için SDN odağında çalışmalar yapılması gerekmektedir. Cep telefonu, bilgisayar, tablet vb. akıllı cihazların kullanımının artmasıyla birlikte bireysel internet kullanımı da artmıştır. 2012 yılında kişisel internet kullanımı %47,4 iken, bu oran 2022 yılında %85'e yükselmiştir. İnternet erişimine sahip olan evlerin oranı ise 2022 yılında %94,1 olup haftada bir ve daha fazla internet kullanan kişilerin oranı %82,7'dir [5].

İnternet kullanımının artması sonucunda, gerçekleşen siber suç sayıları ve çeşitlerinde artışlar gerçekleşmiştir. Şirketlerin %86'sı yıl içerisinde en az bir defa siber saldırıya uğramıştır [6]. Bu doğrultuda siber suçların engellenmesi ve aydınlatılmasının taşıdığı önem de günden güne artmaktadır [7]. Dijital ortamın çoğu parçasının işlenen bir suçun parçasına dönüşebileceği günümüz teknolojisinde, siber suçların bir alt başlığını da internet ve ağ teknolojileri üzerinden işlenen suçlar oluşturmaktadır. Bu durum ağ adli bilişiminin önemini de artırmaktadır.

Adli bilişim, günlük iletişime dair bilgi elde edilmesinin yanı sıra saldırılar açısından da büyük önem arz etmekte ve güvenlik cihazlarına gerekli verileri canlı olarak sağlamakla kalmayıp saldırı sonrasında adli inceleme yapan uzmanlara bilgi beslemesi yapmaktadır. Ağ

adli bilişimi çalışmalarının merkeziyetçi, tutarlı, düşük paket boyutlu, hızlı ve güvenli bir erişime sahip olması adli bilişimin vazgeçilmez unsurlarındandır.

Geçmişte yaşanan bir siber suçun aydınlatılması adli bilişimin ana amaçları arasında yer alsa da adli bilişim sürecinin uygulanması için bir suçun olması zorunlu değildir. Sıradan bir durumun aydınlatılabilmesine dair süreçler de adli bilişim araştırmalarının kapsamına girer. Erişim kayıtlarının eksiksiz ve uygun biçimde tutuluyor olması adli bilişimin en önemli aşamalarındandır. Kayıtların saklanması ve yorumlanması aşamalarının mevzuat ile uyumlu olması zorunludur. Aksi durumda adli bilişim çalışmalarının güvenliği ve geçerliliği olmayacaktır.

Geleneksel ağ yaklaşımları ağ cihazlarının otomatik olmayan yöntemlerle ayarlanması üzerine, hantal ve hataya açık bir yapıdadır. Ayrıca geleneksel ağlarda fiziksel ağ altyapısının da tamamen efektif bir şekilde kullanımı mümkün olmamaktadır. Geleneksel ağlar gelişen teknolojinin taleplerini karşılayamaz hale gelmiştir. Yazılım Tanımlı Ağlar (Software-Defined Network, SDN) ise ağın etkin yönetimi açısından geleneksel ağlara göre daha kolay yönetilebilir bir teknolojidir [8].

Gelişen ağ teknolojileri sayesinde geleneksel ağların yerine SDN'in kullanım oranı artmaktadır. 2020 yılından 2025 yılına kadar geçen 5 yıllık süre zarfında SDN pazarının dünya genelinde 13,7 milyar ABD dolarından 32,7 milyar ABD dolarına çıkması beklenmektedir [9].

Geleneksel ağlara göre daha esnek ve kolay yönetim sağlayan [10] SDN'in kullanımının artması [9] sonucunda, SDN ortamlarında da güvenlik ve adli bilişim çalışmalarının hız kazanması zorunlu hale gelmiştir. Üç farklı katmandan ve bu katmanlar arasındaki haberleşmeyi sağlayan iki arayüzden oluşan [8] SDN mimarisi sayesinde, ağ haberleşmesi, güvenliği ve izlenmesi daha kolay yönetilebilir ve geliştirilebilir süreçler haline gelmiştir [11–15].

Geleneksel ağlarda mevcut olan saldırı türleri SDN için geçerliliğini korurken, ek olarak SDN özelinde yeni saldırı ve güvenlik yöntemleri de mevcuttur. Adres çözümleme protokolü (Address Resolution Protocol, ARP) zehirlemesi, bağlantı katmanı keşif protokolü (Link Layer Discovery Protocol, LLDP) paketleri sahtekârlığı, anahtar ve kontrolcü arasındaki

trafiğin dinlenebilmesi, alan adı sistemi (Domain Name System, DNS) yükseltme atakları gibi yöntemlerle servis dışı bırakma ve bilgi ele geçirme saldırılarını SDN ortamlarında gerçekleştirilebilmek mümkün olsa da [16–20] SDN'in getirdiği yenilikler güvenlik ve adli bilişim açısından avantaj sağlayabilir [21]. Bu avantajın 5G ağlarında da kullanılacak olması daha kolay ve hızlı adli bilişim süreçlerinin uygulanabilir olmasını sağlayacağından kıymetlidir.

SDN ortamları için geleneksel ağ adli bilişiminin ötesinde yöntemlerin geliştirilmesi gereklidir [22]. SDN'de güvenlik boyutlu araştırmalar gerçekleştirilmiştir ancak adli bilişim odaklı araştırmalar yetersizdir [23]. Adli bilişim çalışmaları, saldırganın süreçlerini aydınlatmak amacıyla kim, ne zaman, neden, nasıl ve ne sorularına yanıt arar ve bu süreçlerde kullanılacak verilerin bulunabilir, ulaşılabilir, birlikte çalışabilir ve yeniden kullanılabilir olarak FAIR (Findability, Accessibility, Interoperability, and Reusability) ilkesine uyumlu olması beklenir [24–26].

Problem durumu / Konunun tanımı

4G ve daha önceki nesil mobil iletişim teknolojilerinde ana amaç insan odaklı iletişimin sağlanmasıyken bu durum 5G ve ötesi ağları daha geniş ölçekte hizmet sunmayı hedeflemektedir. 5G ağları çok düşük gecikme ve yüksek hız sağlanmasıyla, araçlar arası iletişimde, akıllı sağlık uygulamalarında ve nesnelerin interneti altyapısında kullanılabilecektir [27]. İnsandan bağımsız olarak işletilebilecek bu teknolojilerin 5G ile kullanılabilir olmasının arka planında hem kablosuz haberleşme altyapısında gerçekleşen yenilikler hem de çekirdek ağ tarafında gerçekleşen yenilikler bulunmaktadır. 5G ağlarındaki baz istasyonu yapısı 4G ağlarına göre çok daha yüksek sayıda bağlantıyı destekleyecek bir tasarımdadır. 5G'nin çekirdek ağ tarafında ise SDN ve NFV uygulamalarının kullanılması bir seçenekten ziyade ağ yönetiminin gerçekleşmesi açısından zorunluluk olarak değerlendirilmektedir [28]. Ağ fonksiyonlarının sanal olarak sunulması ve farklı ağ gereksinimlerine özel ağ dilimleme uygulamalarının geliştirilmesi hususu da 5G'yi önceki nesil mobil iletişim ağlarından ayıran bir yapıya sahiptir. 4G ve öncesi ağlar özelinde gerçekleştirilen çalışmalar mobil ağ kullanıcısının konumunu ve temel kullanıcı bilgilerini bulmaya yönelik olup, önceki nesil ağlar için gerçekleştirilen az sayıdaki adli bilişim çözümleri, 5G ve ötesi ağların karmaşık ve yenilikçi yapısına uygulanabilir değildir [27, 29]. Yüksek sayıda ve farklı türde kullanıcıların bulunduğu büyük bir ağ yapısında adli

bilişim çalışması gerçekleştirmek teknik ve idari açıdan bir problem olarak görülmekte olup, artan siber suçlar ve internet erişimleri de dikkate alındığında 5G ağlarında adli bilişim süreçlerinin gerçekleştirilmesi üzerine bir süreç ve sistem geliştirilmesi bu tezin motivasyonunu oluşturmaktadır.

Adli bilişimin alt alanları, bilgisayar, ağ ve gömülü sistemler olarak farklı başlıklarda değerlendirilebilir. Siber suçları aydınlatmak amacıyla gerçekleştirilecek bu adli bilişim çalışmalarının idari ve adli süreçlerde geçerli ve güvenilir olması için mevzuatla uyumlu olması bir zorunluluktur. Teknik, idari ve adli açılardan ele alınması gereken adli bilişim süreçleri için yol haritalarının siber güvenlik ihlallerinden önce hazırlanması gerekmektedir ve bu durum son derece kritiktir. Ülkeler ve üye oldukları kuruluşlar çeşitli dokümanlarla siber güvenlik stratejilerini oluşturmayı hedeflerken aynı zamanda adli bilişim politikalarını da oluşturmaktadırlar [30–32]. Ülkesel anlamda farklılıklar gösteren mevzuatlar bulunmakta olup adli bilişim hazırlığının sağlanması amacıyla, bazı ülkeler özelindeki adli bilişim süreçlerini idari açılardan ele alan çalışmalar gerçekleştirilmiştir [33–41]. Siber suçlara yönelik cezalar, adli bilişimde hangi hukuk normlarının ele alınacağı, kolluk kuvvetlerinin görevleri, ülkelerin teknik hazırlıkları ve devlet yapılaşması açısından durum tespiti, dijital delil elde etme süreçleri gibi konular ele alındığında üretici şirketlerin de dâhil olduğu sınır ötesi çalışmaların gerekli olduğu görülmektedir [42–45].

Ağ adli bilişim çalışmaları hem idari hem de teknik bakış açısı gerektirdiğinden dolayı ileri düzey bilgi sahibi olunmasını gerektirir. İçerdiği detay bilgiler ve hızlı teknolojik gelişim göz önüne alındığında, ağ adli bilişim çalışmalarının önceden belirlenmiş standart bir süreç kapsamında yönetilmesi gerekir. Bugüne kadar gerçekleştirilen çalışmalar incelendiğinde delil elde edilmesi, siber güvenlik ve adli bilişim seviyelerinin belirlenmesi, bilişim suçları kapsamında değerlendirmeler, adli bilişim program analizleri gibi araştırmaların geleneksel ağlar odağında olduğu görülmektedir [25, 46–52]. 5G ağlarının çekirdek ağ yönetimi SDN ile gerçekleştirilmekte olsa da, mevcut çalışmalarda SDN tabanlı 5G ağlarında adli bilişim özelinde değerlendirme ve iyileştirmeler bulunmamaktadır. 5G ağları için yapılan adli bilişim çalışmaları yok denecek kadar azdır ve dar bir kapsamdadır.

Adli bilişim üzerine idari ve teknik boyutlardan farklı araştırmalar var olsa da [53–55], ağ adli bilişim gereksinimlerini ülke mevzuatı ve uluslararası uygulamalar çerçevesinde ele alan ağ adli bilişim süreci oluşturma araştırmaları eksiktir. Süreç oluşturulmasının da

ötesinde ağ adli bilişim çalışmalarının hangi mevzuat ve uygulamalara dayandığı bilgilerini tek bir referans kaynak olarak içeren bir çalışma da bulunmamaktadır. Mevzuat, geleneksel ağ süreçlerine göre kurgulanmış olup SDN tabanlı 5G ağları ortamlarının mevzuata uyum sağlayıp sağlayamayacağı hususunda da çalışmalar mevcut değildir. Ağ adli bilişimine dair farklı kaynak ve rehberlerde bulunan bu bilgilerle adli bilişim süreçlerinin sağlıklı ve kolay bir şekilde gerçekleştirilmesi de mümkün olmamaktadır.

Tüm bu değerlendirmeler kapsamında bir ağ adli bilişim sürecinin ilgili mevzuat [56–65], uluslararası çalışmalar ve standartlar [66] da ele alınarak oluşturulmasının elzem olduğu değerlendirilmiştir. Geleneksel ağ adli bilişimi için tasarlanan süreçlerin SDN için geçerli olup olmadığı ve SDN tabanlı 5G ağlarında mevzuata uygun adli bilişim gerçekleştirilip gerçekleştirilemeyeceğinin bilinmemesi de ayrı bir problemdir. Otomatik olmayan bir adli bilişim süreci, sorumluları adli ve idari yaptırımlarla karşı karşıya bırakacaktır. Bu sebepten uluslararası çalışmaları da temel alarak oluşturulacak bir ağ adli bilişim sürecinin ötesinde oluşturulan sürecin otomatik ve mevzuata uygun şekilde işletileceği bir adli bilişim sisteminin bulunmaması da bu tezde belirlenen ana problemler arasında yer almaktadır.

Tezin amacı ve kapsamı

Tezin ana amacı, mevzuatta yer alan idari ve adli süreçlere uygun ve SDN tabanlı 5G ağlarıyla da uyumlu bir adli bilişim sistemi geliştirmektir. Literatürde bir ilk özelliği taşıyan bu sistemin bir adli bilişim sürecine uygun çalışması gerekmektedir. SDN ortamlarının güvenlik ve rutin iletişim bakış açıları kapsamında incelenmesine dair detaylı bilgilerin literatürde olmadığı ve kapsamlı adli bilişim çalışmalarının gerçekleştirilmediği görülmüştür. Bu sebepten, bir ağ adli bilişimi süreci ve sistemi oluşturmak için öncelikle SDN tabanlı 5G ağ ortamlarında adli bilişim durumunun tespit edilmesi hedeflenmiştir.

5G ve SDN ortamlarında bugüne kadar gerçekleşen güvenlik ve adli bilişim çalışmalarının, saldırı hazırlığı ve siber saldırı senaryolarını da içeren genel bir bakış açısında olmadığı görülmüştür. SDN kontrolcülerinin adli bilişim açısından durum tespitinin yapılmadığı ve delil elde etme üzerine yeterli çalışmanın gerçekleştirilmediği görülmüştür. Standart bir ağ adli bilişim süreci oluşturmak için mevcut durumun teknik tespitinin elzem olduğu değerlendirilmiştir. Bu sebepten farklı SDN kontrolcülerinin çalıştığı deney ortamlarında güney arayüzü ve sanal anahtarlarda biriken paketlere odaklanılarak, farklı test ve saldırı

araçlarıyla deneyler gerçekleştirilmiştir. Bu deneylerde, yaygın olarak kullanılan dört farklı kontrolcünün aynı topoloji ve altyapıda çalışan adli bilişim bakış açısıyla incelenmesi hedeflenmiştir. Aynı deney ortamında farklı kontrolcülerin kullanımı sonucunda SDN ortamının farklı katmanlarından elde edilen bilgilerin adli bilişim açısından yeterli olup olmadığının tespitinin gerçekleşmesi amaçlanmıştır. Adli bilişim açısından en başarılı SDN kontrolcüsünün seçiminin mümkün olup olmadığı ve güney arayüzü verilerinin adli bilişim açısından yeterli olup olmadığının tespiti de hedefler arasındadır.

Deneyler sonucunda, kontrolcülerin değişmesiyle hem güney arayüzünde hem de anahtarlar üzerinde farklı türde, boyutta ve özelliklerde paketler oluştuğu gözlemlenmiştir. Güney arayüzü verilerinin bazı testlerde yeterli bilgiyi sağlamasına karşın bazı süreçlerde eksik bilgi sağladığı görülmüştür. Bu durum kontrolcüden bağımsız, veri eksikliği sağlamayacak teknik bir ağ adli bilişim sürecinin gerekli olduğunu ortaya koymuştur.

Gereksinimin ortaya konulmasının ardından, literatürde bir rehber niteliği taşıyacak ve adli bilişim sistemine temel oluşturacak bir süreç tasarımı oluşturulması amaçlanmıştır. Bu sürecin oluşturulması için mevzuatın, uluslararası çalışmaların ve standartların ağ adli bilişimi açısından incelenmesi ve mevcut olan tüm gereksinimlerin tespit edilmesi amaçlanmıştır. Belirlenen gereksinimlerin SDN ve 5G yetenekleriyle gerçekleştirilip gerçekleştirilemeyeceği deneyler vasıtasıyla test edilmiş, olup delil kaynağı olabilecek veriler tespit edilmiştir. Bu çalışmaların sonunda SDN'in geleneksel ağlar için geliştirilmiş olan gereksinimleri yerine getirebileceği görülmüş ve mevzuat uyumlu bir ağ adli bilişim süreci oluşturulmuştur.

Ağ adli bilişim sürecinin oluşturulmasının ardından, tezin ana hedefi olan adli bilişim sisteminin geliştirilmesi aşamasına geçilmiştir. Bu aşamada SDN ortamındaki kayıtların elde edilmesinden yok edilmesine kadar olan süreçte yasal mevzuata otomatik uyum sağlayan, güvenli ve otomatik şekilde çalışan bir sistem geliştirilmesi hedeflenmiştir. Tez kapsamında geliştirilen ağ adli bilişim sürecinde belirlenmiş olan, SDN ortamındaki internet erişimlerinin mevzuat kapsamındaki gereksinimler gözetilip filtrelenerek kayıt altına alınması sistemin hedefleri arasındadır. Bunun ötesinde süreç kapsamında belirlenen diğer gereksinimler olan; yasaklı erişimlerin SDN yetenekleriyle engellenebilmesi, log dosyalarının özetleme, şifreleme, imzalama işlemlerinin gerçekleştirilmesinin ardından yedekli bir yapıda muhafaza edilmesi, saklanan log dosyalarının mevzuatta belirtilen sürenin

sonunda otomatik olarak geri döndürülemez şekilde silinmesi, uluslararası veri sızıntılarının tespiti, saldırılara karşı güvenliği artıracak sistemlerin sisteme entegre edilmesi de amaçlanmıştır.

Bu doğrultuda tezin ana amaçları özetle aşağıdaki şekilde sıralanabilir:

- SDN tabanlı 5G ağlarında adli bilişim durum tespitinin farklı SDN kontrolcüleri kullanılarak gerçekleştirilmesi,
- Mevzuata ve uluslararası uygulamalara tam uyum sağlayan bir ağ adli bilişim sürecinin oluşturulması,
- Oluşturulan adli bilişim süreciyle uyumlu, güvenli ve otomatik şekilde çalışacak SDN tabanlı 5G ağlarıyla uyumlu adli bilişim sisteminin geliştirilmesi.

Tezin katkıları

Tez kapsamında gerçekleştirilen araştırmalarda öncelikle SDN tabanlı 5G ortamlarında rutin iletişim ve saldırılar esnasındaki adli bilişim durumu tespit edilmiştir. Geleneksel ağ ortamlarından elde edilmesi hedeflenen dijital delillerin SDN ve 5G ortamlarından da elde edilebildiği görülmüştür. En az veriyle en fazla bilgiye erişim durumunun ve gerekli bilgilere erişimin kesintisiz bir şekilde sağlanabilmesi durumlarının da göz önüne alındığı araştırma kapsamında farklı SDN kontrolcülerinin farklı avantaj ve dezavantajları olduğu gösterilmiştir. Bazı kontrolcülerin veri boyutu açısından daha avantajlı bir adli bilişim süreci sunduğu, bazılarının saldırı altında dahi kesintisiz hizmet sunabildiği, bazı durumlarda farklı kontrolcüler özelinde hedeflenen bilgilere erişim sağlanamadığı görülmüştür.

Elde edilen sonuçlar literatürdeki bazı çalışmaların aksine, SDN'de adli bilişim süreçleri için herhangi bir kontrolcünün en iyi olarak nitelendirilemeyeceğini ispatlayarak literatüre katkı sunmaktadır. Ayrıca güney arayüzü verilerinin çoğu durumda adli bilişim için gerekli olan bilgileri içerdiği de elde edilen sonuçlar arasındadır. Araştırmalar sonucunda kontrolcü türünden bağımsız, standart olarak kabul edilebilecek bir adli bilişim sürecinin gerekli olduğu gösterilmiştir. Bu araştırma sonuçları hem literatüre katkı sunmakta hem de tezin diğer bölümlerine girdi oluşturmaktadır.

Standart bir ağ adli bilişim süreci oluşturma hedefi kapsamında mevzuat ve uluslararası uygulamalardaki ağ adli bilişimiyle ilişkili çalışmalar incelenmiştir. Mevzuatın yeterli bilgiyi sağlayabildiği değerlendirilmiş olmakla birlikte bu bilgilerin çok sayıda farklı kaynaktan elde edilebildiği görülmüştür. Uluslararası çalışmalar arasında da standart bir ağ adli bilişim süreci mevcut değildir. Bu gereksinimi gidermek adına SDN tabanlı 5G ağlarına da uygun olacak bir ağ adli bilişim süreci oluşturulmuştur. Oluşturulan sürecin uyumu deneylerle gösterilmiş olup, bir ülke mevzuatına ve uluslararası uygulamalara uyumlu bir ağ adli bilişim süreci literatürde ilk defa gerçekleştirilmiştir. Bu sürecin SDN ve 5G adli bilişim çalışmaları açısından da öncü olduğu ve gelecek çalışmaları etkileyeceği düşünülmektedir.

Tasarlanan adli bilişim sürecinin kurum/şirket yetkililerinin sorumluluğuna, bilgi birikimine ve dikkatine bırakılmadan işletilmesi sürecin sağlığı ve yaptırımların önüne geçilmesi açısından büyük fayda sağlayacaktır. Tüm ağ adli bilişimi sürecinin otomatik olarak işletilmesi hem dijital delillerin sağlıklı ve eksiksiz şekilde elde edilmiş olması açısından hem de delil elde etmekle mükellef olan kişilerin işlerini kolaylaştırmak açısından son derece önemlidir. Bu sebepten tez kapsamındaki araştırmalar adli bilişim süreci geliştirilmesinin ötesinde bu ağ adli bilişim sürecinin otomatik olarak işletilebileceği, SDN/5G uyumlu adli bilişim sistemi geliştirilmesiyle devam etmiştir. Sistemin geliştirilmesi sonrasında gerçek internet verisiyle deneyler gerçekleştirilmiş olup, sistemin oluşturulan süreç gereksinimlerini eksiksiz şekilde sağladığı görülmüştür.

En güncel ve güvenilir yöntemler kullanılan bu adli bilişim sisteminin geliştirilmesi aşamasında ücretsiz yazılımlar kullanılmıştır. Akış tabanlı yöntemlerle SDN ortamında erişim kayıtlarını tutma, internet erişimini SDN yetenekleriyle engelleme, uluslararası veri sızıntısı uyarılarını tespit etme süreçlerinin bir ilk olarak sunulduğu sistem, SDN tabanlı 5G ağları adli bilişim çalışmalarını mevzuata uygun şekilde otomatik olarak gerçekleştiren ilk sistem olma özelliğini taşımaktadır. Sistem kişisel verilerin güvenli bir ortamda saklanması ve muhafaza süresinin sonunda yok edilmesi özellikleriyle de ön plana çıkmaktadır. Türkiye'de gerçekleştirilecek SDN adli bilişim çalışmalarına tam uyum sağlayan sistemde kullanılan teknikler küresel olarak kabul görmüş olduğundan, sistemin tüm ülkelerin kullanımına uygun olacağı ve uluslararası adli bilişim çalışmalarına katkı sağlayacağı düşünülmektedir. Sınır ötesi adli bilişim çalışmalarına da hizmet edebilecek bu adli bilişim süreci ve sisteminin, sorumlu olan paydaşlara fayda sağlayacağı ve adli bilişim hazırlık seviyesini artıracağı düşünülmektedir.

Sınırlılıklar

Deneylerde saldırgan rolü verilen kullanıcılar dışında ortamda saldırgan olmadığı, kullanılan programların ve işletim sisteminin zararlı yazılım içermediği varsayılmıştır. Deneyler literatürde kabul edilmiş yöntem ve süreçler dâhilinde sanal ağ emülatörü Mininet ve OpenvSwitch sanal anahtarlar kullanılarak gerçekleştirilmiştir. Altyapı olarak bir dizüstü bilgisayara kurulu sanallaştırma sistemi olan VirtualBox'ın ücretsiz sürümü kullanılmıştır. Çok kullanıcılı yerel ağ deneyleri için uygun olan bu durum çok kullanıcıya internet erişim desteği vermesi açısından bir sınırlılık oluşturmuştur.

Akış tabanlı bir yöntem olan sFlow ile erişim kayıtlarını elde eden sistem, sFlow destekleyen tüm geleneksel ağ ortamları ve SDN ile uyum içerisinde çalışabilir. Ancak trafik engelleme alt sistemi, sistemde tercih edilen Ryu kontrolcüsünün yeteneklerine bağımlıdır. Sistem altyapısında OpenFlow 1.3. versiyonu kullanılmıştır [8, 15].

SDN ve 5G adli bilişimi alanındaki çalışmalar yeterli sayıda olmadığından yol gösterici ve öncü çalışma bulunması süre yönetimi açısından zorlu bir süreç olmuştur. Bu kapsamda yaşanan sınırlılıktan dolayı, ilk defa gerçekleştirilen çalışmaları içerisinde barındıran bu tezin etkisinin yüksek olacağını düşündürmektedir. Aynı doğrultuda, çok sayıda mevzuat ve farklı uluslararası çalışmaların incelenmesi sonucu önerilen adli bilişim sürecinin alanında öncü olacağı değerlendirilmiştir.

Tezin organizasyonu

İkinci bölümde tezin ana konusunu içine alan 5G ve SDN'de güvenlik ve adli bilişim konusunun kavramsal çerçevesi açıklanmıştır. 5G ve SDN mimarisi, 5G ve SDN'in getirdiği yenilikler, 5G ve SDN'in kullanım alanları konularında genel bilgiler sunulmuştur.

Üçüncü bölümde tezin ana amacı olan SDN tabanlı 5G adli bilişim sistemi geliştirilmesine giden sürecin tamamına dair literatürde yapılan çalışmalar hakkında bilgiler aktarılmıştır. Öncelikle 5G ve SDN adli bilişimi konusunda gerçekleştirilen çalışmalar aktarılmış olup, ardından adli bilişim süreci geliştirilmesi için gerekli olan idari ve hukuki çalışmalar hakkında bilgilere yer verilmiştir. Son olarak, uluslararası kapsamda ilk defa gerçekleştirilen bu çalışmanın literatürdeki çalışmalardan farkı somut bir şekilde ortaya konulmuştur.

Dördüncü bölümde SDN adli bilişiminin mevcut teknik durum tespitini yapmak amacıyla gerçekleştirilen deneyler hakkında bilgiler aktarılmıştır. Rutin iletişim ve çeşitli saldırılar esnasında gerçekleştirilen deneylerin kapsamı ve elde edilen bulgular aktarılmıştır. Farklı SDN kontrolcülerini içeren geleneksel veya 5G ağ ortamlarında adli bilişim süreçlerinin birbirinden farklılaştığı gösterilmiş olup, standart bir adli bilişim sürecinin gerekliliği ortaya konulmuştur.

Beşinci bölümde standart bir ağ adli bilişim süreci oluşturulması hedeflenmiştir. Bu kapsamda mevzuat, uluslararası uygulama ve standartlarda yer alan teknik, idari ve hukuki bilgiler aktarılmıştır. SDN ve 5G ağ ortamlarında yer alabilecek dijital delillere dair teknik ve idari değerlendirmeler de aktarılmıştır. Ardından tespit edilen gereksinimler doğrultusunda oluşturulan mevzuat uyumlu standart ağ adli bilişim sürecine dair bilgiler aktarılmıştır.

Altıncı bölümde ise oluşturulan ağ adli bilişim sürecinin otomatik olarak uygulanacağı sistemin geliştirilmesi sürecine dair bilgiler verilmiştir. Süreç kapsamında belirlenen adımların hangi teknik kullanılarak geliştirildiği ve bu yöntemlerin neden seçildiğine dair bilgiler bu bölümde yer almaktadır. Geliştirilen sistem gerçek internet kullanımı altında test edilmiş olup, sistemin mevzuatta belirtilen gereksinimleri otomatik ve güvenli bir şekilde sağladığı gösterilmiştir.

Yedinci bölüm gerçekleştirilen tüm çalışmayı geniş bir bakışla tartışmayı içermektedir. Bu bölümde SDN ve 5G adli bilişimi odağında mevzuat kapsamında yapılabilecek iyileştirmeler ve ülke adli bilişimi politikasını geliştirilebilecek düzenlemeler, uluslararası uygulamalar da dikkate alınarak tartışılmıştır. Ayrıca geliştirilen adli bilişim sisteminde elde edilen dijital delillerin, diğer ortamlardan elde edilebilecek dijital delillere göre önem, efor, uçuculuk ve öncelik açısından kıyaslamasına dair bilgiler sunulmuştur.

Son olarak sekizinci bölümde tez çalışmasında elde edilen bulgular aktarılmış, problemlere yönelik çözümler sunulmuş ve sonuçlar değerlendirilmiştir. Ayrıca tez çalışmasının literatüre katkıları açıklanmış, karşılaşılan zorluklar ele alınmış ve gelecek çalışmalar hakkında bilgiler sunulmuştur.

2. 5G AĞLARI VE GÜVENLİK YAPISI

Bu bölümde 5G ağları ve SDN mimarilerine ilişkin gerekli bilgiler aktarılmakta, mimarileri hakkında bilgiler verilmekte, kullanım alanları açıklanmakta ve her iki alana ve ortak kullanımlarına ilişkin güvenlik süreçleri üzerine incelemeler gerçekleştirilmektedir.

2.1. 5G Ağ Mimarisi

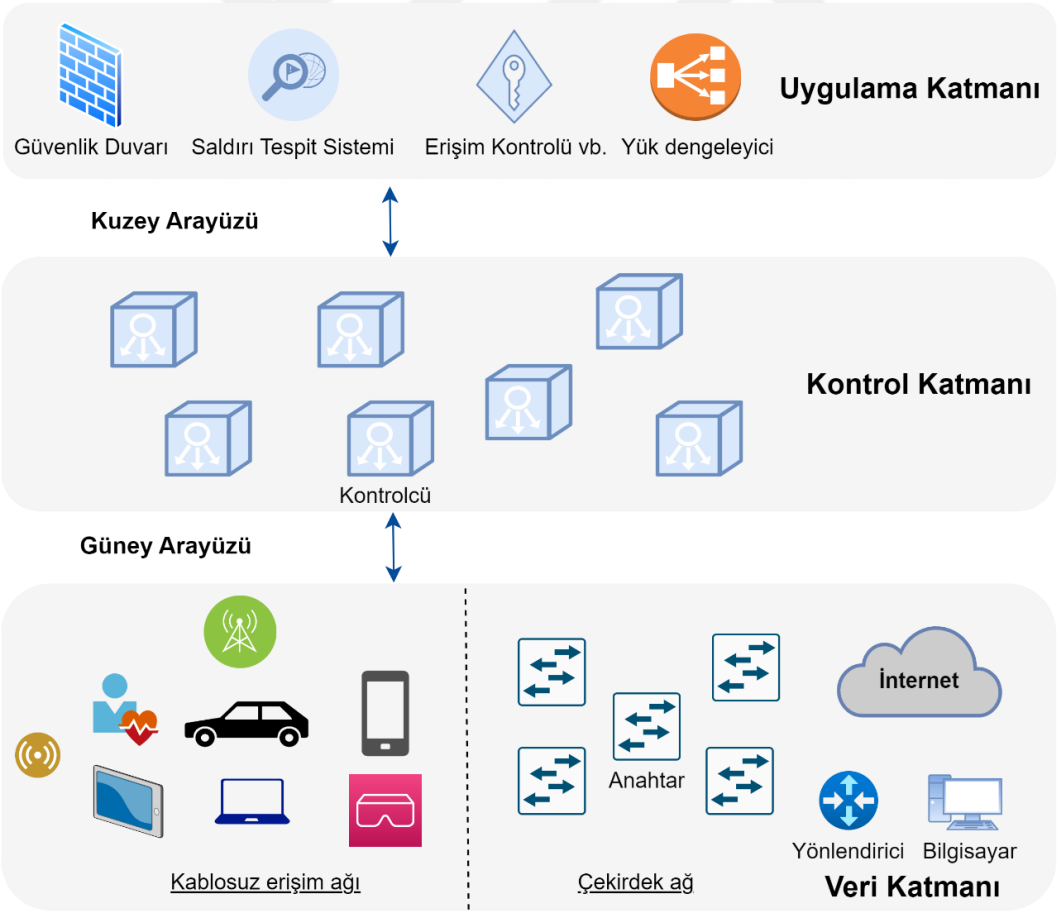
SDN ve NFV'nin 5G ağlarının temelinde yer alması hususu artık literatürde kabul görmüş bir konudur. 5G teknolojisine özel yeni bir çekirdek ağ yapısı oluşturmak yerine SDN ağlarının 5G'ye uyumlandırılması üzerine kurulan süreçler üzerinden 5G ağları tasarlanmaktadır. Bir ağ yapısının bütünsel olarak ele alınması gerektiğinden 5G ağlarının ön taşıyıcı (fronthaul) tarafındaki yüksek kalite beklentilerinin çekirdek ağ tarafından da karşılanabilir düzeyde olması gerekir. 5G'de kapasite ve gecikme beklentilerinin çözümlenmesi için uzak radyo ünitelerinin (Remote Radio Units, RRU) ve merkezi işlemcinin aralarında fiber optik kablolarla destekli altyapıların bulunması gerekir. Ayrıca ortak genel radyo arayüzü standartlarını sağlamak için de gecikmenin 100 ms'nin altında olması, dalga bozulumu (jitter) değerinin ise 65 ns'nin (nano saniye) altında olması beklenir [67].

SDN'in kontrol katmanı ve veri katmanını ayırması sayesinde ağ yönetimi daha kolay hale gelmektedir. 5G'deki çekirdek ağların yapılarının net olmaması ise SDN'i 5G ağlarında ön plana çıkarmakta ve vazgeçilmez kılmaktadır. Bu durum 5G'nin yüksek QoS beklentilerine de uygundur. Bulut bilişim ve veri merkezlerinde SDN'in kullanılıyor olması ve kolay yönetilebilir olması da 5G ağları için SDN altyapısının önemini desteklemektedir. SDN'i hücresel ağların temelinde kullanan çok sayıda çalışma yapılmış olup, kontrol katmanı sayesinde çok sayıda cihazın internet protokolü (Internet Protocol, IP) tabanlı ağ yönetiminin gerçekleştirilebilir olması durumunun 5G ağları için de avantaj sağladığı gösterilmiştir [68].

Mevcut hücresel ağların donanım bağımlı ve esnek olmayan yapısı da 5G gibi gelişen teknolojilere hızlı uyum sağlamanın önüne geçmektedir. Bu durum kapsama alanından, bağlı cihaz sayısına kadar farklı açılardan ağ gelişimini kısıtlamaktadır. Ağ kaynaklarının verimli bir şekilde paylaştırılarak yönetilmesi ve radyo ağlarındaki kazanımların gerçek manada kullanılabilmesi de SDN sayesinde mümkün olmaktadır [69]. Şekil 2.1'de gösterildiği üzere

5G kablosuz erişim ağının yönetimi için SDN altyapısı kullanılmakta olup, SDN'in kolay yönetilebilir ve izlenebilir yapısı sayesinde 5G'nin hizmet sunacağı çok yüksek sayıdaki kullanıcı için ağ hizmeti sunma işlemleri gerçekleştirilebilir olmaktadır. Uç bilgi işlem (edge computing) işlemleri, kullanıcı işlemleri ve altyapı dikkate alındığında SDN tabanlı kontrolün 5G'de güvenlik, bağlantı ve hareketlilik sürelerine katkı sunacağı da görülmektedir. Bu sayede gecikme süresi ve ağ güvenilirliği de artmaktadır [70]. SDN tabanlı 5G ağlarının standart 5G ağlarına göre %62'ye kadar daha az gecikme sunduğu gösterilmiştir [71].

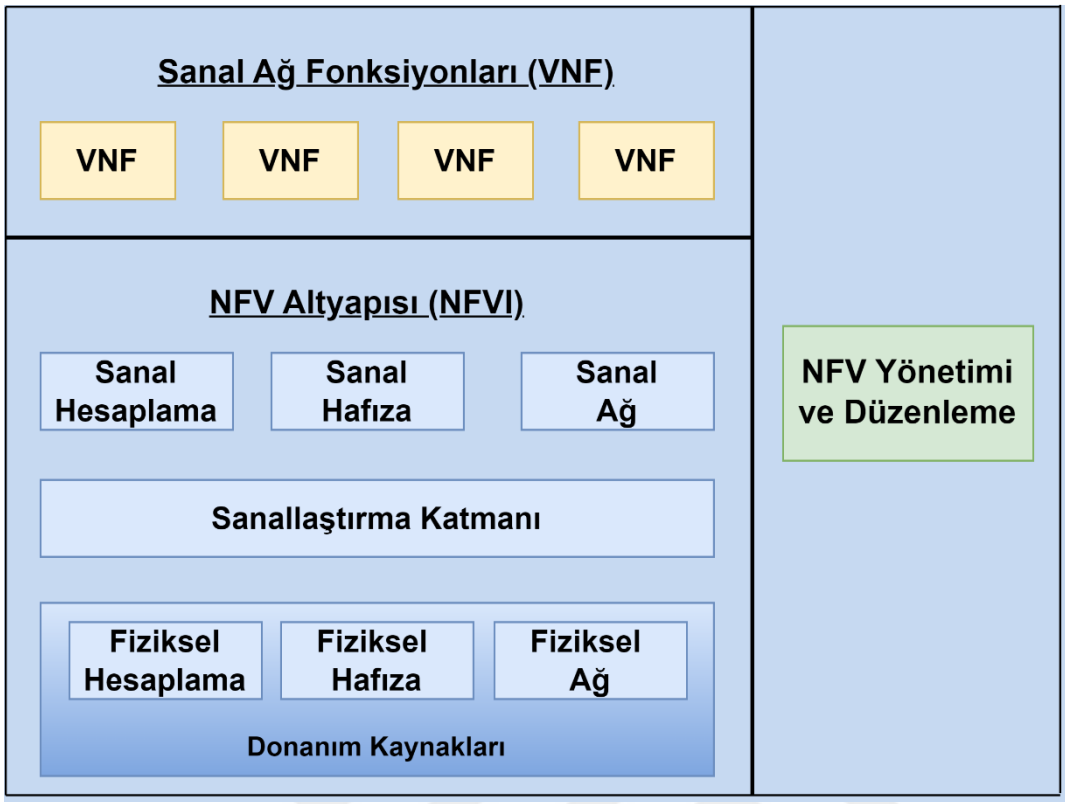
Yakın gelecekte akıllı şehir, askeri uygulamalar, akıllı trafik gibi farklı uygulamalardaki haberleşme altyapısı 5G ve SDN'in bütünleşmesiyle çözümlenecektir. 5G ve SDN'nin ortak kullanımıyla modern ağ iletişiminin mimari ve güvenlik açısından devrim yaratacağı sonucuna varılabilir [72].



Şekil 2.1. SDN tabanlı 5G ağları [73]

5G ağlarının temelinde SDN ve NFV teknolojileri yer almakta olup bu teknolojilerin 5G'de uygulanabilir olmasını kolaylaştıran çözümler arasında ağ dilimleme bulunmaktadır. Ağ dilimleme sayesinde bir ağ altyapısının sanal olarak ayrışması ve farklı çözümlerin bütünsel bir açıdan yönetilebilmesi sağlanmış olur. Ağ dilimleme kullanıcı özelinde ağ hizmeti verme, saldırı anında ağın yapısını değiştirme ve maliyet azaltma açısından da fayda sağlamaktadır. Geleneksel ağlarda donanımsal olarak hizmet veren saldırı tespit sistemi ve güvenlik duvarı gibi uygulamalar 5G'de sanal ağ güvenliği fonksiyonları (Virtual Network Security Function, VNSF) kullanılarak hizmet verebilecektir [74].

5G ağlarının Gbps düzeyinde hız sunması, yük ve maliyet gereksiniminin az olması, kolay değiştirilebilir yapıya sahip olması ve güvenilir yapıya sahip olması için çekirdek ağ kısmında teknolojik yenilikler gerekmektedir. Farklı kalite ve hızda beklentileri olan ağların bölünebilmesi ve farklı dilimlerde yönetilebilir olması 5G'nin büyük kazanımlarındandır. Örneğin akıllı sağlık uygulamaları ve akıllı otomotiv uygulamaları dilimleri birbirinden ve diğer uygulamalardan ayrılarak daha düşük gecikme sunan bir yapıda hizmet sunulabilir. Bu hizmetlerin sunulabilmesi SDN ve NFV'nin birlikte 5G altyapısı için kullanılmasıyla mümkündür. Donanımsal olarak ayrışması mümkün olmayan bu yapıları ancak yazılım ve sanallaştırma teknolojileriyle ayırmak mümkündür. NFV'nin yönetim ve düzenleme (Management and Orchestration, MANO) özelliğiyle sanal olarak oluşturulan ağ fonksiyonlarını donanım hatalarından bağımsız olarak hızlıca geri çalışır duruma getirmek mümkündür. Şekil 2.2'de gösterildiği üzere NFV kullanımıyla, donanımsal altyapının hafıza, hesaplama ve ağ yapıları olarak ayrılması ve yönetilmesi mümkün kılınmaktadır ve bu sayede daha yüksek seviyelerde hizmet sunmak mümkün olacaktır. Bu sanal ağ fonksiyonları (Virtual Network Function, VNF) servis fonksiyon zincirleri kullanılarak (Servis Function Chain, SFC) yönlendirilir. Bir ağ servisi oluşturulması için karar bu şekilde alınmış olur. Sadece belirli markalara ait donanımlarda çalıştırılması için tasarlanan programların yerini marka bağımsız bir sürecin almış olması da ağ kurulması ve yatırımı açısından olumlu bir gelişmedir. VNF'ler genellikle sanal makineler olarak karşımıza çıkmaktadır. 5G'nin ağ dilimlerinin yönetiminde NFV MANO ağ dilimi servislerinin arasındaki karışık yönetimi üstlenir. Performans, güvenlik, hata uyarıları, hareketlilik yönetimi, enerji yönetimi, servis güvenilirlik yönetimi, QoS yönetimi, VNF yaşam döngüsü yönetimi ve sanallaştırılmış altyapı yönetimi MANO üzerinden işletilmektedir [75].



Şekil 2.2. Temel NFV mimarisi [76]

Teknolojik gelişmeler internet servis sağlayıcılarına (İSS) ağ servislerini sanallaştırılmış olarak yönetme imkânı sunmaktadır. Ancak bahsi geçen 5G ağlarına bağlı cihaz sayısı ve farklılaşan ağ beklentileri göz önüne alındığında karmaşık ve zor yönetim içeren bir süreç karşımıza çıkmaktadır. Bu durumun çözümü için SFC'lerin dağıtım ve tasarımında yapay zekâ ve makine öğrenmesi yöntemlerinin kullanımı da yaygınlaşmaktadır [76].

5G teknolojisi doğrudan insanların kullandığı veya nesneler yardımıyla insanların hizmetine sunulan ağ cihazlarına çok farklı kapsamda amaçlar için hizmet eder. Bu ağ cihazları sabit olabileceği gibi hareketli durumda da olabilirler. İnternet mühendisliği görev gücü (Internet Engineering Task Force, IETF) SFC çalışma grubu, ağ servis başlığını (Network Service Header, NSH) katmandan bağımsız bir kapsülleme olarak tanımlamıştır. NSH paketin geçtiği zincirin bir tanımlayıcısını, zincirde ulaşılan noktanın bir göstergesini, paket döngülerini önleyen bir TTL alanını ve meta veriler için bir alanı içerir. NSH yük paketi türünden bağımsızdır (IP, MPLS, ethernet vb.) ve hizmet işlevlerinin yükü nasıl işleyeceğini bilmesi için bir sonraki protokol alanını kullanır. Ancak NSH desteği, yeni donanım yeteneklerinin yanı sıra ağ işlevlerinin mevcut yazılım gerçekleştirmelerine yönelik uzantıların geliştirilmesini gerektirebilir. Hizmet işlevleri başlatıldıktan ve

yapılandırıldıktan sonra kullanıma hazır hale getirilmeleri gerekir. Her bir SFC'nin servis fonksiyonu ileticiye (Service Function Forwarder, SFF) bağlanması gereklidir. Ayrıca belirli bir SFC'deki paketlerin hizmet işlevlerine teslim edilmek üzere SFF'ler arasında yönlendirilebilmesi için konumlarının duyurulması gerekir ve böylece hizmet işlev zincirleri planlanabilir [77]. Tahmini olarak 1000 katına çıkacak bir ağ trafiği ihtiyacının karşılanması için 5G ağlarının geçmişteki cihazlarla da uyum sağlaması gereken durumlar olabilir. Yatırım ve işletme maliyetlerini de göz önüne alarak kullanıcı cihazları tarafında beklenen servis kalitesinin sağlanması için ağ dilimlerinin çevik ve kolay değiştirilebilir bir yapıda olması gerekir ve NSH, SFC teknolojileri bu durumlar için kullanılmaktadır [78].

Ağ düğümlerinin sanallaştırılması ve bulut hizmetlerinin devreye alınması erişim hızı, düşük paket kaybı, düşük enerji tüketimi gibi kriterlerde avantaj sağlayarak radyo kaynak yönetimi (Radio Resource Management, RRM) açısından avantaj sağlar. Heterojen ağların kullanımı QoS ve deneyim kalitesi (Quality of Experience, QoE) açısından da çözümler sunmaktadır. Mevcut SDN teknolojileriyle uyumlu olması gereken veya SDN teknolojilerinin geliştirilerek kullanılmasını gerektiren 5G ağlarında yüksek hız ve düşük gidiş geliş süresi (Round Trip Time, RTT) gerekmektedir. SDN kontrolcüsü tarafından ağa uygulanan politikaların da bu çerçevede ele alınması gerekmektedir [79].

5G ağlarının servis temelli yönetiminde de SDN ve NFV teknolojileri ayrı ayrı kullanılabileceği gibi, bu iki teknoloji birlikte de kullanılabilir. Bir servis yönetim katmanı servis yönetiminden sorumluyken SDN kontrolcüleri ağ fonksiyonlarını planlar, yönetir ve trafik planlaması yapabilir. Bu sayede ağ yönetim maliyetleri azaltılabilir [80].

2.2. 5G Ağlarında Güvenlik

5G güvenliğini sadece ses/video iletişimi olarak ele almak yeterli değildir. 5G güvenliğini; gizlilik, bütünlük, erişim kontrolü, kimlik doğrulama ve erişilebilirlik olarak sınıflara ayırarak değerlendirmek mümkündür. Gizlilik ilk kademede ele alınacak bir ölçüt olup, 5G ağları da ortadaki adam, dinleme saldırıları, yeniden iletim tehditleri gibi saldırılara karşı açıklıklar içerebildiğinden, 5G ağlarının güvenlik ve şifreleme açılarından ele alınması gerekmektedir. 5G'nin yeni radyo teknolojisi, kullanıcı düzleminde bütünlük koruması gerektirdiğinden dolayı mesaj içeriklerinin bütünlüğünün korumasına da katkı sağlamaktadır. Kimlik doğrulamanın sağlıklı olması için de sinyal aşamasından itibaren

mekanizmaların geliştirilmesi gerekmektedir. SDN tabanlı 5G ağlarının hataya karşı olan toleransı göz önünde bulundurulduğunda 5G'nin çok yüksek seviyede erişim sağlayabileceği değerlendirilmektedir. 5G'nin kendi doğasında gelen güvenlik hizmetlerinin ve çözümlerinin sayıları SDN'in güvenlik çözümlerine göre daha azdır. Ancak iki teknolojinin birlikte kullanılması özellikle erişim kontrolü ve gizlilik açısından güvenlik çözümlerinin sayısını ve niteliğini artırmaktadır [72].

5G'de kullanıcılar güvenlik kapsamı farklı olan hizmetlere abone olabilir ve bu ağlar VNSF'ler kullanılarak yönetilebilir. Farklı aboneliklere sahip olan 5G ağlarının enerji tüketimi açısından verimli olarak tasarlanması da dikkat edilmesi gereken hususlardır ve bu kapsamda sezgisel algoritmalarla trafiği yönlendiren SDN kontrolcüsü geliştirilmiştir [74].

SDN'e karşı güvenlik tehlikeleri 5G ağları için de geçerlidir [67]. 5G ve ötesi ağlarda güvenliğin sağlanması için uçtan uca SDN güvenlik tasarımlarının gerçekleştirilmesi gerekmektedir [79]. SDN mimarisi, veri katmanının anında yeniden programlanabilir merkezi görünümü aracılığıyla ağdaki güvenlik uygulamalarına izin verme, bunları basitleştirme veya artırma potansiyeline sahiptir [72]. SDN tabanlı 5G ağlarında sahte veya tuzak telefon aramalarının önüne geçilmesi de yönetilebilmektedir. Normal aramalardan ayırt edici olan bu aramaları SDN mimarisindeki güvenlik denetleyicisine ileterek ağ akış tabloları sayesinde verilerin iletilip iletilmemesine dair karar SDN altyapısı sayesinde süratle alınabilir [81]. SDN'in 5G güvenliğine getirdiği katkıların aksine SDN'in kendi yapısına karşı olan güvenlik açıkları dezavantaj oluşturabilir. Rutin SDN güvenlik çözümlerinin ötesine geçerek kriptografik kimlik doğrulama çözümlerinin çok yüksek düzeyde hizmet sağlama hedeflerini aksatmayacak şekilde SDN ağlarına da uygulanması gerekmektedir [73].

SDN ve NFV teknolojilerinin yanı sıra 5G mimarisinde güvenlik sağlanması için farklı çözümler gerektirmektedir. NFV ağının gelişimiyle gelen güvenlik ihtiyaçlarının yanı sıra 5G ağı gerçek zamanlı anahtar yönetiminin çok fazla sayıda kullanıcı için yapılması gibi geleneksel ağlarda karşımıza çok çıkmayan sorunlarla baş etmek zorunda kalacaktır. Ultra yoğun ağ (Ultra-dense Networking, UDN), kitlesel çoklu anten sistemleri (Massive Multiple-input and multiple-output, mMIMO) gibi teknolojilerin de güvenliğinin sağlanması gerekir. Kullanıcı gizliliğinin daha fazla ele alınması gereken 5G ağlarında, 4G ağlarında kullanılan güvenlik çözümleri tek başına yeterli olmayacaktır. Ağ erişim ve ağ

alanı güvenliği, kimlik doğrulama ve anahtar yönetimi, ağ dilimleri güvenliği, yönetim güvenliği gibi hususlar açısından da yaklaşarak çözümler sunulması gerekmektedir. Ağ mimarisinden ve elektromanyetik yayılma mekanizmasından eski güvenlik unsurları çıkarılmalı ve yeni savunma mekanizmaları geliştirilmelidir [82].

Sıralanan hususların yanı sıra erişimsiz katman (Non-access stratum, NAS) çözümlerinin de yeni ve farklı sinyal yapısı göz önüne alınarak sistemlere entegre edilmesi gerekmektedir. Altyapıya yönelik hizmet engelleme (Denial of Service, DoS) atakları, son kullanıcıya yönelik DoS atakları, operatör dolaşımlarındaki güvenlik durumları ve kullanıcı katmanındaki şifreleme eksiklikleri de güvenlik çözümleri bulunması gereken konular arasındadır. SDN, NFV ve bulut teknolojilerinin güvenlik açıklarına karşı savunmasız olabilecek 5G ağlarında ortadaki adam saldırıları, tarama saldırıları, DoS saldırıları, ele geçirme saldırıları, kaynak hırsızlıkları, IP sahtekârlığı, zorla giriş saldırıları, uluslararası mobil abone kimliği (International Mobile Subscriber Identity, IMSI) yakalama gibi saldırıların gerçekleştirilmesi mümkün olup bunlara karşı güvenlik sağlanmalıdır [83].

5G ağlarında SDN kullanımına odaklanıldığında kimlik taklit etme, veri değiştirme, trafik dinleme, anahtar ele geçirme ve uygulama katmanına yönelik saldırılar da karşımıza çıkmaktadır. Kontrolcü ele geçirilmesi durumu tüm ağı etkileyebileceğinden SDN tabanlı 5G ağlarında da en önem verilmesi gereken husus olarak karşımıza çıkmaktadır. OpenFlow anahtarlarının kolay ele geçirilebilir olması da bir başka güvenlik problemidir. 5G ağlarında güvenlik beklentilerinin belirlenerek mobil ağ güven ilişkilerinin sağlıklı bir şekilde belirlenmesi gerekmektedir. Erişim noktaları/baz istasyonlarının kimliklerinin sağlam bir şekilde korunması, açık standartları temel alan güvenlik politikaları geliştirilmeli, tüm SDN katmanlarının güvenliği sağlanmalı, kontrolcü ve erişim noktaları arasındaki operasyonel veri güven altına alınmalı, tanınmayan cihazların da takibi sağlanabilmeli ve yönetilebilir güvenlik kontrolleri analiz edilmelidir. Geleneksel güvenlik anlayışında yer alan hususlara da önem gösterilmesi gerekmektedir. Bunlar arasında; sistemlerin güncel olması, sadece yetkili kişilerin kontrolcü ve kritik noktalara erişim sağlayabilmesi, genel güvenlik rehberleri oluşturulması, genel ağ izlemesi gerçekleştirilmesi, beyaz ve kara liste uygulamaları, güvenlik duvarı kullanımı, etkin ağ izlemesi gerçekleşmesi ve şifreleme yer almaktadır [84].

Üreticiden bağımsız bir şekilde ağ fonksiyonlarını yönetme sürecinde 5G'nin parçası olan NFV teknolojisi yatırım maliyetlerini, enerji tüketimini düşürmekte ve çevik bir yönetim sunmaktadır. SDN ve NFV'nin birlikte kullanılması da somut avantajlar sunmaktadır. Örneğin NFV sayesinde SDN kontrolcüsünün yer değişiklikleri kolaylıkla yapılabilir ve bu durum ağın daha kolay tasarlanmasını sağlar. SDN sayesinde de NFV dinamik bir ağ bağlantısı kazanmış olur. NFV'nin içerdiği sanal ağ hizmeti sunan servislerin dışında NFV'nin kendisi de altyapısıyla (NFV Infrastructure, NFVI) güvenlik sağlamak durumundadır. Aksi durumda tüm altyapı tehdit altında olabilir. NFV düzenleyicisi kaynakların tahsisi üzerine yetkilendirme ve yönetimi gerçekleştirir. VNF'lerin taklit edilmesiyle sanal makine yönetimine saldırılar düzenlenerek yönetimi ele geçirebilir ve bu sayede gerçek kullanıcıların erişimini engellemek mümkündür. Benzer saldırı türleri kullanarak sahte VNF'ler oluşturulması da mümkündür. 5G'nin servis anlaşmaları politikalarına uyum da bu saldırılarla zedelenebilir ve servis sağlayıcılar cezai yaptırımlarla karşı karşıya kalabilir [85]. 5G ağlarının daha fazla yaygınlaşmasıyla birlikte NFV kullanımına yönelik saldırılar da artacaktır. Bu sebepten NFV'de güvenliği bütüncül bir açıdan ele alarak bu konudaki çalışmaların güvenlik düzeyini tespit etmekten öte düzeyi artırıcı yönde olması ve referans güvenlik mimarilerinin geliştirilmesi gerekmektedir [86]. Her ağın yapısına uygun olarak tasarlanmaya çalışılan standartların bazı özel ağ ihtiyaçlarına cevap veremeyeceği zamanlarda, bu tarz geliştirilen güvenlik mimarilerinin hızlı bir şekilde işler hale getirilmesi de güvenlik açısından önemlidir [87].

5G teknolojisi sayesinde hastanelere, akıllı evlere, araçlara artan ağ kapasitesi ve verimlilik gelecektir. Çoklu giriş çoklu çıkış (Multiple-input/multiple-out, MIMO) teknolojisinin bu süreçte katkısının büyük olacağı bilinse de güvenlik açısından detaylı inceleme yapılması önem arz etmektedir. Çünkü geleneksel ağlarda kullanılmayan yeni teknolojiler yeni saldırı çeşitlerine karşı savunmasız kalabilir. Örneğin MIMO'da kaynak tahsisinin daha detaylı şekilde araştırılması gerekmektedir. Fiziksel katmanda veri güvenliğini sağlamak için yapay zekâ ve büyük veri uygulamalarının kullanılması konusunda da araştırmalar yapılarak çözümlerin geliştirilmesi gerekmektedir. SDN sayesinde kontrol ve veri katmanının ayrılmasıyla yönetimi kolaylaşan ağ yapısının da bazı yeni açıklıklar oluşturabileceği düşünülmektedir. Bu katmanlar arasında ele geçirilmiş olan ağ düğümleri de güvenlik açıklıkları oluşturabilmektedir. 5G ve ötesi ağlarda blokzincir ve bulut bütünleşmesi de gizlilik açısından katkı sunacaktır. Ancak bu durum sistemin kurucuları açısından yeni zorluklar getirmekte olup yatırım maliyeti ve sistem tasarımı açısından yoğun emek

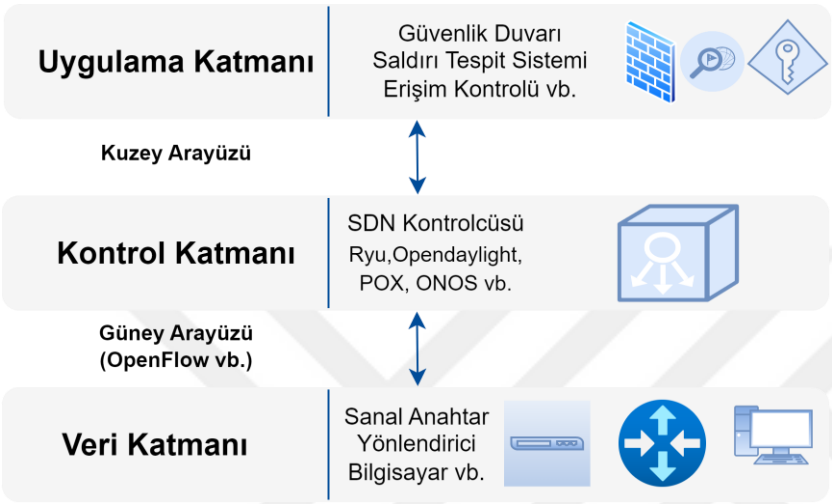
gerektiren süreçler arasındadır. Endüstriyel alanda ve kullanıcıların günlük süreçlerine hizmet eden alanlarda çok farklı süreçlere hizmet edecek olan IoT cihazlarının güven modelleri 5G için yeterli olmayacaktır. Aynı altyapı kaynaklarının dilimlenerek kullanılmasına imkân tanıyan yeni teknolojilerde, kaynakların dinamik olarak belirlenmesi süreçlerini de güvenli olarak gerçekleştirilmesi gerekmektedir. Aksi durumda küçük bir sensör dahi sistemde güvenlik açıkları oluşturabilir [88].

2.3. Yazılım Tanımlı Ağ (SDN) Mimarisi ve Avantajları

SDN, herhangi bir üreticiden gelen ağ cihazının SDN ile kontrol edilebildiği, donanımdan bağımsız, yeni nesil ağ yapısı olarak kabul edilir. SDN kontrolcüsü, tüm ağın yönetiminden sorumluyken, ağ anahtarları, SDN kontrol birimi aracılığıyla dağıtılan talimatlara dayanarak çalışmaktan sorumludur. Şekil 2.3'te gösterilen SDN mimarisi; Uygulama katmanı, Kontrol katmanı ve Veri (Altyapı) katmanlarını içermektedir. Veri katmanı yönlendirici, anahtar ve erişim noktası gibi ağ aygıtlarından oluşur. OpenvSwitch, Indigo, Pica8, Nettle, Open Flowj gibi sanal anahtarlar bu katmanda yer almaktadır.

SDN yapısının merkezinde yer alan kontrol katmanı tüm SDN fonksiyonlarını kontrol etmektedir. Bu katman, altyapı katmanı ve uygulama katmanı için aracı olarak görev yapar ve SDN kontrolcüsü de bu katmanda yer alır. Kontrolcü tüm trafik akışını yönetmekten sorumludur ve yalnızca programlamada yönlendirme, akış iletme ve paket bırakma hakkında kararlar alır. Kontrolcülere örnek olarak Ryu, POX, OpenDaylight (ODL) ve ONOS verilebilir [89–92]. Kontrol katmanı ve altyapı katmanı, OpenFlow, NetConf vb. gibi güney arayüzü (southbound interface) vasıtasıyla birbirleriyle iletişim kurar [8, 13]. Şekil 2.3'te gösterildiği üzere kontrolcü ve veri katmanı arasındaki iletişimi sağlamak için kullanılan en yaygın protokol OpenFlow'dur. OpenFlow yenileşmeyi kolaylaştırır ve etkin hizmet düzenleme ve otomasyonu sağlar [12]. Ağ yönetimi, güvenlik uygulamaları, yük dengeleme gibi farklı görevler, kontrolcü tarafından oluşturulan ve OpenFlow mesajları kullanılarak veri katmanına gönderilen akış kuralları ile gerçekleştirilir [14]. OpenFlow özellikli veri katmanı cihazları, paketlerin nasıl iletileceğine ilişkin bilgileri içeren kuralları depolamak için akış tabloları içerir. Farklı versiyonları olan ve ihtiyaca göre güncellenen OpenFlow'un geleneksel ağlardan geçişte hibrit ağlarda da etkin olabilmesi mümkündür [15].

Uygulama katmanı yazılımla ilgili iş ve güvenlik uygulamalarını bünyesinde barındırır. Ağ sanallaştırma, saldırı tespit ve önleme sistemleri (Intrusion Detection System, IDS & Intrusion Prevention System, IPS), güvenlik duvarı ve hareketlilik yönetimi bu katman tarafından ele alınan uygulamalar arasındadır. Bu katman, kuzey arayüzü (northbound interface) aracılığıyla kontrol katmanı ile iletişim kurar.



Şekil 2.3. SDN mimarisi

Ağdaki akıllı programlanabilir cihazların gittikçe daha yaygın olması nedeniyle, SDN genel ağ performansını artırmak için güvenlik, enerji verimliliği ve ağ sanallaştırması sağlar. SDN, programları kullanarak anahtarlar, yönlendiriciler ve güvenlik duvarları gibi tüm ağ elemanlarındaki işlevleri yöneten ve otomatikleştiren bir kontrolcü aracılığıyla tüm ağın merkezi kontrolünü sunar. Bu özellikler genel ağ performansını ve güvenliğini artırmak için akışları dinamik olarak ayarlamaya yardımcı olur [8].

Kontrol katmanına, veri katmanının ağ akışını işlemek için bir akış kuralının bulunup bulunmadığının sorulması gibi temel SDN özellikleri kullanılarak, bir ağ uygulaması ağ akışlarını dinamik olarak kontrol edebilir. Bu özellik dinamik yük dengeleme ve ağ yönetimi uygulaması gibi akış kontrolü için ağ uygulamalarında kullanılır. Veri katmanları, kontrol mesajlarını almak için merkezi bir kontrol katmanına bağlanır. Ek olarak, kontrol katmanı bir istatistik sorgu mesajı göndererek veri katmanından ağ durum bilgisini toplar. Bu nedenle kontrol katmanında çalışan bir ağ uygulaması doğal olarak veri katmanının bilgisine sahiptir ve merkezi bir şekilde kontrol sağlayabilir. SDN ağındaki tüm veri katmanları bir ağ uygulama programı tarafından kontrol edilebildiğinden, SDN yeni ağ işlevlerini

etkinleştirmek için güçlü bir yetenek sağlar. Temel olarak, SDN mimarisi veri katmanını kontrol katmanından ayırır ve bu nedenle veri katmanı nispeten basit bir mantığa sahiptir. Tüm yapı ele alındığında SDN'in sağladığı ana avantajlar; dinamik akış kontrolü, merkezi kontrol ile ağ genelinin görünür ve programlanabilir olması ile basitleştirilmiş veri katmanı olarak sıralanabilir [16].

SDN getirdiği tüm yeniliklerle, geleneksel ağlara kıyasla daha esnek ve kolay yönetime sahiptir [10]. Bu sayede ağ yöneticilerinin trafik izleme ve genel ağ süreçlerine daha kolay müdahale imkânı sunar [11]. Ek olarak artırılmış güvenlik, kolay politika yönetimi ve daha az enerji kullanımı da SDN'in avantajları arasındadır [93].

2.4. SDN Kullanım Alanları

Yeni bir ağ hizmeti başlatmak için genellikle başka bir çeşitlilik gerekir ve bu kutuları barındıracak yer ve gücü bulmak giderek zorlaşır. Donanıma dayalı cihazlar hızlı bir şekilde kullanım ömrüne ulaşır. Bu durum ağ merkezli uygulamaların arttığı günümüzde yatırım maliyetleri sebebiyle yenilikleri kısıtlamaktadır.

NFV birçok ağ donanım türünü, veri merkezleri, ağ düğümleri ve son kullanıcı tesislerinde bulunabilecek endüstri standardı yüksek hacimli sunucular, anahtarlar ve depolama alanlarıyla birleştirmek için standart sanallaştırma teknolojisini kullanarak bu sorunları gidermeyi amaçlar. NFV, sabit ve mobil ağ altyapılarında herhangi bir veri katmanı paket işleme ve kontrol düzlemi işlevine uygulanabilir durumdadır. NFV teknolojisi, SDN için son derece tamamlayıcıdır ancak iki teknoloji birbirine bağımlı değildir. NFV, SDN gerekmeden uygulanabilir ancak iki kavram birleştirildiğinde daha büyük bir potansiyel oluşmaktadır. Ancak, kontrol ve veri katmanlarının ayrılmasına dayanan SDN mimarisi, NFV performansını artırabilir, mevcut dağıtımlarla uyumluluğu basitleştirebilir, işletme ve bakım maliyetlerini düşürebilir [94].

Yeni nesil ağlarda, operatörlerin farklı uygulama trafiğini belirli müşteri ağlarından veri merkezlerine, 5G radyo erişim ağlarına (Radio Access Networks, RAN), IoT cihazlarına, bulut / sis düğümlerine aktarması gerekecek. 5G ağlarındaki uygulamalar farklı uçtan uca QoS gereksinimlerine tabi tutulabilmektedir. Ayrıca trafik yalıtımı, güvenlik ve performans izleme gibi ek gereklilikler hedeflenmektedir. Ağ trafiğinin hedefe ulaşmasından önce

uygulanacak bu birleşik işlevlerin seçilen akışlara dinamik olarak uygulanması SFC olarak adlandırılır ve SDN'e entegre bağlamında yeni bir konudur. SFC basamaklandırılmış servislerin kurulumunda NFV tarafında da çabuk kabul görmüş ve uygulamaya başlanmıştır [95].

SFC, SDN kabiliyetlerini kullanarak güvenlik duvarları, ağ adresi dönüştürme (Network Address Translation, NAT), IPS gibi ağ servislerine bağlı olan bir zincir kurar ve bu ağ servislerini birbirine sanal olarak bağlar. Bu özellik ağ operatörleri tarafından farklı özelliklere sahip birçok servis için tek bir ağ bağlantısının kullanılmasını sağlayan bağlı servislerin takımlarını veya kataloglarını ayarlamak için kullanılabilir [96]. Kısa ömürlü ağ servisleri, belirli bir süre için bağlantı performansını yükseltilmesi, hizmetin sadece hedeflenen kullanıcılara ulaştırılması veya kullanıcı hizmeti hareketliliğini desteklemek gibi taleplerin mevcut teknolojileri kullanarak gerçekleştirilmesi zor olsa da, bu hususlar SFC desteğiyle kolay bir şekilde kullanılabilir duruma gelecektir. Bu sayede bir çevrim içi oyun merkezine bağlantıda gecikmesiz bir ağ hizmeti sunmak, sadece belirlenen tekil bir ağ kullanıcısına üst kalite veya ek güvenlik özellikli hizmet sunmak, kendi aboneliğini başka ağların üzerinde kullanmak gibi süreçler daha kolay yönetilebilir durumda olacaktır [97].

5G iletişim sistemlerin gelişmiş özellikleri, sahadaki uç noktalara 1-10 Gbps bağlantı sunma, 1 ms gecikme, birim alanda 1000 kat bant genişliği, 10-100 kat arası bağlı durumda cihaz sayısı, %99.999 kullanılabilirlik, %100 kapsama, %90 oranında şebeke enerji kullanımının azaltılması ve düşük güçlü cihazlar için on yıla varan pil ömrü olarak sıralanabilir. Bu performans gereksinimlerini karşılamak için, heterojen ağlar, MIMO, mmWave, cihazdan cihaza (Device to Device, D2D) iletişim, SDN, NFV ve ağ dilimleme gibi teknolojiler 5G sistemlerine uygulanır [98]. Bir veri merkezinde, bağlantı SDN aracılığıyla etkinleştirilebilir. Ancak SDN bununla sınırlı değildir, geniş alan ağlarını kontrol etmek için de kullanılabilir. 5G ağlarında mimari kararlara bağlı olarak SDN ve RAN uygulama bütünleşmesiyle dağıtılmış bölgeleri birbirine bağlayan geniş alan ağlarına uygulanabilir [99].

2.5. SDN Güvenliği

SDN güvenliği, genel güvenlik çerçevesinin dışında düşünülmemelidir. Geleneksel ağlardaki birçok güvenlik sorunu SDN için de geçerli olsa da, bu genç alanda yeni fırsatlar

ve yeni zorluklar ortaya çıkmıştır. SDN'de güvenlik çalışmaları, SDN'in çalıştığı ortamların güvenliğini sağlamak ve SDN'in kendi güvenliğini sağlamak olarak iki çerçevede ele alınabilir [12]. Dolayısıyla mevcut güvenlik açıklarının üzerine [16–20] SDN'in yapısından kaynaklı diğer açıkların ekleneceği değerlendirilmektedir ve bu durum yeni yaklaşımlar gerekmektedir [22, 100].

SDN teknolojisi, güvenli ağ iletişimi sağlamak adına izinsiz giriş, kötü amaçlı yazılım saptama ve istenmeyen trafik kontrolü gibi güvenlik çözümleri uygulamak için kullanılabilir. SDN kontrol cihazlarına izinsiz girişler, kontrol katmanı ile veri katmanı arasında kimlik doğrulaması gibi bir dizi yeni saldırı ve güvenlik açığına SDN'e geçişle birlikte maruz kalınabileceği tahmin edilmektedir. Güvenlik üzerinde önemli bir odaklanma olmadan, SDN ile ilişkili gelişen tüm yeteneklerin desteklenmesi mümkün olmayacaktır [12].

Diğer güvenlik araştırmalarına kıyasla SDN güvenliği üzerine yapılan araştırmalar nispeten yavaş ilerlemektedir. Ancak, SDN'in bazı hususlarda ağ güvenliği işlevlerini geliştirebileceği söylenebilir. Örneğin, ağ akışını dinamik olarak kontrol etme yeteneği, ağ üzerinde güvenlik fonksiyonlarının daha esnek bir şekilde yerleştirilmesini sağlayabilir. Çünkü bu durum ek aygıtlar kurmadan SDN özellikli ağ cihazlarında güvenlik fonksiyonlarını etkinleştirmemizi sağlar. Ayrıca SDN, ağ genelinde daha iyi izlenebilirlik sağlayacağından, güvenlik açısından ağ genelinde görünürlüğü artıracaktır. Bu yetenek bütünsel bir bakış açısı sunar ve böylece internette yaygın olarak gerçekleştirilen ağ taraması veya dağıtık hizmet engelleme (Distributed Denial of Service, DDoS) saldırıları eski ağ izleme sistemlerine göre daha verimli bir şekilde kavranabilir. SDN ayrıca programlanabilirliği daha gelişmiş ağ güvenliği işlevlerinin geliştirilmesine yardımcı olabilir. Çok fazla çaba sarf etmeden bir prototip güvenlik sistemi kolayca uygulanabilir. Bu nedenle yeni ve gelişmiş ağ güvenliği işlevlerinin gelişimini hızlandırmakta SDN özelliklerinden yararlanılabilir [16].

SDN teknolojisi sunduğu avantajlara rağmen, anomali saldırıları, izinsiz giriş saldırıları, DoS saldırıları gibi birçok saldırı türüne karşı savunmasız olabilir [8]. Kötü niyetli kullanıcılar, erişim kontrol politikasını yeniden yapılandırabilir ve uygun şekilde hazırlanmış paketlerle kontrol politikalarını atlatabilir. Bir dizi sanal IP adresini tarayan kötü niyetli bir kullanıcı, uygulanan yük dengeleme politikasını yeniden yapılandırabilir ve belirli

bir fiziksel ağ kaynağını devre dışı bırakmak için, belirli sanal IP adreslerine yönelik bir DoS saldırısı başlatabilir [101].

Geleneksel ağlarda erişim kontrolü için bağımsız sistemler kurmak gerekliyken SDN'in dinamik akış kontrolü sayesinde erişim kontrolü de dinamik şekilde uygulanabilir. Bu sayede güvenlik duvarı, bal küpü gibi ek sistemler, yerini SDN'in kendi yetenekleriyle oluşan uygulamalara bırakabilir. SDN'in merkezi kontrol ve izleme özelliklerini temel alarak, her ağ cihazından ağ istatistiği bilgileri toplanabilir ve akış isteği mesajları alınarak ağ geneli kolayca izlenebilir. Bir ağ uygulamasından istek mesajları gönderilerek ağ istatistikleri bilgileri kolayca yakalanabilir ve bir ağ uygulaması, ağ aygıtlarından gelen akış isteklerini analiz ederek genel ağ topolojisi ve yönlendirme bilgilerini anlayabilir. Ağ yöneticisi ağ durumu değişikliğini izleyerek ağ genelinde saldırıları tespit etmek için anomali analizi yapabilir. SDN'in ağ genelindeki görünürlüğünün yardımıyla, ağ akışının nereden geçtiği ve güvenlik cihazlarının nereye yerleştirildiği anlaşılabilir. Ağ akışlarının bazı gerekli ağ güvenliği cihazlarından geçmelerini sağlamak için ağ akışları yeniden yönlendirilebilir. Bütünsel ağ görüntüsü aynı zamanda ağ saldırılarının tespit edilmesini ve savunulmasını kolaylaştırır. Ek donanım kutuları veya programlar satın almak yerine mevcut teknolojilerin kullanıyor olabilmesi, maliyet açısından da SDN'i geleneksel ağlara göre ön plana çıkaran bir unsurdur [16].

SDN, programlanabilirlik özellikleri sayesinde çeşitli güvenlik saldırılarına karşı savunma çözümleri sunar. Ancak SDN kullanımının bir sonucu olarak ortaya çıkan yeni tehditler de bulunmaktadır. Kötü niyetli kullanıcılar erişim kontrol politikasını yeniden yapılandırabilir ve SDN'deki güvenlik açıkları tüm ağı tehlikeye atabilir ve performansı düşürebilir. SDN'e yapılan saldırılar, kontrolcü, sanal makineler ve sanal anahtarlar gibi farklı ağ bölgelerinde gerçekleşebilir. SDN ile birlikte ortaya çıkan bazı yeni saldırılar da bulunmaktadır. Veri katmanında SDN cihazlarının iletişimi sırasında sahte trafik akışları oluşturulabilir. Bu saldırı meşru akışların sahte kimliği veya cihazın sahte kimliği kullanılarak gerçekleştirilebilir. Veri katmanında ayrıca SDN anahtarları da trafiğin içeri veya dışarı akışında saldırılara maruz kalabilir. Anahtarların kontrolcüyle haberleşmesi esnasında yapılacak saldırılar da bu duruma örnek olarak gösterilebilir. Doğrudan kontrolcüye veya kontrol katmanıyla uygulama katmanı cihazları arasındaki kuzey arayüzüne yönelik saldırılar da gerçekleştirilebilir. Özetle SDN'in getirdiği yenilikler ek güvenlik sağlayabilmekle birlikte, yeni yapısı sebebiyle yeni tür saldırılara da maruz kalabilir [8].

Kontrol katmanına yönelik saldırılar, veri katmanındaki anahtarları, kuzey arayüzünü, güney arayüzünü ve uygulama katmanını içeren çeşitli modüllerden yönlendirilebilir. DoS / DDoS, anomali ve izinsiz giriş saldırıları kontrol katmanında meydana gelebilecek olası saldırılardır. Sanal anahtarlar yalnızca paketleri iletme gibi temel görevleri gerçekleştirme yeteneğine sahiptir. Ancak anahtarlara yönelik tehdit tüm ağda büyük bir hasara neden olabilir. DoS, DDoS, sahtekârlık saldırıları ve izinsiz giriş saldırıları, veri katmanıyla ilişkili bazı saldırılardır. Uygulamaların başarısızlığı, kötü amaçlı uygulamaların enjeksiyonu, anomali ve izinsiz giriş saldırıları gibi yazılımla ilgili saldırılar uygulama katmanındaki en yaygın tehditlerdir. Güney ve kuzey arayüzleri, katmanlar arasındaki iletişimi sağlamada önemli bir rol oynamaktadır. Arayüzlere yapılan saldırıların çoğu diğer katmanlarda gerçekleşen saldırılara benzer. Arayüzün ele geçirilmesi durumunda, sistemdeki kötü niyetli trafiğin ileri ve geri akışı sağlanabilir [8].

SDN'de güvenlik araştırmaları diğer alanlar odağında gerçekleştirilen güvenlik araştırmalarına göre daha azdır. Ancak SDN'in içerdiği basitleştirilmiş yönetim ve diğer yeni özellikler sayesinde ağ güvenliğinin geliştirilmesine katkı sağlayabileceği değerlendirilmektedir [16]. Öte yandan bahsi geçen yeni özelliklerin doğrudan saldırıların hedefi haline gelmesi de mümkün olabilir.

SDN güvenlik araştırmaları, birçok farklı türde saldırı ve protokole odaklanmıştır. Örneğin, saldırgan bir kontrolcü yardımıyla yeni bir akış tablosu oluşturarak yeni kuralları ağa iletebilir veya LLDP paketleri aracılığıyla kullanıcıların zayıf noktalarından yararlanarak ağ yanıltılabilir veya konum sahteciliği oluşturabilir [17]. Sağlam bir altyapıda, anahtarlar ve kontrolcüler arasındaki kimlik doğrulama hizmeti güçlü bir şekilde sağlanmalıdır. Aksi halde trafiğin saldırgan tarafından incelenmesi mümkün hale gelir [18]. Saldırgan, akış tablolarını değiştirerek SDN kullanan bir ağ ortamında DoS saldırısı gerçekleştirebilir [16]. Ayrıca smurf saldırısı, fraggle saldırısı, DNS yükseltme saldırısı vb. saldırı türleri ile DoS saldırıları gerçekleştirilebilir. Bu tür saldırılarda kontrolcünün devre dışı kalma olasılığını azaltan yöntemler geliştirilmiştir [19]. Ayrıca ARP zehirleme saldırısı kullanılarak SDN'in en merkezi ve en önemli parçası olan kontrolcünün kimliği değiştirilebilir ve tüm ağ elemanları aldatılacağı için ağ ele geçirilmiş sayılabilir [20].

Bir başka saldırı türü olarak saldırı kaynağının tespiti ile ağın işleyişini etkileyecek faktörler için planlar oluşturulabilir ve sistemlerin siber güvenlik seviyeleri arttırılabilir. Örneğin

kaynak tespiti en zor olan DoS saldırısının kaynağının ve türünün belirlenmesi son derece önemlidir. Araştırmacılar bu amaçla derin öğrenme yöntemlerini kullanarak çalışmalar gerçekleştirmiştir [102]. Bu açıdan bakıldığında SDN adli bilişim çalışmaları ile siber güvenlik çalışmalarının birbirini destekleyerek büyümeye devam ettiği söylenebilir.

Gerçekleştirilen araştırmalar neticesinde 5G ağlarının çekirdek ağ yönetimi, ağ kontrolü, ağ izlemesi, ağın esnek hale getirilmesi ve ağ güvenliğinin sağlanması gibi açılardan SDN ile doğrudan bağlantılı olduğu değerlendirilmiştir. IP tabanlı iletişimin SDN ile yönetildiği 5G ağlarında ağ üzerinden gerçekleşen işlemlere dair adli bilişim çalışmalarının da SDN altyapısı ile gerçekleştirilmesi gerekmektedir.

3. 5G AĞLARINDA ADLİ BİLİŞİM

Bu bölümde öncelikle genel ağ adli bilişim süreçleri üzerine bilgiler aktarılmaktadır. Ardından 5G ağları ve SDN ortamlarındaki adli bilişim çalışmalarına dair bilgiler aktarılmaktadır. Adli bilişim üzerine gerçekleştirilen idari ve hukuki çalışmalar hakkında bilgilerin aktarılmasının ardından da tez çalışmasının literatürle karşılaştırılması gerçekleştirilmektedir.

3.1. Ağ Adli Bilişimi

Ağ analiz çalışmaları ağ üzerinde gerçekleştirilen işlemlerin sayısı arttıkça değer kazanmaktadır. Kurumlarda/şirketlerde bilgi güvenliğini sağlamak amacıyla güvenlik duvarı, IDS vb. yapılar kullanılmakta olup bu cihazların geliştirilmesinde de ağ analiz çalışmalarının yeri büyüktür. Çünkü bu cihazların engelleyemediği veya tespit edemediği atakların ardından yapılan çalışmalarda saldırganın nasıl atak yaptığı veya hangi cihazlara sızdığı gibi birçok bilgi elde edilebilmekte ve bu bilgiler kullanılarak ağ güvenlik cihazlarına güncellemeler geçilebilmektedir. Bu da ağ analizi konularında çalışmalar yapılmasını ve bu çalışmaların günden güne büyüyerek devam etmesini zaruri kılmaktadır [103].

Dijital adli analizlerde genellikle durağan bilgiler üzerinde çalışmalar gerçekleştirirken, ağ analizlerinde durum farklıdır ve akışkan bilgiler üzerinde de çalışmalar yapılabilmektedir. Ağ analiz çalışmaları paketlerin tamamının yakalanıp depolandığı veya sadece belirli verilerin yakalanarak depolandığı iki başlık altında incelenebilir. Tüm adli analiz çalışmalarında olduğu gibi ağ analizi çalışmalarında da, hukuksal zemine uyum sağlanması amacıyla, olayın zaman bilgisinin güvenilir bir şekilde ve güvenilir ortamlarda tutulması gerekmektedir. Ağ analizi genel itibariyle ağ üzerinde akan verinin canlı olarak veya kaydedildikten sonra incelenmesidir. Bir ağ ortamına veri sağlayan güvenlik duvarı, IDS, IPS, DNS sunucusu, anahtarlar, yönlendiriciler, vekil sunucu vb. gibi ağa dâhil olan tüm cihazlardan elde edilebilecek her türlü veri adli analiz işlemlerinde kullanılabilir. Saldırgan tespit edilirse, tespitinden sonraki tüm adımları incelenmeli ve tüm faydalı deliller toplanmaya çalışılmalıdır. Ağ analizi saldırganın aktiviteleri üzerine odaklanmalıdır. Fakat yerel ağın bu şekilde kontrol altına alınmasının yanı sıra İSS tarafında da bilgiler yer almaktadır ve İSS'nin de üzerine düşen sorumluluklar bulunmaktadır [24].

Ağ analizi esnasında “Ne yaşandı?”, “Neden yaşandı ve kim yaptı?” ve “Saldırı esnasında ne kadar zaman harcandı ve hangi saldırı teknikleri kullanıldı?” sorularına cevap aranmaktadır. Ağ analiz teknikleri proaktif ve reaktif yöntemler olmak üzere ikiye ayrılmaktadır. Proaktif ağ analizi, ağ saldırıları esnasında yani saldırılar tespit edildiğinde canlı analiz yapılan yöntemdir. Analiz üzerindeki yükü (maliyeti) ve zamanı azaltmaktadır. Analiz esnasında elde edilen delilleri az olabilmekle birlikte karar verici mekanizmaya yardımcı olmaktadır. Tüm fazları incelendiğinde hazırlık, tespit etme, olay tepkisi, toplama ve ele geçirme, koruma, kopyalama ve transfer etme gibi aşamalar içeren yöntemler sunulmuş farklı analiz süreçleri bulunmaktadır. Reaktif ağ analizi ise geleneksel bir yöntemdir ve saldırı yapıldıktan sonra analiz işleme konulduğundan dolayı daha fazla zaman ve maliyet almaktadır. Tüm fazları incelendiğinde inceleme, rapor, analiz, soruşturma, sunum, kimlik, koruma, karar verme ve toplama gibi aşamalar içeren farklı süreçleri bulunmaktadır [25].

Anomali tabanlı ağ saldırı tespit sistemlerini eğitmek ve değerlendirmek için etiketli veri setleri gereklidir. Paket tabanlı veri genellikle pcap formatlı olur. Geçiş kontrol protokolü (Transmission Control Protocol, TCP), kullanıcı veri bloğu iletişim kuralları (User Datagram Protocol, UDP), internet kontrol mesaj protokolü (Internet Control Message Protocol, ICMP) ve IP gibi farklı protokoller olmakla birlikte, TCP güvenli bir taşıma protokolüdür. Sağlama, bayraklar, sıra numarası gibi özellikleri vardır. UDP ise başlığında kaynak, hedef, uzunluk ve sağlama olarak dört alan içerir. Akış temelli veride ön tanımlı olan beş tanımlama grubu kaynak IP adresi ve port, hedef IP adresi ve port ile taşıma protokolüdür. Akış tabanlı formatlara Netflow, IP-FIX, sFlow ve OpenFlow örnek verilebilir. Veri setlerinde genel kavram FAIR (Findability, Accessibility, Interoperability and Reusability) olarak adlandırılmıştır ve bilimsel verilerin yerine getirmesi gereken dört prensibi tanımlamaktadır: Bulunabilirlik, Erişilebilirlik, Birlikte Çalışabilirlik ve Yeniden Kullanılabilirlik [26].

Adli bilişim süreçleri beş aşamada ele alınmaktadır. Bilgi edinme, strateji oluşturma, delil toplama, analiz ve raporlama olarak beş farklı adımdan oluşan ve literatürde kabul görmüş olan bu yönteme OSCAR (Obtain information, Strategize, Collect evidence, Analyze and Report) adı verilmektedir. Bu yöntemde elde edilen veya üretilen verilerin FAIR ilkesine uyumlu olması beklenmektedir [26, 104]. Bir adli bilişim sürecinin OSCAR ile uyumlu çalışıyor olması ve verilerinin FAIR kapsamına uygun olması zorunlu bir gereksinimdir.

3.2. 5G Ağlarında Adli Bilişim Çalışmaları

Ağ saldırılarının çeşitliliği artmaktadır. Buna istinaden kendilerini savunabilen veya saldırıların başlatılmasını önleyebilecek anlık kararlar alabilen ağlar oluşturmaya yönelmek gerekmektedir. Bu amaçla, ağların yapısını ve yapılandırılmasını yalnızca bir saldırı sırasında değil, saldırıdan önce de dinamik olarak değiştirmek için hareketli hedef savunma mekanizmalarının sistemlere uygulanmasına başlanmıştır. Böylece ağ keşfi yapmanın daha zor hale gelmesi düşünülmektedir. Ayrıca bir savunma mekanizması olarak saldırıların kaynağının ve türlerinin belirlenmesine yardımcı olmak için çeşitli ağ adli bilişim mekanizmaları oluşturulmaktadır. Gelişen SDN ve NFV teknolojileri bahsedilen mekanizmaları verimli bir şekilde uygulamak için fırsatlar sunmaktadır. Bu kapsamda araştırmacılar İSS bağlamında konuyu ele almışlar ve NFV yardımıyla sahte ağlar oluşturarak çözüm önerilerinde bulunmuşlardır. Bu sayede DoS ataklarına karşı keşif paketleri dinamik bir şekilde değiştirilebilir ve adli amaçlar için kullanım gücünü artırabilir [105].

5G ağlarında adli bilişim ve delil elde etme aşamaları SDN ve NFV üzerinden elde edilen bilgilerden geçmektedir. Ağ işlemleri üzerine yönlendirmeler SDN katmanında olduğundan, temel olarak SDN'den elde edilen bilgiler kullanıcıların internet erişimlerine dair bilgiler vermesi açısından yeterli olarak değerlendirilebilir. Ağların ve ağ fonksiyonlarının sanallaştırılmasıyla birlikte, bağlı olan sanal sunucular üzerindeki süreçler için de karmaşık bir yapı oluşmuştur. Sanal sunucu göçü ve sanal ağ arayüzü gibi yeni süreçler paket yakalama süreçleri açısından zorluklar içerebilir ve daha fazla detay sürece ihtiyaç duyulabilir. SDN'deki adli bilişim süreçleri kendi başına karmaşık bir yapıya sahipken farklı ağ dinamikleri de eklenince adli bilişim zorluk seviyesi artacaktır. Örneğin sanal ağ altyapısında yeni bir sanal özel ağ (Virtual Private Network, VPN) işletilmesi durumunda da tüm iletişim modu değişebilir ve paket yakalama süreci zorlaşabilir. Bu kapsamda SDN üzerinden elde edilen temel bilgilerin adli bilişim açısından çok kıymetli olduğu değerlendirilmektedir [106].

5G'nin büyük yapısı ele alındığında proaktif adli bilişim çözümlerinin uygulanmasının doğru olacağı düşünülmektedir. Saldırı esnasında sadece karşılık vermekle yetinmeyip, bu saldırılara ve kullanıcı erişimlerine dair ileride delil oluşturabilecek verilerin de toplanıyor olması tüm adli bilişim çalışmalarında olduğu gibi 5G adli bilişiminde de önem arz eder. 5G

adli bilişiminde ağın her an adli bilişim çalışması yapmaya hazır olması gerekmektedir. Aksi durumda erişim ve saldırılara dair bilgilerin elde edilmesi mümkün olmayacaktır. Saldırı ve erişim öncesinde ve esnasında adli bilişim çalışmalarının gerçekleştirilmesi proaktif adli bilişim çalışmaları olarak değerlendirilebilir. 5G adli bilişim çalışmalarında elde edilecek bilgiler, ağ yapısında SDN kullanılıyor olması sebebiyle uygulama katmanı, kontrol katmanı ve veri katmanından elde edilecek bilgiler olarak üç farklı katmanda ele alınabilir. Ayrıca bir diğer veri elde etme konumu olarak son kullanıcıların da dikkate alınması fayda sağlayabilir. Ancak bu durum çok farklı üreticiden gelen, farklı tür ve formatta verilerden dolayı adli bilişim süreçlerinde merkezi olarak rol alamaz. Daha önce adli bilişim odağında farklı açılardan incelenmiş olan akıllı telefonlar için dahi uygulanması kolay olmayan bu sürecin, adli bilişim çalışmaları çok kısıtlı olan akıllı araçlar, sağlık uygulamaları gibi diğer kullanım alanlarında uygulanabilmesi daha da zor bir süreçtir. Ağ adli bilişim çalışmalarının kapsamının geniş tutulmaması performans, kalite ve veri büyüklüğü açısından önemlidir. 5G ağlarında adli bilişim uygulanması için en az veri boyutuyla en fazla anlamlı verinin elde edilmesi üzerine kurgulanan bir adli bilişim sistemi gerekmektedir [107].

5G'de adli bilişim çalışmalarının ağlar dışında kalan bir kısmı ise mobil şebeke üzerinden gerçekleştirilebilir. Daha önceki mobil iletişim nesilleri için yapılan çalışmaların bir kısmı 5G için geçerli olsa da bazı farklılaşmalar mevcuttur. Gerçekleşen iletişimde kaynak ve hedef bilgileri, kullanılan servisler vb. bilgiler kolluk kuvvetleri tarafından talep edilebilir. Bu kapsamda tanımlayıcı olarak IMSI, uluslararası mobil cihaz kodu (International Mobile Equipment Identity, IMEI), mobil istasyon uluslararası abonelik dizin numarası (Mobile Station International Subscriber Directory Number, MSISDN) gibi bilgiler kullanılabilir. Kanuni müdahale (Lawful interception, LI) gerektiren durumlarda bir kimlik numarası atanarak bu sabit değer de kullanılmaktadır (LI identification number, LIID). Operatörler kullanıcı trafiği ve sinyal trafiği olarak iki farklı mobil veriyi elde edebilirler. Kullanıcı trafiği LEMF formatında (ses veya pcap dosyaları) tutulur. Sinyal trafiği ise IRI (Interception-Related Information) referansıyla farklı IRI formatlarında tutulabilir ve bu sayede kaynak ve hedef telefon numarası, arama süresi, arama zamanı gibi bilgilere erişim sağlanabilir. İletişim içeriğinde yer alan ses dosyaları farklı ses tanıma teknikleri kullanarak çözümlenebilmektedir. Ayrıca farklı teknikler kullanarak kullanıcıların konumlarının bilinmesine dair adli bilişim yöntemleri de uygulanabilir [28]. Yine mobil tarafta yer alan başka bir husus da ardışık girişim iptalidir (Successive interference cancellation, SIC). Alıcı tarafındaki veri alımı sürecinde aynı anda gelen paketlerin kod çözümlemesine dair olan bu

işlemin güvenli şekilde gerçekleşmesi için özel anahtar mekanizmaları devreye sokulmalıdır. Aksi durumda adli bilişim çalışmalarına yanıltıcı bilgiler sağlanmış ve haberleşme güvenliği tehlikeye atılmış olacaktır [108]. 5G kablosuz ağlarına yönelik olarak IMSI yakalama-sayfalama, kimliği doğrulanmamış IMEI talebi saldırıları, kullanıcı ve ağ arasındaki kimlik doğrulama süreçlerine yönelik ataklar da sistemin güvenliğini ve adli bilişim çalışmalarını tehlikeye atabilir. Bu kapsamda anahtar yönetimi sürecinin güçlendirilmesi gerekmektedir. 5G adli bilişimi ve güvenliğinin birlikte yorumlanarak ve araştırılarak geliştirilmesi gerekmektedir [109]. Bu kapsamda yol haritalarının belirlenmesi, 5G'ye yönelik uygulanabilir risk senaryolarının ve fırsatların sistematik şekilde uygulamaya dâhil edilmesi gerekmektedir. Fiziksel katman güvenliği, veri paylaşımı ve mahremiyet konularında geliştirme sağlanmalı, uçtan uca güvenlik çözümleri üzerine geliştirmeler gerçekleştirilmelidir [110]. 5G'nin mobil altyapısındaki çalışmalar, 5G çekirdek ağlarını odağına alan bu tezin kapsamı dışındadır.

Geleneksel ağlar için geçerli olan tehdit türleri 5G ağları için de geçerliliğini korumakta olup 5G ağları için yeni tehditler de oluşabilir. Bilişim altyapısına ve iletişimin sürekliliğine büyük zararlar veren DDoS atakları 5G ağlarında da güncelliğini çeşitli yeni yöntemlerle devam ettirmektedir. Bu saldırı türüne karşı etkin ve yeni savunma yöntemlerinin de devreye alınması gerekmektedir. Ancak cihaz sayısının yüksek olması ve işlenen verinin büyüklüğü ve çeşitliliği bu saldırı türüne dair bilgi elde etmeyi zorlaştırmaktadır. 5G ağlarında DoS saldırılarına karşı adli bilişim süreçleri için de SDN kullanılabilmektedir. Farklı katmanlardan elde edilen bilgiler sayesinde saldırıların sistemin herhangi bir bölgesine aşırı yük bindirmeden tespit edilebilmesi mümkündür [111].

3.3. SDN Ortamlarında Adli Bilişim

SDN ortamlarının güvenliğini sağlamayı hedefleyen ve tüm süreci mevzuatlar kapsamında otomatik şekilde işleten bir adli bilişim sisteminin tasarımı için çalışmaya siber güvenlik, adli bilişim, hukuk ve yazılım/sistem mühendisliği pencerelerinden bakılması gerekmektedir.

SDN odaklı güvenlik çalışmaları gerçekleştirilmiş olsa da adli bilişim açısından SDN çalışmalarının yetersiz olduğu görülmektedir [23]. Geleneksel ağlarda kullanılan teknikler SDN saldırılarını tespit etmek için de yeterli değildir. Ancak veri boyutu, trafik izleme,

kontrol katmanının olayların merkezinde yer alması gibi yeniliklerinden dolayı, SDN olay esnasında veya sonrasında inceleme yapılması için yenilikler getirecektir. Bunlardan öte SDN adli bilişiminin kontrolcü ele geçirme, tek kontrolcü bulunması, mimari eksiklikler, yetkisiz veri değişikliği, iletişim doğrulama eksikliği, ağ kaynakları sınırı gibi dikkate alınması ve geliştirilmesi gereken yönleri de bulunmaktadır [21].

Adli bilişim bakış açısıyla güvenlik sorunlarını tespit etmek ve kayıtları sağlıklı bir şekilde elde etmek önem taşımaktadır. SDN özelinde durum öncelikle, ilgili verilerin ağın hangi konumlarından elde edilebileceğidir. Her SDN katmanı şüpheli hareketlere karşı delil olabilecek bilgiler içerebilir. Uygulama katmanında şüpheli uygulamalardan gelen ataklarla ilgili olarak uygulama programlama arayüzü (Application Programming Interface, API) ve çeşitli uygulamalar vasıtasıyla üretilen kayıtlar kullanılabilir. Kontrol katmanındaki kullanıcı takip sistemi IP adresi, fiziksel adresi (Media Access Control, MAC), yerel alan ağı (Local Area Network, LAN) kimliği ve konum bilgileriyle ilgili bilgiler sunar. Veri katmanında da OpenFlow tablolarıyla kaynaktan hedefe giden ağ akışları bilgileriyle çeşitli adli bilişim faaliyetlerinde bulunulabilir.

Adli bilişimin gelişmesi için güvenlik çalışmalarının da gelişmesi gerektiğini öngördüğümüz SDN alanında bazı araştırmacılar güvenlik analizinin ötesine geçerek sistem gereksinimlerini çözebilecek modüller geliştirmiştir. Örneğin web istatistiklerini çıkarmak için web sunucusu erişimlerini analiz eden Python tabanlı POX kontrolcüsünde bir modül geliştirilmiştir. Adli bilişim alanına hizmet edeceği düşünülebilecek bu modül sayesinde SDN altyapısında web trafiği ve web dışı trafik akışlarını ayırt etmek mümkündür. Makine öğrenmesi kullanılarak eğitilen “scikit learning” isimli algoritmada ağaç topolojisinin kullanıldığı bir ortamda anomali tespit ederek POX kontrolcü üzerinde ping flood saldırı paketlerinin engellenebileceği gösterilmiştir [112]. OpenFlow kullanarak TCP'nin güneye giden arayüze yeniden iletim zaman aşımını kullanarak DoS saldırıları deneyi gerçekleştirilmiş ve bu konuda yaşanan güvenlik açıkları test sonuçlarında ortaya koyularak dayanıklı bir model önerilmiştir [113].

Kontrolcü, yapının merkezinde olduğundan en önemli delil noktalarındandır. Ancak kontrolcü en büyük hedef olduğundan, direkt saldırı altında olduğunda sağlıklı veri üretemeyebilir. Uygulama katmanında farklı standartlarda veriler üretilebilir ancak OpenDaylight kontrolcüsü Open Services Gateway initiative (OSGi) mimarisi kullanarak

uygulama kayıtlarını alabilmektedir. Altyapı katmanında anahtarlar kullanılarak şüpheli trafiğin üretildiği portlar tespit edilip engelleme vb. işlemler gerçekleştirilebilir. Kuzey ve güney arayüzleri kontrolcüyü uygulamalara ve altyapıya bağlayan yerler olduğundan haberleşme kayıtlarını kullanarak adli bilişimde faydalı olabilirler [114].

OpenFlow tabanlı mimari, güney arayüzü olarak en yaygın kullanılan SDN mimarisidir. OpenFlow temelli SDN platformlarının adli bilişim açısından incelenmesi için yapılan bir çalışmada bir çerçeve sunulması istenmiş. Bu hedef için Mininet üzerinde sanal bir SDN ortamı kullanılmıştır. Güney arayüzü verilerini içeren pcap dosyalarının ve anahtarların hafıza görüntülerinin analizi ve karşılaştırılması, adli delillerin başarılı bir şekilde alınmasını sağlamıştır. SDN kontrolcüsünün, yönlendirici ve anahtarların vb. her bileşenin kaydını tutmak elbette ki adli bilişim açısından yeterli verinin olacağı anlamına gelse de bu denli büyük bir veriyi kontrol etmek ve anlamlandırmak zordur. Bu sebeple bir şekilde çoğu verinin geçeceği güney arayüzü üzerinde çalışmanın daha doğru ve az veri almak açısından yerinde bir tercih olacağı yapılan çalışmada tespit edilmiştir. Fakat yasalar da göz önüne alındığında SDN anahtarlarının belleklerinin de alınmasının yerinde olacağı belirtilmiştir. Veri madenciliği çalışmaları ile verinin daha anlamlı hale getirilmesi de sağlanabilmektedir. Çalışmalarda veri elde etmek için farklı yollar denenmiş ve ilgili veriler Wireshark ortamında incelenmiştir. Bu aşamada üç farklı SDN kontrolcüsü (OpenDaylight, Floodlight ve Ryu) kullanılmıştır. Deneylerin sonucunda güney arayüzünün veri elde etmek için en iyi bölge olduğu görülmüştür. Pyhton tabanlı bir aracın da üretildiği bu çalışmada OpenDaylight kontrolcüsünün adli bilişim açısından en başarılı sonuçları verdiği anlaşılmıştır [23].

Adli bilişim çalışmaları için yeni bir adli bilişim katmanı önerisinde bulunulan bir çalışma da mevcuttur. İlgili çalışmada kuzey arayüzü kapsam dışı tutulmuş, kuzey arayüzü dışında ayrıca merkezi bir katman konularak ağ cihazları tarafından üretilen veriler incelenirken, SDN yapısına dağıtılmış durumda olan katmanda ise kontrolcünün güncellenmesi esnasında enjekte edilen değiştirilmiş bilgileri keşfetme işlemleri gerçekleştirilir. Tasarlanan katmanda bu bilgiler sürekli paylaşılıp yorumlanmaktadır [115].

Başka bir çalışmada ise Ryu kontrolcünün, Mininet ve OpenFlow ile birlikte olduğu bir ortamda bazı saldırı türlerinin (DoS attack, flow table overflow, host location hijacking, link fabrication attack vb.) denemeleri 6 kullanıcı, 6 anahtar ve 1 kontrolcüden oluşan bir ortamda 100 Mbps (Megabits per second) bant genişliği ile gerçekleştirilmiştir. Çalışmada

kontrolcülerden elde edilen veriler üzerinde yeterli düzeyde durulmadığından da bahsedilmiştir. Yapılan saldırılarda servisin neden çöktüğü, kurbanın kim olduğu, saldırının ne zaman olduğu, saldırının ne zaman gerçekleştiği sorularına cevap aranmıştır. Elde edilen pcapng dosyalarının özeti de çalışmada bilgi olarak paylaşılmış durumdadır. Bu çalışmada daha çok veri katmanı ile kontrol katmanı arasındaki farklara değinilmiş olup güney ara yüzü ve veri katmanı arasındaki farkların detayları çalışmada yer alan tablolardan elde etmek mümkün olmamıştır. Çalışmada ayrıca farklı OpenFlow sürümlerinin ve çok sayıda farklı kontrolcünün olduğuna da vurgu yapılmıştır. Bu çalışma sonucunda DoS ataklarının tespiti için kontrolcüde oluşan kayıtların faydalı ve yeterli olacağından bahsedilmiştir. Ancak akış tablosunun geçici olmasından dolayı topoloji zehirleme ataklarının kontrolcülerde tutulmasının zor olacağından bahsedilmiş. Saldırılarda veri katmanı ve kontrolcü katmanında hangi bölgelerin (arayüz, port, anahtar, kontrolcü vb.) zarar gördüğü bilgisi de verilmiştir [116].

Forcon ismi verilen diğer bir çalışmada araştırmacılar güney arayüzü ve OpenvSwitch anahtarlardan elde ettiği bilgilerle “Sanal Ağ Adli Bilişim Süreci” isimli bir adli bilişim yöntemi geliştirilmiştir. Bu çalışmada da ağ üzerinden akan paketlere odaklanılmış olup kontrolcüden gelen kayıtlar göz ardı edilmiştir. Çalışmada Ryu ve Floodlight kontrolcüleri seçilmiştir [117].

Bir başka çalışmada ise akış kurallarının ağa bağlı bir kullanıcı tarafından tahmin edilebilir olduğundan bahsedilmektedir. OpenFlow kurallarının üzerine kurgulanmış ağ politikalarının kötü niyetli bir kullanıcı tarafından kullanılabileceği ve daha fazla kötü niyetli saldırı amacıyla kullanılabileceği belirtilmiştir ve bu çalışmada uygulanan tekniklerle bu tarz durumların önüne geçilebileceği gösterilmiştir [101].

Bir diğer çalışma kapsamında ise güvenlik vb. bir sebeple bağlantı ve paket iletiminde yaşanan eksiklikleri kontrol ve veri katmanında arayarak durumun sebebini arayan “Forenguard” isimli bir adli bilişim aracı geliştirilmiştir. Bu sistem Floodlight kontrolcü üzerine yerleştirilmiş ve gerçek kontrol katmanı ataklarının teşhisinde kullanılmak için, kontrol ve veri katmanlarının arasında tasarlanmıştır. Sonuçların SDN açısından fayda sağladığı gösterilmiştir. Geliştirilen araç, çıkarım tabanlı yaklaşım yöntemini kullanarak, kontrol ve veri katmanlarındaki tüm faaliyetleri izleme yeteneğine sahiptir [118].

SDN adli bilişimi için “SDNForensics” adlı bir çerçeve önerilmiştir. SDN adli bilişim alanında daha önce çok fazla çalışma yapılmadığının vurgulandığı bu çalışmada güvenlik perspektifi dikkate alınarak SDN'in farklı seviyelerinde adli bilişim uygulamaları yapılmıştır. Çalışma zamanı logları, hafıza ve ağ paketlerinin üç farklı katmandan alındığı çerçevede, kullanıcılardan hafıza bilgilerinin ve logların toplanması öngörülmektedir. Bu çalışma, farklı ortamlardan ve kullanıcılardan elde edilen verilerin tek bir formata getirilmesini önermektedir. Elde edilen verilerin güvenlik alanında kullanılabilmesi için makine öğrenmesi yöntemleri ile anomali tespiti yapılabileceği, güvenlik tetikleyicilerinin oluşturulabileceği ve nihai verilerin doğru formatlarda ve veri tabanlarında saklanması gerektiği belirtilmiştir [119].

Bir başka çalışmada ise SDN programlama dilleri, SDN simülatörleri, ağ güvenliği, ağ yönetimi ve SDN kontrolcüleri kapsamında literatürde gerçekleşen çalışmalar ele alınmış ve ötesinde SDN kullanım tekniklerine dair kıyaslamalar gerçekleştirilmiştir. Bu çalışmanın ana kapsamı adli bilişim olmasa da, adli bilişim özelinde yapılacak çalışmalara ilham verebilecek bir yapıdadır. SDN deneyleri gerçekleştirirken ve SDN uygulamaları geliştirirken faydalı olabilecek bilgiler içeren bu çalışma, tez kapsamında incelenecek olan SDN kontrolcülerin yapılarına dair bilgiler de içermektedir. Ağ adli bilişiminde ağ cihazlarından bilgi toplamanın suç kanıtlarını doğrulamak için etkin bir yöntem olduğu belirtilen bu çalışmada SDN kontrolcülerinin adli bilişim odaklı karşılaştırmalı analizi gerçekleştirilmemiştir [120].

Geleneksel ağlar için gerçekleşen adli bilişim çalışmaları, yapısal yenilikler içeren SDN için doğrudan uygulanabilir değildir ve yeni yöntemler gerektirir [22]. Özetle güvenlik çalışmaları kadar yeterli olmayan SDN adli bilişim çalışmalarında [23] ise adli bilişim için; yeni katman ve teknolojiler öneren, servis dışı bırakma saldırılarında iz süren, istatistikleri toplamayı hedefleyen, makine öğrenmesi, derin öğrenme temelli yöntemlerle saldırıları kontrolcü tabanlı engelleyen çalışmalar gerçekleştirilmiştir [112, 113, 115, 119, 121]. Güney arayüzü, delil elde etmek için en iyi bölgelerden birisidir, ancak veri katmanıyla kontrol katmanı arasında iletişimi sağlayan güney arayüzünde işletilen ağ süreçleri saldırganların ilk hedefleri arasındadır [22, 23]. Tüm SDN katmanları adli bilişim açısından faydalı bilgiler içeriyor olsa da kontrol katmanı, sistemin merkezinde yer aldığından delil elde etme açısından önemli bir konumdadır. Kontrolcü saldırı altındayken büyük bir yük altında olacaktır. Bu durumda hizmet verme aşamasında eksiklikler yaşanabilir [122]. Bu katman

saldırı esnasında yoğun bir yük altında olabileceğinden, gerekli tüm delilleri üretemeyebilir [101, 114, 116]. Bu durum göz önüne alındığında, kurulacak adli bilişim sisteminin kontrol katmanına yük bindirmeyen yapıda olması ve veri toplamak için sadece kontrol katmanına odaklanmamış olması gerekir [117, 118]. Sadece SDN ortamından değil, işletim sistemi, hafıza ve günlük dosyaları gibi çevre birimlerden alınan kayıtlar da suçların aydınlatılması açısından önemli bir yer tutabilir [48, 119].

Gerçekleştirilen çalışmalarda çok fazla verinin farklı ortamlardan elde edilmesi prensibine dayalı süreçler önerilmiş olsa da, SDN adli bilişimi için teknik olarak hangi katmana nasıl bir süreçle odaklanılması gerektiğini belirten çalışmalar mevcut değildir.

3.4. İdari ve Hukuki Çalışmalar

Uluslararası çapta ülkeler özelinde gerçekleşen çalışmalar [33–41] SDN için adli bilişim politikalarının yeterli düzeyde olmadığını göstermektedir [123]. Ülke temelli uygulamaları değerlendiren çalışmalarda, adli bilişim açısından bir ülke stratejisini ve ülke temelli adli bilişim süreçleri için yol gösterici bilgi rehberlerini oluşturma dışında standart ağ adli bilişim süreci çalışmalarının bulunmadığı görülmektedir [30, 32]. Asya ülkelerinin siber suçlara yönelik cezaların artırılması yönünde adımlar attığı görülse de [41] tüm ülkeler arasında standart bir süreç üzerinde uzlaşı ve sınır ötesi iş birliğinin gerekli olduğu değerlendirilmiştir [37]. Ancak kişisel verilerin ülkeler arasında paylaşılması durumunun nasıl ele alınması gerektiği büyük bir sorun olarak karşımıza çıkmaktadır. Bir adli bilişim kurumunun eksikliği, adli bilişimde töre gibi bölgesel olarak etkili olan, yazılı olmayan kuralların da dikkate alınması konuları her ülke özelinde değerlendirilmesi gereken konular olarak karşımıza çıkmaktadır [39, 40]. Uluslararası mecrada kabul görmüş bir standart olan ISO 27001'de, ilgili ülkedeki mevzuatın kurumlar tarafından açıkça tanınması ve uygulanması gerektiği belirtilmiş olup ülkelerin kendi mevzuatı ve uluslararası anlaşmalar doğrultusunda doğan uygulamalarına uyum sağlanması gereklilikleri belirtilmiştir. Ayrı bir bakış açısı olarak yazılım geliştiren şirketlerin anti adli bilişim politikaları, bazı durumlarda suçların aydınlatılmasının önüne geçmekte olduğundan [43] küresel adli bilişim çalışmalarında ülkeler, çerçeve kuruluşlar ve şirketlerin ortak paydada buluşması son derece önemlidir.

Devletlerin internet erişimleri üzerinde tam bir hâkimiyet kurması teknik açıdan zor ve hatta bazı durumlarda mümkün olmayan bir durumdur. Ancak devletler bazı kanunlar yardımıyla

siber suçlarla mücadele etmeyi hedeflemektedir. Siber suçlara örnek olarak izin alınmaksızın sistemlere girilmesi, içeriklerin değiştirilmesi, zararlı programların yüklenmesi ve sistemin çalışmasının engellenmeye çalışılması verilebilir [59]. Siber suçları aydınlatmak amacıyla Türkiye'de erişim kayıtlarını tutma zorunluluğu verilen yapılar; internet servis sağlayıcıları, web hizmeti sunarak içerik sağlayanlar, sosyal içerik sağlayıcıları ve bünyesindeki kişilere ticari veya ticari olmayan yollara internet erişimi sağlayan toplu kullanım sağlayıcılarıdır [56, 57, 61–63]. Bu yapıların trafik bilgilerini kayıt altına almaları ve mevzuatta belirtilen süre kadar güvenli ve yedekli bir yapıda saklamaları gerekmektedir. Doğruluk, bütünlük ve gizlilik ölçütlerinin sağlanarak, elektronik imza ile imzalanarak ve zaman damgalı şekilde muhafaza edilmesi gereken bu kayıtların mevzuatta belirtilen sürelerin sonunda yok edilmesi gerekir. Aksi durumunda bu sürecin yetkililerine bir ile iki sene aralığında hapis verilmesi cezası uygulanmaktadır [59, 124]. Kişisel verilerin korunmasına dair mevzuatta detaylarına da yer verilen verilerin yok edilmesi süreci, verilerin geri döndürülemez şekilde silinmesini ifade etmektedir [125, 126]. Avrupa Birliği'nde (AB) de kişisel verilerin korunması amacıyla GDPR (General Data Protection Regulation) yürürlükte olup, geliştirilecek SDN ortamlarında bu düzenlemeye de uyum sağlamak gereklidir [123, 127].

Adli bilişimin hukuki ayağına ilişkin yapılan çalışmaların da yeterli sayıda olmadığı ve hiçbir ülkenin kendi mevzuatı doğrultusunda bir adli bilişim sürecine sahip olmadığı görülmüştür. Bu doğrultuda tez kapsamında bir ağ adli bilişim süreci oluşturulacak olduğundan mevzuat ve uluslararası uygulamalara dair bilgilerin detayı tezin beşinci bölümünde aktarılacaktır.

3.5. Tez Çalışmasının Literatürle Karşılaştırılması

Tez kapsamındaki çalışmaları ana hatlarıyla; SDN kontrolcülerinin kıyaslanması ve SDN tabanlı 5G ağlarındaki adli bilişimin durum tespiti, ağ adli bilişim süreci geliştirilmesi ve SDN tabanlı 5G ağlarında uyumlu adli bilişim sistemi geliştirilmesi olarak üç ana başlıkta ele almak mümkündür.

Süreç oluşturmak için yeterli teknik veri olmadığından öncelikle SDN kontrolcülerinin kıyaslanması çalışmaları gerçekleştirilmiştir. Bu kapsamda gerçekleştirilen saldırı türleri daha önce literatürde ele alınmış saldırılar değildir. Ayrıca dört farklı kontrolcüyle bu deneylerin gerçekleştirildiği çalışma da bulunmamaktadır.

İncelenen kaynakların ötesinde en çok kullanılan kontrolcülerden, daha önce üzerine adli bilişim açısından çalışma tespit edilemeyen ONOS kontrolcüsü ve az sayıda çalışma yapılmış olan Ryu kontrolcüsünün de aralarında bulunduğu dört farklı kontrolcünün kullanıldığı deney ortamlarında saldırı simülasyonları gerçekleştirilmiştir. Saldırı esnasında kontrolcülerin, sanal anahtarlardan ve güney arayüzünden elde edilen paketlerin ne tür bilgiler içerdiği, sadece veri katmanından elde edilen bilgilerde ne gibi farklılıklar bulunduğu ve bu farkların kontrolcü değişimleriyle ne denli değiştiği adli bilişim bakış açısıyla incelenmiştir. Kontrolcüler arasındaki farklar ve kontrolcülerin birbirlerine karşı üstünlükleri bu bakış açıları ile ortaya konulmuştur. Ayrıca bu saldırılar sayesinde, yapılacak yeni çalışmaların temellerinin daha sağlam atılabileceği düşünülmektedir.

Ağlarda akan verinin büyüklüğü mesajlaşma programlarındaki çok küçük boyutlu mesajlardan, çok yüksek kalitedeki videoların indirilmesine kadar bir çerçevede düşünüldüğünde çok büyük bir adli analiz verisi oluşacaktır. Adli bilişim incelemeleri için incelenecek veri boyutunun düşük olması saldırıların anlık tespit edilebilmesi açısından da önem arz eder. Bu sebepten tezin bu aşamasındaki deneylerde mümkün olan en az boyut ve sayıdaki paket arasından, adli bilişim açısından en anlamlı iletişim verisinin elde edilmesine odaklanılmıştır. Farklı kontrolcülerin kullanıldığı test ortamında ağ adli analiz çalışmaları standartlarına göre çalışmalar gerçekleştirilmiştir. Elde edilen veriler bulunabilir, erişilebilir, birlikte çalışılabilir ve yeniden kullanılabilir olarak paket tabanlı ve akış temelli olarak elde edilmiş ve sonuçlar bu bakış açıları ve ağın genel topolojisi de göz önüne alınarak yorumlanmıştır.

Özetle tezin ilk aşaması olan SDN kontrolcülerinin kıyaslanması ve SDN tabanlı 5G ağlarında adli bilişim durum tespiti sürecinin sonucunda, hem saldırı türleri hem de hizmet sunma kalitesi açısından farklılıklar görülmüştür. Literatürdeki bazı çalışmalarda, gerçekleşen olaylara dair zaman bilgisinin elde edilemediği görülse de tez kapsamındaki deneylerin tamamında güney arayüzü ve sanal anahtarlardan zaman bilgisi elde edilebilmiştir. Bu çalışmalar hem veri katmanı hem güney arayüzü verilerini her kontrolcü değişiminde ele alması ve paket sayısı ile paket boyutu açısından kıyaslamasıyla da literatürden farklı bir noktaya gelerek katkı sunmaktadır [117]. Adli bilişimdeki en iyi kontrolcüyü seçen çalışmaların aksine [23], gerçekleşen deney sonuçları hem elde edilmesi hedeflenen bilgilerin değişmesi hem de paket boyutu farklılıkları görüldüğünden dolayı herhangi bir kontrolcünün adli bilişim açısından en başarılı olarak nitelendirilemeyeceğini

ispatlamıştır. Bu durum ayrıca bir SDN adli bilişim standardına olan ihtiyacı da göstererek literatüre katkı sunmaktadır.

Elde edilen bulguların ardından tez çalışmalarına ağ adli bilişimi standart süreci oluşturma aşamasıyla devam edilmiştir. Ağ adli bilişimiyle ilgili olabilecek olan 5651 sayılı Kanun ve ilgili yönetmelikler, Türk Ceza Kanunu (TCK), Ceza Muhakemeleri Kanunu (CMK), Elektronik İmza Kanunu, ISO 27001 standardı, CBDDO (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi) rehberleri, Uluslararası çapta ülkeler özelinde yapılan çalışmalar, elektronik deliller ve bilirkişilik süreçleri incelenmiştir. Bu incelemelerde ağ adli bilişimini ilgilendirebilecek tüm bilgiler aktarılmış ve bu bilgiler dikkate alınarak idari ve teknik gereksinimleri aktaran bir ağ adli bilişim süreci oluşturulmuştur.

Bu kapsamda teknik olarak hangi verilerin kayıt altına alınması gerektiği belirlenmiştir. Erişim kayıtlarının tutulması dışında kalan diğer teknik gereksinimler olarak ise zaman damgasının tüm sistemler için tek bir referans kaynağa uyumlu şekilde kullanılması, kritik verilerin yurt içinde depolanması, zararlı veya yasaklı olan hedeflerin de kısmi olarak veya tamamen engellenebilmesi, özetleme, şifreleme ve yedekleme yöntemleriyle kayıtların belirlenen süre kadar saklanması, bilgi güvenliği ihlallerine karşı etkin mekanizmaların oluşturulması mevcuttur [56].

Ulusal ve uluslararası kaynaklar arasında herhangi bir ülke mevzuatına, uluslararası uygulamaları da dikkate alarak uyum sağlayan başka bir ağ adli bilişim süreci bulunmadığından tez ile doğrudan kıyaslanabilecek bir çalışma bulunmamaktadır. Süreçte hangi erişimlerin kaydedilmesi ve muhafaza edilmesi gerektiği, nasıl bir silme yöntemine tabi olunması gerektiği, trafiğin engellenmesi ve yetkilendirme gibi çok sayıda konuda öz bilgilerle yönlendirmeler gerçekleştirilmiştir. Oluşturulan süreç alanında bir ilk özelliği taşımaktadır. Süreç hem geleneksel ağlara, hem SDN ortamlarına hem de 5G ağlarına uygulanabilir durumda olup hem tezin son aşamasında geliştirilen adli bilişim sistemine hem de gerçekleştirilecek diğer adli bilişim süreci çalışmalarına yol gösterecek niteliktedir.

Mevzuatta belirtilen adli bilişim aşamalarının teknik olarak hangi yöntemlerle gerçekleştirileceği veya kayıt formatının hangi türde olacağı belirtilmemiştir [56–65]. Bu durum tek bir üreticiye bağımlı teknolojilerin kullanmasını engellemek ve en güncel tekniklere uyum sağlamak açısından avantaj sağlayacaktır. Ancak her kurumun/şirketin üst

düzey teknik bilgi birikimi ve insan kaynağı bulunmamaktadır. Tezin son aşamasında geliştirilen sistem, insan faktörünü aradan çıkararak süreçlerin sağlıklı ve güvenli işlemesini sağlayacak, en güncel yöntemlerin hızlı bir şekilde sisteme dâhil edilmesiyle ücretsiz ve güncel şekilde hizmet sunabilecektir. Bu sayede insan faktöründen kaynaklı gerçekleşen eksiklikler yüzünden hapis veya para cezası gibi yaptırımlar olmayacak ve SDN tabanlı 5G ağlarında sağlıklı bir ağ adli bilişim süreci gerçekleştirilebilecektir.

Mevzuat birbirine uyumlu bir şekilde geliştirilmiş olsa da, mevzuatta çok sayıda teknik detayın verilmediği ve süreçlerin ana hatlarının tarif edilmesinin ardından, idaresinden sorumlu kurum veya kişilerin kararına bırakıldığı görülmüştür. Bu sebepten öncelikle süreç kapsamında belirlenen log toplama işlemlerinin, özetleme, şifreleme, yedekleme, elektronik imzalama, yok etme adımlarının hangi yöntemlerle gerçekleştirileceği belirlenmiştir. Literatürdeki çalışmalarda bu süreçlerin hangilerinin en başarılı olduğuna dair çalışmalar mevcuttur. Çalışmalar kapsamında adli bilişim süreçlerinin hem hızlı hem de güvenilir olması adına seçimler gerçekleştirilmiş ve sürecin detayları da belirlenmiştir. Bu durum oluşturulan ağ adli bilişim süreçlerinin SDN veya 5G ortamlarına uygulanırken hangi yöntemlerin tercih edilebileceği durumuna açıklık getirmiştir. Seçilen yöntemlerin sisteme uygulanması için alt sistemler kurulmuş olup, sistemin geliştirilmesi ve otomatikleştirilmesi ilk defa gerçekleştirilen çalışmalar olarak yerini almaktadır. Zararlı web sayfalarının sadece SDN yetenekleri kullanılarak engellenebilmesi ve servis dışı bırakmaya yönelik saldırıların SDN ortamından alınan akış tabanlı verilerle engellenebilmesi de daha önce gerçekleştirilmemiş araştırmalardır. Ayrıca uluslararası veri tespitini SDN yetenekleriyle yaparak ülke tabanlı uyarı üreten bir sistemin oluşturulması da bilindiği kadarıyla alanda ilk özelliği taşımaktadır. Deney sonuçları çok az sistemsel kaynakla tüm gereksinimlerin sistem tarafından yapıldığını ispatlamış olup, kişi ve kurumlardan bağımsız olarak çalışan bu sistemin istenmeyen idari yaptırımların da önüne geçeceği düşünülmektedir.

Dijital delillerin elde edilmesi sürecinin sağlıklı bir şekilde işletilmesi, delillerin hukuka uygun olması açısından kritiktir. İşletim sistemleri, güvenlik donanımları, sanal anahtar kayıtları, kontrolcü kayıtları, silinmiş veriler, rastgele erişimli bellek (Random Access Memory, RAM) vb. uçucu veriler gibi delil kaynaklarına yönelmektense, hali hazırda mevzuatta belirtilen yapılar tarafından kaydı tutulmak zorunda olan veriler üzerinden adli bilişim çalışmalarının yürütülmesi teknik açıdan daha kolay bir süreçtir [128]. Adli bilişim çalışmalarının OSCAR ilkesine ve bu kapsamda kullanılan verilerin FAIR ilkesine uyumlu

olması beklenmektedir [26, 129]. Oluşturulan sistem sayesinde veriler OSCAR yöntemine uygun şekilde otomatik olarak toplanacaktır. Bu sayede adli süreçlerde bilirkişilerin görevleri de kolaylaşacak ve süreçlere fayda sağlanmış olacaktır [60].

Daha önce mevzuata uygun herhangi bir ağ adli bilişimi sistemi geliştirilmediğinden, alanında bir ilk özelliği taşıyacak olan sistemin oluşturulması aşamasında kullanılan yöntem ve teknikler tezi altıncı bölümünde aktarılacaktır. Sistem teknolojik gelişimle birlikte hızlı bir şekilde güncellenebilecek farklı ve ücretsiz alt sistemlerden oluşmaktadır.

4. SDN KONTROLCÜLERİNİN ADLİ BİLİŞİM SÜREÇLERİNE ETKİSİNİN İNCELENMESİ

5G ağlarının temelini oluşturan SDN teknolojisinin uygulama, kontrol ve veri katmanı olarak üç katmanından da anlamlı veriler elde edilebilir. Bu verilerin her biri hem güvenlik hem de adli bilişim açısından kıymetli olabilecek verilerdir. Ancak adli bilişim çalışmalarının hız, veri boyutu ve veri kalitesi açılarından yüksek bilgi sunacak şekilde tasarlanması gerekmektedir. SDN'de kontrol katmanı ve kontrolcü merkezi durumda olduğundan ağın genel işleyişinden sorumludur. Bu sebepten 5G ağlarının da yönetiminden sorumlu olan SDN kontrolcülerinin adli bilişim açısından kıymetli veriler içerebileceği ön görülmektedir. Ancak gerçekleştirilen araştırmalar sayıca kısıtlı olduğundan dolayı SDN kontrolcüsü odaklı bir adli bilişim sisteminin 5G güvenlik servisleri ve güncel güvenlik açıkları da dikkate alınarak detaylı incelemesinin yapılması gerektiği değerlendirilmiştir.

SDN kontrol katmanında kullanılabilecek çok sayıda kontrolcü bulunmaktadır. Bu kontrolcüler temel aldıkları standartlar bakımından benzerdir. Ancak yazılım geliştirme aşamaları veya uygulanan tekniklerden kaynaklı olarak aralarında hız, güvenlik, altyapı uyumu vb. açılardan farklılıklar bulunabilir. Bu sebepten kontrolcü için en önemli ağ verileri arasında yer alan güney arayüzü verilerinin adli bilişim açısından yeterli olup olmadığının belirlenmesi bu bölümde gerçekleşen çalışmaların ana eksenini oluşturmaktadır. Çalışmanın bir diğer amacı da rutin iletişim ve siber saldırılar altında farklı kontrolcüleri karşılaştırarak adli bilişim açısından en iyi kontrolcünün seçilip seçilemeyeceğini belirlemektir. Bu amaçların ötesinde adli bilişim açısından önemli hususlar olan, adli analiz işlemlerinin minimum veri boyutu ve paket sayısı ile yürütülmesine dair durum tespiti de çalışmada tüm süreçlerde ele alınmıştır.

Soruşturmaların odak noktası sadece rutin iletişim sırasında oluşan trafiğe değil, aynı zamanda farklı saldırılar sırasındaki trafiğe de odaklanmaktadır. Deney senaryoları, SDN ortamlarından yalnızca bilgi tespitinin elde edilebilmesi yaklaşımın ötesindedir. Paket türü ve boyutu, saldırı ve saldırgan tespiti, zaman bilgisi tespiti gibi adli bilgi açısından önemli olan diğer konular açısından da karşılaştırmalar yapılmış ve sonuçlar sunulmuştur.

Farklı SDN kontrolcülerini güncel ağ saldırı senaryoları altında detaylı olarak karşılaştıran ve bu konuları adli bilişim standartları açısından değerlendiren bu bölümdeki çalışmaların yeni katkılarının ayrıntılı bir açıklaması aşağıda verilmiştir:

- Literatürde ilk kez dört farklı kontrolcü ile rutin haberleşme, port tarama ve saldırı senaryoları üzerinden güney arayüzü odaklı adli bilişim deneyleri gerçekleştirilmiştir.
- Deneysel işlemlerde daha önce adli bilişim açısından incelenmemiş olan ONOS kontrolcü de incelenmiştir.
- Bu çalışma, adli bilişim süreçlerinin en önemli parametrelerinden olan paket boyutu ve sayısı odaklı olarak güney arayüzü verilerinin adli analiz süreçleri için yeterli olup olmadığının incelenmesini içermektedir.
- Aynı SDN altyapısında kontrolcünün değiştirilmesi işleminin adli analizlerde farklı sonuçlar verdiği gösterilmiştir.
- Dört farklı kontrolcü üzerinde ilk kez yapılan deneyler sonucunda ortaya çıkan ve adli bilişim açısından önemli olan paket boyutu, sayısı ve yüzdesi bilgileri paylaşılmış olup kontrolcülerin adli bilişim yetenekleri özetlenmiştir.
- Her kontrolcü için siber saldırılar sırasında hizmet sürekliliği analiz edilmiştir.
- İlgili çalışmalardan farklı olarak bu çalışma, seçilen dört kontrolcüden herhangi birinin adli bilişim açısından tüm süreçleri kapsayacak kadar iyi olmadığını göstermektedir.
- Sonuçlar, standart bir adli süreç ve yöntemin gerekli olduğunu göstermektedir.

4.1. Adli Bilişim Deneyleri

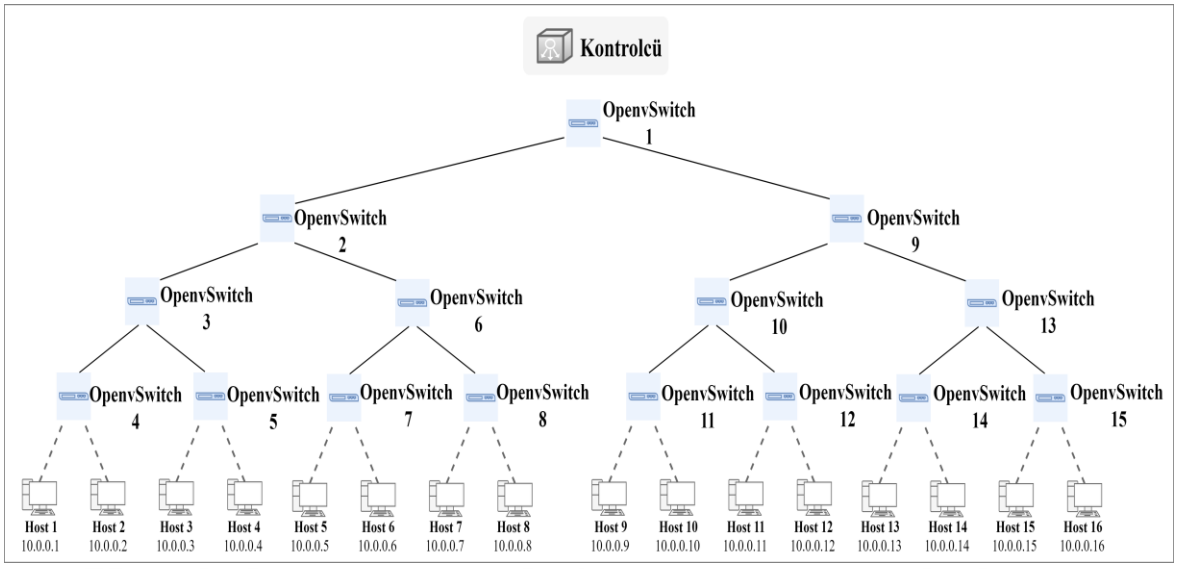
Bu çalışma kapsamındaki deneylerde literatürden farklı olarak her bir kontrolcü ve deney için paket sayıları ve yüzdeleri verilmiş ve karşılaştırılmalar gerçekleştirilmiştir. Bu kontrolcüler için yapılan deneylerde elde edilen güvenlik düzeyi ve hizmet kesintisi durumu dikkate alınarak adli bilişim açısından herhangi bir kontrolcünün en iyi olarak değerlendirilip değerlendirilemeyeceği araştırılmıştır. En önemli yeni katkılardan birisi de çalışmanın temel amaçlarından birini oluşturan güney arayüzü verilerinden elde edilebilecek verilerin kontrolcüler ve deneyler kapsamında karşılaştırılması olmuştur.

4.1.1. Altyapı bilgileri ve genel yöntem

Bir sanal sunucu ortamında Mininet [130] yardımıyla kurulan SDN topolojisinde ağaç topolojisi kullanılmış olup 16 kullanıcı, 15 sanal anahtar ve 1 kontrolcüden oluşan sanal ortam oluşturularak deneyler gerçekleştirilmiştir.

Ryu [89], ONOS [92], OpenDaylight [91] ve POX [90] kontrolcüleri ilgili ortamdaki deneylerde kullanılmıştır. ONOS ve OpenDaylight kontrolcüleri Java tabanlıyken, Ryu ve POX kontrolcüleri Python tabanlıdır. Ryu modülerlik ve ağa uyum sağlamada, ONOS çoklu iş süreçleri yönetiminde, OpenDaylight ölçeklenebilirlikte, POX ise tutarlılıkta avantaj sağlamaktadır. Öte yandan Ryu ve ONOS tutarlılık açısından, OpenDaylight başka bir kontrolcü platformuna (Cisco ONE) dayalı şekilde geliştirilmesi açısından ve POX ise ölçeklenebilirlik açısından dezavantaj sağlamaktadır. Bu SDN kontrolcülerinin adli bilişim açısından birbirlerine olan üstünlükleri, SDN ortamının değişik katman ve arayüzlerinden elde edilebilecek deliller odağında geniş bir deneysel süreçle daha önce incelenmemiştir. Gerçekleştirilecek deneyler sonucunda SDN kontrolcülerinin adli bilişim açısından birbirlerine göre üstünlük ve zayıflıklarının tespit edilmesi ve bu sayede geliştirilecek olan adli bilişim sisteminde ele alınacak yöntemlerin netleştirilmesi amaçlanmıştır [120]. Ortam altyapısında Ubuntu Masaüstü kullanılmış olup [131] sanallaştırma altyapısı olarak VirtualBox [132] üzerine kurulu ve 8 GB (Gigabyte) RAM, 4 sanal işlemci ve 150 GB disk kapasiteli bir sanal bilgisayar kullanılmıştır. Kurulumlar Intel Core i7- 10510U merkezi işlem birimi (Central Processing Unit, CPU) 1,8 GHz, 16 GB DDR4 RAM ve 500 GB kapasiteli katı hal sürücüsüne (Solid State Drive, SSD) sahip olan bir dizüstü bilgisayarda gerçekleştirilmiştir. Deneylerde sanal anahtar olarak OpenvSwitch [133] kullanılmıştır.

Deneylerde adli bilişim süreçlerini gerçekleştirmek amacıyla paket incelemeleri Wireshark [134] ile gerçekleştirilmiştir. Kullanılan diğer programlar ise Yersinia [135], Nikto [136], Iperf [137], Nmap [138], Netcat ve Hping3'tür [139]. Mininet yardımıyla kurulan SDN topolojisinde ağaç topolojisi kullanılmış olup 16 kullanıcı (10.1.1.1-10.1.1.16), 15 sanal anahtar ve 1 kontrolcüden oluşan sanal ortam oluşturularak denemeler gerçekleştirilmiştir. Ryu, ONOS ve POX kontrolcüleri Ubuntu 20.04 kurulu bilgisayar üzerine kurulu durumdayken, OpenDaylight kontrolcü Ubuntu 14.04 kurulu bilgisayar üzerinde çalışmaktadır. Şekil 4.1'de deneylerde kullanılan topolojinin gösterimi yer almaktadır.

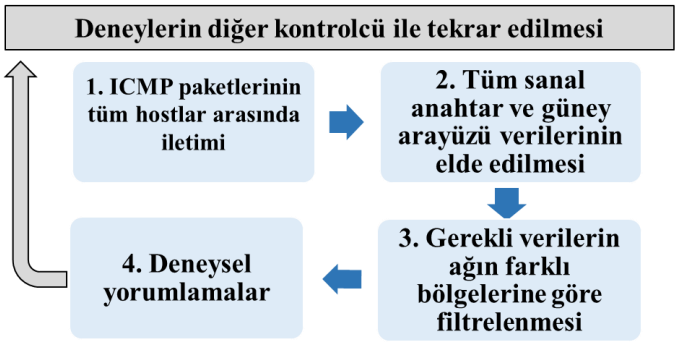


Şekil 4.1. Deney ortamı

Deneylere geçmeden önce tüm kontrolcü türlerinin bağlı olduğu topolojilerde Iperf yardımıyla bant genişliği ölçülmüştür ve hostlar (kullanıcı bilgisayarlar) arasında kontrolcü türüne bağlı değişiklikler olduğu görülmekle birlikte normal çalışma modunda en düşük 1,5 Gbit/s bant genişliği olduğu gözlemlenmiştir. Bu değerlerin yerel ağ ortamında yapılan bu çalışma kapsamında planlanan ölçüm ve çalışmaları yapmak için yeterli olduğu değerlendirilmiştir. Ayrıca kontrolcü değişikliğinin hostlar arasındaki gecikme değerlerini değiştirip değiştirmediği hususu da test edilmiş olup gecikme sürelerinin her kontrolcü için ortalama 0,1ms ile 0,25 ms arasında olduğu gözlemlenmiştir. En düşük gecikme süresi değerlerinin Ryu kontrolcüde ortalama 0,1 ms ile oluştuğu görülmüştür.

4.1.2. ICMP paketleri iletimi

İlk deney olarak tüm hostlar arasında eş zamanlı ICMP paketleri iletimi gerçekleştirilmiştir. En temel düzey sayılabilecek bu ağ haberleşmesinde, veri katmanından elde edilecek bilgilerde ve paket boyutlarında kontrolcülerin farklı olduğu topolojiler arasında ne gibi farklar oluştuğu gözlemlenmeye çalışılmıştır. Şekil 4.2'de tarif edilen deney süreci dört kontrolcü için de tek tek tekrarlanmıştır. Deneylerde SDN ortamındaki tek değişken SDN kontrolcüsü olup güney arayüzü ve sanal anahtarlar üzerindeki tüm veriler deneyler esnasında kayıt altına alınmıştır.



Şekil 4.2. ICMP paketleri iletimi adli bilişim deney süreci

Bu senaryoda kontrolcülerin farklı olduğu topolojilerde güney arayüzünden elde edilen veriler üzerinden zaman, kaynak, hedef gibi tüm bilgilere erişim sağlanmıştır. IP ve MAC adresleri bilgileri de tüm yakalamalarda elde edilebilmiştir. Güney arayüzünden elde edilen veriler Ryu, ONOS ve OpenDaylight kontrolcülerinin çalıştığı ortamlarda OpenFlow 1.3. paketi olarak karşımıza çıkmakta ve ek bilgi olarak yer alan "veri" başlığı altında gerekli bilgiler görülebilmektedir. POX kontrolcüde OpenFlow 1.0. kullanıldığından dolayı kaynak ve hedef adres bilgileri, pcap dosyalarında doğrudan görülebilir durumdadır.

Aynı iletişimi gerçekleştirmek için tüm trafiğe (tüm arayüzler ve güney arayüz toplamı) oranla en fazla güney arayüzü paket sayısı yüzdesinin %68,3 ile POX kontrolcüde olduğu görülmüştür. POX kontrolcüyü % 54,4 ile ONOS izlerken, üçüncü sırada %42,6 ile Ryu yer almaktadır. Büyük bir fark ile OpenDaylight kontrolcü tüm bilgileri elde etmesinin yanı sıra tüm paket sayılarının sadece %6,3'ü kadar güney arayüzü paketini kapsamaktadır.

Paket sayılarının yanı sıra paket boyutlarındaki fark da dikkat çekicidir. En fazla veri boyutu yüzdesinin (tüm arayüzler ve güney arayüz toplamı) %76,9 ile POX kontrolcüde oluştuğu gözlemlenirken en az veri boyutu yüzdesinin %14,7 ile OpenDaylight kontrolcüde oluştuğu görülmektedir. Yüzdelerin paket sayısı ile farklılık göstermesindeki ana sebep kontrolcülerin farklı olduğu durumlarda güney arayüzü üzerinde oluşan tekil paket büyüklüklerinin de birbirinden farklı olmasından kaynaklanmaktadır. Ortalama paket boyutunda ilgili senaryoda en düşük ortalama paket boyutu 137 Byte ile Ryu kontrolcüde gerçekleşmiştir. Çizelge 4.1 dört farklı kontrolcü için gerçekleştirilen deneylerde güney arayüzündeki paket sayısı ve boyutunun tüm trafik boyutuna oranını yüzdesel olarak göstermektedir.

Çizelge 4.1. ICMP paketleri iletimi adli bilişim deneyleri paket sayısı ve yüzdesi bilgileri

Kontrolcü	**Güney arayüzü paket sayısı (%)**	**Güney arayüzü paket boyutu (%)**
Ryu	42,6	61,6
ONOS	54,4	72
OpenDaylight	6,3	14,7
POX	68,3	76,9

Güney arayüzünden geçen paket kıyasında yukarıdaki durumlar göze çarparken host tarafındaki durum farklılık göstermektedir. En az sayıda güney arayüz paket sayısı üreten OpenDaylight'ın hostlarının bağlı olduğu arayüzler üzerinden, birebir aynı süreç için, en fazla sayıda paket ve en büyük boyutta veri geçmiştir. Host tarafında en az sayıda paket ve veri oluşturma durumu ise POX kontrolcünün olduğu senaryoda gerçekleşmiştir. Hostları üzerinden en büyük veri akışı olan OpenDaylight kontrolcüsündeki senaryoda hostlar üzerinden geçen veri boyutunun, hostlar üzerinden geçen veri boyutunun en az olduğu POX kontrolcüsünün 5,9 katı olarak gerçekleşmiştir.

Güney arayüzünden elde edilen verilerin adli bilişim için yeterli olarak görüldüğü bu senaryoda loglarının en az sayıda ve en küçük boyutlu oluştuğu senaryo OpenDaylight kontrolcüde gerçekleşirken, host odaklı log toplamada ise en az paket sayısının ve en küçük paket boyutunun oluştuğu durumun POX kontrolcü kullanılan senaryoda gerçekleştiği tespit edilmiştir.

Bu deney kapsamında sanal anahtarlara ek bir bakış açısı oluşturmak da yararlı olacaktır. Bu nedenle tüm sanal anahtarlar üzerinden veri akışının beklendiği bu deneyde anahtarlar arasındaki paketler üzerine çeşitli karşılaştırmalar da yapılmıştır. Deneysel topolojide, daha yüksek seviyedeki anahtarların (örneğin, sanal anahtar 2&9), topolojinin altında bulunan anahtarlardan (örneğin, sanal anahtarlar 4&5) daha yüksek (yaklaşık yüzde 5) paket sayısına ve boyutuna sahip olduğu gözlemlenmiştir (Bkz. Şekil 4.1). Ayrıca aynı seviyedeki anahtarlar arasındaki paketlerin sayısı ve boyutu aynı sayılabilecek kadar benzerdir.

4.1.3. Mesajlaşma içeriği elde etme

Paketlerin kaynak ve hedef bilgisi, paketin zaman bilgisi gibi detaylarının yanı sıra haberleşmeye esas olan paketlerin içeriğinde yer alan bazı bilgilerin güney arayüzünden elde edilip edilemediği hususu da kontrolcülerin adli bilişim açısından incelenmesinin önemli bir adımı olarak düşünülmektedir. Gerektiği durumlarda iletim sağlanan mesajların içeriğinin elde edilebilmesi de adli bilişim yönetimi açısından önemli bir yer tutmaktadır. Bu deneyde iki host arasında "netcat" yardımıyla, belirlenen bir port üzerinden mesajlaşma gerçekleştirilmiştir. Belirlenen bir port üzerinden host1 dinleme moduna alınmış olup host16 üzerinden host1'e anlamlı kelimeler içeren mesajlar iletilmiştir. Şekil 4.3'te de gösterildiği üzere güney arayüzü ve sanal anahtarlar üzerinden paketler yakalanmış ve yorumlamalar gerçekleştirilmiştir. Bu süreç tüm kontrolcüler için tekrarlanmıştır.



Şekil 4.3. Mesajlaşma içeriği elde etme adli bilişim deney süreci

Bu doğrultuda iletilen mesajlar esnasında ağda akan paketler üzerinde yapılan incelemede anahtarlar üzerinde adli bilişim açısından önemli olduğu düşünülen kaynak, hedef, zaman bilgisi vb. yanı sıra iletilen tüm mesajlaşma içeriğinin anlamlı halde yer almakta olduğu görülmüştür.

Bu duruma dair güney arayüzünde yapılan incelemelerde ise farklı bir sonuç görülmüştür. Test ortamında mesajlaşma süreci boyunca Ryu kontrolcünün çalıştığı ortamda hiçbir mesajın içeriğine güney arayüzü üzerinden erişilemedi. ONOS ve POX kontrolcülerinde ise mesajlaşmaya dair ilk iletilen mesajın içeriğinin görüldüğü tespit edilirken ilk mesajdan sonraki mesajların içeriği ağ akışında bulunamadı. Son olarak OpenDaylight kontrolcüsünün çalıştığı test ortamında ise güney arayüzü verileri üzerinde tüm mesajlaşma bilgilerinin yer

aldığı görülmüştür ve OpenDaylight kontrolcüsü bu deneyde mesaj içeriklerine ulaşma açısından en faydalı sonuçları vermiştir. Ancak Çizelge 4.2'de de görülebileceği üzere tüm senaryoya oranla en yüksek paket sayısı yüzdesinin OpenDaylight kontrolcünün kullanıldığı senaryodaki güney arayüzünde gerçekleştiği gözlemlenmiştir.

Çizelge 4.2. Mesajlaşma içeriği elde etme deneyleri paket sayısı ve yüzdesi bilgileri

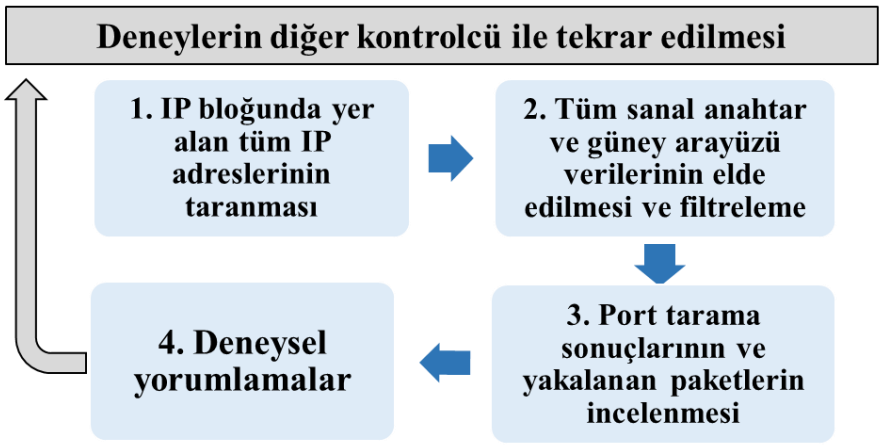
Kontrolcü	**Güney arayüzü paket sayısı (%)**	**Güney arayüzü paket boyutu (%)**
Ryu	57,7	60
ONOS	64,3	84,4
OpenDaylight	77,3	70
POX	49	62

4.1.4. Port tarama

Açık kaynak kodlu olan Nmap bir ortamdaki cihazları ve sunulan hizmetleri keşfetmek ve risk analizi yapmak için kullanılır. Nmap aracını kullanarak ağları taramak mümkündür. Bu taramalarda çeşitli zafiyetler ortaya çıkabilir. Genellikle saldırılardan önce ağı keşfetmek isteyen kötü niyetli kullanıcılar tarafından da nmap kullanılmaktadır.

Kurulan deney ortamında nmap ile tüm IP bloğu üzerindeki (10.1.1.0/24) tüm cihazlar sürüm bilgisi ve gecikme bilgilerini de içerecek şekilde bir taramaya tabi tutulmuştur. Şekil 4.4'te görüldüğü üzere, tarama esnasında Wireshark ile elde edilen tüm verilerin incelenmesi ve deney yorumlarıyla tamamlanmıştır. Dört kontrolcü de aynı topoloji kapsamında çalıştırılmış ve nmap taramaları sonucu en düşük gecikme OpenDaylight kontrolcünün çalıştığı ortamda tespit edilmiştir.

Tüm kontrolcü senaryolarında güney arayüzü üzerinden zaman, kaynak, hedef gibi gerekli tüm verilere erişim sağlanmıştır. Bu verilere erişimin yanı sıra zaman bilgisi de, kontrolcülerin değiştiği her senaryoda de yer alınmaktadır. Kontrolcüler üzerinden host 1'in IP adresiyle yapılan taramalarda sonuç elde edilemese de, detaylı filtreleme teknikleriyle MAC adresi kullanılarak yapılan aramalar sonuç vermiş ve ilgili IP adresi bilgilerine bu paketlerden erişim sağlanması mümkün olmuştur.



Şekil 4.4. Port tarama adli bilişim deney süreci

Çizelge 4.3'te gösterildiği gibi çalışmada en fazla paket sayısı ve ilgili testin tüm trafiğine göre yüzdesinin Ryu kontrolcünün çalıştığı ortamın güney arayüzünde görüldü. En az paket sayısı ve yüzdesinin ise OpenDaylight kontrolcüsünde oluştuğu görülmüştür.

Çizelge 4.3. Port tarama adli bilişim deneyleri paket sayısı ve yüzdesi bilgileri

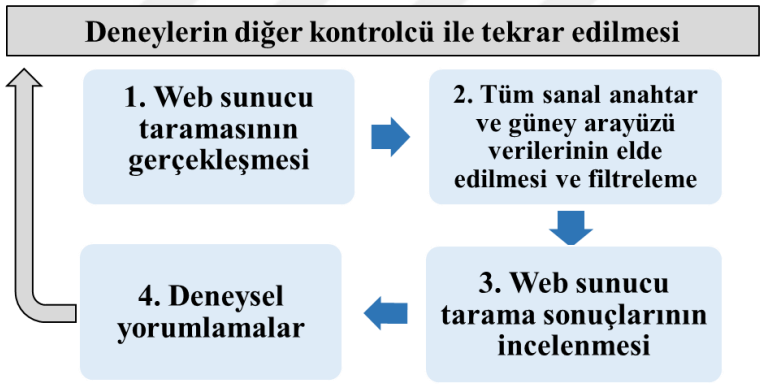
Kontrolcü	**Güney arayüzü paket sayısı (%)**	**Güney arayüzü paket boyutu (%)**
Ryu	56,6	80,2
ONOS	40,7	75,3
OpenDaylight	33,25	63
POX	44,6	69,7

Tarama IP adresi temelli olarak hostlara yönelik olmakla birlikte bu senaryoda hostların bağlı olduğu anahtar arayüzleri özelinde ortalama en düşük sayıda paketin oluştuğu ortamın Ryu kontrolcünün olduğu ortam olarak göze çarpmaktadır. 16 adet hostun bulunduğu Ryu'nun çalıştığı ortamda, aynı tarama için hostlar üzerinde biriken paket sayısı farkının 3 kata kadar vardığı tespit edilmiştir. Örneğin host 2'nin bağlı olduğu arayüzde 157 paket gözlemlenirken host 9'un bağlı olduğu arayüzde ise 479 paket gözlemlenmiştir. Aradaki paket sayısı farkı dikkat çekicidir. Bu duruma yakın oranlar POX ve OpenDaylight kontrolcüsünün çalıştığı ortamda da görülmekle birlikte ONOS kontrolcünün çalıştığı ortamda hostların bağlı olduğu arayüzlerden geçen paket sayılarının neredeyse aynı ve 525 paket sayısı civarında olduğu gözlemlenmiştir. Bu sonuç ise aynı ağ işlevlerinin sadece kontrolcü değişmesiyle birlikte ne denli bir fark oluşturabildiğini gözler önüne sermektedir.

Denemeler sonucunda sadece host tarafından elde edilecek verilerle bir adli bilişim sistemi kurulmak istenmesi durumundaysa Ryu kontrolcünün paket sayısı ve boyutu kapsamında daha avantajlı olacağı değerlendirilmiştir. Gerekli tüm bilgilere anahtarlar ve kontrolcü üzerinden erişilen bu denemede, güney arayüzü odaklı adli bilişimde taramalara karşı en düşük gecikmeyle, en az sayıda ve en düşük boyutlu paketlerle bu analizi yapabilen OpenDaylight kontrolcüsünün avantaj sağladığı görülmüştür.

4.1.5. Web sunucu taraması

Bu deney sürecinde topolojide yer alan bir host üzerine kurulan sunucuya karşı temel düzeyde güvenlik açıklıkları taraması yapan "nikto" isimli açık kaynak kodlu güvenlik zafiyet tarayıcısı kullanarak host 1 üzerinde çalışan web sunucusu için host 16'dan tarama gerçekleştirilmiştir. Süreç Şekil 4.5'te gösterildiği gibi tarama esnasında sanal anahtarlar ve güney arayüzünden paketlerin elde edilmesi, bu paketlerin incelenmesi ve yorumlanması şeklinde dört farklı kontrolcü için ayrı ayrı gerçekleştirilmiştir.



Şekil 4.5. Web sunucu adli bilişim deney süreci

Uygulama dört kontrolcünün bulunduğu topolojide aynı sonucu göstermiştir ve tarama sonuçları aynı çıkmıştır. Tüm senaryolardaki tarama sonuçlarında anahtarlar üzerinde de taramaları ortaya çıkaracak gerekli bilgilerin mevcut olduğu görülmüştür. Tarama sonuçlarında Ryu kontrolcünün bulunduğu senaryoda güney arayüzü paketleri tüm paketlerin sadece %0.1'ini içermekle birlikte zafiyet taramasına dair hiçbir bilgi tespit edilememiştir. OpenDaylight kontrolcüsünde ise paketler arasında paket yapısı itibariyle

şüpheli paket olarak nitelendirilen paketler tespit edilmekle birlikte paket detayında kaynak ve hedef adreslere ulaşılamamıştır.

ONOS ve POX kontrolcüsünün olduğu senaryolarda ise kaynak ve hedef adresleri, şüpheli paket tespiti ve zaman bilgisi gibi gerekli bilgilere erişmek mümkün olmuştur. ONOS kontrolcü senaryosunda güney arayüzünde bu tespit senaryodaki toplam paket sayısını %0,42'si ile gerçekleşirken, POX kontrolcü bu tespiti %35,4'lük bir oranla gerçekleştirmiştir. Bu durum ilgili senaryodaki adli bilişim açısından en uygun kontrolcü seçiminin ONOS olduğunu göstermiştir.

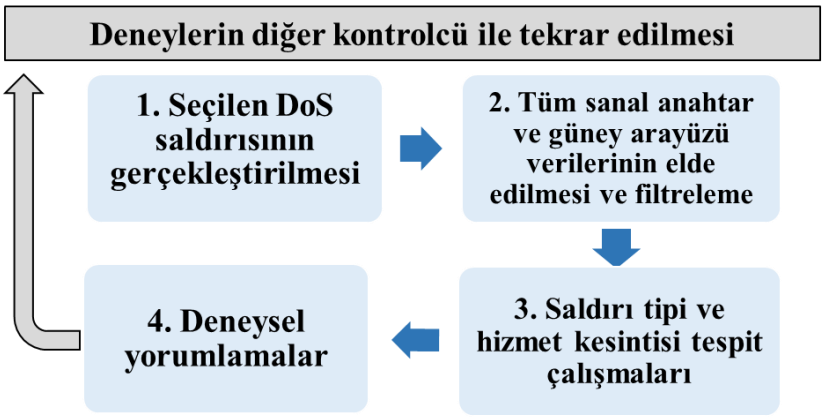
POX kontrolcüde web sunucu taramasının diğer deneylere göre 8-10 kat daha uzun sürmesi dikkat çekici bir durum olmuştur. Ayrıca POX kontrolcünün kullanıldığı deney ortamında ağ üzerinde dolaşan paket sayısının, Ryu kontrolcünün kullanıldığı deney ortamındaki paket sayısının üç katından, ONOS kontrolcünün kullanıldığı ortamdakininse iki katından fazla olduğu görülmüştür.

4.1.6. Hizmet engelleme saldırıları

DoS saldırılarının çok sayıda çeşidi olmakla birlikte, mevcut deney ortamına uygun olan üç farklı türü seçilmiş ve deneyler bu kapsamda gerçekleştirilmiştir.

TCP SYN seli – DoS saldırısı

Günümüzde sıklıkla maruz kalınan DoS ataklarının bir simülasyonu açık kaynak kodlu hping3 aracıyla gerçekleştirilmiştir. Bu saldırıda bir hosta sel halinde sahte kaynak IP adresine sahip paketler gönderilmiştir. Saldırı, saldırganın SYN paketlerini iletip SYN-ACK yanıtının alınmaması üzerine kurgulanan bir servis dışı bırakma saldırısıdır. Şekil 4.6'da deney süreci aktarılmış olup, önceki deneyler gibi saldırı esnasında yaşanan ağ akışı paket incelemesine tabi tutulmuştur. Saldırı esnasında saldırıya dâhil olmayan bir başka hosttan da saldırıya uğrayan host ve çevre birimlerdeki iletişimin kesilip kesilmediği tespit edilmeye çalışılmıştır. Yorumlamaların ardından aynı deney tüm kontrolcüler için tekrarlanmıştır.



Şekil 4.6. DoS saldırıları adli bilişim süreci

Tüm kontrolcüler için senaryolar tamamlanmış ve hiçbir senaryoda iletişimin kesilmediği gözlemlenmiştir. İletişimin kesilmemesinde hostlar arasındaki en düşüğü 1.5 Gbits/s olan bağlantının etkili olduğu değerlendirilmiştir. Saldırıya ait kaynak, hedef adres, zaman bilgisi gibi detaylar tüm kontrolcü senaryolarında güney arayüzü verilerinde saldırganın sahte IP adresi ile birlikte tespit edilmiştir. Paketler arasında "ACK Flag is not set" (ACK Bayrağı ayarlanmadı) uyarısı da görülmüş olup saldırı türü de bu bilgiyle birlikte ortaya çıkmaktadır.

Ryu kontrolcüsü senaryosunda toplam paket sayısının %0,02'siyle gerekli bilgilerin toplamıştır. Ayrıca ortalama paket boyutu ve toplam paket boyutu hususunda da bu atakta en düşük değerleri sağlamayı başarmıştır. Ryu senaryosunda güney arayüzü ortalama paket boyutu 119 Byte iken, en yüksek olarak gerçekleşen POX senaryosunda bu değer 285 Byte olarak gerçekleşmiştir.

STP (Spanning Tree Protocol) saldırısı

Bu saldırının ardından paket seli dışında farklı yöntemlerle de kontrolcülerde devre dışı bırakma atakları denemelerine devam edilmiş olup "yersinia" isimli araç iki farklı senaryoda dört kontrolcü için de tekrar adli bilişim incelemesine tabi tutulmuştur.

Bu saldırılardan ilki yersinia aracının yayılan ağaç protokolüne (Spanning Tree Protocol, STP) karşı hazırlanmış olan köprü protokolü veri birimleri (Bridge Protocol Data Unit, BPDU) atağı olarak gerçekleştirilmiştir. Katman 2 seviyesinde çalışan cihazlarda döngüleri engellemek için STP protokolü port durumlarını BPDU aracılığıyla paylaşmaktadır. Saldırı başlatıldığı anda saniyede yaklaşık 25.000 BPDU paketi hedefe servis dışı bırakma amacıyla

gönderilmektedir. Saldırı süreci bir önceki DoS saldırısı örneğinde olduğu şekilde gerçekleştirilmiştir (Bkz. Şekil 4.6).

Aynı topolojide aynı saldırı yapılmasına karşın OpenDaylight kontrolcü kullanılan senaryoda güney arayüzü üzerinde diğer kontrolcülere göre çok daha az sayıda paket oluşmuştur. Şüpheli paket bilgileri sahte kaynak adresleriyle tüm senaryolarda oluşmuştur ancak çok sayıda STP paketi güney arayüzünde diğer tüm kontrolcülerde gözükmesine rağmen OpenDaylight kontrolcüsünde gözükmeyerek saldırının tespiti adına eksik bilgi sağlamıştır.

ONOS senaryosunda tüm trafikteki paket sayısının %6,8'i ve toplam boyutun %11,6'sıyla ONOS kontrolcü gerekli bilgileri temin etmiş ayrıca diğer kontrolcülerin kullanıldığı senaryolarda saldırı esnasında iletişim devre dışı kalmasına rağmen ONOS kontrolcünün kullanıldığı senaryoda iletişimde hiç devre dışı kalma durumu olmamıştır.

CDP (Cisco Discovery Protocol) saldırısı

Son olarak yersinia aracının Cisco keşif protokolüne (Cisco Discovery Protocol, CDP) karşı hazırlanmış olan CDP tablosu atağı gerçekleştirilmiştir. İşletim sistemi sürümü ve IP adresi gibi doğrudan bağlı, CDP'yi destekleyen diğer ağ cihazları hakkında bilgi paylaşmak için kullanılır. Atağın temel amacı kısa sürede çok sayıda komşuluk isteğinin kurban cihaza ulaşması ve kaynakların tükenerek görevleri yerine getirmemesi, nihayetinde sistemin servis dışı kalmasına yol açmaktır. Süreç yine önceki DoS saldırılarında tarif edildiği şekilde gerçekleştirilmiştir (Bkz. Şekil 4.6).

STP saldırı senaryosunda olduğu gibi bu saldırıda da ONOS kontrolcünün kullanıldığı durumda bir servis dışı kalma durumu yaşanmadı. Ancak farklı olarak bu defa ONOS kontrolcü senaryosunda güney arayüzü verilerinde saldırının izine rastlanılmadı. Bu durum OpenDaylight için de geçerliyken Ryu ve POX kontrolcülerin güney arayüzlerinde CDP paketlerinin sel halinde geldiği görülmekteydi. Detaylı yapılan incelemelerde çok sayıda farklı kaynaktan gelen, şüpheli paketlerin yanı sıra doğrudan CDP paketi türünde görülen ve adli analiz yapan kişiyi rahatlıkla yönlendirebilecek olan paketler yer almaktaydı. Saldırılar boyunca POX senaryosunda iletişim devre dışı kalmış ve hiç geri gelmemiştir. Ryu senaryosunda iletişim kesilmiştir ve atağın sonlandırılmasının ardından hostlar

arasındaki iletişim hala kesik durumdadır ve kısmen geri gelmiştir. OpenDaylight senaryosunda ise saldırı esnasında iletişim kesilmiş ancak saldırı bittikten sonra geri gelmiştir.

Özetle bu saldırı senaryosunda adli analiz açısından Ryu kontrolcü ön plana çıkarken, hem adli analiz açısından önemli ölçütlerden birisi olan servis vermeye devam etme kriterini hem de güney arayüzündeki verilerin birikmesi açısından kıymetli verilerin teminini aynı anda tam anlamıyla sağlayan bir kontrolcü görülmemiştir.

4.2. Bölüm Değerlendirmesi

Gerçekleştirilen deneylere dair bulgular ilgili başlıklar altında paylaşılmıştır. Bunun ötesinde tüm sürecin tekil bir bakış açısıyla incelenebilmesi adına Çizelge 4.4'te saldırıların güney arayüzü verileri kullanılarak tespitine dair sonuçlar paylaşılmıştır. Buradan görülebileceği üzere tüm durumlarda adli bilişim tespiti açısından başarı sağlayan bir kontrolcü bulunmamaktadır.

Adli bilişimin günden güne önem kazandığı ve veri boyutunun büyümesiyle birlikte elde edilen bilgilerin depolanmasının zorlaştığı SDN ortamlarında en sık kullanılan kontrolcülerin dördüyle yapılan bu deneyler sonucunda elde dilen sonuçların, literatürde mevcut durumda var olan bazı örnekleri adli bilişim açısından daha fazla detay içerir biçimde sunarak desteklediği görülürken, bu kontrolcülerin rutin adli bilişim işlemleri ve saldırı esnasındaki dayanıklılıklarının test edilmesi ve adli bilişim açısından incelenerek farklarının ortaya konulması işlemlerinin ilk defa yapıldığı değerlendirilmiştir.

Deneyler sonucunda kontrolcülerin gerek güney arayüzünden elde edilen loglar, gerek kontrolcülerin idaresinde olan anahtarlar, gerekse de saldırılara gösterilen tepkiler açısından birbirinden farklı sonuçlar sergiledikleri gözler önüne serilmiştir. Doğrudan sanal anahtarlar üzerinden elde edilen veriler üzerine adli bilişim çalışmaları yapılmasının boyut açısından dezavantajları olsa da daha fazla bilgiye erişim açısından olanak sunduğu görülmüştür.

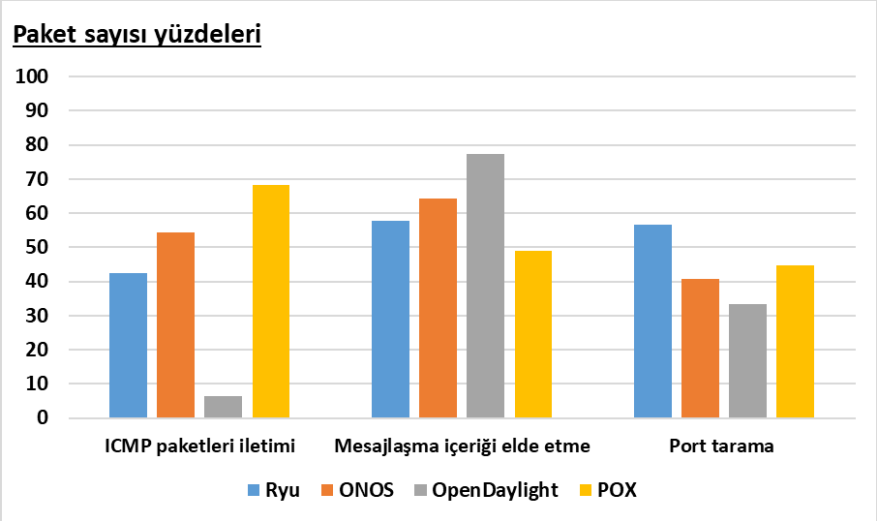
Çizelge 4.4. Uygulanan testlerde güney arayüzünde ilgili adli bilişim tespit durumu (+ : Tespit edildi , ± : Kısmen tespit edildi, - : Tespit edilemedi)

Deney Türü / Güney Arayüzü Tespit Durumu	**Ryu**	**ONOS**	**OpenDaylight**	**POX**
ICMP Paketleri Elde Etme	+	+	+	+
Mesajlaşma İçeriği Elde Etme	-	±	+	±
Port Tarama	+	+	+	+
Web Sunucu Taraması	-	+	±	+
TCP SYN Seli Saldırısı	+	+	+	+
STP Saldırısı	+	+	±	+
CDP Saldırısı	+	-	-	+

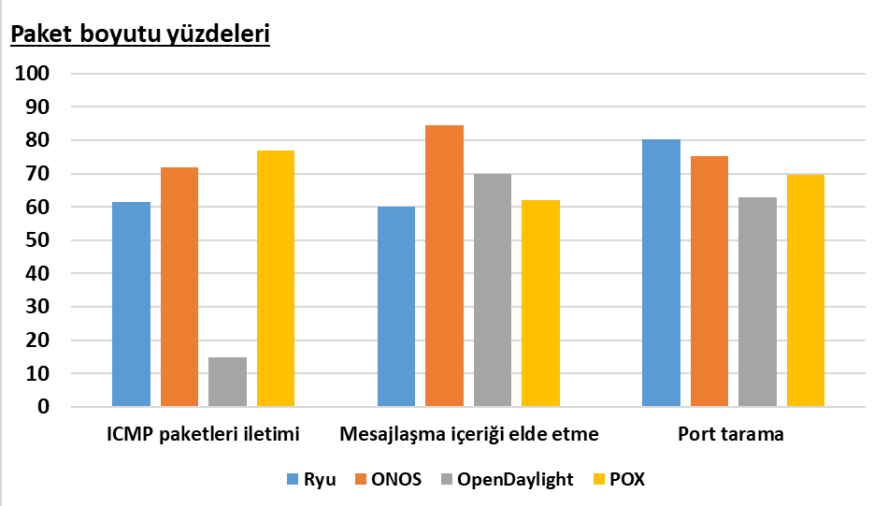
Bu deneyler aynı topoloji üzerinde, aynı şartlarda gerçekleştirilmesine rağmen detayları bu çalışmada da verildiği üzere güney arayüzünde birbirinden farklılık gösteren paket sayısı ve paket boyutu gözlemlendiği gibi ortalama paket boyutunda da ciddi farklar olduğu tespit edilmiştir. Aynı durum özellikle port tarama senaryosunda anahtarların üzerinde biriken paket sayısı ve paket boyutundaki farklılıklar özelinde dahi gözlemlenmiştir. Ayrıca web sunucu açıklarını tarama deneyinde POX kontrolcünün olduğu senaryonun tamamlanma süresinin diğer deneylere göre 8-10 kat daha uzun sürede tamamlanması da dikkat çekici başka bir detay olarak gözlemlenmiştir.

Adli bilişim açısından incelenecek verinin boyutu önem arz etmektedir. Kontrolcülerin değiştirilerek deneylerin tekrarlandığı durumlarda ortaya çıkan küçük yüzdelik farklar dahi büyük bir veri tabanı ele alındığında Terabyte (TB) mertebesine erişebilecek konuma gelecektir. Bu durum adli bilişim incelemesinin hızını ve zorluğunu doğrudan etkileyecektir. Deneyler kapsamında elde edilen paket sayılarının yüzdelerine dair genel sonuçlar Şekil 4.7'de ve paket boyutlarının kıyaslanmasına dair genel sonuçlar Şekil 4.8'de verilmiştir. Paket sayısı yüzdeleri deneyler kapsamında güney arayüzünde biriken paket sayısının, ilgili deneyde tüm ağda biriken paket sayısına olan yüzdesel oranını ifade etmektedir. Paket boyutu yüzdesi ise ilgili paketlerin depolama alanı cinsinden yüzdesel oranını temsil etmektedir. Şekillerden de görülebileceği üzere paket sayısı ve boyutunda da bir standart

bulunmamakta olup, bazı deneylerde en az yüzdeye sahip olan kontrolcü bir başka deneyde en yüksek yüzdeye sahip olabilmektedir.



Şekil 4.7. Güney arayüzü paket sayısı yüzdeleri genel görünümü



Şekil 4.8. Güney arayüzü paket boyutu yüzdeleri genel görünümü

Paket boyutunun yanı sıra, gecikme süreleri, aynı deneyde ağ üzerinde dolaşan toplam paket sayısı, ağın kendi içerisindeki paket sayısındaki değişimler açısından da deney sonuçlarını farklılık içerdiği görülmüştür. Ancak bir adli bilişim süreci için en önemli durum, olay ve olaya ait bilgilerin tespit edilebilmesidir. Sonuçlarda en düşük paket sayısı ve paket boyutu yüzdesinin olduğu kontrolcü, en kıymetli bilgi olarak düşünülebilecek olan iletişim ve saldırı bilgilerinin elde edilebildiği kontrolcü, zaman bilgisinin elde edilebildiği kontrolcü, kaynak-hedef bilgisinin elde edilebildiği kontrolcü, saldırı deneylerinde sistemin devre dışı kaldığı

kontrolcü ve güney arayüzü analizine odaklanınca en kıymetli sonuçların alındığı kontrolcü olarak bir gözlem kıyaslaması yapılmış olup bu bilgilere Çizelge 4.5'te yer verilmiştir. Çizelgeden de bütünsel olarak görüleceği üzere sonuçlar arasında farklılıklar olduğu deneyler sonucunda görülmüş olup, sonuçların bu kapsamda çalışmalar yapacak araştırmacıların kullanım düşüncelerine en uygun kontrolcüyü seçmeleri için faydalı olabileceği düşünülmektedir.

Çizelge 4.5. Uygulanan test ve atakların genel sonucu

Senaryo/ Güney Arayüzü Adli Bilişim Durumu	**En Düşük Paket Sayısı Yüzdesine Sahip Kontrolcü**	**En Düşük Paket Boyutu Yüzdesine Sahip Kontrolcü**	**Senaryo/Saldırı Bilgisi Elde Edilen Kontrolcüler**	**Zaman Bilgisi Elde Edilebilen Kontrolcüler**	**Kaynak-Hedef Bilgisi Elde Edilebilen Kontrolcüler**	**Sistemin Devre Dışı Kalmadığı Kontrolcüler**	**Güney Arayüzü Adli Bilişimi Açısından Öne Çıkan Kontrolcü**
ICMP Paketleri İletimi	ODL	ODL	Ryu, ONOS, ODL, POX	Ryu, ONOS, ODL, POX	Ryu, ONOS, ODL, POX	Saldırı Değil.	ODL
Mesajlaşma İçeriği Elde Etme	POX	Ryu	ODL, ONOS (kısmi), POX (kısmi)	ODL, ONOS (kısmi), POX (kısmi)	ODL, ONOS (kısmi), POX (kısmi)	Saldırı Değil.	ODL
Port Tarama	ODL	ODL	Ryu, ONOS, ODL, POX	Ryu, ONOS, ODL, POX	Ryu, ONOS, ODL, POX	Saldırı Değil.	ODL
Web Sunucu Taraması	Ryu	Ryu	ONOS, POX, ODL	ONOS, POX, ODL	ONOS, POX	Saldırı Değil.	ONOS
TCP SYN Seli Saldırısı	Ryu	Ryu	Ryu, ONOS, ODL, POX	Ryu, ONOS, ODL, POX	Ryu, ONOS, ODL, POX	Ryu, ONOS, ODL, POX	Ryu
STP Saldırısı	ODL	ODL	Ryu, ONOS, POX, ODL (kısmi)	Ryu, ONOS, ODL (kısmi), POX	Ryu, ONOS, ODL, POX	ONOS	ONOS
CDP Saldırısı	ODL	ODL	Ryu, POX	Ryu, POX	Ryu, POX	ONOS	-

Dört farklı kontrolcü için yedi farklı senaryonun uygulandığı bu çalışmada, anahtarlar ve güney arayüz üzerinden yakalanan paketler detaylı bir şekilde paket boyutu, kaynak-hedef tespiti, saldırı ve saldırgan bilgisi ve servis dışı kalma gibi adli bilişim açısından önem arz eden hususlar dikkate alınarak incelenmiştir. Bu çalışmanın sonunda testi yapılan kontrolcülerden herhangi birinin adli bilişim açısından en başarılı seçenek olarak kullanılacağını söylemek mümkün değildir [140].

Bu sonuçlar ve literatür genel kapsamda ele alındığında SDN adli bilişimi ile ilgili kontrolcüler arasında farklılıklar olduğu net bir biçimde görülmekte olup bu durumun

hukuki temeller ve devletlerin kanunları çerçevesinde standart hale getirilmesinin faydalı olacağı aşikardır.

Elde edilen tüm bulgular ve sonuçlar değerlendirildiğinde belli bir kullanıcıya bağımlı olan ve birbirinden farklı sonuçlar verebilecek sistemlerin adli bilişim açısından sağlıklı olmayacağı değerlendirilmiştir. Bu kapsamda ulusal ve uluslararası süreçlere uyumlu standart bir ağ adli bilişim sürecinin oluşturulması gerekliliği ispatlanmıştır. Bu sürecin ağın bir veya birden fazla noktasından alınabilecek veriler üzerine kurulu standart format, hız ve kalitede olması gerektiği ve kesintisiz veri çekebilmek adına SDN tabanlı 5G ağ ortamlarının kaynaklarını çok kullanmadan bu süreçleri yerine getirmesi gerektiği değerlendirilmiştir. 5G ağları gibi çok yüksek sayıda kullanıcıya hizmet verecek bir altyapıda adli bilişim süreçlerinin ağ yapısını zorlamayan ve standart bir yapıda olması elzemdir.

5. MEVZUAT VE ULUSLARARASI UYGULAMALARA UYUMLU AĞ ADLİ BİLİŞİM SÜRECİ GELİŞTİRİLMESİ

SDN'de farklı kontrolcülerle gerçekleştirilen deneylerde elde edilen deney sonuçları standart bir adli bilişim sürecinin gerekliliğini ortaya koymuştur. Bu durum 5G ağlarında adli bilişim süreçleri için de geçerlidir. 5G ağlarının ve SDN'in ötesinde geleneksel ağ adli bilişim çalışmaları için dahi mevzuat uyumlu bir standart süreç/yöntem bulunmamaktadır. Bir adli bilişim sürecinin oluşturulması süreci teknik, idari ve hukuki boyuttan ele alınması gereken bir husustur.

İnternet ortamında teknik açıdan tam bir denetim ve engellemenin tam anlamıyla mümkün olduğu söylenemez. İnternet bir oto kontrol mekanizmasına ve tümüyle kontrol edilemez bir yapıya sahiptir [55]. Ancak mümkün olan en üst düzeyde denetim için çeşitli teknik ve idari süreçlerin tanımlanması da bir zorunluluk olarak görülmektedir. Bugüne kadar gerçekleştirilen çalışmalar incelendiğinde Türkiye Cumhuriyeti'nde yürürlükte olan mevzuatın ağ adli bilişim konuları hakkında analizi üzerine teknik bakış açısıyla genel kapsamda bir çalışma yapılmadığı görülmüştür. Tezin bu bölümünde bugüne dek konuyla ilgili yapılan çalışmaların, bilgi ve iletişim güvenliği ve bilişim suçlarıyla ilişkili mevzuatın, çeşitli standart ve rehberlerin ağ adli bilişimi süreçleri açısından bir teknik ve idari değerlendirmesi yapılmıştır. Mevzuat ve uygulamalar kapsamında SDN tabanlı 5G ağları odağında ağ adli bilişim analizi adına öneriler sunulmuş olup, geleneksel ağlar, SDN ve 5G ağlarıyla uyumlu bir adli bilişim süreci oluşturulmuştur.

5.1. Ağ Adli Bilişimi Odağında Mevzuat İncelemesi

Türkiye Cumhuriyeti'nde bilişim suçlarıyla mücadele odağındaki mevzuatın ilk sırasında 5651 sayılı ve "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" [56] başlıklı kanun yer alır. 2007 yılından beri yürürlükte olan kanun, teknolojide yaşanan gelişime paralel olarak çeşitli değişikliklerle güncellenmiş ve yönetmeliklerle detaylandırılmıştır. Kanun internet suçlarına ve içeriğine dair genel kuralları belirlemekle birlikte, internet altyapısını kullanarak servis veren kurum ve şirketlerin sorumluluklarını da belirtmektedir.

Bahsi geçen Kanunun yanı sıra, “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik” [61], “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik” [62] ve “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik” [63] başlıklı yönetmelikler yürürlükte olup, bu yönetmeliklerde de kapsamlı bilgiler ve kurallar yer almaktadır.

5.1.1. 5651 sayılı kanun ve ilgili yönetmelikler

5651 sayılı Kanunda amaç ve kapsam “Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.” [56] şeklinde ifade edilmiştir. Kanunun yürürlüğe girmesinin ardından gelişen teknoloji ve artan internet kullanımı ve internet yoluyla işlenen suçlardan dolayı kanunda güncellemeler gerçekleştirilmiştir. 7253 sayılı kanun da 5651 sayılı kanunda değişiklik yapılmasına dair bir kanun olarak 2020 yılı Temmuz ayında yürürlüğe girmiştir [57].

Kanun başlığında yer alan İnternet Ortamında Yapılan Yayın ifadesi kanunun tanımlar bölümünde “İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri ifade eder.” [56] şeklinde tanımlanmıştır. Bir veri internet ortamından gelecek erişimlere açıldığında, eğer teknik bir kısıtlama tanımlanmadıysa, dünyanın her tarafından ve herkesin erişimine açık olmaktadır. Bu erişim doğrudan kanunun ifade ettiği şekilde, içeriğe belirsiz sayıda kişi tarafından ulaşıma açık olduğu anlamına gelmektedir. Ancak diğer taraftan bazı özel durumlarda anlam kazanmış verilerimiz olan bilgilerimizi sadece belirli kişilerle paylaşmak isteriz. Bu durumda güvenlik duvarı vb. teknik yapılarla IP adresi tabanlı izin verilerek sadece yetkilendirilmiş olan IP adreslerinden gelen isteklere cevap oluşturulabilir. Bu şekilde sadece belirli IP adreslerine izin verilerek oluşturulmuş olan bir internet yayınında dahi karşı taraftan izin verilen kişilerin tam olarak istenilen kişiler olup olmadığından emin olunması mümkün değildir. Çünkü genellikle aynı LAN’da yer alan çok sayıda kişi sabit ve aynı olan bir IP adresini paylaşmaktadır. IP Adresi “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik”te “Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri

yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adresi ifade eder." şeklinde tanımlanmıştır [63].

Yerel ağ dışındaki erişimlerde internet ortamında yönlendirilebilir olan bu IP adreslerinin kullanılabilmesi için NAT sistemi kullanımı gerekir. Bu durumda aynı LAN üzerinden internete çıkan kişiler aynı IP adresine sahip olmuş olacağından eğer özellikle bir kişiye veya belli kişilere erişim hakkı sağlanması isteniyorsa IP adresi bazlı bir erişim izninden ziyade kimlik doğrulama temelli vb. farklı uygulamaların da tasarlanması gerekmektedir. Aksi durumda Kanunda yer alan "belirsiz sayıda kişiler" [56] ifadesi yine geçerliliğini korumuş olacaktır. Sonuç olarak bu tarz istisnai durumlar dışında, kanunun LAN dışında yer alan ve internet ortamına açık olan tüm verilerimizi kapsadığı değerlendirilmiştir. Kanundaki "İnternet Ortamı" tanımının "Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı ifade eder." [56] şeklinde olması da bu değerlendirmeyi destekler niteliktedir.

Kanunda İçerik Sağlayıcı internete veri veya bilgi sağlayan herkes olarak nitelendirildiğinden bu kapsam bir web sayfası aracılığıyla bilgiyi paylaşan veya bir platformda bilgi paylaşan herkes olarak değerlendirilmiştir. İçerik sağlayıcı sunduğu her türlü bilgiden sorumludur. Başkasına ait bir bilgiyi paylaşmasından sorumlu olmamakla birlikte sunuş biçimine göre genel hükümlerden sorumlu olabilmektedir. Yer Sağlayıcılar hizmetleri bünyesinde barındıran sistemleri sağlayan gerçek veya tüzel kişiler olup özünde veri merkezleri veya web sitelerini vb. bünyesinde barındırma hizmeti veren yapıları tarif etmektedir. Erişim Sağlayıcılar ise "Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri ifade eder." [56] şeklinde tanımlanmış olup genel itibariyle İnternet Servis Sağlayıcılarını ifade etmektedir. Erişim sağlayıcıları Birliği ise doğrudan "Birlik" olarak tanımlanmıştır. Toplu Kullanım Sağlayıcılar ise "Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı ifade eder." [56] şeklinde tanımlanmış olup, bu ifade çalışanına veya ziyaretçisine internet erişimi veren iş yerlerini, kamu kuruluşlarını vb. tarif etmektedir. Sosyal medya ağlarının hızlı gelişimi dikkate alınarak Kanuna "Sosyal Ağ Sağlayıcı" tanımı ve detayları da eklenmiştir. "Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişileri ifade eder." [56, 57] şeklinde tanımlı olan Sosyal Ağ Sağlayıcılar kapsamında çeşitli yükümlülükler de Kanun kapsamında belirlenmiştir.

İnternet yayınlarının düzenlenmesi ve denetlenebilmesi için yapılan işleme “izleme” adı verilmiş olup, farklı kurumlara farklı sorumluluklar yüklenmiştir. İzleme ile yapılan eylem “Trafik Bilgisi” tanımıyla adlandırılmış olup, tanımı “Taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini ifade eder.” [56] şeklindedir.

Yer sağlayıcılar sunduğu hizmetler kapsamındaki trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikle belirlenecek süre kadar saklamakla yükümlüdür. Ayrıca bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. Trafik bilgilerinin saklanması için belirlenen bu süreler erişim sağlayıcılar için altı aydan az ve iki yıldan fazla olmayacak şekilde belirlenmiştir. Belirtilen durumlar trafik bilgilerini sağlıklı bir şekilde toplamak ve muhafaza etmenin son derece önemli ve kaçınılmaz olduğunu gözler önüne sermektedir.

Erişimin Engellenmesi süreci, alan adı veya IP adresi temelli engelleme vb. yöntemlerle gerçekleştirilebilmektedir. Tekdüzen kaynak konumlayıcı (Uniform Resource Locator, URL) adresi ilgili içeriğin yer aldığı tam internet adresini ifade eder. Erişim sağlayıcıların trafik bilgilerini tutma sorumluluğunun ötesinde bu trafiğin hukuka aykırı olup olmadığını kontrol etme yükümlülüğü bulunmamaktadır. İçeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen içerik, yer veya erişim sağlayıcılarına para cezası verilmesi Kanunla tanımlanmıştır. Erişimin engellenmesi kararları ihlalin gerçekleştiği kısımla sınırlı olarak (URL vb. şeklinde) verilir. Ancak bu sürecin teknik olarak mümkün olmadığı ve ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tamamı için erişimin engellenmesi kararı verilebilir.

Gecikmesinde sakınca bulunan hâllerde içeriğin çıkarılması ve/veya erişimin engellenmesi kapsamında işlenen suçların faillerine ulaşmak için gerekli olan bilgilerin içerik, yer ve erişim sağlayıcılar tarafından hâkim kararı üzerine adli mercilere verilmesi esastır. Eğer bu bilgiler verilmezse para cezası verilmesi esas olmakla birlikte fiili daha ağır cezayı gerektiren durumlarda farklı ve daha ağır cezalar verilmesi de mümkündür. Bu husus mevzuat kapsamında belirtilen trafik kayıtlarının tutulması ve yetkili merciler tarafından talep edildiğinde usulüne uygun olarak verilmesinin ne denli önemli bir süreç olduğunu göstermektedir.

Kanunda adli süreçlerin hangi suçlar kapsamında ve nasıl ilerleyeceği belirtilmiş olup, kişilik haklarının ihlallerinde, özel hayatın gizliliğinin ihlallerinde, gecikmesinde sakınca bulunan hallerde erişimin engellenmesi, içeriğin çıkarılması, kararın hangi adli veya idari organ tarafından ne kadar sürede alınması gerektiği gibi süreçlere dair detaylar belirtilmiştir. Ayrıca idari cezaların da belirtildiği Kanunda yer alan bu tür hususlar ağ adli bilişimi odaklı olmadığından bu tezin kapsamı dışındadır.

Kanunun uygulanmasına ilişkin usul ve esasların yönetmeliklerle düzenleneceği Kanunda belirtilmiştir. Bu kapsamda üç adet yönetmeliğe dair bilgiler sıradaki alt bölümlerde paylaşılmaktadır.

İnternet toplu kullanım sağlayıcıları hakkında yönetmelik

5651 sayılı Kanuna dayanılarak, detay süreçlerin sınırlarını belirlemek için hazırlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliğinin amacı "Bu Yönetmeliğin amacı, internet toplu kullanım sağlayıcıları ve ticari amaçla internet toplu kullanım sağlayıcılarının yükümlülükleri ve sorumlulukları ile denetimlerine ilişkin esas ve usulleri düzenlemektir" [61] olarak belirtilmiştir. Yönetmelik ticari ve ticari olmayan toplu kullanım sağlayıcıları iki farklı kategoride ele almış olup teknik ve idari sorumluluklar belirlenmiştir. İnternet toplu kullanım sağlayıcıları; kamu kurumları, meslek odaları, iş yerleri vb. yerleri ifade etmekte olup, bu yerler konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak amacıyla içerik filtreleme sistemini kullanmakla, erişim kayıtlarını kendi sistemine kaydetmek ve iki yıl saklamakla yükümlüdür.

Yönetmelikte hangi bilgilerin kayıt altına alınması gerektiği belirtilmiş olup bunlar erişim kayıtları olarak isimlendirilmiştir. Bunlar arasında iç ağda dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş zamanını ve bu IP adreslerini kullanan bilgisayarların MAC adresini gösteren bilgiler bulunmaktadır. Ayrıca hedef IP adresiyle birlikte kullanıcıya tahsis edilen gerçek IP ve port bilgilerinin de kayıt altına alınması gerektiği yönetmelikte ifade edilmektedir.

Erişim kayıtları hem ticari olan hem de ticari olmayan toplu kullanım sağlayıcılar tarafından tutulmak zorunda olup, kapsamı özellikle LAN üzerinde dağıtımı yapılan IP adres bilgileri ve kullanımı üzerinedir. Bu durum otomatik IP adresi dağıtımının yapılması veya her

kullanıcıya statik bir iç IP adresi tahsis edilmesi olarak iki ayrı kapsamda ele alınabilir. Otomatik IP adresleri, dinamik istemci ayarlama protokolü (Dynamic Host Configuration Protocol, DHCP) sunucuları tarafından sistem yöneticisinin belirlediği kurallara göre dağıtılmaktadır. Bu kurallara göre belirli MAC adresleri için statik bir IP adresi ataması yapılabilmektedir. Yani bir kullanıcı ağa her dâhil olup IP adresi talebinde bulunduğu zaman teknik olarak sürekli aynı IP adresini alması sağlanabilir. Sabit IP adresi yönetmelikte "Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, zamana, oturuma göre değişmeyen ve sistem yöneticisi tarafından belirlenip tanımlanan ve değiştirilebilen IP adresini ifade eder" [61] şeklinde tanımlanmıştır. Bu durum sabit kullanıcıları olan bir toplu kullanım sağlayıcı açısından tercih edilebilir bir seçenek olarak görülebilir. Ancak ticari amaçlı toplu internet kullanım sağlayıcılarında kullanıcıların sürekli değişeceği göz önüne alındığında bu seçeneğin kullanılabilir olmadığı görülmektedir. Dağıtılan bu yerel IP adresleri ticari amaçla internet toplu kullanım sağlayıcıları tarafından, internet ortamında yönlendirilebilir bir sabit IP adresi olarak kullanılmak zorundadır. Ticari olmayan kesimde bu durum bir zorunluluk değilken genel olarak toplu kullanım sağlayıcılarının sabit IP adresi aldığı bilinmektedir. Ancak duruma toplu kullanım sağlayıcılar açısından bakıldığında, sorumluluk zaten internet ortamındaki veriler değil yerel ağ üzerinden elde edilecek verilerden oluşmaktadır. Yani bu şekilde paylaştırılmış IP adresleri değil yerel IP adreslerinin bağlı olduğu MAC adresleri, kullanım bilgileri ve bu yerel cihazların hedef olarak ulaştıkları IP adreslerinin kaydının tutulması gereklidir. MAC adresleri, IP adreslerinin kullanım başlangıç ve bitiş zamanları bilgileri DHCP sunucusu tarafından sunulabilecek bilgilerdir. Ayrıca bu bilgilere yerel ağa yerleştirilmiş ve bu iş için tanımlanmış sunucular tarafından da erişilebilir. DHCP sunucusu olmayan bir ağ üzerinde, bu bilgilere anahtarlar üzerinden de ağ dinlemesi yoluyla erişmek mümkündür. DHCP paketlerinin filtrelendiği ve IP adresleriyle MAC adreslerinin kayıtlarının tutulduğu bir ağ dinlemesi yoluyla bu durum mümkün olacaktır.

Bir başka seçenek olarak, verilen IP adresleri IP dağılımının yapıldığı andan itibaren belirlenen bir süre kadar (örneğin 24 saat veya talep edilen gün bitene kadar) geçerli olacak şekilde de ayarlanabilir. Bu şekilde incelemesi yapılacak gün o yerel IP adresi başka bir kullanıcıya tahsis edilmemiş olacaktır. Kamuya açık alanlarda internet erişim hizmeti sunan toplu kullanım sağlayıcılar ise kısa mesaj servisi vb. yöntemlerle kullanıcıları tanımlayacak sistemleri kurmakla yükümlüdür.

Ticari amaçlı internet toplu kullanım sağlayıcılar internet kafe vb. umuma açık yerlerde ücret karşılığı internet erişim hizmeti veren yerleri ifade etmekte olup bu kesim de filtreleme sistemi kullanmakla yükümlüdür. Ticari olmayan toplu kullanım sağlayıcılardan farklı olarak ticari olanlar, güvenli internet hizmetini sağlamakla da yükümlü olup ayrıca filtreleme sistemini aktif ve güncel halde bulundurarak devre dışı kalmamasını sağlamakla da yükümlüdür. Ticari olan toplu kullanım sağlayıcıları ek olarak erişim sağlayıcılardan sabit IP alıp kullanmak ve bu IP değişikliklerini on beş gün içerisinde mülki idare amirliklerine bildirmekle de yükümlüdür.

Erişim kayıtlarını kendi ortamına kaydetmek ve iki yıl saklamak hususunda ticari olmayan toplu kullanım sağlayıcılarla aynı sorumluluklara sahip olan ticari toplu kullanım sağlayıcıları bu erişim kayıtlarının doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmekle ve bu bilgileri de iki yıl süre ile saklamakla yükümlüdür.

Bu durum bilgilerin değiştirilmemesi ve aynı veri olduğunun ispatlanması amacıyla bazı özetleme mekanizmalarının ve zaman damgası kullanımlarının gerekli ve zorunlu olduğunu göstermektedir. Tutulan erişim kayıtlarının yanı sıra özet değeri ve zaman damgası bilgilerinin de tutulmuş olması yönetmelikte belirtilen doğruluk ve bütünlük kavramlarını sağlamaya yönelik çalışmalardır. Ayrıca verilerin üçüncü kişilerin erişimine kapalı olduğundan emin olunması için erişim kayıtlarının güvenlik sistemleriyle korunması ve kaybolması ihtimaline karşı yedekli çalışma yapılması da gizlilik ihtiyaçlarını gidermek için çeşitli yöntemler olarak düşünülebilir.

Telekomünikasyon kurumu tarafından erişim sağlayıcılara ve yer sağlayıcılara faaliyet belgesi verilmesine ilişkin usul ve esaslar hakkında yönetmelik

Telekomünikasyon kurumu tarafından erişim sağlayıcılara ve yer sağlayıcılara faaliyet belgesi verilmesine ilişkin usul ve esaslar hakkında yönetmeliğinin amacı “Bu Yönetmeliğin amacı; Telekomünikasyon Kurumu tarafından erişim sağlayıcılara ve yer sağlayıcılara faaliyet belgesi verilmesine ilişkin usul ve esasları düzenlemektir.” [62] olarak belirtilmiştir. Faaliyet belgesi verilmesinin yanı sıra erişim sağlayıcı ve yer sağlayıcıların yükümlülükleri ve yaptırımlar da bu yönetmelikle belirlenmiştir. Erişim ve yer sağlayıcıların faaliyet belgesi alabilmesine ve bu faaliyetlerin sona ermesine dair hususlar yönetmelikle belirlenmiştir.

Yönetmelikte veri “Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer” olarak tanımlanmışken, bilgi ise “Verilerin anlam kazanmış biçimi” olarak tanımlanmıştır [62].

Erişim sağlayıcıların ilk yükümlülüğü, herhangi bir kullanıcısının yayınladığı hukuka aykırı olan içerikten kendisine kanun ve mevzuat hükümlerince bildirim yapıldığında teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemesi olarak belirlenmiştir. Ticari amaçlı internet toplu kullanım sağlayıcılarına sabit IP adresi tahsisi yapmak da erişim sağlayıcılarının başka bir sorumluluğudur.

Erişim sağlayıcı trafik bilgisine dair tutulması gereken kayıtlar yönetmelikte belirtilmiştir. Bunlar arasında abonenin adı, soyadı, adresi, telefon numarası, abone başlangıç-iptal tarihleri bulunmaktadır. Ayrıca bağlantı tarih ve saat bilgileri, sisteme giriş ve sistemden çıkış için tarih ve saat bilgileri, IP adresi ve bağlantı noktaları gibi bilgilerin de trafik bilgileri içerisinde yer alması gerektiği ifade edilmiştir. Erişim sağlayıcıları bu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini (hash), zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle yükümlüdür.

Erişim sağlayıcıların kayıt tutma yükümlülükleri ana hatlarıyla toplu kullanım sağlayıcılar için tanımlı yükümlülüklere benzemekle birlikte, daha üst seviyeden bir ağ hizmeti sunulduğundan dolayı temelinde farklılıklar göstermektedir. Toplu kullanım sağlayıcılarından beklenen kayıt özellikleri OSI (Open Systems Interconnection model) katmanında seviye 2 olarak belirlenen veri bağlantı katmanı üzerinden gerçekleşirken, erişim sağlayıcılarda teknik odak seviye 3 olarak gerçekleşmektedir. Bu sebepten dış IP adresinin sabit veya dinamik olarak tahsis edilmiş olması fark etmeksizin, bir parametre olarak kayıt altına alınması yükümlülükler arasına eklenmiştir. Bunun yanı sıra sistem bağlantı ve çıkışlarına ait tarih ve saat bilgisi de kayıt altına alınması gereken diğer hususlardandır. Bu teknik bilgilerin kullanıcı ile eşleşmesi adına yönetmelikte abone adı soyadı, adres, telefon numarası ve aboneliğe dair diğer bilgilerin de erişim sağlayıcıların kayıtları arasında yer alması gerektiği belirtilmiştir. Toplu kullanım sağlayıcılarında olduğu gibi bu bilgilerin gizliliğini sağlamak için gerekli güvenlik ve yedekleme önlemlerini almak da erişim sağlayıcılarının sorumluluğundadır.

Dosya bütünlük değeri yönetmelikte bir tanım olarak “Bir bilgisayar dosyasının içindeki bütün verilerin matematiksel bir işlemden geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapılıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değeri ifade eder.” [62] şeklinde yer almaktadır. Özetleme mekanizmalarının ve zaman damgası kullanımlarının gerekli ve zorunlu olduğu hususu toplu kullanım sağlayıcılarında olduğu gibi, erişim sağlayıcılar için de daha açık bir şekilde ifade edilmiştir.

Bir erişim sağlayıcı faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma (Bilgi Teknolojileri ve İletişim Kurumu, BTK), içerik sağlayıcılarına ve müşterilerine bildirmelidir. Ayrıca kapanma tarihinden önceki bir yıl için gerekli trafik bilgilerine ilişkin tüm kayıtlarını metin dosyası olarak, log formatlarını açıklamalarıyla birlikte ve abone bilgilerini de optik medya ortamında teslim eder. Bu yükümlülükten görüleceği üzere trafik kayıtlarının tutulması zorunluluğu erişim sağlayıcının kapanmış olması durumunda dahi devam etmekte ve belirtilen bir yıllık süreyi kapsamaktadır. Trafik bilgisi için beklenen bilgiler yönetmelikte tarif edilmiş olmasına rağmen bir log formatı verilmemiştir ve bu durum yönetmelikte de belirtilmiştir. Farklı erişim sağlayıcılarının farklı cihaz ve sistemler kullandığı göz önüne alındığında bu durumun faydalı olduğu değerlendirilmiştir.

Erişim sağlayıcılar, erişimi engellenecek adreslere ilişkin işlemleri derhâl yapabilmek için gerekli donanım ve yazılımları kurmakla yükümlüdür. Erişim sağlayıcılar erişimi engellemekle yükümlü olmasına karşın erişimin o esnada erişimi yasal veya izinli olan adreslere kendisi aracılığıyla erişilmesi durumu için bir hukuksal analiz yapmak zorunda değildir.

Yer sağlayıcılar da ilgili Kanun ve mevzuat hükümleriyle haberdar edilmesi durumunda ve teknik olarak engelleme imkânı bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür. Erişim sağlayıcılarında belirtilen derhâl engelleme için kurulması gereken donanım ve yazılım hususu yer sağlayıcılar için yönetmelikte zorunluluk olarak belirtilmemiştir.

Yer sağlayıcıların trafik bilgisini saklaması üzerine karar “Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle

yükümlüdür.” şeklinde yer almaktadır. Erişim sağlayıcıların bir yıl saklamakla mükellef olduğu bu süre yer sağlayıcılarda altı ay olarak belirlenmiştir.

5651 sayılı kanunda belirtilen trafik bilgisi hususuyla yer sağlayıcı trafik bilgisi hususu birbirinden farklılıklar içermektedir ve yönetmelikte "yer sağlayıcı trafik bilgisi” olarak ifade edilen tanım detaylı kayıtları tarif etmektedir. Yer sağlayıcı trafik bilgisi yönetmelikte “İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih-saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgisi gibi bilgileri ifade eder.” [62] şeklinde tanımlanmıştır. Bu ifadeden yer sağlayıcıların web sunucuları vb. barından veri merkezleri olarak görüldüğü çıkarımı yapılmıştır. Bu sayfaların adresleri ve erişimle ilgili nihai sonucun yer sağlayıcıdan beklenmesinin yanı sıra sağladığı hizmetlerin hangi IP adresi üzerinden verildiği ve bu adrese hangi adres üzerinden ne zaman bağlantı kurulduğunun da kayıt olarak tutulması beklendiği görülmektedir. Yapılacak incelemelerde yer sağlayıcıdan hizmet alan iç kullanıcılara yapılacak bu bağlantıların, erişim sağlayıcılar üzerinden de ne zaman, nereden, kim tarafından bağlantı kurduğu anlaşılabilecek ve gerekli durumlarda erişim toplu kullanım sağlayıcılar üzerinden geldiyse, oradan da alınacak kayıt dosyalarıyla doğrulanabilir bir yapıya dönüşmüş olacaktır. Özetle sorumluluk yüklenen tüm yapıların tuttuğu trafik kayıtlar neredeyse tek başına çok sayıda adli bilişim sürecine ışık tutabilecek bir yapı oluştururken, mevzuat kapsamında tüm paydaşlardan elde edilecek kayıt dosyalarıyla ağ üzerinden akan tüm bilgilere erişim mümkün olacaktır ve bu kayıt dosyaları da birbirlerini doğrular nitelikte kullanılabilecektir. Yer sağlayıcılar da erişim sağlayıcılarda olduğu gibi, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

<u>İnternet ortamında yapılan yayınların düzenlenmesine dair usul ve esaslar hakkında yönetmelik</u>

İnternet yayınlarının düzenlenmesi için yürürlükte olan başka bir yönetmelik de “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik” olup genel çerçeve ile diğer iki yönetmelikle aynı çizgidedir ve benzer bilgileri içermektedir. Teknik anlamda yüklenen ekstra bir sorumluluk olarak erişim sağlayıcılar için tasarlanmış olan vekil sunucu trafik bilgisi hususu teknik anlamda dikkat çeken bir detaydır.

Vekil sunucu trafik bilgisi yönetmelikte "İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi" olarak tanımlanmıştır [63]. Erişim sağlayıcılar eğer vekil sunucu hizmeti sunuyor ise; vekil sunucu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle yükümlüdür. Vekil sunucu internete erişim sırasında isteklerin doğrudan internet ortamındaki hedefe değil ilgili vekile yapıldığı ve geri dönen bilgilerin de üzerinden alındığı sunucuyu tarif etmektedir. Yönetmeliğin eski formlarında vekil sunucu trafik bilgisi tanımının sonunda "gibi bilgiler" ifadesi yer almaktaydı ve bu durum açıkça sayılmayan bilgilerin de tanıma eklenmesi ihtimalini doğurmaktaydı. Vekil sunucu kullanıldığı durumda en az yönetmelikte belirtilmiş olan bilgilerin doğrudan sunucu üzerinden alınarak harici bir depolama sunucusunda tutulmasının gerekli olduğu açık olmakla birlikte, diğer trafik bilgileri tanımlarında geçen kayıt beklentilerinin de (abone bilgileri, işlem (GET, POST) bilgilerinin vb.) tutulmasının faydalı olacağı düşündürmekteydi. Ancak son durumda güncel yönetmelikte 2022 yılına ait Danıştay kararıyla kesinleşen bir değişiklik yapıldığı ve tanımın netleştiği görülmektedir. Bu doğrultuda güncel yönetmelik adli bilişim süreçleri açısından tutulacak kayıtları net bir şekilde tanımlanmaktadır.

5.1.2. 5070 sayılı elektronik imza kanunu

Zaman damgası, 5070 sayılı Elektronik İmza Kanununda "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı ifade eder." [124] şeklinde tanımlanmıştır. Bu tanımlamada elektronik imzanın nitelikli olup olmama durumundan bahsedilmemiştir. İlgili yönetmeliklerde erişim ve yer sağlayıcılar için belirtilen zaman damgası mecburiyetinin elektronik imza ile imzalanıp imzalanmayacağına dair bir zorunluluk görülmemiş olsa da, zaman damgasının 5070 sayılı kanunda yapılan tanım gereği nitelikli veya niteliksiz elektronik imza ile imzalanarak kayıtlara aktarılmasının daha uygun olacağı değerlendirilmiştir [141]. Ayrıca 5651 sayılı Kanunun getirdiği düzenlemeler ile ilişkili olarak; 5809 sayılı "Elektronik Haberleşme Kanununun" da sayılabileceği düşünülmesine karşın, yapılan incelemelerde 5809 sayılı Kanunun içeriğinde ağ adli bilişimi açısından bir odak bulunmadığı değerlendirilmiştir [58, 141].

5.1.3. 5237 sayılı Türk ceza kanunu

5651 sayılı Kanun ve yönetmeliklerde belirtilen kayıtların incelenmesi sonucunda suç teşkil eden bir unsur bulunması halinde verilecek cezalar TCK ile belirlenmiştir. Bilişim Alanında Suçlar 5237 sayılı Türk Ceza Kanunu'nun Onuncu Bölümünde ele alınmıştır [59]. Madde 243-246 arasında doğrudan Bilişim Suçları yer almaktadır. Bu maddeler sırasıyla "Bilişim Sistemine Girme, Sistemi engelleme, bozma, verileri yok etme veya değiştirme, Banka veya kredi kartlarının kötüye kullanılması, Yasak cihaz veya programlar, Tüzel kişiler hakkında güvenlik tedbiri uygulanması" şeklindedir.

Bu maddelerin yanı sıra; haberleşmenin engellenmesi (Madde 124), hakaret (madde 125), haberleşmenin gizliliğini ihlal (madde 132), kişiler arası konuşmaların dinlenmesi ve kayda alınması (madde 133), kişisel verilerin kaydedilmesi (madde 135), verileri hukuka aykırı olarak verme veya ele geçirme (madde 136), verileri yok etmeme (madde 138) başlıklı maddelerin de Bilişim Suçlarıyla ilişkili olan maddeler olduğu değerlendirilmiştir.

TCK Madde 138-1'de "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir." [59] ifadesi yer almaktadır. 5651 sayılı Kanun ve ilgili yönetmeliklerde toplu kullanım sağlayıcı, yer sağlayıcı ve erişim sağlayıcı için trafik ve erişim bilgilerinin ne kadar tutulması gerektiği belirtilmiş olmasına karşın bu verilerin yok edilmesi hususu tarif edilmemiştir [56, 61–63]. TCK'da açıkça belirtildiği üzere verilerin belirlenen sürelerden sonra yok edilmesi hususunun detaylandırılmasının daha faydalı olacağı değerlendirilmiştir. Verilerin silinmesinde hangi yöntemin kullanılacağı, kimler tarafından silineceği, tam olarak ne zaman silinmesi gerektiği, silindikten sonra gerçekleştirilecek bilgilendirme gibi bazı hususların, doğrudan Kanunda olmasa dahi belirlenecek süreçlerde netlik kazanması, adli bilişim sürecini daha sağlıklı bir duruma eriştirecektir.

5.1.4. 5271 sayılı ceza muhakemeleri kanunu

Ağ verileri kayıtlarının tutulması toplu kullanım sağlayıcılar, yer sağlayıcılar ve erişim sağlayıcılar için zorunlu tutulmuş olup ilgili verilerin sayılan kesimlerden elde edilmesinin teknik olarak mümkün olduğu değerlendirilmiştir. Zaten kanun koyucunun ilgili mevzuatı

geleneksel ağ yöntemlerinde teknik olarak mümkün adli bilişim hususlarını değerlendirdikten sonra yürürlüğe aldığı değerlendirilmiştir. Bu sebepten her bireysel internet kullanıcısının ağ verilerinin kayıtlarını almasına ve yedeklemesine gerek yoktur. Suçun hangi dijital teknik veya yöntemle gerçekleştirildiğinden bağımsız olarak delil elde edilebilmesi için şahıslara ait sabit diskler, bilgisayarlar, telefonlar vb. kaynakların dijital delil hükmünde kullanılabilmesi hususu CMK'nın 134. Maddesinde yer alır. El koyma yapılabilecek bu sistemlerde yer alan bütün verilerin yedeklemesinin yapılması gerekmektedir. Ardından bu yedeklerin bir kopyası elde edilerek şüpheliye ve vekiline verilmelidir [60]. Bu tür adli bilişim süreçleri kolluk kuvvetleri tarafından uygulanmaktadır. Kolluk kuvvetlerine bağlı bu birimler siber suçlarla ilgili soruşturmaları gerçekleştirir ve adli bilişim süreçlerinde görevler alırlar [55].

5.2. ISO 27001 Standardı

Uluslararası Standardizasyon Teşkilatı (International Organization for Standardization, ISO) tarafından oluşturulan ISO standartlarının geliştirilmesi genellikle yaklaşık üç yıl sürmektedir [142]. Üç yıllık süre boyunca gerçekleşen süreçlerde üye ülkelerin uzmanları ihtiyaçlar kapsamında çalışmalar gerçekleştirir. Uzman görüşlerine dayalı olarak oluşan bu standartlara uyum sağlanması, kurumları daha verimli çalışmasına olanak sağlar. Standartlar işin nasıl gerçekleştirileceğine dair bilgileri içermekten ziyade ne yapılacağını tarif etmektedir [143]. Türkiye Cumhuriyeti'nin ISO temsilcisi TSE'dir (Türk Standartları Enstitüsü) [144].

Sürekli gelişen ve ihtiyaç duyulan teknoloji kullanımı, siber güvenlik alanında paydaşların ihtiyaç duyduğu bilgi ve uygulamaların, anlaşılabilir ve belirlenmiş süreç adımlarını içerir şekilde işletilebilmesi için bir standart olarak yer almasını zorunlu kılmaktadır. Bu çerçevede ISO 27001 Bilgi Güvenliği Yönetim Sistemi küresel çapta bir temel oluşturmaktadır. Siber güvenlik uygulamalarının temelini oluşturan ISO 27001 standardı süreci sadece bilişim sistemleri güvenliği açısından ele almamaktadır. İnsan kaynakları ve fiziksel olarak altyapının güvenliğin sağlanması gibi hususlar da kapsam içerisindedir. ISO/IEC JTC 1/SC 27 Komitesi 191 adet standart yayınlamıştır. Tüm bu standartların tümüyle uygulanmasının katkı düzeyini artıracağı düşünülmektedir [143].

ISO 27001 sertifikaları kamu kurumlarının alacağı hizmetler kapsamında çıkılan ihalelerde tedarik/hizmet sağlayacak olan şirketlerde aranan bir ön şart olarak karşımıza çıkmaktadır. Ayrıca bazı kamu kurumları yönetmelik ve süreçlerinde de ISO 27001'e atıf yapmaktadır. Örneğin "Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği" kapsamında Belgelendirme Kuruluşu "TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre belgelendirme yapmak üzere akredite edilmiş kurum veya kuruluşu ifade eder" [145] şeklinde tanımlanmıştır. Ayrıca aynı yönetmelikte Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı "TS ISO/IEC 27001 veya ISO/IEC 27001 standardını ifade eder." şeklinde tanımlıdır.

Bilgi güvenliği yönetimine sadece siber güvenlik açısından bakarak planlama yapmak yerine tüm birimlerin ve süreçlerin göz önünde bulundurulduğu bir sistem tasarlamak gerekmektedir. Aksi durumda, başta insan faktörü sebebiyle, yüzde yüze yakın bir güvenlik oluşturmak mümkün olmayacaktır. ISO 27001'in ana maddelerine ek olarak 114 adet daha kontrol mevcuttur. Bunlarda A.12 maddesinde işletim güvenliği yer alır. Veri kayıpları oluşması ihtimaline karşın koruma oluşturulması, kural dışı durumlara ve hatalara karşı kayıtlar üretilmesi gerektiği bu maddede belirtilmiştir. Bu kayıtların düzenli olarak kontrol edilmesi gerekmektedir. Tüm bu süreçlerde gerçekleşecek işlemlerin referans olarak temel alınacak bir zaman sunucusuna göre işletilmesi ve zaman bilgilerinin de tutulduğu bu kayıtların yedeklemelerinin belirlenen periyotlarda yapılması gerekir. Bir başka önemli ek madde olan A.16'da da delil oluşturabilecek olan bilgilerin tespit edilebilmesi, toplanabilmesi, elde edilebilmesi ve muhafaza edilmesi için süreçlerin belirlenmesi ve bu süreçlerin uygulamaya alınması gerektiği belirtilmektedir. Ek madde A.18'de sözleşmelerden doğan süreçler, yasal yükümlülük ve mevzuatın kurum tarafından yazılı olarak tanımlaması ve güncelliğinin korunması gerektiği belirtilmektedir. Yetkilendirilmemiş erişimlere karşı koruma oluşturulması gerekmekte olup kriptografik kontroller uygulanarak muhafaza edilen kayıtların sahtecilik ve yok etme gibi durumlara karşı korunması gerektiği de belirtilmektedir [146].

ISO 27001 standardı eklerinde yer alan yukarıdaki üç madde bilginin kayıt altına alınması konusunda bir standart belirlemiştir. Bu kapsamda standartlar nasıl yapılması gerektiğini değil ne yapılması gerektiğini belirtir durumda olduğunda dolayı beklendiği gibi genel hatlarla tarif edilmiş olup, bu hususların adli bilişim açısından önemli ana hedefler oluşturduğundan bahsetmek mümkündür.

Bu durumlar göz önüne alındığında ISO 27001 standardının siber güvenlik yönetimini sağlarken, aynı zamanda mevcut ülke yasa ve ölçütlerini göz ardı etmeme üzerinde durduğu açıkça görülmektedir. Tez kapsamında belirtilen mevzuat ve oluşturulan süreç de özünde ISO 27001'e uyum sürecinin bir gereksinimidir. Sonuç olarak ISO 27001 bu çalışmada da dile getirilmiş olan adli bilişim adımlarının yerine getirilmesi için gerekli tüm adımların yerine getirilmesini zorunluluk olarak karşımıza çıkarmaktadır.

TS ISO/IEC 27001: 2022 Bilgi Güvenliği, Siber Güvenlik Ve Gizlilik Koruması- Bilgi Güvenliği Yönetim Sistemleri- Gereksinimler başlıklı yeni sürüm 2022 yılı aralık ayı içerisinde yayınlanmış olup, belge talep eden kuruluşların 31 Ekim 2023'ten itibaren başvuru yapmaları gerektiği belirtilmektedir [147].

5.3. Bilgi ve İletişim Güvenliği Rehberi

Özellikle kamu kurumlarını ilgilendiren ancak altyapı hizmetleri sağlayan işletmeleri de kapsamına alan "Bilgi ve İletişim Güvenliği Tedbirleri" konulu Cumhurbaşkanlığı genelgesi 6 Temmuz 2019'da yürürlüğe girmiştir. Bu genelgede, milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik verilerin güvenliğinin sağlanması amacıyla bazı tedbirler alınmıştır. Bu tedbirlerde kamu kurumlarındaki kritik verilerin, internet erişimi olmayan, fiziksel ortam olarak da güvenliği sağlanmış bir ağ altyapısında, erişim kayıtları güvenli olarak tutularak saklanması gerektiği belirtilmiştir. Genelgedeki durum internete açık verilerin adli bilişim özelliğiyle aynı sınıfta olmayıp, bir özel ağ yapılandırması üzerinde durulmuş olsa da ağ üzerinden akan verilerin değiştirilemez bir şekilde kayıt altına alınması üzerinde durulmuştur [148].

Bu genelgenin yürürlüğe girmesinden bir yıl sonra (Temmuz, 2020) CBDDO'nun hazırladığı "Bilgi ve İletişim Güvenliği Rehberi" başlıklı kılavuz hazırlanarak duyurulmuştur. Rehberin amacı "Bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilginin/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır." şeklinde belirtilmiştir [64].

Rehberde bilgi güvenliğini artırmak için alınacak tedbirler, varlık gruplarına, uygulama ve teknoloji alanlarına ve sıkılaştırmaya yönelik olacak şekilde açıklanmıştır. İncelenen mevzuatlarda bilişim sistemlerine ait tanımların, genel bir çerçeveden verildiği görülmekle birlikte rehberde tedbirlerin IoT ve bulut bilişim gibi güncel ve detaylı konular özelinde de verildiği görülmektedir. Bilgi güvenliği tedbirlerini artırmanın adli olayların yaşanma durumunu doğal bir sonuç olarak azaltacağı ve adli bilişim süreçlerine katkı sağlayacağı kabul edilebilir. Ancak özellikle adli vakalarda delilin bulunması ve sağlıklı olması açısından bilgi güvenliği tedbirleriyle uyum sağlamak elzemdir.

Rehberdeki "Ağ ve Sistem Güvenliği" alt başlığında log elde edilmesi odağında üç adet tedbir olduğu görülmektedir. Bunlar "İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi", "Siber Güvenlik Olay Yönetimi" ve "Kimlik Doğrulama ve Erişim Yönetimi" olarak sıralanmaktadır. Envanter yönetiminde yer alan "DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti" ve "DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti" tedbirlerinde otomatik IP dağıtımı gerçekleştiren DHCP mekanizmalarında ve eğer mevcutsa IP adreslerine dair yönetim araçlarında kayıt mekanizmalarının aktif olması gerektiği tanımlanmış olup bu hususun İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliğinde yer alan gereksinimle de aynı doğrultuda olduğu değerlendirilmiştir [61, 64].

Ağ adli bilişimi ile ilgili olmasa da verilerin korunması adına "Sabit Disk Güvenliği" tedbiri rehberde mevcuttur ve bu tedbirde kullanıcı bilgisayarlarındaki sabit disklerin verilerin tekrar geri getirilemeyecek şekilde silme işlemine tabi tutulduktan sonra sistemlere dâhil edilmesi hedeflenmiştir. Bu işlem sonucunda bir kullanıcı tarafından gerçekleştirilen, suç içeren veya içermeyen işlemlerin başka bir kişi tarafından gerçekleştirilmiş olarak görülme riskinin önüne geçilmiştir.

Misafir ağı yönetimi başlığında, izole edilmiş olarak kullanılması gereken bu ağlara bağlanmak için kimlik bilgilerinin doğrulanması gerektiği ve bu ağdan yapılan tüm erişimlerin kayıt altına alınması gerektiği belirtilmiştir. Kayıt altına alınması durumunun teknik detayı rehberde verilmemiştir. Başka bir tedbirde ise tüm isteklere ait URL bilgilerinin kaydedilmesi gerektiği belirtilmiştir. Bu tedbirlerin de İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliğinde yer alan hedef IP adresi tutulması gibi bilgilerle

ilişkili olduğu değerlendirilmiş olup tüm istekler ifadesinin daha fazla teknik detay içerecek şekilde ifade edilmesinin soru işaretlerini ortadan kaldırabileceği değerlendirilmiştir.

Ağ adli bilişimi açısından en önemli görülebilecek ve en kapsamlı olan tedbirlerin birisi de "Ağ Paketlerinin kaydedilmesi" olarak karşımıza çıkmaktadır. İhtiyaç duyulduğunda tüm trafiğin gözlemlenebilmesi ve incelenebilmesi amacıyla kayıt sistemlerinin kurulması gerektiği belirtilmiştir. Ayrıca ağ kenar cihazları üzerinde bağlantı trafiği, kullanıcı işlemleri vb. bilgilerin kaydedilmesi gerektiği de rehberde belirtilmiştir.

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikte yer alan ve rehberle bağlantılı bulunan başka bir tedbir de "Ağ Tabanlı URL Filtreleri Kullanımı" olup ilgili kurumun onaylamadığı veya mevzuatla erişimi yasaklanan sitelere bağlantıyı engellemek amaçlı ağ tabanlı URL filtrelerinin uygulanması gerektiği bildirilmiştir.

Veri sızıntısı önleme başlığı altında ağdaki kritik verilerin taşınmasında VPN teknolojileri, güvenli soket katmanı (Secure Sockets Layer, SSL) veya taşıma katmanı güvenliği (Transport Layer Security, TLS) gibi güvenli protokollerin kullanılması gerektiği ve ağ teknolojileri kullanılarak veri sızıntılarının önlenebilmesi adına sistemler kurulması gerektiği belirtilmiştir. Bu takip mekanizmalarının da ana amacı ağ adli bilişimi olmamakla birlikte ağ üzerinde etkinin artması sonucunda log tutma yeteneklerini artıracağı düşünülmektedir.

Ağ kayıtlarının tutulmasına dair en önemli ana başlıklardan birisi de rehberde "İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi" olarak yer almaktadır. Bu kapsamdaki tedbirlerde kayıtların mevzuattaki kayıt süreleri kadar tutulması gerektiği ve belirlenen saklama sürelerinin bitmesiyle birlikte güvenli bir şekilde yok edilmesi gerektiği belirtilmiştir. Bu çalışmada da vurgu yapıldığı üzere ilgili Kanun ve Yönetmeliklerde kayıtların silinmesi üzerine sorumluluklar yer almaktayken, yok edilmesi hususundan doğrudan bahsedilmemektedir. Bu husus rehberde açıklık kazanmış olup kayıtların güvenli bir şekilde yok edilmesi gerektiğinden bahsedilmiş olup, teknik bir detaya veya yönteme rehberde de yer verilmemiştir.

Sistem yöneticilerinin ve kullanıcıların işlemlerinin kaydedilmesi, kayıtların korunması ve belirli aralıklarla incelenmesi gerektiği hususunun belirtildiği rehberde ayrıca ağa bağlı tüm

sistemlerin periyodik şekilde zaman bilgilerinin alınması ve zaman sunucusu kullanımının yedekli şekilde çalışması gerekliliği de belirtilmiştir. Sistem iz kayıtlarının detaylı bir şekilde tutulması gerekliliğinin yanı sıra merkezi bir kayıt yönetiminin kayıt analizi araçlarıyla birlikte hata oluştuğunda uyarı verecek bir yapıda kullanılması gerektiği belirtilmiştir. Rehberde yer alan kullanıcı hesaplarına dair işlemler ve erişim isteklerinin önceden belirlenmiş bir süreç ile izlenmesi ve kayıt altına alınması tedbiriyle, gizlilik dereceli verilerin saklandığı sistemlere açılan oturumlarda gerçekleştirilen faaliyetlerin kayıt altına alınması gerektiğini belirten tedbirlerin ağ üzerinde oluşacak yetkisiz erişimlere karşı ağ analizi hususunda yardımcı olabilecek başka bir tedbir olabileceği değerlendirilmiştir.

Adli analiz açısından bir başka önemli tedbir başlığı da "Felaket Kurtarma ve İş Sürekliliği Yönetimi" başlığında ele alınmış olup, yedekleme planı oluşturulması, planın belirli periyotlarla ele alınarak tekrar incelenmesi, yedekleme işlemlerine dair süreçlerin kaydedilmesi, yedeği alınmış kayıtlarından ana kayıtlara geri dönebilmek amacıyla testlerin gerçekleştirilmesi ve yedeklemelerin tutulduğu ortamların saklanması üzerine tedbirler alınmıştır. Bu kayıtların da adli analiz açısından önem arz eden yedeklilik ve verilerin kaybolmaması açısından önemli olduğu değerlendirilmiştir.

Bir başka tedbir de oturum kimliğinin URL içerisinde ve uyarı kayıtları ve mesajları içerisinde yer alma hususuyla rehbere eklenmiştir. URL içerisine oturum kimliğinin yeniden yazılmasının engellenmesinin gerektiği belirtilmiştir. Bu sayede erişim sağlanan web sayfaları IP adresi tabanlı kayıt tutulmasının ötesinde giriş yapılan kullanıcı bazında da kayıt altına alınmaktadır.

Veri tabanı üzerinde bulunan tüm kullanıcıların gerçekleştirdiği işlemlerin denetim kayıtlarının oluşturulması beklenmektedir. IoT cihazlarının güvenliği başlığında ağ portlarının kısıtlanması, merkezi bir yönetim gereksinimi ve ağ üzerinden gönderilen verilerin şifrelenerek iletilmesi ve cihaz üzerinde yer alan veri yedeklenmesi gibi tedbirler alınmış olsa da bu cihazların ağ erişimlerinin kayıt altına alınması hususuna değinilmemiştir. Her geçen gün sayısı hızla artan ve günlük kullanıma sunulan IoT cihazlarının erişim bilgilerinin analiz edilebilmesi için bazı kayıt ölçütlerin getirilmesinin faydalı olabileceği değerlendirilmiştir.

Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri ana başlığı altında kişisel verilerin güvenliğinin nasıl sağlanacağına dair açıklamalar yer almakta olup, kişisel verilere gerçekleştirilen erişim kayıtlarının, mevzuatlara uygun şekilde arşivlenmesi gerektiği belirtilmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanununda kişisel veri, kimliği belirlenebilecek olan gerçek kişiye dair tüm bilgileri içerecek şekilde tarif edilmiştir [125]. 6698 sayılı Kanunda silme veya yok etmeye dair bir çerçeve çizilmemiş olmakla birlikte bu hususta bir yönetmelik bulunmaktadır. "Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik" içerisinde kişisel verinin kaydedildiği bir ortamdaki verinin silinmesi "Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir." şeklinde tanımlanmıştır [126]. Ayrıca kişisel verilerin yok edilmesi de "Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir." şeklinde tanımlanmıştır [126]. Bu kapsamda yapılacak işlemlerin belirli politikalar dâhilinde veri sorumluları tarafından periyodik olarak yapılacak imha işlemlerinde gerçekleştirilmesi gerektiği de yönetmelikte belirtilmiştir. Silme işlemi ilgili kullanıcıların tekrar ulaşamayacağı şekilde kullanılamaz hale getirilmesi şeklinde tanımlanmışken, yok etme işleminin ardından kişisel verilere hiç kimse tarafından erişim sağlanamaması gerektiği belirtilmiştir. Tüm bu durumlar göz önüne alındığında yer sağlayıcı, toplu kullanım sağlayıcı vb. paydaşların mevzuata uyum amacıyla sakladığı trafik ve erişim bilgilerini belirlenen azami sürenin sonunda depolama birimlerinden geri döndürülemez şekilde silmesi yani yok etmesi gerektiği değerlendirilmiştir.

Önemli bir husus olarak Bulut Bilişim Güvenliği başlığında bulut hizmeti kullanımında kritik verilerin yurt içinde depolandığı ve yurt dışında barındırılamayacağı ve güvenlik göstergelerinin kurum tarafından denetlenmesi gerektiği belirtilmiştir. Kritik veriler arasında nüfus, sağlık, biyometrik ve genetik veriler örneklendirilmiştir. Verilerin yurt içinde barındırılması durumu 5651 sayılı Kanun ve ilgili mevzuatlarla uyum göstermektedir. Yurt dışındaki veriler üzerinde denetleme mekanizmasının daha zor bir duruma düşecek olması sebebiyle, engelleme, el koyma, arama vb. süreçler de dikkate alındığında verilerini yurt içinde depolayacak bir bulut bilişim hizmetinin alınmasının doğru olacağı değerlendirilmiştir. Rehberde ayrıca kişisel verilerin yurt dışına aktarım durumu olması durumunda açık rıza metninde belirtilerek kişinin rızasının alınması gerektiği belirtilmiştir. Mesajlaşma uygulamalarının sunucularının yurt içinde bulunmasının tercih edilmesi gerektiği de veri sızıntılarına karşı alınmış başka bir tedbirdir. Trafiğin yurt içinde kalması

amacıyla operatörlerin tedbir uygulamaları da belirtilen başka bir husustur. Bu kapsamda yurt içinden yurt içine gidecek bir trafiğin ülke içinde kalması sağlanması gerektiği, hiç yurt dışına çıkmadan doğrudan iletişim kurulacak şekilde düzenlemelerin yapılması gerektiği aktarılmıştır.

Bulut Bilişim hizmeti veren bir şirketin 5651 sayılı Kanunda tarif edilen yer sağlayıcı tanımına uygun olduğu değerlendirilmiş olup bu hizmeti sunan şirketlerin ilgili mevzuat hükümlerini de yerine getirmesi beklendiği değerlendirilmiştir. Rehberde servis sağlayıcı olarak geçen hizmet sunucular bulut ortamının güvenliğini de sağlamak zorundadır. Bulut sistemlerinde gerçekleştirilen yönetimsel işlemlerin de kayıt altına alınması gerektiği belirtilmiştir.

Bulut hizmeti kapsamında kurum kuruluşlarına hizmet vermek için servis sağlayıcılar sanal makineler oluşturmaktadır. Bu sanal makinelerden birisinin artık kullanılmayacak olması durumunda bulut sunucularındaki bellek ve disk ortamlarının da otomatik şekilde geri döndürülemez bir yapıda silinmesi gerektiği belirtilmiştir. Bulut hizmeti sunan kurumların yer sağlayıcılar kapsamında değerlendirilebileceği düşünülmektedir. Erişim kayıtlarının eşleşebilmesi adına belirtilen sanal makine hizmetlerinin silinmesi esnasında tutulan erişim kayıtlarının korunuyor olmasına dikkat edilmesi durumunun önemli olduğu değerlendirilmiştir.

Kripto uygulamaları ve kritik altyapıların güvenliğine dair sıkılaştırma tedbirleriyle sonlanan rehberde, diğer başlıklarda yer alan kayıtların saklanması sürecinin her duruma özel olarak işletilmesi gerektiği belirtilmiştir [64].

Detay bilgileri aktarılan bu rehbere ek olarak bu rehberdeki süreçlerin denetime tabi tutulabilmesi amacıyla CBDDO tarafından “Bilgi ve İletişim Güvenliği Denetim Rehberi” yayınlanmıştır. Bu rehber sayesinde denetimlerin önceden belirlenen bir yöntem kapsamında gerçekleştirilmesi, gerçekleşecek denetimlerin bağımsız bir usulle gerçekleştirilmesi, denetime dair elde edilen sonuçların CBDDO’ya iletilmesi ve bu süreçleri gerçekleştirecek denetçilere yol gösterilmesi amaçlanmıştır. Bu rehber denetime dair yöntemler ve adımlar üzerine bilgiler sunduğundan dolayı ağ adli bilişimi ve süreçlerine dair bir bilgi sunmamaktadır [65].

Hem bilgi ve iletişim güvenliği rehberinde hem de bilgi ve iletişim güvenliği denetim rehberinde 5G ve SDN özelinde bir çerçeve çizilmemiş olup, konu ve kapsam geleneksel ağlar üzerinden ilerlemiştir.

5.4. SDN Tabanlı 5G Ağlarında Adli Bilişimin İdari Açıdan İncelemesi

5G ağlarında adli bilişim çalışmaları da özünde geleneksel ağlarda gerçekleşecek adli bilişim çalışmalarına uyumlu olmak durumundadır. Ancak ek olarak bazı hususlara da dikkat edilmesi gerekmektedir. 5G ağlarında IP tabanlı iletişim SDN yardımıyla gerçekleştiğinden dolayı ilk başta SDN ağlarındaki iletişimin adli bilişimine odaklanmak gerekmektedir. Ancak 5G'nin kablosuz haberleşme altyapısı dikkate alındığında IMEI, IMSI, MSISDN ve LIID bilgilerinin kayıt altına alınması hususunun olası bir adli bilişim çalışmasına katkı sunabileceği değerlendirilmiştir. Kullanıcı ve sinyal trafiğine dair paket dosyalarının, kaynak ve hedef telefon numarası, arama süresi, arama zamanı bilgilerinin de tutulması sürece katkı sağlayacaktır. Adli bilişim açısından önem arz eden bir diğer önemli bilgiyse kullanıcıların konum bilgileridir. IP tabanlı hizmetler sayesinde bu bilgilerin büyük kısmı elde edilebilir olsa da kablosuz haberleşme bilgileriyle birlikte daha fazla bilgiye sahip olunacak ve bu durum adli bilişim süreçlerine katkı sunmuş olacaktır.

"Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğin Korunmasına İlişkin Yönetmelik" içeriği incelendiğinde elektronik haberleşme şebekelerini odağına aldığı görülmektedir. İlgili yönetmelikte konum verisi tarifi yapılmış olup, coğrafi olarak konum verisinin 5G ağlarında da tutulabileceğini ve ötesinde tutulması gerektiği değerlendirilmiştir. Ancak bu konum verilerinin milli güvenlik yurt dışına çıkarılmaması gerekmektedir. Bu durum ağ altyapısının güvenliğinin sağlanmasına dayalıdır. Konum verileri dışında diğer kişisel verilerin güvenliğinin sağlanması ve belirlenen sürelerin sonunda silinmesinden bu yönetmelikte de bahsedilmektedir. Trafik ve konum verilerine dair bilgilerin üçüncü taraflarla paylaşılması gereken durumlarda verinin kapsamı, tarafın adı ve açık adresi, aktarma amacı ve süresi, yurt dışında bir tarafla paylaşılması durumundaysa verinin aktarılacağı ülkenin adının belirtilmesi zorunludur. Ek olarak kişisel verilere erişime dair kayıtların da iki yıl boyunca saklanması gerektiği yönetmelikte belirtilmektedir [149].

NFV altyapısını kullanan 5G ağlarında sanallaştırma altyapısına karşı gerçekleşen saldırıların kayıtlarını tutacak mekanizmaların ve hata günlüklerini kaydedecek sistemlerin

oluşturulmasının önem arz eder. Ancak IP bazlı erişimlerde SDN altyapısının hizmet vermeye devam ettiği durumlarda ağ haberleşmesine dair gerekli veriler tutulabilir olacaktır. SFC veya VNF yardımıyla oluşturulan sanal ağ fonksiyonları ve zincirlerle bir trafiğin farklı ağ ortamlarından geçmesi gerekebilir. Ağ dilimleme yardımıyla farklı hizmetlere farklı öncelikler tahsis edilebilir ancak bu durumda merkezi SDN adli bilişiminin ötesinde bir ek bilgi getirmeyecektir. Buna rağmen trafik mühendisliğine dair işlemlerin yardımcı donanım ve sistemler tarafından tutuluyor olması adli bilişim süreçlerine katkı sunacaktır. En önemli olan durumsa özünde her ayrı SDN ortamının bu tez kapsamında oluşturulan süreçlere uygun adli bilişim çalışmalarını gerçekleştiriyor olmasıdır.

Bu tezin kapsamını oluşturan 5G ağlarındaki adli bilişim süreçleri için SDN'e odaklanmak gerekmektedir. Ağ katmanlarının ayrıştırılmasıyla oluşan esnek ağ mimarisiyle SDN çok sayıda 5G kullanıcısına hizmet vererek, performanslı bir altyapı için vazgeçilmez bir teknolojidir. Kullanıcıların internet erişimlerinin kayıt altına alınmasının yanı sıra saldırı tespitleri de yine 5G'nin ağ altyapısında gerçekleştirilebilecek süreçlerdir. Bu sebepten hem internet erişimlerinin kayıtlarını tutacak hem de güvenlik olaylarını raporlayacak bir adli bilişim sistemi SDN altyapısı sayesinde mümkündür.

5.5. Ağ Adli Bilişiminde Uluslararası Durum Tespiti

AB üyesi ülkelerin siber güvenlik stratejilerini belirleyen bir merkezi kurum olan ENISA (The European Union Agency for Cybersecurity) 2017'den beri aktif olarak çalışmaktadır [31]. Üye ülkelerdeki siber suçların engellenmesine yönelik çok sayıda teknik doküman ve rehber çalışması bulunan kurumun adli bilişim odağı siber güvenlik kadar yüksek değildir. ENISA tarafından hazırlanan, hafıza birimleri ve diğer ortamların adli bilişim işlemlerinde nasıl kullanılacağına dair bilgiler yer alan rehberler bulunmaktadır [150–152]. Ağ adli bilişimi odağında ise verilerin nasıl elde edileceğine dair yönlendirmeler [30, 153], işletim sistemleri ve kayıt formatları hakkında öneriler yer almaktadır. Ancak AB merkezli veya AB üyesi ülkeler özelinde yürürlükte olan mevzuatın adli bilişim süreçlerine yönelik bilgiler dokümanlar arasında yer almamaktadır.

Avrupa'da adli bilişimin de içerisinde yer aldığı adli araştırma konularında kalite artırma hedefi olan bir kurum olarak ENFSI (The European Network of Forensic Science Institutes) mevcuttur. Türkiye Cumhuriyeti'nde Jandarma ve Emniyet Kriminal Daire Başkanlıkları,

İstanbul Üniversitesi-Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü ve Adli Tıp Kurumunun üyesi olarak yer aldığı bu kurum, 17 alt teknik alan özelinde araştırmalar yapmaktadır [154]. ENFSI'nin web sayfası incelendiğinde ağ adli bilişimi adına yönlendirici rehber niteliğinde bir doküman veya çalışma olmadığı görülmüştür.

Ağ adli bilişimini hem geleneksel ağlar için hem de SDN odağında teknik ve idari açıdan ele alınan bir çalışma literatürde bulunmamaktadır. Bazı çalışmalar adli bilişimini hukuki açıdan ele alarak ceza ve yaptırımlara yer vermiştir. Bu çalışmalarda delil elde etme süreçleri de idari açıdan ele alınmıştır. Ülke özelinde gerçekleştirilen çalışmalarda İtalya'da delillerin bütünlüğü, yeniden üretilmesi, kopyalanması gibi adli bilişim aşamalarında hukuka uygunluğun sağlanmasına odaklanılmıştır [36]. Kişisel veri hakları ve kolluk kuvvetlerinin sorumluluklarını delil açısından ele alan bir çalışma da mevcuttur [35]. Adli bilişimin önemi vurgulanan ve İtalya'da gerçekleşen bu çalışmalarda ağ adli bilişimi özelinde bir bilgi veya süreç önerisi mevcut değildir. Latin Amerika özelinde gerçekleşen bir diğer çalışmada siber güvenlik kavramının tekil olarak ele alınamayacağı belirtilmiş ve ülkeler arası iş birliğinin önemi vurgulanmıştır [37]. Ülke özelinde önerilerin ötesinde siber güvenlik veya adli bilişim yazılımları geliştiren şirketlerin dâhil olduğu bir politikanın gerektiği de vurgulanmıştır [43].

Yapılan incelemelerde her ülkenin adli bilişim olaylarına karşı hazırlık düzeyinin artırılması gerektiği değerlendirilmiştir. Kanunlar özelinde ülkeler incelendiğinde Almanya, ABD, Güney Kore ve Birleşik Krallık arasındaki uygulama farklılıkları dikkat çekmektedir. Asya ülkeleri son yıllarda siber suç kapsamındaki cezalara dair stratejik çalışmalar gerçekleştirmiştir [41]. ABD'de hangi hukuk dallarının adli bilişim aşamalarında ele alınması gerektiği belirlenmiştir. Bu hukuk dalları arasında ceza, mülkiyet, sözleşme ve delil hukuku alt alanları yer almaktadır [42]. Bu durum adli bilişim çalışmalarında nerelere başvurulması gerektiği açısından kıymetlidir. Ayrıca ABD'de kolluk kuvvetlerinin yasalara uyumlu adli bilişim çalışmalarında hangi adımları takip etmesini gerektiğini belirten bir rapor örneği NIJ (National Institute of Justice) tarafından oluşturulmuştur [32]. Bu çalışma adli analiz yapacak olan sorumluya teknik açıdan büyük kolaylık sağlamıyor olsa da adımların unutulmaması açısından faydalıdır. Diğer ülkelere göre ABD özelinde daha fazla adli bilişim çalışması yapıldığı ve daha hazır bir durum olduğu görülüyor olsa da bu çalışmalar da ağ adli bilişimi odağında standart süreçler değildir.

Endonezya özelinde dijital delillerin nasıl ele alınması gereken bir çalışma yapılmış olsa da bu çalışma bir adli bilişim sürecinden ziyade ülke özelindeki siber suçları azaltmayı hedefleyen genel bilgileri içermektedir [38]. Adli bilişimin kültür ayağının da ele alındığı bir çalışma Avusturalya özelinde gerçekleştirilmiştir [40]. Akredite bir kuruluşun eksikliği vurgulanan Çin'de delil toplama süreçlerinin güvenilirliğinin artırılması hedeflenmiştir [39]. Bahsi geçen ülkelerin yanı sıra Suudi Arabistan'da delillerin elde edilmesi açısından kanuni eksiklikler bulunmaktadır. Ayrıca hapis ve para cezaları siber suçlar kapsamında ele alınan çalışmalar bulunmakta olup delil korunması da eksik olan bir diğer husus olarak ülke özelinde karşımıza çıkmaktadır [33]. Gana için de benzer şekilde adli bilişim açısından kanunların ve kuruluşların eksikliğine vurgu yapılmış olup, adli bilişim hazırlık düzeyi daha yüksek olan ülkelerle iyileştirme çalışmalarının yapılması gerektiği vurgulanmıştır [34].

Avrupa Komisyonu adli bilişim çalışmalarının insan hakları normları gözetilerek gerçekleştirilmesi gerektiğini belirtmektedir. Birleşmiş Milletler Genel Kurulu da adli bilişim çalışmalarında kişisel gizlilik ve özgürlüğün korunması gerektiğine vurgu yapmaktadır [44]. Bahsi geçen tüm adli bilişim süreçlerinin, geliştirilme aşamasından gerçekleştirme aşamasına kadar hukuki süreçlerle uyumlu olması gerekmektedir [45].

Kişisel verilerin korunması amacıyla AB'de GDPR yönetmeliği yürürlüktedir. Bu kapsamda geliştirilen bir SDN çalışmasında uygulama katmanıyla veri katmanı arasındaki iletişimde gerçek zamanlı veri işleme gerçekleştirilerek kişisel verilerin erişimine dair kontrol yapılması mümkün kılınmıştır [127]. Kişisel verilerin korunması kanunu ülkemizde yürütülecek uygulamalarda dikkate alınmalı ve yeni geliştirilecek sistemler özelinde mevzuat uyumlu düzenlemeler yapılmalıdır [155]. GDPR haricinde AB'de haberleşme ağlarıyla ilgili düzenlemeleri içeren EECC (European Electronic Communications Code) yönergesi bulunmaktadır. Bu yönergeye uymanın SDN adli bilişim alanında da kazanımlar içerebileceği değerlendirilse de yönerge kapsamında bir SDN değerlendirmesi veya politikası bulunmamaktadır [123].

5.6. SDN Adli Bilişiminde Delil Kaynakları ve Bilirkişilik

Ceza muhakemesinde delillerin genel özellikleri; gerçekçi olması, geçmişteki somut olayı temsil edici olması, akla uygun olması, elde edilebilecek formatta olması, kanuna uygun şekilde ele geçirilmiş olması ve tarafların bilgisine sunulabilecek şekilde bilgi içerebilmesi

olarak sıralanabilir [54]. Elektronik deliller bir uzman tarafından teknik anlamda incelenmek zorundadır. Klasik deliller genellikle gözle görülebilir nitelikte iken, elektronik deliller teknik inceleme olmaksızın soyut bir niteliğe sahiptir. Örneğin bir depolama aygıtının kendisi değil ancak içindeki verilerin anlamsal bütünlük kazanmış hali bir delildir. Bu elektronik delillere örnek olarak fotoğraflar, videolar, yazışmalar vb. gösterilebilir.

Günümüzde suç işlenmesinin ardından elde edilebilecek deliller düşünüldüğünde, parmak izi, suç aleti vb. delillerden elde edilebilecek bilgiden daha fazlasının arama kaydı, mesajlaşmalar, fotoğraflar, silinmiş bazı bilgi ve belgelerin kurtarılmasından elde edilebileceği değerlendirilmektedir. Bu sebepten elektronik delillerin kanunda tanımlanmasının çok önemli olduğu değerlendirilmiştir. Kanunda dolaylı olarak tarif edilen delil elde etme ve arama gibi hususların, özet alma tekniklerinden, veri arama ve kurtarma tekniklerine kadar, tüm ürünlerin uyum sağlayabileceği bir formda standartlaşmış şekilde kanunda tarif edilmesinin bu denli hassas bir konuda hem adli birimler tarafından karar vermenin kolaylaşması hem de kolluk birimlerince uygulanacak adımların netleşmesi açısından faydalı olacağı değerlendirilmiştir.

Adli bilişim çalışmalarını gömülü cihaz, bilgisayar ve ağ alt başlıklarına ayırmak mümkündür. Gömülü cihaz ve bilgisayar adli bilişimi genellikle depolanmış veriler üzerinden delil elde etmeye odaklanırken, ağ adli bilişimi akan veri veya bu akan verinin depolanmış halleri üzerinden gerçekleştirilir [54]. Gerçekleştirilen adli bilişim çalışmaları OSCAR yöntemi kapsamında “bilgi edinme, strateji oluşturma, delil toplama, analiz ve raporlama” aşamalarından oluşmaktadır [156]. Ağ adli analizi için kullanılan programlar ağda canlı akan verileri veya bu verilerin depolanmış sürümleri üzerinden inceleme yapılmasına olanak tanır. Bu sayede paket yakalama, verileri filtreleyerek port, protokol, adres vb. bilgileri elde etme gibi süreçler gerçekleştirilebilir [46]. Bu programlar yardımıyla gerçekleşen analizlerde geçmişe yönelik veya canlı incelemeler esnasında “ne zaman, neden, nerede, ne, nasıl ve kim” sorularına cevaplar aranır [25, 26]. İncelemelerde bir veri seti elde edilebilir veya hazır bir veri seti üzerinden çalışmalar gerçekleştirilir. Elde edilecek veya incelenecek verilerin FAIR ilkesine uyumlu olması gerekir [26].

CMK Madde 134’te analizlerde elde edilen verilerin delil olabilme durumları yer almaktadır. Sabit diskler, bilgisayarlar vb. ortamlardan elde edilen bu sistemlere veya verilere el konulabileceği, bütün verilerin yedekleme sürecine tabi tutulması, kopyalarının alınarak

şüpheliye ve vekiline tutanakla verilmesi hususları CMK'da yer almaktadır [60]. Bu süreçlerin uygulanması başta kolluk kuvvetleri tarafından yapılmaktadır. Bu birimler siber suçları önleme ve soruşturma aşamalarında görev almaktadır [55]. Delillerin genel özellikleri arasında başta kanuna uygun yollarla elde edilmiş olması gelmektedir. Gerçekleşen olayları somut şekilde temsil etmesi gereken delillerin ayrıca gerçekçi olması ve tarafların bilgisini sağlayacak şekilde olması gereklidir [54].

Çözümü için teknik bilgi birikimi gereken konularda CMK 63-1'e istinaden bilirkişiler atanabilir. Bilirkişiler adli bilişim çalışmalarında sayısal delil içerebilecek sabit disk, program vb. her türlü ortamdan veri elde edebilir. Ancak vaka artışlarında son yıllardaki on kata varan artışlar delillere en kolay ve hızlı şekilde ulaşılmasını gerektirdiğinden delil kaynaklarını bir önceliklendirmeye tabi tutmak gerekebilir. Cumhuriyet savcısı tarafından verilen arama kararına istinaden olay yerinde veya inceleme aşaması için laboratuvar ortamında önceliklendirme yapılabilir. Adli bilişim çalışmalarını yürütecek bilirkişiyse deliller arasında ikinci defa önceliklendirme yapabilir. Arama kararı kolluk birimleri tarafından gerçekleştirilen bir bilirkişilik sürecini ortaya çıkarır ancak teknik açıdan delillere ulaşmak için ayrıca bilirkişiler de görevlendirilebilir. İnceleme aşamasında kısa süre içinde kaybolacağı düşünülen veriler önceliklendirilmelidir. Ayrıca delil içermesi daha muhtemel kaynaklar da önceliklendirme kapsamına alınabilir [47].

En çok kullanılan işletim sistemlerinden Windows'ta kayıt defterleri, internet geçmişi, dosya işlemleri ve geçici bellek bilgilerine erişim sağlanabilir. Buna benzer erişim süreçleriyle şifre değiştirme, oturum bilgileri, açılan belgeler gibi bilgilere erişim sağlamak mümkündür. Sanallaştırma sistemine ait adres bilgileri, ağ bağdaştırıcısına ait bilgiler, son oturum süresi, ağ bağlantılarına dair bilgiler de erişim sağlanabilecek diğer bilgiler arasında yer alır [48]. Bir diğer sık kullanılan işletim sistemi Linux'te de benzer şekilde ağ durumu, dosya değişiklik kodu, modül değişiklikleri gibi bilgiler elde edilebilir [49]. Silinmiş dosyalara ait verilerin kurtarılması, programlar yardımıyla mümkündür ancak süreçler uzun süre ve uğraş gerektirebildiğinden yüksek efor harcamak gerekir. Diskte mevcut olan veya silinmiş şekilde yer alan dosyalar arasından anahtar kelimeler kullanarak arama yapılması ve bu sayede süreçlerin odaklı sürdürülmesi mümkündür [51]. Mobil cihazlar üzerindeki verilerin elde edilmesine yönelik, imajının alınmasından verilerin elde edilmesine kadar bir süreç mevcut olup, sıklıkla kullanılan mobil cihazlar adli bilişimin vazgeçilmez bir parçasını oluşturur [50]. Verilerin dinamik oluşu, yerlerinin tespit edilmesi gibi delil elde etme aşamalarında

zorluklar çıkarabilecek bulut bilişim açısından da süreçlerin henüz yasal standardı mevcut değildir. Teknik ve idari açıdan ele alındığında bulut bilişim süreçleri diğer adli bilişim dallarını kapsayabileceğinden dolayı yeni yöntemlere ihtiyaç duyulmaktadır [52].

Geçici bilgilerin tutulduğu çevre birimleri de adli bilişim açısından önemli bilgileri içerebilir. Bu kapsamda tespitler gerçekleştirebilen program ve yöntemler mevcuttur. RAM vb. bölgelerden temin edilebilecek bu uçucu verilerin kayba uğramaması için cihazların normal kapatma yöntemi yerine direkt güçten kesme yöntemiyle kapatılması gereklidir. Bu şekilde gerçekleştirilmezse ön bellek, swap ve hazırda beklet dosyaları gibi dosyalarda yer alan bilgiler kaybedilebilir [51]. RAM üzerinden bilgi elde etmek için imaj dosyasının sistem çalışırken alınması önem arz etse de sistem kapansa dahi bilgi elde etmek mümkündür [49].

Ağ bağlantılarına dair bilgiler de geçici bilgiler kategorisine alınabilir. Aktif durumdayken kayıt altına alınmayan ağ verilerine tekrar erişmek zor bir süreçtir. Çünkü bu bilgilerin sadece bir kısmı geçici süreyle anahtarlarda, kayıt defterinde, etki alanı vb. çevre birimlerinde yer alır [51]. Sağlıklı adli bilişim gerçekleştirilmesi için tüm delil kaynaklarının efor, önem, uçuculuk ve öncelik kriterleri çerçevesinde, her durum özelinde değerlendirilerek adli bilişim süreçlerinin gerçekleştirilmesi gerekir.

5.7. Mevzuat ve Uluslararası Uygulamalara Uyumlu Ağ Adli Bilişim Sürecinin İdari ve Teknik Gereksinimleri

Mevzuat, ulusal rehberler, uluslararası çalışmalar, uygulamalar, politikalar ve standartların ağ adli bilişimi odağında incelenmesi sonucunda, bu kaynaklarda yer alan bilgilerin genel çerçeveden bilgiler olduğu, teknik detay ve yönlendirmelerin yer almadığı görülmüştür. İncelenen tüm kaynaklar doğrultusunda oluşturulacak ağ adli bilişim süreçlerinin asgari olarak aşağıdaki şartları yerine getirmesi gerektiği değerlendirilmiştir:

- Siber suçların aydınlatılmasına yönelik aktif kayıt sistemlerinin kullanılması [56, 61–64],
- Kayıtların mevzuat uyumlu ve elektronik delil sayılabilecek doğrultuda ele geçirilmesi [60],
- Kayıtların yedekli sistemlerde ve güvenli altyapılarda muhafaza edilmesi [62, 64, 66],

- Muhafaza edilen kayıtların mevzuatta belirtilmiş olan azami süreler bittiğinde geri elde edilemeyecek şekilde silinerek yok edilmesi [59, 126],
- Kayıtların doğruluk, bütünlük ve gizlilik ölçütlerini sağlamak amacıyla güvenlik mekanizmalarının kurulması, özetleme sistemlerinin kullanılması ve zaman damgası sürecinin işletilmesi [61, 66, 124],
- Tek bir kaynaktan zaman damgası kullanılarak kayıt dosyalarına dair zaman bilgisinin eksiksiz şekilde tutulması ve elektronik imza ile kayıtların onaylanması [66, 124, 146],
- Normal olmayan durumlar, hatalar gibi durumlarda kayıtların üretilerek saklanması ve bunların gözden geçirilmesi [64–66],
- Güvenlik ihlalleri durumlarında ve rutin olarak toplanan kayıtlarda mevzuata, standartlara, politikalara vb. uygun bir sürece uyum sağlanması [66],
- Bu sürecin denetimlere tabi olması ve denetim sonucu ortaya çıkan önlemlerin alınması [65, 66],
- Kritik verilerin yurt içinde depolanması ve zaten yurt içinde yer alan bir hedefe giden erişimlerin yurt dışına çıkmadan erişimin sağlanması [64],
- Gizli verilerin internet erişimi olmayan ve fiziksel güvenliği sağlanmış ortamlarda, etkin kayıt sistemleriyle saklanması [64],
- Ağ adli bilişimi için ek bilgi sağlayabilecek olan kayıtların tutulduğu depolama birimlerinin güvenlik ve erişim süreçlerinin belirlenmesi [66],
- IP adresi veya URL temelli filtreleme süreçleriyle erişimin kısmen veya tamamen engellenebiliyor olması [61, 62, 64],
- İnternet erişimi olan IP adreslerinin sabit olarak kullanımı ve IP adres bilgilerinin kaydedilmesi [61, 62],
- Trafiğin izlenebilmesi için etkin kayıt sistemlerinin kurulması [56, 61–63],
- Sadece gerekli görülen kullanıcıların ve hizmetlerin internet ortamına gidiş için yetkilendirilmesi [64, 66],
- Teknik erişim bilgileriyle kullanıcı veya abonelerin belirleyici bilgilerinin (ad, soyad, kimlik numarası vb.) eşleştirilerek kullanılabilmesi [62].

Genel bir ağ adli bilişim sürecinin kurulabilmesi için yukarıdaki gereksinimlerin yerine getirilmesi gerekmektedir. Belirtilen hususların yerine getirilmesi için teknik yöntem zorunluluğu belirtilmemiş veya bu konularda tavsiye verilmemiştir. Bu sebepten süreçlerin yerine getirilebilmesi kaydıyla kabul görmüş yöntemlerden birisi seçilerek süreçlerin

gerçekleştirilmesi mümkündür. Ancak mevzuata uyumlu kayıt oluşturmak ve delil elde etmek için aşağıda belirtilen teknik kayıtların zorunlu olarak net biçimde kayıt altına alınmış olması gerektiği değerlendirilmiştir:

- Kaynak ve hedef IP adreslerinin bilgileri [56, 61, 62, 141],
- Protokol ve bağlantı portu bilgileri [56, 61, 63],
- Gerçekleştirilen hizmetin başlama ve bitiş zamanları ve türü [56, 62, 63],
- Aktarımı sağlanan verinin boyutu [56],
- Otomatik IP dağıtımındaki IP adres bilgileriyle bu adreslerin dağıtımına dair başlama ve bitiş zamanları ve ilgili kullanıcının MAC adresi bilgileri [61],
- Talep edilen URL bilgileri [62, 63],
- Web erişim taleplerinde; hedef site adresleri, GET-POST süreci detay bilgileriyle birlikte işleme ait sonuç bilgileri [62].

Bu bilgilerin de teknik olarak paket tabanlı veya akış tabanlı vb. hangi yöntemlerle elde edilmesi gerektiği belirtilmemiştir. Belirtilen bu teknik detayların tüm paydaşlar tarafından bütünsel bir şekilde ele alınarak eksiksiz olarak kayıt altına alınması bir zorunluluk olup, adli analiz süreçlerinin sağlıklı gerçekleştirilmesi ve geçerli olması için önemlidir.

5.8. Bölüm Değerlendirmesi

Mevzuatın ağ adli bilişimi odağında tüm detaylarıyla incelenmesi sonucu ortaya çıkan bu sürecin adli analizden sorumlu kişi ve kurumların iş süreçlerini kolaylaştıracağı düşünülmektedir [128]. Ele alınan mevzuatın ilgili bölümlerinin ve tabi olunan standartların birbiriyle uyumlu ve karşılıklı doğrulama oluşturan bir yapıda olduğu görülmüştür. Otomatik IP adreslerinin dağıtılmasına dair verilerin kayıt altına alınması ve URL temelli filtreleme yeteneğinin bulunması zorunluluğu bu duruma örnek olarak gösterilebilir [61, 64]. İlgili ülkenin mevzuatına uyum sağlanması gerektiği belirtilen ISO 27001 standardına uyum sağlanması da doğal olarak tüm süreçlerin eş zamanlı bir şekilde işlemesini sağlamaktadır.

Mevzuatın genelinde teknik detaylara yer verilmediği görülmüştür. Örneğin kayıtların tutulması gereken dosya formatı veya depolama ünitelerinin özellikleri belirtilmemiştir [56–59, 61–65, 148]. Bu sayede üretici şirketlere olan bağımlılık azaltılmış ve tek markaya

muhtaç olunmasının önüne geçilmiştir. Öte yandan bu durum, kişi ve kurumların çok sayıda markaya ait olan cihazlar üzerine bilgi sahibi olması ve farklı uzmanlıklara sahip olunması gereksinimlerini de doğurmuştur. Özetleme yöntemleri, verileri geri döndürülemez şekilde silme süreçleri gibi yöntemler de standartlaşmamış olup bu tarz süreçlerin başarısı ispatlanmış ve literatürde kabul görmüş yöntemlerle gerçekleşmesinin faydalı olacağı düşünülmektedir. Mevzuatın hızlıca güncellenmesi zor olduğundan Kanun veya Yönetmeliklerde doğrudan belirtilmemesi faydalı bulunsa da, politika veya rehber niteliği taşıyan belgelerde doğrudan yöntem tavsiyesi sunulmasının, olası yanlış yöntem seçimlerinin önüne geçebileceği değerlendirilmiştir.

Bazı teknik süreçlerin net bir şekilde belirtilmemesinin aksine doğrudan gereksinim duyulan bazı verilerin de mevzuatta belirtildiği görülmüştür. Örneğin GET ve POST bilgilerinin kaydedilmesi teknik açıdan sadece HTTP (Hyper Text Transfer Protokol) türündeki bağlantılarda mümkündür [62]. Bu durum mevzuatta açıkça belirtilmektedir. HTTPS (HTTP Secure) bağlantılarında teknik olarak kullanıcılarla güven ilişkisi kurulacak bir sertifika sayesinde trafik izlemesi yapabilmek mümkün olsa da bu durumun hukuki altyapısı açık değildir. Bağlantı türünden bağımsız olarak beklenen diğer trafik bilgilerinin erişiminde yöntemsel farklılık kaynaklı bazı zorluklar olabilecek olsa da, tüm yöntemlerin bu bilgilere erişim sağlamada kullanılabileceği düşünülmektedir.

Kayıtların muhafaza süresinin dolmasının ardından silinmesi veya yok edilmesi hususunda gereksinimler mevcuttur [59, 64]. Belirtilen yok etme işleminin fiziksel yok etmeden ziyade kayıtların geri getirilemeyecek şekilde verilerin üzerine yazılmasının ardından silinmesi işlemi olduğu değerlendirilmiştir. Bu şekilde silme yöntemleri disk üzerindeki verinin üzerine farklı sayıda ve farklı içerikte veri yazılması yöntemiyle gerçekleştirilir. Bu yöntemin seçimine dair bir tavsiyeye de yer verilmemiştir. Ancak bu durumun da bir politika olarak belirlenmesi faydalı olacaktır.

Ulusal ve uluslararası çapta mevzuat ve standartlar ele alınarak oluşturulan bu ağ adli bilişim sürecinin teknik detaylarının belirlenmesinin zaruri olduğu değerlendirilmiştir. Bu kapsamda altıncı bölümde teknik hususlar tartışılacak olup, belirlenen teknik süreçlere uygun olan ve SDN tabanlı 5G ağlarına uyumlu bir adli bilişim sisteminin geliştirilmesi süreci aktarılacaktır.

6. SDN TABANLI 5G AĞLARINA UYUMLU ADLİ BİLİŞİM SİSTEMİ

Oluşturulan adli bilişim süreçlerinin bir politika olarak belirlenmesi, sorumlu kurumlar ve kişiler açısından yol gösterici ve bağlayıcı olacak ve adli bilişim çalışmalarına hazırlık düzeyinin artmasına katkı sunacaktır. Ancak sorumluların teknik bilgisi her durumda sürecin tamamını takip etmek için yeterli olmayabilir. Bilgi açısından yeterli olunan durumlarda ise teknik altyapı sürecin takibi açısından yeterli olmayabilir. Takip süreçlerinde insana bağımlı, yani otomatik olmayan süreçlerin izlenmesi teknik açıdan sağlıklı adli bilişime ulaşılmasını zorlaştıracağı gibi, sorumluların herhangi bir süreci unuttuğu aşamada kişi ve kurumların idari ve adli yükümlülüklerle karşı karşıya kalmasına sebebiyet verecektir. Bu gerekçelerle, oluşturulan adli bilişim süreçlerinin otomatik şekilde işletileceği SDN uyumlu adli bilişim sistemi geliştirilmesi hedeflenmiştir. Sistemin ana amacı mevzuat kapsamında belirlenen teknik kayıt gereksinimlerinin müdahaleye gerek kalmaksızın, altyapının türü ve tercih edilen markalardan bağımsız şekilde standart olarak toplanabilmesidir.

Geleneksel ağların ötesinde bir mimariye sahip olan SDN tabanlı 5G ağlarına da uyumlu olan sürecin geliştirilmesinin tamamlanmasının ardından bu sürece uyumlu bir sistem tasarımı hedeflenmiştir. 5G ağlarında adli bilişim çalışmalarının merkezinde SDN ve sanal altyapılar bulunmaktadır. Geliştirilecek adli bilişim sistemi de sanal altyapı kullanılarak ve SDN uyumlu geliştirilmesi hedeflenmiştir. Bu sayede gerçek ortamlara uygun bir sistem geliştirilerek literatüre katkı sunulacaktır. Geliştirilen sistem alt sistemlerden oluşmakta olup hem adli bilişim hem güvenlik yönetimi açısından 5G ağlarına hizmet edecektir.

Bu çalışmayla ortamdaki kayıtların elde edilmesinden yok edilmesine kadar olan süreçte yasal mevzuata otomatik uyum sağlayan, güvenli ve otomatik bir sistem geliştirilerek literatürdeki boşluğun doldurulması hedeflenmiştir. Beşinci bölümde tanımlanan süreçteki tüm gereksinimler göz önüne alınarak geliştirilen sistem, farklı kaynaklardan güvenlik olaylarını toplayıp analiz ederek, güvenlik operasyon merkezleri (Security Operation Center, SOC) için önemli bir rol alan güvenlik bilgi ve olay yönetimi (Security Information and Event Management, SIEM) ürünlerine [18, 104, 157] bilgi sağlamak için anormal akış sayısı ve bant genişliğinin oluştuğu durumlarda uyarı vermektedir. Ayrıca yurt dışına bilgi akışının olmaması gereken durumlarda coğrafi tespitler yapılmasına imkân sağlayan alt sistemler de içermektedir.

Bu adli bilişim sisteminin amaçları aşağıda sıralanmaktadır;

- SDN ortamındaki internet erişimlerinin mevzuat kapsamındaki gereksinimler gözetilerek kayıt altına alınması,
- Zararlı ve/veya yasaklı internet erişimlerinin SDN yetenekleriyle engellenebilmesi,
- Kayıt dosyalarına özetleme, şifreleme, imzalama işlemlerinin gerçekleştirilmesinin ardından yedekli bir yapıda muhafaza edilmesi,
- Saklanan kayıt dosyalarının mevzuatta belirtilen sürenin sonunda geri döndürülemez şekilde silinmesi,
- Servis dışı bırakma ataklarına karşı tüm sistemin güvenliğini artıracak sistemlerin SDN odağında geliştirilmesi,
- Ülke dışına gitmesi yasaklı olan verilerin sızma durumunun tespit edilmesi,
- Geliştirilen tüm alt sistem ve modüllerin otomatik çalışacak şekilde sisteme dâhil edilmesi.

Tüm amaçlara dair geliştirmeler hakkında bilgi verilmesinin ardından sistemin performans ve güven testleri gerçekleştirilmesi için gerçekleştirilen deneyler hakkında bilgiler aktarılacak olup, elde edilen sonuçlar da bu bölüm içerisinde paylaşılacaktır.

6.1. Sistemin Tasarlanması

Genel olarak ağ izleme ve anormallik tespiti yardımıyla saldırı tespit sistemlerinde kullanılan sFlow'un tespit edilen gereksinimlere uygun şekilde kullanılarak logların elde edilmesi sistemin ana amacıdır. Sistemin geliştirme aşamasında güncel teknikler kullanılmış olup [158–161], alt sistemler python kullanarak geliştirilmiş ve açık kaynak sistemlerden faydalanılmıştır.

6.1.1. Logların elde edilmesi

Ağ üzerinden geçen verilerin paket tabanlı ve akış tabanlı yöntemlerle elde edilmesi mümkündür. Kontrolcü veya sanal anahtarlar üzerinden elde edilebilecek verilerin yanı sıra güney arayüzü de, SDN'de önemli delil merkezleri arasında yer almaktadır [140]. Akışta keskin artış durumunda OpenFlow kullanılan yöntemlerde akış tablosunda tıkanıklık yaşanacaktır. Akış tabanlı sistemler anormallik mekanizmasını etkilemeden istatistik

toplamak amaçlı kullanılabilir. Mevzuatta kayıtların tutulması konusunda özellikle herhangi bir yöntem belirtilmemiş olduğundan ve sisteme daha az yük oluşturacağından dolayı, geliştirilecek sistemde akış tabanlı bilgi toplama yöntemlerinin tercih edilebileceği değerlendirilmiştir [158].

SFlow ağ izleme, istatistik toplama, performans ölçme gibi sistemlerin [162–168] yanı sıra ARP saldırılarına, DNS yükseltme saldırılarına, botnet tabanlı servis dışı bırakma saldırılarına vb. karşı tespit amaçlı kullanılmıştır. Gerçekleştirilen çalışmalarda genellikle sFlow'un örnekleme yetenekleri üzerinden ilerleyen süreçler kullanılmış olup, ağ üzerindeki anormalliklerin tespitinde başarılı sonuçlar alınmıştır [169–178].

Sistemde farklı üreticilerin ürettiği ağ cihazlarına uyum sağlayabilmek ve aynı zamanda SDN ortamına yük bindirmemek adına kayıt sistemi altyapısında akış tabanlı sFlow çalışmaktadır. Servis dışı bırakma saldırılarından korunma ve yurt dışına veri sızıntısı tespiti sistemlerinde de sFlow tercih edilmiştir.

SFlow'un örnekleme oranı (sampling rate) ve yoklama aralığı (polling interval) ayarları, tüm zaman dilimlerini her bir saniye kontrol edecek ve her paketi kayıt altına alacak şekilde tasarlanmıştır. Bu sayede örnek üzerinden değil her bir akış üzerindeki gerekli bilgilerden faydalanılmakta olup, bu kapsamda bilindiği kadarıyla literatürde ilk defa sFlow ile log tutma işlemi gerçekleştirilmektedir. Ayrıca beşinci bölümde belirtilen teknik kayıt gereksinimlerindeki başlıklara uygun olan akışların tüm akışlar arasından filtrelenerek log dosyasına yazdırılması amacıyla python kullanarak bir alt sistem geliştirilmiştir. Geliştirilen sistemin sözde kodu Çizelge 6.1'de gösterilmiştir. Bu sistem sayesinde sFlow-rt [179] ile uyumlu çalışan, json formatına uygun formatta veriler çekilerek belirtilen dosyaya yazdırılmaktadır. Dosya türü ne olursa olsun format bozulmadığından dolayı, kayıtlar tüm dosya türleriyle uyumludur.

Çizelge 6.1. Log elde edilmesi sözde kodu

Adım No	Sözde Kod
1	Gerekli modülleri çağırma *(Import request, json & datetime)*
2	Her teknik gereksinim için akış filtresi tanımlama *(IP: source/destination; MAC: source/destination; DNS request and reply; TCP and/or UDP ports; HTTP: URL, method, requests, status; DHCP: Discover, offer, request, ACK, Release; IP protocol)*
3	Akan trafik boyutunu kaydetme ve bu bilgiyi akışa ekleme
4	Her akışın tam gerçekleşme zamanını akışa ekleme *(Unix timestamp & NTP server date - time)*
5	Filtrelenmiş akış bilgilerini, veri boyutlarını ve zamanları yazdırma *(ayrıca web arayüzüne gönderme)*

Sistemde filtrelenen akışlar hem web arayüzü üzerinden canlı olarak izlenebilmekte hem de eş zamanlı olarak log dosyasına yazdırılmaktadır. Adli bilişim açısından olayın gerçekleştiği zaman bilgisinin doğru şekilde kayıt altına alınması kritik önemdedir [24]. Sisteme dahil tüm sistemler Ubuntu ağ zaman protokolü (Network Time Protocol, NTP) sunucusu [180] ile eşzamanlı çalışacak şekilde ayarlanmıştır. Kayıt altına alınan akışların zaman bilgileri yedekli ve birbirini doğrular şekilde, Unix zaman damgası formatında ve sistemin diğer alt sistemleriyle uyumlu olması açısından Ubuntu NTP sunucusundan alınan "Yıl-Ay-Gün-Saat" formatında ayrı ayrı kayıt altına alınmaktadır. Sistemde filtrelenerek elde edilen kayıtlar hangi dosya türüne yazılırsa yazılsın, kayıtlar parametreler arasında virgül, tırnak işareti ve iki nokta vb. ile belirtilen, anlaşılabilir bir formatta yer almaktadır.

Açık veri ve açık kaynak programlar, ücretsiz kullanım ve erişim olanağı sebebiyle küresel çapta desteklenmektedir. Tutulan kayıtlar csv, xlsx ve json vb. dosya formatlarında olabilmekte ve bu dosyalar ülke planlarına göre değişebilmektedir [181]. Piyasadaki bazı güvenlik yönetimi ürünlerinin log ve olay yönetimi açısından, farklı firmaları desteklememe ve satış politikası açısından bazı eksikleri mevcuttur [182]. Hadoop gibi büyük miktarda veri ile hesaplama yapmaya yarayan ortamlar için geliştirilmiş olan parquet gibi eklentilerin yerine text içeren formatların kullanılması daha fazla üreticiye uyum açısından faydalı olarak düşünülebilir [183]. İnceleme altına alınacak verinin boyut ve bilgi açısından büyümesiyle birlikte, verilerin vurgulu olması için çeşitli filtreleme ve grafiksel inceleme

uygulamalarının kullanılması gerekebilir. Csv ve xlsx uzantılı dosyalar Microsoft Excel gibi uygulamalarla veya ücretsiz tablo gösterim programlarıyla açılabilmektedir [184].

Tüm bu durumlar göz önüne alınarak kayıtlar ön tanımlı olarak, erişimi kolay olan ücretsiz programlarla açılabilen bir format olan xlsx dosyasında tutulmaktadır. Ek olarak geliştirme aşamasında boyut kıyası amacıyla, kayıtlar csv ve txt dosyalarına da yazdırılmıştır.

6.1.2. Özetleme

Tutulan kayıtların zaman damgalı şekilde ve doğruluk, bütünlük ve gizlilik ölçütlerinin sağlanarak tutulması gerekmektedir. Mesaj özetleme sistemleri kullanılarak verinin değiştirilmeden saklandığının teyit edilmesi mümkündür. MD5 (Message-Digest Algorithm 5) kaba kuvvet ve doğum günü akını ataklarına karşı güvenlik açıkları içermekte olduğundan ve farklı mesajların aynı özete sahip olma ihtimali olduğundan artık kullanılmamaktadır. Bu yöntemin yerini alan SHA1 (Secure Hash Algorithm) içinse, Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST) kullanmama tavsiyesi vermiştir. Daha güncel özetleme mekanizmalarından SHA2; TLS, SSL ve IPSec gibi alanlarda ve DNSSEC için kullanılmaktadır. Geliştirilen sistemde ise donanım ve yazılım açısından daha hızlı bir teknik olan ve diğer tekniklere göre daha yüksek güvenlik sunan SHA3-512 kullanılmaktadır [160, 185]. Sistemde tutulan kayıt dosyalarının özeti alınmakta ve zaman damgalı şekilde oluşturulmaktadır. Dosyaların özeti .txt formatında alınmaktadır. Dosya adı ise zaman sunucusundan otomatik olarak alınan bilgi doğrultusunda tarihsel formatta (ör: 202212251901) oluşturulmaktadır.

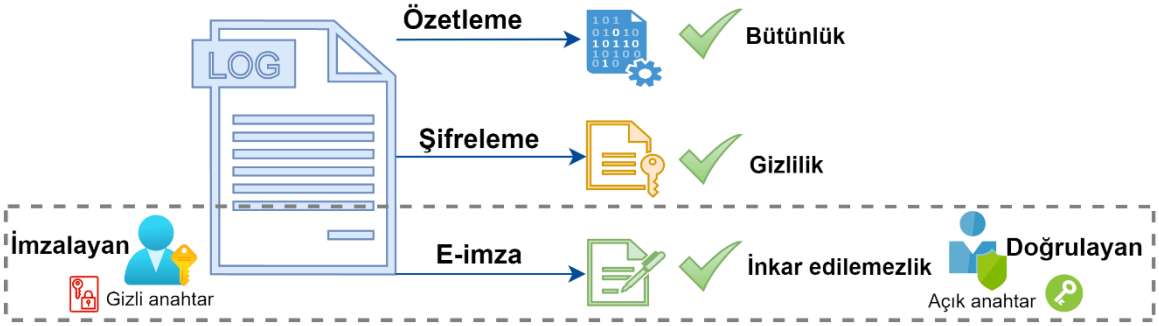
6.1.3. Şifreleme

Çok sayıda güncel program, şifreleme yöntemi olarak simetrik bir şifreleme algoritması olan gelişmiş şifreleme standardı AES'i (Advanced Encryption Standard) tercih etmektedir. Anahtar oluşturma (KeyExpansion), Bayt değiştirme (SubBytes, Shiftrows), Sütun karıştırma (MixColumns) ve Anahtar ekleme (AddRoundKey) aşamalarından oluşan AES'in CBC (Cipher Block Chaining Mode) modu özdeş veri bloklarını her zaman tamamen farklı şifreli metne dönüştürerek daha güçlü güvenlik sağlar. Sadece yetkilendirilmiş kullanıcıların şifreleme süreçlerini gerçekleştirebileceği şekilde tasarlanan sistem, hız ve güvenlik parametreleri de göz önüne alınarak AES-256-CBC algoritması kullanacak şekilde

geliştirilmiştir [159]. Ham log dosyası ve özet dosyası şifrelenerek muhafaza edilmekte ve dosya isimleri tarihsel format olacak şekilde kayıt edilmektedir.

6.1.4. Elektronik imza

Muhafaza edilecek kayıtların nitelikli veya nitelikli olmayan elektronik imza ile imzalanması gerekmektedir [124]. Hukuki açıdan geçerli ve inkâr edilemez bir yapının oluşturulması için nitelikli elektronik imza kullanılması gerekmektedir. Sistem nitelikli elektronik imzaların kullanımı için hazır hale getirilmiş olsa da sistemin deneme amaçlı kullanılması durumu göz önüne alınarak imza süreçleri deneme amaçlı oluşturulan bir imza ile gerçekleştirilmektedir. İmzanın hangi yöntem ile oluşturulacağı ve teknik altyapısı kanunda belirtilmemiştir. GPG (GNU Privacy Guard) ile imza atan yetkilinin bilgileri sisteme tanımlanmış ve RSA-4096 bitlik bir yöntem kullanarak imzalama süreçleri gerçekleştirilecek şekilde sistem hazır hale getirilmiştir [186]. İmza süreci gizli anahtar kullanılarak yapılmakta ve dosyanın doğruluğu açık anahtar kullanılarak teyit edilebilmektedir [187]. Şekil 6.1'de özetleme, şifreleme ve e-imza süreçlerinin katkıları sunulmuş olup, e-imza atılma ve doğrulama süreci de görselleştirilmiştir. Özetleme sayesinde bütünlük, şifreleme sayesinde gizlilik ve e-imza süreci sayesinde inkâr edilememezlik ilkeleri sağlanmış olmaktadır.



Şekil 6.1. Özetleme, şifreleme ve elektronik imza süreci ve katkıları

İmzalama sürecinde kullanılacak şifreyi sistemsel olarak kaydederek imzalamayı gerçekleştirmek teknik olarak mümkün bir süreç olsa da, kanuna göre e-imzalama işleminin sahibinin tasarrufu ile gerçekleştirilmesi gerektiğinden ve e-imza oluşturulmadan önce imzalanacak verinin görülebilmesi gerektiğinden dolayı şifre sisteme kayıt edilmemiştir [124]. Bu sebepten sistemde e-imzalama için görev otomatik olarak oluşturulmakta, e-

imzalama içinse yetkili kişinin şifreyi girmesi gerekmektedir. Görev oluşturulduktan sonra yetkili kişi istediği zaman şifresini girerek görevi sonlandırabilmekte ve bu durum diğer süreçlere etki etmemektedir. İmza dosyası da, diğer elde edilen dosyalar gibi dosya ismi tarihsel format olacak şekilde kayıt edilmektedir.

6.1.5. Yedekleme

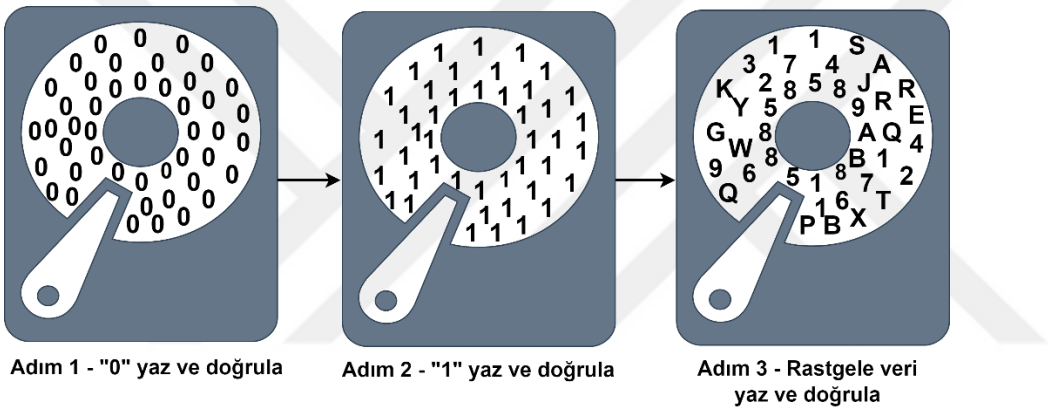
Disk teknolojilerinin yatırım maliyetlerinin yükselmesini ve tutulacak veri miktarını göz önüne alarak, sistemde minimum depolama alanıyla güvenli bir şekilde yedekleme sağlanması hedeflenmiştir. Yedekleme süreçlerinde yedekten dönüş hızı da önemli bir parametredir ve bazı disk sistemlerinde yedeklenen veriyi tekrar elde etmek zaman kaybına neden olmaktadır. Bu sebeple adli bilişimin süratli şekilde gerçekleşmesi gereken durumları da göz önüne alarak, hızlı erişimin sağlanabilmesi amacıyla tutulan kayıtların özeti, şifreli versiyonu ve imzalı versiyonunun yanı sıra ham versiyonu da tutulmaktadır. Yedek güvenliği ve disk yatırımının optimize edilmesi amacıyla da RAID 1 mantığı kullanılarak ham log, özet, şifreli log ve imzalı log dosyaları iki farklı bölgeye yedeklenmektedir. Bu durumda disklerden birisi arızalandığı durumda gerekli dosyalara diğer diskten erişmek mümkündür [188, 189]. Logların yedeklenmesi periyodunu uzun bir süre olarak belirlemek, bu periyotta yaşanabilecek sistemsel arızalara karşı dosyaları savunmasız bırakacağından, sistem her gün iki defa (07:00-19:00) log yedekleme işlemlerini gerçekleştirmektedir.

6.1.6. Verilerin yok edilmesi

Kayıtların mevzuatta belirtilen hükümlere uygun şekilde ve zamanda silinmemesi durumunda iki yıla kadar hapis cezası tanımlıdır [59]. Normal silme işlemine tabi tutulan kayıtlar sadece dosya ve diskin sistemsel olarak bağlantısını koparmakta ve bu veriler çeşitli yöntemlerle tekrar elde edilebilmektedir. Mevzuatta belirtilen silme işleminden kasıtsa kayıtların tekrar kullanılamaz şekilde silinmesidir [64, 126]. Çalışan veya müşterilerine internet hizmeti veren toplu kullanım sağlayıcılar için verilerin iki yıl süreyle saklamasının gerekli olduğu belirtilmiştir ancak verilerin yok edilmesi sürecinde hangi yöntemin kullanılacağı belirtilmemiştir [61].

Verilerin yok edilmesine dair çok sayıda yöntem olup bu yöntemler genellikle mevcut veri üzerine değişen sayılarda sabit veya rastgele verilerin yazılması üzerine kuruludur. Seçilen

silme yöntemi diskin türüne (HDD, SSD veya USB disk), dosya sistemine (NTFS veya FAT vb.) ve diskte olması muhtemel dosya türlerine göre değişiklikler gösterebilmekte ve veri elde etme aşamasında farklı başarılar sergilemektedir. Sistemde başarısını kanıtlamış olan DoD 5220.22-M yöntemi kullanılmakta olup, Şekil 6.2'de görüldüğü üzere bu yöntem verilerin üzerine "0" yazıp doğrulama, "1" yazıp doğrulama ve rastgele karakter yapıp doğrulama adımlarından oluşur [161]. Sistemde toplu kullanım sağlayıcıların gereksinimleriyle uyumlu olacak şekilde iki yıllık sürenin dolmasının ardından, yani log oluşturma tarihinin üzerinden 731 gün geçmesinin ardından, sistem gece yarısı 00:00'da öncelikle DoD 5220.22-M yöntemiyle dosyaların üzerine verileri yazmakta ve ardından silerek yok etme işlemini gerçekleştirmektedir.



Şekil 6.2. DoD 5220.22-M yöntemi adımları

6.1.7. URL filtreleme – trafik engelleme

Yasalara aykırı içerikler veya zararlı yazılım içermesi sebebiyle bazı web sayfalarına getirilen yasakların kurumlar tarafından engellenmesi gereksinimi için sistemde bir filtreleme alt sistemi oluşturulmuştur. Filtreleme sistemi için makine öğrenmesi sistemlerini kullanan yöntemler çalışılmış olsa da [190], sistemin ülke uyumluluğunu sağlamak ve doğrudan SDN yetenekleriyle sistemi oluşturabilmek için Türkiye'de kullanılan yasaklı ve zararlı siteler veri tabanı kullanılmıştır [191, 192]. USOM (Ulusal Siber Olaylara Müdahale Merkezi) tarafından günlük olarak güncellenen zararlı bağlantılar listesi iki dosya türünde (xml ve txt) indirilebilmektedir. Dosya içeriğinde sıra halinde ilgili web sayfalarının adresleri bulunmaktadır.

Engelleme işlemi sistemde kullanılacak kontrolcü olan Ryu üzerinde gerçekleşmektedir [89, 193]. Yazılan betik sayesinde USOM listesindeki adresleri IP adreslerine çevrilmekte ve engellenmesi amacıyla kontrolcüye POST yöntemiyle iletilmektedir. Sayfaları tamamen engellemek mümkün olduğu gibi port temelli (örneğin 80 ve 443) engellemek de mümkündür. USOM'a eklenen zararlı bağlantılar günlük olarak sistemde de güncellenerek kontrolcüye iletilebilmektedir. İlgili dosyada USOM veri tabanı dışında başka veri tabanları kullanılabileceği gibi, isteğe bağlı eklenebilecek diğer adreslerin de bu sistem yardımıyla engellenmesi mümkündür. Bu sistem sayesinde sadece zararlı web sayfalarına erişimin engellenmesinin ötesinde, saldırıların geldiği tespit edilen kaynakların engellenmesi ve bu sayede saldırı engelleme sistemi oluşturulması da mümkündür.

6.1.8. Uluslararası veri sızıntısı tespiti

Bazı uygulamalarda bazı verilerin yurt içinde kalması gerektiği tanımlanmıştır. Örneğin; kurumsal kritik veriler, nüfus verileri, genetik ve biyometrik veriler yurt içinde kalmalıdır. Ayrıca yurt içi iletişim trafiğinin yurt dışına çıkarak tekrar yurt içine dönmesi durumu da engellenmelidir [64]. Bu gerekçeler göz önüne alınarak yurt dışına giden verilerde uyarı oluşturan bir sistem geliştirilmiştir. "GeoLite2-Country.mmdb" veri tabanı kullanarak ülkelerin IP adres bloklarının sistem tarafından tanınması ve süreçlere entegre çalışması sağlanmıştır.

Çizelge 6.2. Uluslararası veri sızıntısı tespit sistemi sözde kodu

Adım No	**Sözde Kod**
1	Gerekli modülleri çağırma *(Import request, json & datetime)*
2	Akış filtresi tanımlama *(IP: source/destination; TCP and/or UDP ports; IP protocol; Destination country is not Türkiye)*
3	Filtreye uygun tüm akışları tutma *(eşik değer "0")*
4	Filtrelenmiş akış bilgilerini, olay numarasını ve zamanlarını yazdırma
5	Veri sızıntısı uyarısı verme

Sözde kodu Çizelge 6.2'de belirtilen ve Python kullanarak geliştirilen sistem sayesinde, belirlenen kaynaklardan ülke dışına giden her bir paket için uyarı oluşturulmaktadır. Nüfus,

biyometrik, genetik vb. kritik kişisel verilerin, bu amaca hizmet etmesi için ayrılan sunucularda muhafaza edilmesi gereklidir. Sistem sayesinde oluşturulan uyarılarla kişisel verileri bünyesinde barındıran sunuculardan yurt dışına giden verilerin takibi, trafik engelleme sistemiyle de bu bağlantıların engellenmesi ve sonlandırılması mümkündür.

6.1.9. Eşik tabanlı uyarı sistemi

Sistemde log toplama amacıyla kullanılan sFlow, veri sızıntısı tespit sisteminin yanı sıra saldırı tespit sistemlerinde de kullanılmaktadır [167–176]. Donanımsal açıdan güçlü olmayan sistemlerde de başarılı sonuçlar vermesi hedeflenen sistemde saldırı uyarı sisteminde süreçler, bant genişliğindeki ve akış sayısındaki anormallikler üzerinden işletilmektedir. Kullanıcılara tahsis edilen bant genişliğinin, kullanıcı bazında %90 ve üzerine eriştiği durumlar ve saniyedeki akışın 500 adetin üzerine çıktığı durumlar anormal düzeyler olarak tanımlanmış olup, bu eşiklerin aşıldığı durumlarda saldırı uyarı sistemlerinin canlı uyarılar üretmesi sağlanmaktadır.

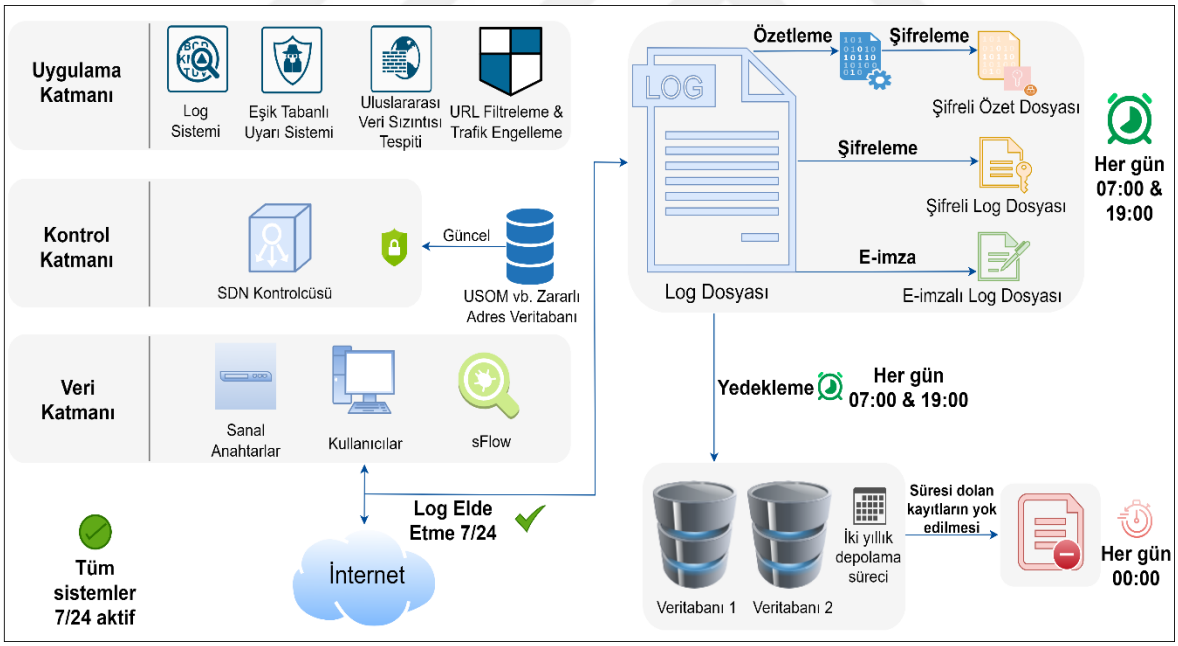
Çizelge 6.3. Eşik tabanlı uyarı sistemi sözde kodu

Adım No	**Sözde Kod**
1	Gerekli modülleri çağırma *(Import request, json & datetime)*
2	Akış filtresi tanımlama *(IP: source/destination; TCP and/or UDP ports; IP protocol)*)
3	Filtreye uygun tüm akışları tutma *(eşik değerler: %90 bant genişliği ve 500 akış/sn)*
4	Saldırı türünü, filtrelenmiş akış bilgilerini, olay numarasını ve zamanlarını yazdırma
5	Eşik tabanlı uyarı üretme

Çizelge 6.3'te yer alan süreçle python kullanılarak oluşturulan sistem sayesinde; saldırıların, yurt dışı veri sızıntılarının, zararlı bağlantıların tespit edilmesi mümkündür. Bu bağlantıların kontrolcü tarafından engellenmesi mümkündür. Üretilen uyarıda kaynak ve hedef IP adresleri ile port bilgilerinin yanı sıra protokol ve ülke bilgisi de yer almaktadır.

6.1.10. Sistemin otomatizasyonu

İçerdiği tüm sistemler bash betikler kullanılarak çalışabilir hale getirilen sistemin otomatik çalışarak tüm süreçleri otomatik şekilde gerçekleştirebilmesi için gerekli ayarlar Crontab kullanılarak gerçekleştirilmiştir [131]. Crontab kullanarak bir işlemin hangi gün veya hangi saatte tekrarlanarak çalıştırılacağı tasarlanabilmektedir. Log toplama, özetleme, şifreleme, e-imza süreçleri her gün saat 07:00 ve 19:00'da başlayıp birbirinin ardından gerçekleşecek şekilde tasarlanmıştır. Her 12 saatlik döngü için aynı süreçlerden ikişer tane tanımlanmış olup süreç karışıklığının önüne geçilmiştir. Veri yok etme süreci ise otomatik olarak her gece 00:00'da çalışacak şekilde tasarlanmıştır. URL filtreleme, uluslararası veri sızıntısı tespiti ve eşik tabanlı uyarı sistemleri ise sürekli çalışır durumdadır. Geliştirilen sistem Şekil 6.3'te tarif edilmiş olup, logların elde edilmesi, özetlenmesi, şifrelenmesi, imzalanması, yedeklenmesi ve yok edilmesine kadar tüm süreç, mevzuata uyumlu şekilde güvenli, otomatik ve kesintisiz çalışacak şekilde tasarlanmıştır.

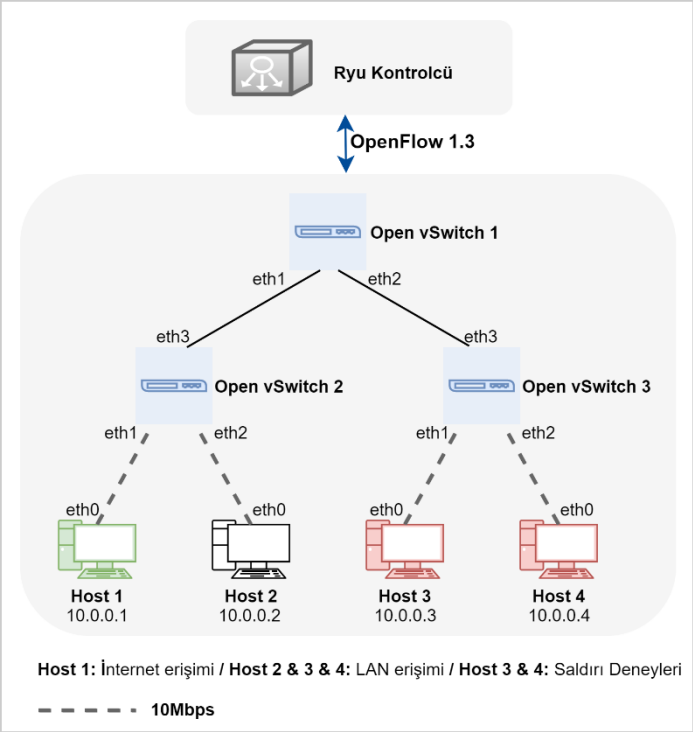


Şekil 6.3. Sistemin genel tasarımı

6.2. Deneysel Çalışmalar

Şekil 6.4'te verilen deney ortamında Mininet kullanılarak oluşturulan SDN ortamında üç sanal anahtar ve bu sanal anahtarlara bağlı dört kullanıcıdan oluşan, ağaç topolojisinde bir ağ altyapısı tanımlanmıştır. Mininet, ön tanımlı olarak LAN'da çalışmaktadır. Ancak

sistemde elde edilecek kayıtlar internet ortamına giden verilerin elde edilmesiyle oluşturulacağından dolayı host 1'e internet bağlantısı verilmesi için sanallaştırma sistemi üzerinden bir adet daha bağdaştırıcı atanmıştır. Ayrıca alan adı sorgularının Google DNS üzerinden gerçekleştirilmesi için sistemsel tanımlamalar yapılmıştır. Sadece saldırı tespit sistemi deneyleri LAN üzerinden gerçekleştirilmiş olup diğer deneyler gerçek internet trafiği üretilerek gerçekleştirilmiştir.



Şekil 6.4. Deney ortamı topolojisi

Deney ortamında kullanıcılara tanımlanan bant genişliği 10Mbps olarak belirlenmiştir. Bu değerin günlük rutin internet erişimleri için yeterli olduğu değerlendirilmiştir. Mininet, sFlow-RT ile uyumlu olarak çalıştırılmış olup, kullanıcıların MAC adresleri de sıralı olacak şekilde belirlenmiştir. SFlow-RT her koşulda coğrafi veri tabanı bilgisini içererek başlayacak şekilde tasarlanarak sisteme dâhil edilmiştir. Hiçbir erişim kaydını kaçırmamak için, sFlow'da akış ve zaman perspektifindeki örnekleme süreci devre dışı bırakılmış ve her akışın elde edilerek işleme alınması sağlanmıştır. Her akış incelenmekte ve filtrelemelere uygun olan tüm akışlar kayıt altına alınmaktadır.

Zararlı hedefler için kullanılacak liste otomatik olarak kontrolcüye iletilmektedir. Kontrolcü ve anahtarlarda bir zararlı olmadığı ve yetkilendirme işlemlerinin güvenliği olduğu

varsayılmıştır. OpenFlow versiyonu olarak versiyon 1.3. olarak tercih edilmiş olup, SDN ortamında sistemsel ekstra yük oluşturmaması adına asgari yeterliliği sağlayan dört kullanıcılı bir topoloji kurulmuştur.

6.2.1. Altyapı bilgileri

Adli bilişim sistemi bir dizüstü bilgisayarda dahi çalışacak şekilde, sisteme yük bindirmeyen özellikler gözetilerek geliştirilmiştir. Log elde edilmesi amacıyla kullanılan sFlow aynı zamanda veri sızıntısı ve eşik tabanlı saldırı uyarı sistemlerinde de kullanılmıştır. Otomatikleştirme için sistemin öz kaynaklarının kullanıyor olması, kaynak tüketimini artırmadığından avantaj sağlamaktadır. SDN ortamında kontrolcü odaklı olmayan, akış tabanlı alternatif bir sistemin çalışmakta olması da kaynak tüketimini artırmayan ana unsurlardandır. Deney ortamı olarak bir dizüstü bilgisayarda yer alan sanallaştırma sistemi kullanılmış, SDN ortamı olarak ise Mininet kullanılmıştır. Çizelge 6.4'te SDN ortamında kullanılan sistemler dâhil tüm altyapı bilgileri görülmektedir.

Çizelge 6.4. Deney ortamı altyapısı

Sistem	**Detay Bilgi**
Dizüstü Bilgisayar	Intel Core i7-10510U CPU 1.8GHz, 16GB DDR4 RAM ve 500GB SSD Disk kapasitesi
Sanallaştırma Sistemi	VirtualBox [132] (8 GB RAM, dört sanal işlemci ve 150 GB HDD)
İşletim Sistemi	Ubuntu Desktop [131]
SDN Ortamı	Mininet [130]
SDN Kontrolcüsü	Ryu [89]
SDN Sanal Anahtar	OpenvSwitch [133]
Paket Yakalama	Wireshark [134]
Trafik Üretme	Iperf [137]
Saldırı Düzenleme	Hping3 [139]

6.2.2. Deney süreçleri

Deneyler SDN topolojisinin (Bkz. Şekil 6.4), oluşturulan adli bilişim sisteminde (Bkz. Şekil 6.3) çalıştırılması ile gerçekleştirilmiştir. Sistemin bir tam kayıt döngüsü için en az 24 saat (07:00-19:00 & 19:00-07:00) gerekmektedir. Son işleminin ardından süreçlerin tekrar devam edip etmediğinin kontrolü, süreçlerin ne kadar sürede tamamlandığının

gözlemlenebilmesi ve otomatik silme işleminin gözlemlenebilmesi amacıyla sistem bir saat daha açık tutulmuş ve bu şekilde sistem yirmi beş saat kesintisiz çalıştırılmıştır.

Veri sızıntısı tespit ve eşik tabanlı uyarı sistemleri sürekli (7/24) çalışmakla birlikte log tutma süreçlerine dair sistemler 07:00 ve 19:00'da yerini diğer 12 saat için çalışacak denk döngüye bırakmaktadır. Akış tabanlı log kaydında sistemin yeniden başlatılmadığı durumlarda eski akışların, yeni oluşan log dosyasına yazılması riski mevcuttur. Bu riski bertaraf etmek için bu sistemde de uygulandığı gibi kayıt dosyalarının yeni akışla ilişkilendirilmesini sağlamak gereklidir.

Deney sürecinde, gündüz mesaisi sunan bir kurumda çalışan ve mesaisi saat 17:00'da tamamlanan bir kullanıcının muhtemel internet erişimleri gerçekleştirilmiştir. Akşam saatlerinde kullanıcıların internet erişimi sağlamayacağı kabul edilmiş olsa da sistemin bir günlük döngüsünü tamamlama durumunu test etmek amacıyla küçük bir internet trafiği oluşturulmuştur. Kurumun yerel dosya sunucularına erişim, evrak yönetim uygulamaları gibi yerel alan ağında iş süreçleriyle ilgili erişimlerin dışında, çalışanlar iş dışı amaçlarla interneti kullanmaktadırlar. Siber aylaklık olarak tanımlanan bu durumda çalışanlar çeşitli ceza ve yaptırımlarla karşı karşıya kalabiliyor olsa da çalışanların %60 ile %80 aralığındaki bölümü iş dışı amaçlarla internet erişimi gerçekleştirmektedir. Yaş, cinsiyet, ilgi alanı, eğitim düzeyi gibi faktörler kullanıcıların internet erişim alışkanlıklarını etkiliyor olsa da, çalışanlar genel olarak video, müzik, haber, alışveriş, yeni iş arama, finans, sosyal medya, kamu siteleri gibi başlıklarda sitelere erişim sağlamaktadır [194, 195]. Deney sürecinde de bu durum göz önüne alınarak, host 1 üzerinden toplam 45 dakika süreyle 360p-720p kalite aralığında video izlenmiş, iki saat de bahsi geçen diğer sitelerde web sörf yapılırken, yarım saatlik bölümünde eş zamanlı olarak müzik de dinlenmiştir.

İnternet erişimleri esnasında web trafiğinin engellenebilmesi durumu ve yurt dışına giden verilerin tespit edilip edilmediği canlı olarak gözlemlenmiştir. Sistemin güvenliğini artırmak amacıyla geliştirilerek sisteme dâhil edilen eşik tabanlı uyarı sistemlerinin test edilmesi amacıyla host 3 ve 4 arasında Iperf kullanarak yüksek bant genişliğine sahip bir trafik üretilmiş ve Hping3 yardımıyla da ping seli atağı düzenlenmiştir.

19:00 ve 07:00'da oluşması gereken log dosyalarının durumu, özetleme, şifreleme, elektronik imza süreçlerinin tamamlanması, verilerin otomatik olarak yedeklenmesi ve yok

edilmesi süreçleri de gözlemlenmiştir. Sistemin tasarımında verilerin silinmesi süreci için iki yıllık süre geçmiş olması gerekse de deney ortamında silme işleminin denenmesi adına bu süre 12 saat olarak belirlenmiş ve her gün saat 07:30'da çalışacak bir görev olarak oluşturulmuştur. Her akışın kayıt altına alındığını ispatlayabilmek ve tutulan log dosyalarıyla kıyaslayabilmek için, güvenilirliği ispatlanmış olan Wireshark ile tüm portlarda aktif olarak paket dinleme işlemi de gerçekleştirilmiştir.

6.2.3. Deney sonuçları

Deney süreci 25. saat sonunda tamamlanmıştır. Sistem çalışmadığı zaman, yani sistem boşta iken yaklaşık %15'lik CPU kullanılırken, sistemin aktif olarak çalıştığı zamanlarda ise CPU düzeyinin %50'lerde olduğu görülmüştür. Toplam RAM ihtiyacının ise yaklaşık 1 GB olduğu tespit edilmiştir.

Saat 17:00'ye kadar web sitelerini ziyaret süreçleri tamamlanmış olup akşam 19:00'dan sonra sistem otomatik olarak 12 saatlik kayıt dosyasını (19:00), özetini (19:01), şifreli (19:02) ve imzalı (19:03) versiyonlarını oluşturup ilgili dizinlere, yedekli bir şekilde (ikişer adet) kaydetmiştir. Özetleme, şifreleme ve imzalama (passphrase girerek) süreçlerinden her biri 30'ar saniyeden az sürmekte ve sisteme yük bindirmemektedir. Bu süreçler ertesi gün 07:00'de da başarılı bir şekilde otomatik olarak tekrar etmiştir.

Kayıtların doğruluğunu teyit etmek amacıyla erişilen web sayfaları ve saat bilgileri el ile de not altına alınmıştır. Tutulan notlar ve Wireshark paket dinlemeleriyle elde edilen pcap dosyası kıyaslanmış olup teknik kayıt gereksinimlerinde belirtilen hususların başarıyla kayıt edilebildiği ve pcap dosyasıyla xlsx uzantılı log dosyasındaki kayıtların uyumlu görülmüştür.

Port ve protokol bilgisi, hizmet başlama-bitiş saatleri, aktarılan veri miktarları, DHCP sunucusundan alınan ve internet erişiminde kullanılan 10.0.4.16 (host 1 internet) IP adresine dair detaylar (IP allocation, IP renewal and IP release) [196], URL istekleri ve web erişimlerine dair tüm detayların log dosyasında mevcut olduğu görülmüştür. Aşağıda "www.gazi.edu.tr" web sayfasına erişim için Google DNS'e sorgu yapan host 1'in talebinin, log dosyasına yazılmış olan örnek akış kaydı formatı gösterilmiştir.

{"flowKeys": "10.0.4.16 8.8.8.8 www.gazi.edu.tr." "agent": "127.0.0.1" "name": "dns" "start": 1671942348391 "end": 1671942348391 "dataSource": "6" "value": 79 "flowID": 4}RelatedFlowID&time 7 2022-12-25 07:25:48.395095

Zararlı web sayfalarına erişim denemelerinde de başarı sağlanmış olup belirtilen hedeflere erişimin mümkün olmadığı gözlemlenmiştir. Engelli web sayfaları arasında zararlı olmayan, güvenli olduğuna emin olunan Kamu kurumları ve Üniversitelere ait web sayfalarından da üç adet hedef eklenmiş olup, ilgili hedeflere erişimin engellendiği gözlemlenmiştir. Bu hedeflere gidiş için yapılan talepler kontrolcüye ulaşmaktadır ancak engellenmektedir. Bu sayede hangi kullanıcıların hangi zararlı/engelli hedefleri talep ettikleri de log dosyalarında görülebilmiştir.

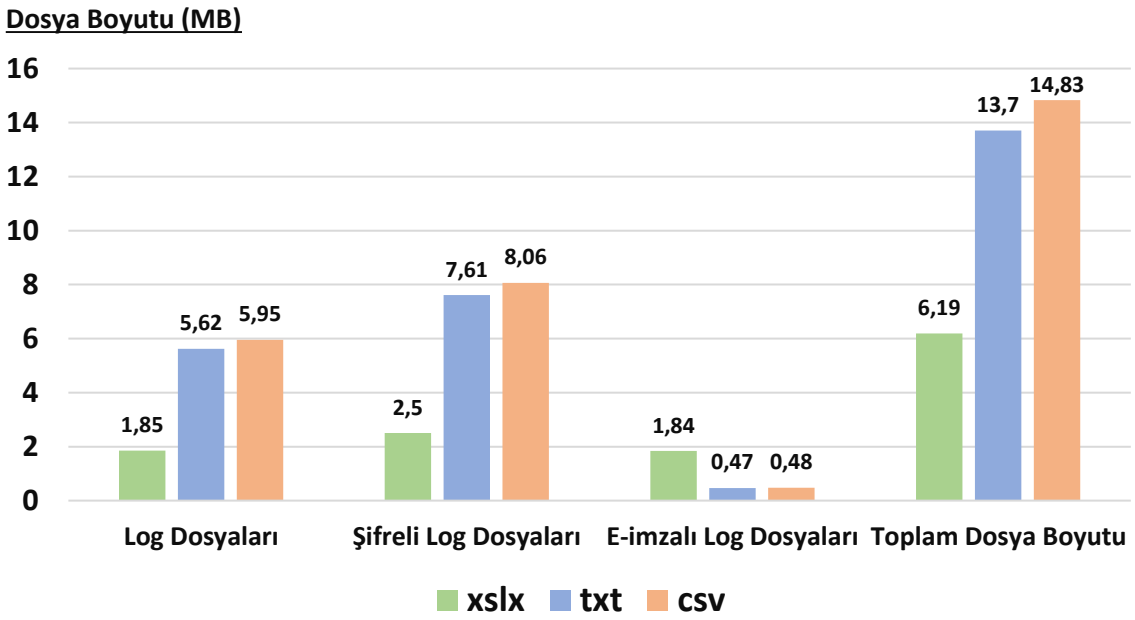
Elde edilen kayıtların özetleri, elle girilen özet alma komutu ve web üzerinden özet alma süreci sağlayan sistemlerle tekrar özetlenmiş olup, özetlerin sistemde alınan sonuçlarla aynı olduğu görülmüştür. Şifreli log dosyasından deşifre edilerek elde edilen log dosyasıyla ham log dosyasının aynı içerikte olduğu da tespitler arasındadır. Ayrıca imzalı logların hangi merci tarafından imzalandığı bilgisine ve geçerlilik bilgilerine erişimin de mümkün olduğu görülmüştür.

İnternet erişimleri esnasında tutulan pcap dosyasında 395.461 adet paket yer almaktadır. Sistemde yer alan log toplayıcı sistem ise 21.883 adet akışı kayıt altına alarak mevzuat açısından gerekli olan bilgileri, satır sayısı bazında pcap dosyasındaki satır sayısının %5,5'i kadar satırla elde etmeyi başarmıştır. İnternete erişim esnasında 715 MB'lık (Megabyte) bir veri aktarımı gerçekleştirilmiş olup, Çizelge 6.5'te gösterildiği gibi bu veri trafiğine dair erişimler 1,85 MB'lık bir log dosyası ile kayıt altına alınmıştır. Özet, şifre ve imza süreçleri de eklenince, kayıt edilen dosyalar sistemde disk başına günlük 6,19 MB'lık alan kaplamaktadır. Bu dosya boyutu toplam trafik boyutunun %0,87'sine denk gelmektedir.

Çizelge 6.5. Log dosyaları ve trafik boyutları

Dosya İçeriği	**Veri Boyutu**
Log Dosyası (.xlsx)	1,85 MB
Şifreli Log Dosyası	2,5 MB
Log Dosyasının Özeti	132 Byte
Şifrelenmiş Özet Dosyası	220 Byte
İmzalı Log Dosyası	1,84 MB
Kayıt Edilen Toplam Dosya Boyutu (Günlük)	6,19 MB
Aktarılan Veri Boyutu (Günlük Trafik)	715 MB

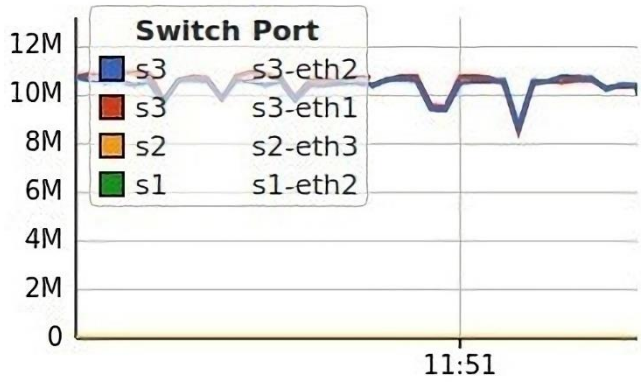
Deneylerin tamamlanmasının ardından dosya uzantılarına göre tutulan log dosyalarının boyutunun değişip değişmediğine dair bir araştırma gerçekleştirilmiştir. Üç farklı uzantıda (.xlsx & .csv & .txt) birebir aynı verileri içeren kayıtların boyutları arasındaki farklılık dikkat çekicidir. Şekil 6.5'te görüldüğü üzere xslx uzantılı log dosyası, csv uzantılı log dosyasının yaklaşık %31,1'i kadar yer kaplamaktadır. Özet dosyaları (132 Byte) ve şifreli özet dosyaları (220 Byte) tüm dosya uzantılarında aynı miktarda alan kaplamaktayken tüm türlerde csv ve txt uzantılı dosya türlerinin benzer miktarlarda alan kapladığı da görülmektedir. Log dosyalarından xlsx uzantılı olan versiyonun imzalı hali hemen hemen ham log dosyası kadar boyuta sahipken, csv ve txt uzantılı versiyonlarda imzalı log dosyası boyutu ham log dosyasının yaklaşık %8'i boyutunda olması da dikkat çekici başka bir bulgudur. İmzalı log dosyasındaki handikapa rağmen sistemde xslx uzantılı dosya türü kullanılması durumunda disk ihtiyacının minimum olacağı ve en yakın veri boyutuna sahip olan txt uzantılı versiyona göre dahi yaklaşık %55'lik bir disk tasarrufu sunacağı görülmüştür. Oluşan bu boyut farkı, xlsx'in doğası gereği sıkıştırılmış bir yapıda olmasından ve aynı yapıdaki verileri tekilleştirip sadece bir kopyasını depolamasından kaynaklanmaktadır. Diğer dosya türlerine göre boyut avantajı sağlayan xlsx'in bu tarz sistemlerde kullanılması ciddi bir avantaj sağlayacaktır [197, 198]. İki yıllık bir kullanımda, 100 kişilik bir kurum için xslx uzantılı dosya için disk başına 441,3 GB gerekirken, txt uzantılı kayıt için 976,7 GB disk alanı, csv uzantılı kayıt için yaklaşık 1 TB'lık alan ihtiyacı olacaktır. Dosya türü olarak .xlsx kullanıldığı durumlarda imzalı log dosyasının hemen hemen ham log dosyası kadar boyutu olmasının sebebinin de xlsx'in sıkıştırılmış/değiştirilmiş yapısından kaynaklandığı düşünülmüştür.



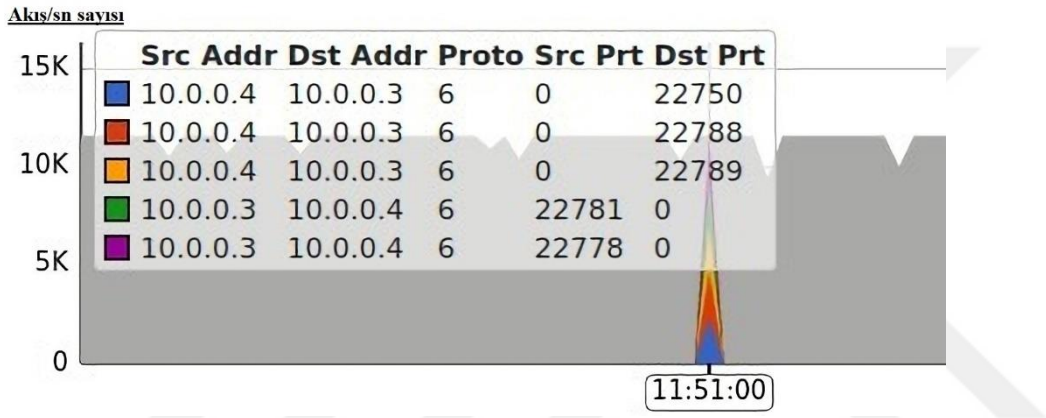
Şekil 6.5. Farklı dosya uzantılarının boyut kıyaslaması

Verilerin yok edildiğinin gözlemlenebilmesi sürecinin 12 saatten önce oluşturulan dosyaların silinmesi şeklinde güncellenmesi sürecinin doğru çalıştığını gözlemlemek için 07:30'da sistem kontrol edilmiştir. Kayıtların var olduğu ilgili dizinlerde deneyin ilk gününde 07:30'da bir dosya bulunmamaktadır ve bu sebepten bir gözlem yapmak mümkün değildir. Ancak deneyin 24'üncü saatinden yarım saat sonra (07:30'da), oluşturma tarihi 12 saat ve öncesi olan dosyaların geri döndürülemez olarak silinmesi süreci otomatik olarak başlamıştır. Sürecin sağlıklı şekilde tamamlandığı ve günün ilk yarısında saat 19:00 döngüsünde oluşturulmuş olan dosyaların silindiği görülmüştür. Küçük boyutlu olan özet dosyalarının silinmesi süreci birkaç saniye içerisinde tamamlanırken, diğer dosyaların silinmesi süreci için dosya başına birkaç dakikalık süreç gerekmiştir. İki dizinde yer alan dosyaların silinmesi süreci toplam 21 dakika sürmüş ve 07:51'de tamamlanmıştır.

Saldırılar esnasında sistemin CPU kullanımının %70-80 bandına yükseldiği görülmüştür. Portlar 10Mbps ile sınırlandırılmış olsa da, Resim 6.1'de görüldüğü üzere bazı anlarda portlara ait bant genişliğinin saldırı etkisiyle 11Mbps'a kadar erişebildiği görülmüş olup, Resim 6.2'de görüldüğü gibi kaynak-hedef adresler ve port bilgilerine de erişim sağlanabilmiştir.



Resim 6.1. Saldırı esnasındaki bant genişliği (Mbps)

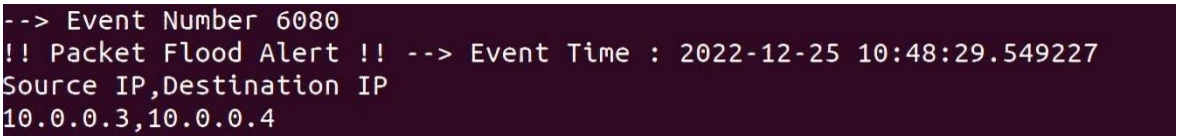


Resim 6.2. Saldırı ve akış/sn bilgileri

Saldırı tespiti için host 3 ve 4 arasında Iperf ve Hping3 kullanarak oluşturulan yüksek bant genişliği ve ping seli sonucunda, sistemler her iki durum için ayrı ayrı olacak şekilde, Resim 6.3'te ve Resim 6.4'te görülen şekilde uyarıları oluşturarak potansiyel saldırılara karşı uyarı oluşturmayı başarmıştır. Saldırılara uyarı üretme durumunda bir eksik yaşanmasa da yaklaşık bir saat süren denemelerde tutulan kayıt dosyasında üretilen akış bilgilerinin 1.048.576 satırından sonraki bilgilerin, maksimum satır sayısına ulaşılmasından dolayı saldırı log dosyasında yer almadığı görülmüştür.

```
--> Event Number 6079
!! Bandwidth %90 limit exceeded !! --> Event Time :  2022-12-25 10:48:28.255172
Source IP,Destination IP
10.0.0.3,10.0.0.4
```

Resim 6.3. Bant genişliği eşiği tabanlı uyarı örneği



Resim 6.4. Akış/sn eşiği tabanlı uyarı örneği

Deneylerde verilerin yurt içinde kalmadığı durumlarda uyarı vermesi üzerine geliştirilen sistemin de tamamen başarılı bir şekilde çalıştığı görülmüştür. Kaynak-hedef IP adresi/port ve hedef ülke bilgilerinin, zaman bilgisiyle birlikte uyarılarda Resim 6.5'teki gibi yer aldığı görülmüştür.



Resim 6.5. Uluslararası veri sızıntısı tespit örneği

6.3. Bölüm Değerlendirmesi

Sistemin kaynak ihtiyacı internet erişimi olan bir kullanıcı üzerinden hesaplanmış olup saldırı esnasında çok fazla sayıda paket için uyarı ürettiğinden dolayı CPU düzeyinin %70-80 düzeyine ulaştığı görülmüştür. Bu sebepten çok kullanıcılı yapılarda saldırı esnasında kesintisiz hizmet sunabilmesi için, özellikle işlemci ve RAM açısından daha güçlü bir sunucuda çalıştırılmasının daha uygun olacağı düşünülmektedir. Güçlü bir altyapıya sahip olunmaması durumunda ise saldırı tespit sistemlerinin farklı bir bilgisayar üzerinde çalıştırılması sistemlerin yükünü azaltacaktır. Deneylerde kontrolcü, SDN topolojisi ve sistem aynı bilgisayar üzerinde çalıştırılmış olup, bu yapıların birbirinden ayrı konumlarda yer alması da mümkündür. Adli bilişim sisteminin tüm alt sistemleri tek bir bilgisayarda veya ayrı ayrı bilgisayarlarda çalışmak için uygun yapıdadır ve uzak sunucularda çalışan kontrolcü ve SDN topolojileri ile uyumlu çalışmaya müsaittir.

Deneylerde tek bir kullanıcıya internet erişimi verilmesi hususu, altyapının eksikliğinden kaynaklı bir kısıtlılıktır. Sistemin çok kullanıcılı yapılarda nasıl fayda sağlayacağının denenmesi de faydalı olacaktır. Haftanın her günü açık olan orta büyüklükteki bir kurumda, mesai saatlerinde internet erişimi sağlayan 100 kişi olduğu ve bu kullanıcıların deney ortamındaki internet erişimlerinin aynısını gerçekleştirdiği kabul edilirse, iki yıllık süreyle 49,8 TB'lık bir trafik akışı olacağı ve saklanacak loglar için disk başına 441,3 GB'lık alan

gerekeceği görülmektedir. İki yıldan önce oluşturulan veriler silineceğinden dolayı disk boyut ihtiyacı sürekli artmayan bir yapıda olacak ve ikinci yıldan itibaren durağan bir yapıda olacaktır.

Eşik tabanlı uyarı sistemleri deneyleri sonucunda belirtilen 1.048.576 satır log kaydına ulaşma durumu, sadece tespit edilmesine rağmen durdurulamayan ataklarda oluşabilecek bir durumdur. Deneylerde tespitin sürekliliğinin ve sistemin sağlıklı çalışmasının gözlemi için saldırı engelleme işlemi gerçekleşmemiştir sadece tespit süreci gerçekleştirilmiştir. Ancak sistemde tespit edilen zararlı kaynakların engellenmesi, trafik engelleme modülüne kaynak IP adreslerinin bildirilmesiyle, sadece birkaç saniye içerisinde mümkün olacaktır. Altyapının daha güçlü olduğu ortamlarda saldırı tespit edilen kaynaklardan belirlenen eşik üzerinde uyarı oluşturan kaynakların otomatik olarak kontrolcüye bildirilmesiyle saldırı tespit sistemi, saldırı engelleme sistemine dönüştürülebilir. Kaynakların çok daha fazla olduğu ortamlarda ise makine öğrenmesi ve derin öğrenme tabanlı saldırı engelleme sistemlerinin sisteme dâhil edilmesi mümkün olacaktır. Deneylerde 15 dakikada yaklaşık 510.000 saldırı akışının kayıt altına alındığı görülmüştür. Eş zamanlı farklı kaynaklardan gerçekleşecek saldırılarda bu sayı artacaktır. Saldırıların tüm çabalara rağmen engellenemediği durumlarda excel dosyalarının maksimum satır sayısı olan 1.048.576'ya ulaşılmasından sonra yine de saldırıya dair tespitlerin kayıt altına alınması için, satır sayısını kontrol edip yeni bir kayıt dosyasına geçen bir modülün geliştirilmesi ve sisteme dâhil edilmesinin gerekli olduğu değerlendirilmiştir.

Güçlü altyapılarda, zararlı hedeflere çok sayıda talepte bulunan yerel kullanıcıların da bant genişliğinin otomatik olarak kısıtlanması veya tamamen engellenmesi gibi süreçler sisteme dâhil edilebilir. Sistem zararlı web sayfalarını engellese dahi kullanıcıların talepleri kayıt altına alındığından bu sürece de uygun durumdadır.

Yanlış pozitif uyarı sayılarının önemi bir sistem için yüksek öneme sahiptir. Normal bir güvenlik yönetiminde günlük 1000-3000 arası uyarı hedeflenmekte olup daha fazla uyarı veren bir sistemde örnekleme yaparak süreçler gerçekleştirilebilir. Yakın gelecekte, tespit edilen olayların 10 katına çıkacağı öngörüldüğünden dolayı örnekleme ve kayıtların önem derecesinin belirlenmesi durumu kritik öneme sahiptir [104]. Satır sayısı sınırına takılmamak ve daha az uyarı oluşmasını sağlamak için örnekleme yaparak saldırı tespit sistemini kullanmak da mümkündür. Ancak bu durumda oluşacak uyarıların saldırının

gerçek başlama vaktinden bir süre sonra oluşacağı göz önüne alındığında sistemin güvenlik düzeyinde azalma olacağı riski de düşünülmelidir. Sistemin mevcut tasarımındaki eşiklerinse genel olarak uygun olduğu görülmüştür.

Uyarı sistemleri için belirlenen eşik değerlerin, yerel ağdan dışarıya giden rutin internet erişimleri için de sağlıklı çalıştığı görülmüştür. İnternet erişimlerinde, rutin bir web erişimi için sadece iki adet paket saldırısı uyarısı alınmıştır. Yapılan incelemelerde ilgili hedefe giderken eş zamanlı olarak çok sayıda başka sayfalara yönlendirme gerçekleştiği görülmüştür. Yönlendirilen sayfalardan birine ait olan erişim talebi bir paket seli saldırısı olmasa da sistem tarafından tehlike olarak görülüp uyarı oluşmuştur.

Hedef engelleme süreci doğrudan URL temelli değil, IP adresi temeliyle dolaylı olarak URL temelli olarak işletilmekte olup, hem IP hem URL temelli hedef engelleme sürecinin sisteme entegrasyonu da fayda sağlayacaktır. Zira USOM zararlı hedeflerinde yer alan URL adreslerinin bağlı olduğu IP adreslerini elde etme işlemi uzun sürmektedir. Bazı hedefler doğrudan İSS tarafından engelli olduğundan IP adresini çözme işlemini çok uzatmaktadır. Örneğin yaklaşık 6.000 adet başarılı sonuç için yaklaşık 5,5 saatlik bir sorgu süreci gerekmektedir. Bu süreç otomatik sorgu şeklinde gerçekleşmekte olup tüm listenin tek seferde sorgulanması yerine, listenin 1.000'er kayıt şeklinde bölünerek sorgulanması ve sonuçların birleştirilmesi daha hızlı sonuçlar verecektir.

Tüm sistemler SDN dışındaki ağ sistemleriyle de uyumlu halde çalışmaya elverişlidir. Bazı geliştirmeler yaparak sFlow ile uyumlu çalışabilen, geleneksel ağ cihazları içeren ortamlarda da kullanılması mümkün olacaktır. Trafik engelleme modülü ise deney ortamında kullanılan Ryu kontrolcüsüne bağımlı olup bu tarz bir engelleme yöntemi için trafiğin izlenmesinin veya istatistik toplanmasının ötesinde bir süreç gereklidir. Bu sistemi tüm ağ cihazlarına uygun şekilde tanımlamak zor bir süreç olsa da, tüm trafiğin önce vekil sunucuya yönlendirildiği ve internet erişiminin vekil sunucu üzerinden gerçekleştirildiği bir ağ ortamında merkezi bir şekilde yerel ağdan dışarıya giden trafiği engellemek mümkün olacaktır. Aynı şekilde internet ortamından yerel ağa gelen zararlı bağlantılar için de güvenlik duvarı gibi ağ çevre donanımlarıyla süreç işletilebilir. Ancak bu çalışmanın ana hedefi SDN yetenekleriyle bir adli bilişim sistemi oluşturmak olduğundan bu tarz çevre ekipmanlar kullanılmamış ve trafiğin engellenmesinde doğrudan SDN kontrolcüsünün yetenekleri kullanılmıştır.

Ryu kontrolcüsü yerine bir başka kontrolcü kullanıldığı senaryoda veya farklı bir OpenFlow sürümü kullanıldığı senaryoda ağ üzerinden akan trafiğin boyut ve saldırı tepkileri açısından karakteristikleri değişebilir [140]. Ancak sFlow kullanarak, doğrudan ağ cihazlarından aynı teknikle çekilen veriler kullanıldığından, kontrolcü değiştiği durumlarda veya geleneksel ağ ortamında çalıştığında, sistemin vereceği performans ve güvenlik sonuçlarının etkilenmeyeceği değerlendirilmektedir. Ayrıca sistem, yönlendirilebilir IP adreslerinde süreçlerin değişkenlik göstermesinden dolayı İSS'lerle uyumlu çalışmak için hazır durumda olmasa da, yapılacak modifikasyonlarla sistemin SDN altyapısına sahip İSS'lerle de uyumlu duruma gelebileceği düşünülmektedir.

Bu sistemin düşük gecikme, yüksek bant genişliği, çok sayıda kullanıcıya hizmet sunma gibi 5G ağları beklentilerine hizmet edebileceği değerlendirilmektedir. 5G ve ötesi ağlardaki güncellemelerle içerdiği alt sistemlerin de kolaylıkla güncellenebilecek bu sistemin güvenlik yönetimi açısından da 5G ağlarına katkı sunacağı düşünülmektedir.

7. TARTIŞMA

Tez kapsamında gerçekleştirilen çalışmalara ait bulgular ve ilgili bölümler özelinde bir sonraki bölüme geçilmeden önce tartışılması gereken hususlar bölüm değerlendirmesi alt başlıklarında sunulmuştur. Bu bölümde ise tez kapsamındaki çalışmalar idari ve teknik açıdan genel olarak tartışılacaktır. Ayrıca çalışmanın adli bilişim ve delil elde etme açılarından tartışması gerçekleştirilecektir.

7.1. İdari Açıdan Tartışma

Mevzuat ve uygulamalarda yer alan idari ve adli süreçlerin, teknolojik gelişmelerin ardından yürürlüğe alındığı görülmektedir. Mevzuatın sürecinin belirlenmesi ve yürürlüğe alınması için öncelikle ilgili konuda bir gereksinim oluşmasının beklenmesi doğaldır. Ancak mevzuatın yürürlüğe alınmasından önceki hazırlık aşamasında kapsamlı çalışmalar yapılmakta ve ilgili tüm kurumların görüşleri alınmaktadır. Teknolojik gelişim ve güncellemelerin süratle ilerlediği günümüzde, gelişmekte olan süreçler için yapılacak mevzuat değişikliklerinin genel çerçeve ile hazırlanarak yürürlüğe konulması ve gereksinim duyulduğu anda, çeşitli alt basamak normlarla şekillendirilmesinin daha hızlı bir süreç olabileceği düşünülmektedir. Normlar hiyerarşisi dikkate alındığında Kanun ve Yönetmeliklerin genel çerçevede olması ve sorumluların belirlenmesinin ardından, sorumlu Kamu Kurumlarının idari işleyişi hızlandıracak Esas çalışmalarını ivedilikle gerçekleştirmesi daha hızlı ve daha kolay güncellenebilir bir süreç olacaktır. Hızla gelişen bir teknoloji olan SDN'in adli bilişim çalışmaları için mevcut durumda büyük değişiklikler gerekmediği değerlendirilmiş olsa da detay bilgilerin Esas düzeyinde değişikliklerle gerçekleştirilebileceği veya uyulması zorunlu tutulan politikalarla sürecin işletilebileceği değerlendirilmiştir.

Ana eksenini SDN tabanlı 5G ağlarının adli bilişim süreçlerinin mevzuat ve uluslararası uygulamalar doğrultusunda test edilerek yorumlanması hususlarının oluşturduğu bu tezin, özellikle süreç oluşturma aşamasında çok sayıda akademik ve kurumsal kaynaktan faydalanılmıştır. Bu kapsamda bilgiye erişmek için çok sayıda farklı kaynağa başvuruluyor olması, bu bilgilerin dağıtık bir yapıda, yeterince yorumlanmamış ve derlenmemiş olduğunu göstermektedir. Bu durum sonucunda tespit edilen kazanımlar da çeşitli kurum ve

kuruluşlardan beklenen adli bilişim çalışmalarının yerine getirilmesi için tek bir referans kaynağa ihtiyaç duyulduğunu ispatlar niteliktedir. CBDDO tarafından hazırlanmış olan Bilgi ve İletişim Güvenliği Rehberinde belirtilen teknik hususlar arasında, bu çalışmada da incelenen ağ adli bilişimi ve diğer adli bilişim süreçleri odağında konular da bulunmaktadır. Öte yandan adli süreçlerden, idari süreçlere, teknik süreçlerden kolluk birimlerinin görevlerine kadar geniş bir açıdan incelenmesi gereken bir konu olan adli bilişim alanının da tüm boyutlarıyla incelenerek, rehber olabilecek bir kılavuzun hazırlanması ve Kamu Kurumları ile özel sektörün bilgisine sunulmasının fayda sağlayacağı düşünülmektedir. Bu doğrultuda bir kılavuz hem bağlayıcı olacak hem de süreçlere yol göstererek kurumsal anlamda karşı karşıya kalınabilecek idari yaptırımların da önüne geçebilecektir.

Siber güvenlik alanında gerçekleşen çalışma ve hazırlıklar ile ülkemizin bu alana yapmış olduğu yatırımlar göz önüne alındığında, adli bilişim alanında da uzman olarak çalışabilecek insan kaynağı ve teknolojinin ülkemizde var olduğu değerlendirilebilir. Ancak siber güvenlik ve adli bilişim kavramlarının birbiriyle ilişkili konular olmasına rağmen süreçleri ve bakış açıları olarak birbirinden ayrı şekilde işletilmesi gereken alanlar olduğu düşünülmektedir. Adli bilişim teknolojisinin ve bilgi birikiminin gelişmesi, siber güvenlik çalışmalarına doğrudan girdi olabilecek çıktılar elde edilmesini sağlayacaktır.

Adli bilişim alanında Kamu kurumlarının araştırmalarının yanı sıra, Türkiye'de Üniversitelerin de eğitim programları bulunmaktadır. TÜBİTAK, Adalet Bakanlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı gibi mevcut durumda adli bilişim çalışmaları yapan kurumların yanı sıra özel sektörün de kamu kurumları ve üniversitelerle iş birliği içerisinde yürüteceği çalışmalarla süreç geliştirilmesi ve araştırmaların mevcut durumun ötesine taşınabileceği düşünülmektedir [53].

Tez kapsamında geliştirilen ağ adli bilişim sistemi internet servis sağlayıcıları, kamu kurumları, üniversiteler ve veri merkezleri tarafından kullanılmaya uygun durumdadır. Sistemin gerçek ortam testlerinin yapılmasına öncelikle az kullanıcılı kamu kurumlarından başlanılması ve devamında bünyesinde barındırdığı değişken kullanıcı sayısı daha fazla olan üniversitelerden devam edilmesi sağlıklı olacaktır. Son aşamada da internet servis sağlayıcılarının altyapılarında deneysel çalışmalar gerçekleştirilerek tüm potansiyel kullanıcı yapılarda deneylerin gerçekleştirilmesi sağlanabilir. Geliştirilen ağ adli bilişim sisteminden elde edilen delillerin Emniyet Genel Müdürlüğü ve Jandarma Genel

Komutanlığı bünyesinde gerçekleştirilecek adli bilişim çalışmalarına da katkı sağlayacağı ve adli bilişim hazırlık seviyesini artırarak bilirkişilik süreçlerini de kolaylaştıracağı düşünülmektedir.

Adli Tıp Kurumu altında Adli Bilişim İhtisas Dairesi yer almaktadır. Bu birim adli konularda talep edilen konularda bilişim sistemlerini inceler, araştırma ve raporlama yapar [199]. Belirtilen görevlerin ötesinde, artan siber suçlar dikkate alındığında ülkemizdeki tüm adli bilişim süreç ve araştırmalarından sorumlu bir kuruluş tayin edilmesi veya yeni bir kuruluşun kurulmasının, mevzuat ve uygulamaların geliştirilmesinde ve süreçlerin takibinde ana görevi yüklenmesinin de teknik ve idari açıdan fayda sağlayacağı düşünülmektedir. Bu şekilde bir yapının var olması adli vakalarda bilirkişilik hizmetlerinden, adli bilişim eğitimleri genel politikasına, adli bilişim çalışmalarında yerli ve milli ürün geliştirme süreçlerinden, mevcut durumda kolluk kuvvetleri tarafından gerçekleştirilen süreçlerin tek elden ve standart şekilde gerçekleştirilmesine kadar birçok konuda fayda sağlayabilecektir. Siber suçların artışıyla birlikte yaşanabilecek vaka analizi ihtiyacını karşılayacak insan gücüne sahip olması beklenen bu yapının hazırlayabileceği ulusal adli bilişim stratejik planı kapsamında da gelecek yıllarda yapılabilecek çalışmalar belirlenerek ihtiyaçların tespiti ve giderilmesi hususunda adımlar atılabilir. Bununla birlikte tüm kurumlarda siber güvenlik ekiplerinin yanı sıra adli bilişim ekiplerinin de olmasının birbirini denetler yapıda iki farklı birimin daha sağlıklı çalışmasını sağlayabileceği düşünülmektedir.

Kurumlar özelinde oluşturulacak birbirini denetleyen yapıların varlığı adli bilişim sistemlerinin çalışmasında ve uygulama planlarının düzenli olarak gözden geçirilmesinde kritik öneme sahiptir. Her ne kadar tez kapsamında geliştirilen adli bilişim sistemi ağ adli bilişim sürecini otomatik şekilde gerçekleştirebiliyor olsa da, adli bilişim uygulama süreçlerinin uygunluğunun kurum içi denetim mekanizmalarının ötesinde oluşturulacak üst denetim yapılarıyla da denetlenmesinin önemli olduğu değerlendirilmiştir. Aksi durumda oluşturulan süreç ve sistemler özelinde farklı uygulamaların gerçekleştirilmesi veya kurum içi sorumlulukların yerine getirilip getirilmediği durumları tespit edilemeyebilir. Ağ adli bilişim sisteminde otomatik olarak gerçekleştirilmeyen tek husus, Elektronik İmza Kanunu gereğince kurum yetkilisinin log dosyasını gördükten sonra şifresini kendisinin girmesi sürecidir [124]. Mevzuatsal bir gereksinim olan bu adımla birlikte, sistemlerin çalışmasının kontrolünün de sorumlu personel tarafından doğal olarak sağlanacağı ve bu durumun nitelikli e-imza kullanımını da yaygınlaştırabileceği değerlendirilmiştir.

Ağ adli bilişimi çalışmalarının mevzuat uyumunu teknik bakışla değerlendiren bir çalışma bulunmamaktadır. Ayrıca AB'de ve diğer ülkelerde de SDN politikaları da mevcut değildir [123]. Geleneksel ağ adli bilişime yönelik yapılan çalışmalarda da, bakış açısının ve ilgililerin genişletilmesi gerektiği, eksikliklerin bulunduğu belirtilmiştir [33, 34, 43]. İnternet ortamının sınırları ülkelerin sınırlarının çizildiği gibi çizilemeyeceğinden dolayı ağ adli bilişim adına çözüm tek bir ülkenin sorumluluğundan veya politikasından geçemez. En sağlıklı ağ adli bilişiminin gerçekleştirilmesi için sınır ötesi iş birlikleri mecburidir [37, 43]. Bazı kritik verilerin yurt içinde saklanması gereklidir [64]. Kişisel verilerin korunmasına yönelik ülkemizin ve diğer ülkelerin kuralları bulunmaktadır. Bu sınır ötesi çalışmalarda uyum sağlanması için çerçevelerin belirlenmesinin faydalı olacağı değerlendirilmektedir. Adli bilişim ve güvenlik programlarını geliştiren şirketlerle de iş birliği kurulmasının bu kapsamda zorunluluk içereceği değerlendirilmektedir [43]. Az sayıda olsa da, yurt dışında bazı örnekleri bulunan adli bilişim süreçlerine dair teknik detay bilgi de içeren kılavuzların gerçekleştirilmesinin de süreçlere katkı sunacağı değerlendirilmektedir [30, 32, 153].

Ülkemizde 5G teknolojisinin kullanımı henüz aktifleşmemiştir. 2023 yılı içerisinde frekans tahsislerinin gerçekleşmesinin ardından önümüzdeki senelerde kullanımının ülkemizde de hızlı bir şekilde artması beklenmektedir. 5G teknolojik altyapısı da bu kullanımla birlikte oluşturulacaktır ve yeni güvenlik açıkları oluşabilecektir. Ancak zaten araştırılmış olan güvenlik açıklarına karşı sağlam bir tespit mekanizması ve ötesinde mevzuatta belirtilen gerekliliklerin sağlanması gerekmektedir. Hem teknik açıdan gelişmeler dikkate alınarak gerekli sistemsel geliştirmelerin gerçekleşmesi gerekmektedir, hem de bu teknik gelişmelere bağlı olarak gerekli idari çalışmaların yapılması gerekmektedir. Hem mobil operatörlerin üzerine düşen sorumlulukların, hem 5G teknolojisini kullanacak kişi ve cihazlara dair uygulama süreçlerinin netleştirilmesi önem arz etmektedir.

7.2. Teknik Açıdan Tartışma

SDN'in getirdiği yeniliklerin başında kontrolcü ve sanal anahtarlar yer alır. Kontrolcünün belirlediği kurallar uygulayan sanal anahtarlarda [11] komşuluk bilgileri yer alır. Geçici süre ile anahtarlar üzerinde yer alan bu verilerin sFlow, NetFlow vb. akış tabanlı veya paket tabanlı sistemlerle elde edilmesi mümkündür [164]. Bu sistemlerin tüm paketleri elde etmesi veya örnekleme ile işlem yapması mümkündür. Mevzuatta adli bilişim süreçleri için hangi tekniklerin kullanıldığı belirtilmediğinden akış veya paket tabanlı vb. yöntemlerden birini

seçerek topolojinin herhangi bir katmanından elde edilmesiyle bir süreç tanımlanması mümkündür. Ancak log tutma süreci için örnekleme yapılmadan kayıt işleminin gerçekleşmesi gerekir.

Bu tez kapsamında akış tabanlı sFlow kullanan bir log toplama sistemi geliştirilmiş olup belirlenen tüm teknik kayıt gereksinimlerinin SDN ortamlarından elde edilebildiği gösterilmiştir. Sistemde altyapı olarak OpenvSwitch kullanılmıştır. Farklı sanal anahtarların kullanımı durumunda da, sFlow'un standart veri çekme mantığı dikkate alındığında adli bilişim süreçlerinin farklılık göstermeyeceği değerlendirilmiştir. Adli bilişim çalışmalarında farklı cihaz ve tekniklerin kullanılması durumunda alınan neticelerin birbirinden farklılık göstermiyor olması önemlidir. Akış tabanlı log toplama sistemine alternatif olarak güney arayüzünden veri elde eden bir log toplama yöntemi de geliştirilebilir. Tez kapsamında yapılan çalışmalar kontrolcü değişikliklerinde OpenFlow paketleri üzerinden elde edilen bilgilerin, sanal anahtarlar üzerinden elde edilenlere kıyasla daha az değişiklik gösterdiğini göstermiştir. Bu durumun ana sebebi güney arayüzünde zaten standartlaşmış olan bir arayüzün kullanılmasıdır. OpenFlow versiyonuna göre elde edilebilecek bilgilerin de değişebileceği unutulmamalıdır. Ancak odağı adli bilişim olan bir yazılım geliştirme sürecinin OpenFlow gibi standartlara uygulanmasının ve akabinde güney arayüzü odaklı adli bilişim standartlarının geliştirilmesini de gerekli olduğu değerlendirilmiştir. Bu sayede adli bilişim çalışmaları daha az paket sayısı ve boyutu ile gerçekleşebilir olacaktır. Bu durum hem saklanacak verinin boyutu açısından hem de adli bilişim süreçlerinin hızı açısından önem arz eder. GET-POST bilgileri HTTP paketleri üzerinden elde edilebilecek olduğundan, mevzuatta elde edilmesi gerektiği belirtilen bu bilgilerin OpenFlow üzerinden elde edilmesi de teknik açıdan mümkün değildir. Ancak paket içeriklerinden HTTP taleplerinin gerçekleştiği ve sürecin sonuçlandığını yorumlamak mümkündür. Bu sebepten, tüm bu teknik değerlendirmelerin ötesinde SDN adli bilişim çalışmalarının teknik detaylarının doğrudan mevzuatta veya resmi bir politika belgesinde ana başlıklar halinde yer almasının da faydalı olabileceği değerlendirilmiştir.

Bazı hususlar içerik sağlayıcılar, toplu kullanım sağlayıcılar ve yer sağlayıcılar için değişiklik göstermektedir. Bu sebepten tez kapsamında oluşturulan sürecin kurumların niteliğine göre de ele alınması gereklidir. Oluşturulan bu sürecin kurumlar tarafından personellere tebliğ edilmesi de kurum bilinci açısından da önemlidir. Bilgi güvenliği ve adli bilişim süreçleri için belirlenen uzmanların haricinde tüm personelin bilgi birikiminin ve

farkındalığının artması süreçlerin daha sağlıklı işlemesini sağlayacaktır. Mevzuatta abone/kullanıcı bilgileriyle teknik bilgilerin eşleşmesinin gerekli olduğu belirtildiğinden, kullanıcıların kimlik numaralarıyla IP ve MAC adreslerinin eşleştirilmesi de önemlidir. Süreçte belirtilen özetleme, şifreleme, e-imzalama, yedekleme, güvenliği sağlama, veri yok etme vb. diğer teknik süreçler tez kapsamında geliştirilen sistem sayesinde mevzuat uyumlu olarak otomatik şekilde gerçekleştirilmektedir.

5G ağlarında SDN dışında kullanılan bir diğer temel teknoloji olan NFV'nin 5G adli bilişimi açısından incelenmesinin de kıymetli olacağı değerlendirilmiştir. Bu tez kapsamında 5G çekirdek ağlarından internet erişim kayıtlarının toplanması için SDN'e odaklanma gerçekleştirilmiştir. Bu doğrultuda deneyler kapsamında SDN kontrolcüleri karşılaştırılmış ve 5G ağlarına uygun adli bilişim sistemi SDN tabanlı olarak geliştirilmiştir. Bu sürecin iletişimlerin kayıt altına alınması açısından yeterli olacağı değerlendirilmiş olsa da NFV MANO odağında deneysel adli bilişim çalışmalarının ve sistem geliştirme süreçlerinin de 5G adli bilişimine katkı sunacağı değerlendirilmiştir. Bu odakta bir çalışma ile NFV MANO ile yönetilen ağ dilimleme, SFC, QoS yönetimi açısından da bulgular elde edilebilecektir [75]. Bu çalışmalar sayesinde sanal sunucuların göçü ve ağ bağdaştırıcısının değiştirilmesi gibi süreçlerdeki adli bilişim yaklaşımlarına dair çözümler elde edilebilmesi de mümkün olacağı değerlendirilmiştir [106].

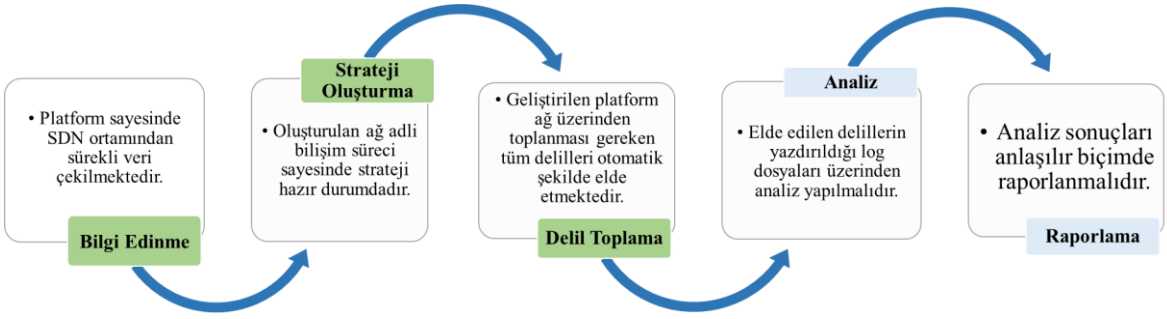
Bu tez kapsamında, daha basit ağ yönetimi [200] ile gerekli dijital delillere ulaşmanın mümkün olduğu gösterilmiştir. Bu verilerin tam olarak elde edilmesi makine öğrenmesi temelli saldırı tespit sistemleri ve gelecek saldırılara dair tahminler üretmek açısından da kıymetlidir [201, 202].

5G'ye geçişin ardından iletişim kuran cihaz sayısının ciddi miktarda artması beklenmektedir. Bu durum ağın yönetimine dair zorlukları da beraberinde getirmektedir. Çok sayıda cihazın bağlanması gereken bu durumun yönetimi donanım tabanlı olarak gerçekleştirilemez. Bu büyüklükte bir ağ yönetimini ancak yazılım ve sanallaştırma sistemleri kullanılarak gerçekleştirmek mümkündür. Ayrıca 5G'deki QoS hedeflerini, gecikme düzeyini, dinamik ve yüksek bant genişliği gerçekleştirmek için de SDN kullanımı gerekmektedir. Kullanıcılara tahsis edilecek kaynaklar ve bu tarz bir dinamik yönetim için 5G'de yatırım maliyetleri yüksek olacak olsa da işletme sürecinin daha az yatırımla devam ettirilebileceği değerlendirilmektedir. Ağ altyapısının işletilmesi esnasında SFC kullanımı

olan ağların da bu tez kapsamında önerilen adli bilişim sistemine sahip olması farklı beklentileri ve kuralları olan ağlara giden trafikler için de adli bilişim sürecinin ve internet erişimlerinin kesintisiz ve sağlıklı şekilde yapılabilmesine olanak tanıyacaktır. İSS'lerin 5G ağları odağında yapacağı teknik çalışmalarda bu tezde geliştirilen adli bilişim süreci ve sistemini kullanmalarının faydalı olacağı değerlendirilmiştir.

7.3. Adli Bilişim ve Delil Elde Edilmesi Açılarından Tartışma

Sistemin kullanımı siber suçların aydınlatılması amacıyla, adli vakalarda görevlendirilen bilirkişilerin süreçlerini kolaylaştıracak ve vakaların daha kolay aydınlatılmasını sağlayacaktır. Oluşturulan sistem sayesinde OSCAR yönteminde "bilgi edinme, strateji oluşturma, delil toplama, analiz ve raporlama" aşamalarından ilk üçüne dair süreçler Şekil 7.1'de gösterildiği gibi hali hazırda tamamlanmış olacak ve geriye sadece "analiz" ve "raporlama" aşamaları kalmış olacaktır. Kalan iki basamağın gerçekleşmesi de, mevcut olan verilerle son derece hızlı bir şekilde yapılabilecektir. Ayrıca ilk üç aşama için dijital delilin güvenilirliği çok önemli olup, sistemin kullanımıyla elde edilen veriler FAIR ilkesine uyumlu ve mevzuat kapsamında gerekliliği belirtilmiş olan veriler olduğundan vaka aydınlatma sürecinin güvenilirliği artmış olacaktır.



Şekil 7.1. Sistemin OSCAR kriterleri açısından değerlendirmesi

SDN ortamı ve çevre birimlerdeki dijital delil kaynaklarının adli bilişim çalışmalarında önemli olan bir diğer ölçüt olan "Önem, Efor, Uçuculuk ve Öncelik" kıyasının yapılması mümkündür. Tüm ortamlar dikkate alındığında sistemde elde edilen kayıtlarla sanal anahtar, kontrolcü, güvenlik çevre birimleri, işletim sistemi birimleri, sabit diskler, silinmiş veriler ve RAM, ROM vb. verilerin kıyaslaması gerçekleştirilmiştir.

Sistem sayesinde elde edilen IP adres bilgileri, kaynak-hedef bilgileri, veri miktarı vb. bilgilerin tamamı mevzuat kapsamında tutulması zorunlu olan veriler olduğundan dolayı, bu verilerin birbirleri arasında önem derecesinin eşit düzeyde önem, efor, uçuculuk ve önceliğe sahip olduğu söylenebilir. Bu veriler benzer süreçlerle elde edilmiş, aynı esaslara dayalı şekilde muhafaza edilmiş veriler olduğundan bu sonuca ulaşılmıştır. Bu sebepten bu verilere süreç gereksinimleri adı altında tek başlıkta yer verilmiştir. Süreç gereksinimleri ayrıca tez kapsamında geliştirilen sistem tarafından tutulan verileri de ifade etmektedir.
Süreç gereksinimleri mevzuatla zaten tutulması zorunlu kılınan veriler olduğundan, sistem sayesinde ek bir araştırmaya ihtiyaç olmadan hazır durumda olacaktır. Bu durum süreç gereksinimlerini en önemli noktaya taşırken, aynı zamanda zaten her an hazır durumda olacaklarından dolayı süreç gereksinimleri verilerini en az eforla erişilebilecek veriler arasına sokmaktadır. Silinmiş verilerin kurtarılma süreci göz önüne alındığında en yüksek eforla elde edilebilecek veriler olduğu değerlendirilmiştir.

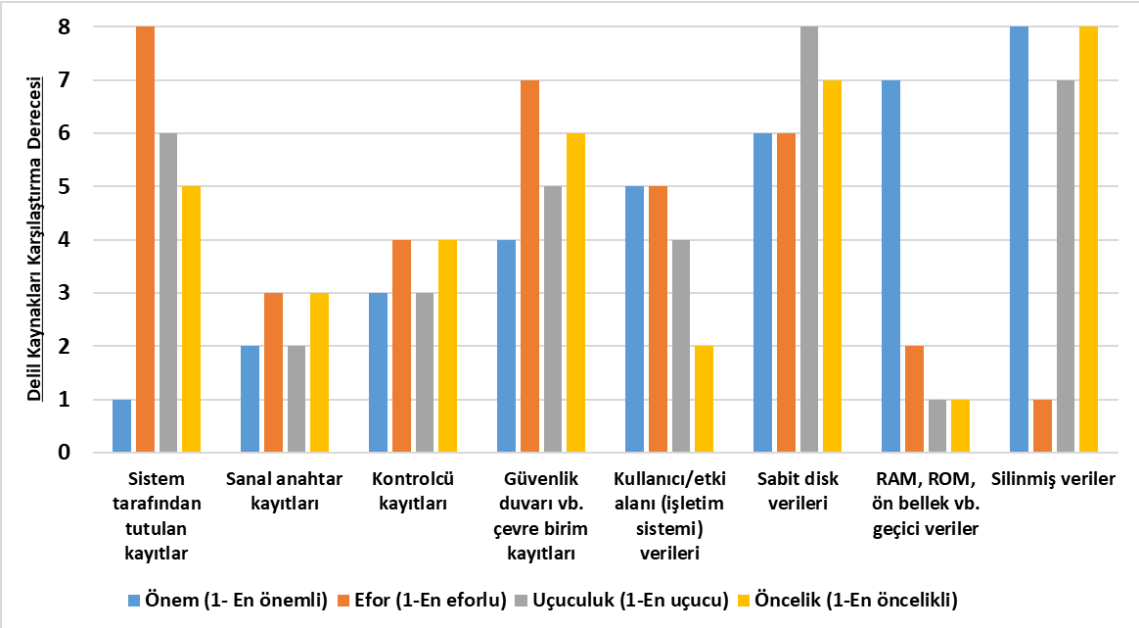
RAM üzerinden elde edilebilecek veriler doğası gereği geçici olarak tutulduğundan dolayı, en uçucu deliller oldukları değerlendirilmiştir. Bu sebepten öncelik sıralamasında en önde yer alması beklenir. Aksi durumda bu bölgeden elde edilebilecek deliller kaybolacak ve soruşturmayı tehlikeye atacaktır. Süreç gereksinimlerindeki veriler mevzuat kapsamında belirlenen süre kadar saklanmak zorunda olduklarından dolayı diğer çevre birimlerine göre daha az uçucudur.

Öncelik ve uçuculuk ölçütleri genellikle birbirine yakınsamaktadır. Ancak bu ölçütler her zaman aynı sırada yer almayabilir. Örneğin silinmiş veriler de sabit disk üzerinde yer alan veriler olmasına karşın, disk üzerinde yer alan ve silinmemiş olan diğer verilerden daha uçucudur. Bunun sebebi ise silinmiş verilerin üzerine tekrar veri yazılması ihtimalidir. Bu durumda ilgili silinmiş veriye tekrar ulaşılamayabilir veya daha zor ulaşılabilir. Silinmiş bir verinin tekrar elde edilmesi süreci çok uzun sürebileceğinden, elde edilebilecek bilginin katma değeri de düşünüldüğünde silinmiş veri kurtarmaya daha az öncelik verilmesi gerekmekte olduğu değerlendirilmiştir.

Saldırı tespit sistemleri, güvenlik duvarı vb. çevre birimlerinden sağlanabilecek delillerin saklanma süreleri ve formatlarının standartlaştırılması zorunlu değildir. Bu sebepten bu verilerin süreç gereksinimlerine göre daha uçucu ve daha az öncelikli olduğu değerlendirilmiştir.

Özetle süreç gereksinimleri en önemli ve en az efor gerektiren verileri içermektedir. RAM üzerinden elde edilebilecek deliller en uçucu ve en öncelikli veriler olarak değerlendirilmiştir. Silinmiş verilerse en çok eforla elde edilebilecek olan verilerdir.

Belirlenen sekiz ölçüt özelinde "Önem, Efor, Uçuculuk ve Öncelik" kriterlerine dair karşılaştırılma Şekil 7.2'de sunulmuştur.



Şekil 7.2. Delil kaynaklarının karşılaştırılması

Kişisel verilerin güvenli ve yedekli şekilde korunması ve belirtilen sürelerin sonunda yok edilmesi süreçleri bu sistemle birlikte güvence altına alınmıştır. AB'nin GDPR tüzüğüne uyum sağlamak amacıyla da gerekli güncellemelerin gerçekleştirilmesi faydalı olacaktır. Ancak küresel anlamda tüm ülkelerin kişisel verilerin korunmasına yönelik tek bir referans kaynak oluşturması ve veri paylaşımlarına yönelik kararlar almasının gerekli olduğu değerlendirilmiştir. Ayrıca sınır ötesi siber suç operasyonları için de ülkeler arasında çerçeve mevzuatların belirlenmesini gerekli olduğu değerlendirilmiştir. Aksi durumda ülke sınırları gibi sınırların çizilmesinin mümkün olmadığı internet ortamında, ülkeler arası veri paylaşım sorunları sebebiyle suçların aydınlatılması ve sağlıklı adli bilişimin yapılması zor bir süreç olarak kalmaya devam edecektir.

8. SONUÇ VE ÖNERİLER

5G ağlarında adli bilişim süreçlerinin teknik açıdan durumunun net bilinmiyor olması ve idari bakış açısına sahip adli bilişim sürecinin var olmaması problemlerine çözümler içeren bu tez çalışmasında SDN tabanlı ağlarda adli bilişim süreçlerinin teknik durum tespitinin gerçekleştirilmesinin ardından bir adli bilişim süreci oluşturulmuştur. Bu sürece uygun ve SDN tabanlı 5G ağlarına uyumlu adli bilişim sistemi geliştirilerek tespit edilen problemlere çözüm oluşturulmuştur. 5G ağlarında güvenlik servisleri yönetiminin de incelendiği bu tez kapsamında aşağıda yer alan alt başlıklarda tez kapsamında yapılan çalışmalar özetlenmiş, çalışmanın literatüre katkıları belirtilmiş, karşılaşılan zorluklar aktarılmış ve gelecek çalışma önerileri sunulmuştur.

8.1. Sonuçlar ve Değerlendirme

5G ağlarına uyumlu adli bilişim sistemi geliştirilmesi amaçlanan bu tez çalışmasında öncelikle SDN ortamlarında adli bilişim tekniklerine dair durum tespiti yapılması problemine odaklanılmıştır. Bu kapsamda farklı SDN kontrolcüsü kullanımında adli bilişim süreçlerinin nasıl etkilendiğinin net olarak bilinmemesi ve hangi SDN katmanlarının ne tür delilleri içerebileceği hakkında literatürde yer alan eksik adreslenmiştir. Tezin ilk aşamasında gerçekleştirilen bu çalışma süreci ve sonuçları aşağıda sunulmaktadır:

- Literatürde ilk defa yedi farklı senaryoda, dört farklı kontrolcü kullanılarak deneyler gerçekleştirilmiştir.
- Deneylerde veri katmanı ve güney arayüzünden elde edilebilecek bilgiler detaylı şekilde incelenmiştir. Adli bilişim açısından önem arz eden paket boyutu, kaynak-hedef tespiti, saldırı ve saldırgan bilgileri, saldırı esnasında servis dışı kalıp kalmama durumları dikkate alınmıştır. Saldırı deneyleri farklı kontrolcülerin kullanıldığı test ortamlarında bahsi geçen temel adli bilişim gereksinimlerinin tespiti ve servis vermeye devam etme açısından kontrolcüler arasında farklılıklar olduğunu göstermiştir.
- Adli bilişim açısından anlamlı olabilecek bilgilerin elde edilmesinin ötesinde bu verilerin en düşük veri boyutuyla elde edilmesi de tespitin hızı ve saklama alanı açısından önem arz etmektedir. Deney sonuçları farklı kontrolcülerin kullanıldığı test ortamlarında paket boyutları arasında farklılıklar olduğunu göstermiştir.

- Farklı kontrolcüler üzerinde gerçekleşen deneylerde güney arayüzü verilerinden elde edilen bilgilerin de, bilgiye erişim ve paket boyutu açısından farklılıklar gösterdiği görülmüştür. Güney arayüzünden elde edilen bilgiler farklılık göstermiş ve bazı bilgilere erişilememiştir. Ancak adli bilişim çalışmalarının diğer SDN katmanlarına göre daha standart hale gelmiş olan güney arayüzü üzerinden sürdürülmesinin servis kalitesi, veri boyutu ve üreticiden bağımsız bir standarda erişim açısından faydalı olabileceği de değerlendirilmiştir.
- Deney sonuçları kontrolcü odaklı bir ağ adli bilişiminin standart hale getirilmesi için çalışmalar gerçekleştirilmesini ispatlar niteliktedir. Tüm deneylerde tam başarı gösteren bir kontrolcü bulunmamaktadır. Farklı deney senaryolarında en başarılı olan kontrolcü, diğer senaryolarda başarısız sonuçlar verdiğinden, adli bilişim açısından en başarılı kontrolcüyü seçmenin mümkün olmadığı ispatlanmıştır. Bu sebepten teknik açıdan kontrolcü geliştirme süreçlerinin standartlaşması gerektiği değerlendirilmektedir. Genel olarak SDN ortamı sadece kontrolcülerden oluşmadığından tüm ağ ortamları üzerinde aynı adli bilişim süreçlerinin gerçekleştirilebileceği bir sürecin oluşturulmasının gerekli olduğu sonucu ortaya çıkmıştır.

SDN tabanlı 5G ağlarında adli bilişim gerçekleşebilmesi açısından mevcut durumda teknik açıdan bir standart olmadığının görülmesinin ardından idari ve hukuki açıdan ağ adli bilişim çalışmalarının incelemesini yaparak bir adli bilişim süreci oluşturulmasına odaklanılmıştır. Mevzuat ve uluslararası uygulamalardaki mevcut durum aktarılarak adli bilişim sürecine dâhil edilmesi gereken alanlar adreslenmiştir. Bu çerçevede gerçekleştirilen çalışmalar ve elde edilen sonuçlar aşağıda sıralanmıştır:

- Ağ adli bilişimi süreçlerini belirlemek için çok sayıda ve dağınık yapıda olan mevzuatın incelenmesi gerekmiştir. Ağ adli bilişimine girdi olabilecek mevzuatın teknik açıdan yeterli ve kendi içerisinde uyumlu olduğu görülmüştür.
- Mevzuatın yanı sıra kurumsal rehberler, bilirkişilik süreçleri ve uluslararası uygulama ve standartların da ele alınmasıyla bir ağ adli bilişim süreci oluşturulmuştur. Oluşturulan süreç; hangi logların kayıt altına alınması gerektiği, kayıtların nasıl muhafaza edilmesi gerektiği, ne kadar süre ile saklanması gerektiği, muhafaza süresi sona eren kayıtların nasıl silinmesi gerektiği, verilerin depolanma yerleri, trafiğin

engellenmesi gerektiği durumlarda nasıl aksiyonlar alınması gerektiği ve yetkilendirme süreçleri gibi çok sayıda bilgiyi içermektedir.

- Oluşturulan adli bilişim süreci mevzuat kapsamında zorunluluk getirilen durumları içermekte olup paydaşların bu sürece uyumunun mecburi olduğu değerlendirilmiştir.
- Sürecin geleneksel ağların yanı sıra SDN ortamlarına ve 5G ağlarıyla da uyumlu olduğu değerlendirilmiştir.
- Geliştirilen süreç, mevzuat ve uluslararası uygulamalara uyumlu bir adli bilişim süreci olarak literatürde bir ilk özelliği taşımaktadır. Bu sürecin tez kapsamında geliştirilmesi hedeflenen sistemde kullanılmasının ötesinde uluslararası idari ve teknik adli bilişim çalışmaları için de yol gösterici nitelikte olacağı değerlendirilmektedir.

İncelenen mevzuat ve ülke uygulamalarının teknik açıdan adli bilişim yapılması için yeterli yönlendirmeleri içerdiği görülmekle birlikte, birçok detayın teknik birimlerin sorumluluklarına bırakıldığı görülmüştür. Tezin son aşaması, sürecin oluşturulmasının ötesinde sorumlu kurum ve kişilerin belirlenen süreci eksiksiz şekilde uygulayabilmesi için sistem oluşturulmasına odaklanılmıştır. SDN tabanlı 5G ağlarına uyumlu, güvenliği sağlarken, mevzuata uyumlu olarak adli bilişim hazırlık seviyesini artıran ve tüm süreçleri otomatik şekilde işletebilen adli bilişim sistemi geliştirilmiştir. Güncel ve güvenli tekniklerin kullanıldığı sistem, bir ülke mevzuatına uygun ağ adli bilişimi sistemi olması açısından bir ilk özelliğini taşımaktadır. Türkiye Cumhuriyeti mevzuatının gereksinimlerini sağlamasının yanı sıra küresel çapta adli bilişim süreçlerine katkı sunabilecek olan sistemin sınır ötesi adli bilişim çalışmalarında kullanılmasının da mümkün olduğu görülmüştür. Oluşturulan sisteme dair bulgu ve sonuçlara aşağıda yer verilmiştir:

- Geliştirilen sistem mevzuatta belirtilen tüm teknik kayıtları hiçbir müdahaleye gerek kalmaksızın otomatik olarak toplayan, güvenli ve yedekli bir ortamda belirlenen süre kadar muhafaza eden, muhafaza süresinin dolmasının ardından geri döndürülemez şekilde silen alt sistemleri içermektedir. Ayrıca zararlı hedefleri engelleyen, eşik tabanlı uyarı sistemi sayesinde servis dışı bırakma saldırıları için uyarı veren ve uluslararası veri sızıntılarını tespit eden sistemleri de içermektedir.
- Geliştirilen adli bilişim sistemi gerçek internet verisi üretilerek bir günü aşkın süre aktif şekilde çalıştırılarak test edilmiştir. Deney sonuçları; gereksinim duyulan kayıtların akış tabanlı log toplama sistemi sayesinde elde edilebildiğini, servis dışı bırakmaya yönelik saldırıların tespit edilebildiğini ve engellenebileceğini, zararlı ve

engelli web erişimlerinin engellenebildiğini, log dosyalarının geri döndürülemez şekilde silinebildiğini göstermiştir.

- Yedekli yapıda tutulan log kayıtları ile felaketlere karşı hazır bir kurtarma planı da içeren sistemin geliştirilmesi sürecinde, mevzuat kapsamında belirtilen yurt dışına giden veri sızıntılarının SDN ortamında tespitine dair bir çalışma da ilk defa gerçekleştirilmiş ve kritik verilerin yurt dışına çıkması durumunda tespit ve engel süreçlerinin gerçekleştirilebildiği görülmüştür.
- Zararlı/engelli web sayfalarının devletin belirlediği veri tabanı kullanılarak SDN yetenekleriyle engellenmesi de sistemde ilk defa gerçekleştirilen süreçlerin arasındadır.
- Akan trafik boyutunun sadece %0,87'sine karşılık gelen bir alanla gereksinim duyulan tüm kayıtların tutulması, sistemin disk kapasitesi açısından verimli çalıştığını da ispatlamıştır. İşlemci ve RAM açısından da büyük kaynak gerektirmemesi ve tüm süreçlerin ücretsiz/açık kaynak araçlarla geliştirilmiş olması da sistemin öne çıkan avantajları arasında yer almaktadır.
- SDN tabanlı 5G ağları ile uyumlu çalışabilecek bu adli bilişim sistemi geleneksel ağlarla da uyumlu olabilecek şekilde geliştirilmiştir. Sistem otomatik şekilde tüm süreçleri gerçekleştirmekte, kişi ve kurumlardan bağımsız bir düzen içerisinde çalışmaktadır. Bu sayede insan faktörü devre dışı bırakılmış olup, istenmeyen adli veya idari yaptırımların önüne geçilmiştir.

Adli bilişim sisteminin geliştirilmesi için teknik durum tespitinin yapıldığı ve ağ adli bilişim sürecinin oluşturulduğu bu tez kapsamında gerçekleştirilen çalışmalar birbirini takip eder ve iç içe geçmiş bir yapıdadır. Bölümler özelinde yukarıda sıralanan katkıların ötesinde tezin en önemli katkılarından birisinin, adli bilişim incelemelerinde ele alınacak delillerin mevzuata uygun, hazır ve eksiksiz şekilde elde edilmesi olduğu değerlendirilmiştir. Sistem bu sayede kurumların ve internet servis sağlayıcıların adli bilişim hazırlık düzeyini artırabilecek niteliğe sahip ilk ağ adli bilişim sistemi olma özelliğini göstermektedir.

Belirlenen problemlere dair gerçekleşen çalışmaların sonuçları yukarıda aktarılmış olup, tez kapsamında literatüre yapılan temel katkılar aşağıda belirtilmiştir:

- SDN kullanılan ağ ortamlarında güvenilir ağ adli bilişimi için standart bir sürecin gerekli olduğu gösterilmiştir,

- Mevzuat ve uluslararası uygulamalar dikkate alınarak ağ adli bilişim gereksinimleri belirlenmiş ve ilk defa bir ağ adli bilişim süreci oluşturulmuştur,
- Belirlenen ağ adli bilişim süreci ile uyumlu, otomatik ve güvenli SDN tabanlı 5G ağlarıyla uyumlu ağ adli bilişim sistemi literatürde ilk defa geliştirilmiştir.

8.2. Karşılaşılan Zorluklar

Bu tezin gerçekleştirilmesi aşamasında aşağıdaki zorluklarla karşılaşılmıştır:

- SDN ve 5G alanlarında gerçekleşen adli bilişim çalışmaları yeterli değildir. Bu sebepten adli bilişim sistemi oluşturmak için gerekli teknik durumun tespiti için çok sayıda deney gerçekleştirilmiştir.
- Bir ağ adli bilişim süreci oluşturmak için mevzuat ve uluslararası uygulamalar incelenmiştir. Sayıca yeterli olarak değerlendirilen bu çalışmaların ayrık yapıda olması süreç oluşturulması sürecini uzatmıştır. Öte yandan bu kaynakların tek bir referans kaynak olarak bu tezde toplanmış olmasıysa tezin etki potansiyelini güçlendirmektedir.
- Tüm deneyler bir dizüstü bilgisayar üzerinde yer alan sanallaştırma sisteminde gerçekleştirilmiş olup, bu durum ağ bağdaştırıcısı açısından bir kısıtlılık oluşturmuştur. Ancak bu kısıtlılığın aksine, sanallaştırma sisteminde alınan anlık görüntüler alınan hataların süratle önüne geçilebilmesini sağlamış ve tez çalışmalarına sürat kazandırmıştır.
- Deneylerde ve özellikle sistem geliştirilmesinde örnek kaynak kodların eksikliği bir zorluk oluşturmuştur. Bu durum kod yazma ve sistem geliştirme süreçlerinin uzamasına sebep olmuştur.
- Sistemin tüm bileşenlerinin sağlıklı çalışma durumunun test edilmesi için gerçek internet verisi üretilmiştir. Bu testlerin sağlıklı gerçekleşmesi için en az bir günlük kesintisiz teste ihtiyaç olması başka bir zorluktur.

8.3. Gelecek Çalışma Önerileri

Bu tezde sistem mühendisliği, yazılım mühendisliği, bilişim hukuku ve adli bilişim gibi farklı disiplinlerin bakış açıları ve yeteneklerini kullanarak bir adli bilişim sistemi geliştirilmiştir. Gelecek çalışma önerileri aşağıda sıralanmaktadır:

- Sistemin çok kullanıcılı gerçek kurumlarda deneme süreçlerinin tamamlanmasının ardından sistem ticarileşebilir. Bu sayede bir ürün olarak kurumların, İSS'lerin veya mobil iletişim sağlayıcıların hizmetine sunulabilir.
- Sistemde erişim kayıtları sFlow ile elde edilmekte olup, kayıtların farklı mekanizmalarla daha hızlı veya daha düşük boyutlu şekilde elde edilmesi üzerine araştırmalar gerçekleştirilebilir.
- Sistem mevcut durumda tekil bir yapıda çalışmakta olup, alt sistemlerin dağıtık yapıda kullanımı gerçekleştirilebilir.
- Sistemin bulut hizmeti olarak sunulması için çalışmalar gerçekleştirilebilir.
- Uygulama katmanındaki verileri standart bir şekilde işleyecek yöntemin de sisteme dâhil edilmesiyle adli bilişim kalitesi artırılabilir.
- Sisteme dâhil edilen saldırı tespit sistemlerine güncel makine öğrenmesi teknikleri de dâhil edilerek güvenlik düzeyi artırılabilir.
- Çok sayıda SDN kontrolcüsünün kullanıldığı ortamlara uygun bir SDN adli bilişim sistemi geliştirilebilir.
- Farklı servis sunma politikası içeren ağlarda, farklı kalite hedefi olan ağ dilimlerinde, özellikle NFV ve SFC üzerinden farklı ağlara dahil olunan ortamlarda adli bilişim çalışmalarına dair araştırmalar gerçekleştirilebilir ve oluşabilecek adli bilişim farklılıklarına dair önlemler alınabilir.
- Kişisel verilerin anonimleştirildiği ortamlarda adli bilişim çalışmalarının yapılabilmesi üzerine durum tespiti ve araştırmalar gerçekleştirilebilir.
- Ülkelerin siber güvenlik ve adli bilişimden sorumlu birimlerinin, uluslararası çapta üretim yapan şirketler ve çerçeve kurumlar iş birliğinde küresel çözümler üretmesi adına politikalar geliştirilebilir.

Bu çalışmanın yürürlüğe alınacak adli bilişim politikalarına, bağlayıcı adli bilişim kılavuzlarına ve kuruluşların SDN tabanlı 5G ağlarında adli bilişim çalışmaları doğrultusundaki sorumluluklarının belirlenmesi hususlarına öncü ve yol gösterici nitelikte olduğu değerlendirilmektedir. Güvenlik, bütünlük ve erişilebilirlik gereksinimlerini eksiksiz şekilde sağlayan sistemin tüm ülkeler tarafından kullanılması mümkün olup, hem hukuki hem de teknik açıdan gelecek çalışmalara yön verecek bir tasarımda olduğu düşünülmektedir. Adli Bilişim yol haritası mevcut olan ülkelerin bu tarz sistemlerin geliştirilmesine yönelmesinin faydalı olacağı, adli bilişim hazırlık düzeyi düşük olan

ülkelerinse bu süreçleri örnek alarak hukuki ve teknik açıdan yeni yöntem ve süreçleri kullanıma alabileceği değerlendirilmiştir.

KAYNAKLAR

1. Türk Telekom (2018). 5G Beyaz Kitap. URL: https://www.turktelekom.com.tr/tt-hakkimizda/duyurular/Documents/tt-5g-final-version-03082018.pdf, Son Erişim Tarihi: 20.04.2023.

2. İnternet: Markets and Markets (2022). 5G Services Market. URL: https://www.marketsandmarkets.com/Market-Reports/5g-services-market-226908556.html?gclid=CjwKCAjw9pGjBhB-EiwAa5jl3AIb2ry9Sa02ITjuWLhX4VRdKj6kKpsrWZ58T9c82r07NLu4yaLRXBoCaA4QAvD_BwE, Son Erişim Tarihi: 20.04.2023.

3. Vodafone Türkiye (2023). Vodafone 5G. URL: https://www.vodafone.com.tr/5g, Son Erişim Tarihi: 20.04.2023.

4. Bilgi Teknolojileri ve İletişim Kurumu (BTK). (2018). 5G ve Ötesi Beyaz Kitap. URL: https://www.btk.gov.tr/uploads/announcements/5g-ve-otesi-beyaz-kitap/beyaz-kitap-son.pdf, Son Erişim Tarihi: 20.04.2023.

5. Türkiye İstatistik Kurumu (TÜİK) (2022). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması. URL: https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2022-45587#:~:text=TÜİK Kurumsal&text=Hanehalkı bilişim teknolojileri kullanım araştırması,Birimleri Sınıflaması (İBBS) 1., Son Erişim Tarihi: 20.04.2023.

6. Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2022). Dijitalleşen Dünyada Bilişim suçları ve Mücadele Yöntemleri. URL: https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri-6218e2417eaea.pdf, Son Erişim Tarihi: 20.04.2023.

7. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S. ve Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access*, 8, 137293–137311.

8. Rawat, D. B. ve Reddy, S. R. (2017). Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. I*EEE Communications Surveys and Tutorials*, 19(1), 325–346.

9. İnternet: Markets and Markets (2020). Software-Defined Network Market. URL: https://www.marketsandmarkets.com/Market-Reports/software-defined-networking-sdn-market-655.html#:~:text=%5B465 Pages Report%5D The global,productivity for field-based services, Son Erişim Tarihi: 20.04.2023.

10. Abdelaziz, A., Fong, A. T., Gani, A., Garba, U., Khan, S., Akhunzada, A. ve Choo, K. K. R. (2017). Distributed controller clustering in software defined networks. *PLoS ONE*, 12(4), 1–19.

11. Van Adrichem, N. L. M., Doerr, C. ve Kuipers, F. A. (2014). OpenNetMon: Network monitoring in OpenFlow software-defined networks. In *IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a*

Software Defined World. IEEE Computer Society.

12. Yan, Z., Zhang, P. ve Vasilakos, A. V. (2016). A security and trust framework for virtualized networks and software-defined networking. *Security and Communication Networks*, 9(16), 3059–3069.

13. Chourishi, D., Miri, A., Milic, M. ve Ismaeel, S. (2015). Role-based multiple controllers for load balancing and security in SDN. In *2015 IEEE Canada International Humanitarian Technology Conference, IHTC 2015, Ottawa, Canada*, 1–4.

14. Al-Najjar, A., Layeghy, S. ve Portmann, M. (2016). Pushing SDN to the end-host, network load balancing using OpenFlow. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, NSW, Australia*, 1–6.

15. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S. ve Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1), 14–76.

16. Shin, S., Xu, L., Hong, S. ve Gu, G. (2016). Enhancing Network Security through Software Defined Networking (SDN). *In 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA*, 1–9.

17. Nguyen, T. H. ve Yoo, M. (2017). Analysis of link discovery service attacks in SDN controller. In *2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam*, 259–261.

18. Chi, P. W., Kuo, C. T., Guo, J. W. ve Lei, C. L. (2015). How to detect a compromised SDN switch. In *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft), London*, 1–6.

19. Bawany, N. Z., Shamsi, J. A. ve Salah, K. (2017). DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. *Arabian Journal for Science and Engineering*, 42, 425–441.

20. Hong, S., Xu, L., Wang, H. ve Gu, G. (2015). Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures. In *Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA*, 1-15.

21. Waseem, Q., Alshamrani, S. S., Nisar, K., Din, W. I. S. W. ve Alghamdi, A. S. (2021). Future technology: Software-defined network (SDN) forensic. *Symmetry*, 13(5), 1–18.

22. Akbari, I., Tahoun, E., Salahuddin, M. A., Limam, N. ve Boutaba, R. (2020). ATMoS: Autonomous Threat Mitigation in SDN using Reinforcement Learning. In *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary*, 1–9.

23. Pandya, M. K., Homayoun, S. ve Dehghantanha, A. (2018). Forensics Investigation of OpenFlow-Based SDN Platforms. In A. Dehghantanha, M. Conti, & T. Dargahi (Eds.), *Cyber Threat Intelligence*, 281–296.

24. Shrivastava, G. (2016). Network forensics: Methodical literature review. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India,* 2203–2208.

25. Shrivastava, G., Sharma, K. ve Kumari, R. (2016). Network forensics: Today and tomorrow. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India,* 2234–2238.

26. Ring, M., Wunderlich, S., Scheuring, D., Landes, D. ve Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers and Security*, 86, 147–167.

27. Akinbi, A. O. (2023). Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. *WIREs Forensic Science*, e1496, 1-21.

28. Sharevski, F. (2018). Towards 5G cellular network forensics. EURASIP *Journal on Information Security,* 2018:8, 1-16.

29. Falih, M. D. ve Satrya, G. B. (2019). Radio Cellular Forensics Analysis: Where is the Adversary? *2019 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), Kuala Lumpur, Malaysia,* 208–213.

30. ENISA (2019). Introduction to Network Forensics Final Version 1.1. URL: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf, Son Erişim Tarihi: 20.04.2023.

31. ENISA (2017). National Cybersecurity Strategies. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies, Son Erişim Tarihi: 20.04.2023.

32. National Institute of Justice (NIJ) (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. URL: https://nij.ojp.gov/library/publications/forensic-examination-digital-evidence-guide-law-enforcement, Son Erişim Tarihi: 20.04.2023.

33. Al-murjan, A. ve Xynos, K. (2008). Network Forensic Investigation of Internal Misuse / Crime in Saudi Arabia : A Hacking Case. *ADFSL Conference on Digital Forensics, Security and Law*, 15–32.

34. Apau, R. ve Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, 2, 299–309.

35. Lasagni, G. (2021). The Handling of Digital Evidence in Italy. in M. Caianiello – A. Camon (a cura di), Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations, Wolters Kluwer/CEDAM, Collezione di giustizia penale, 87-121.

36. Fenu, G. ve Solinas, F. (2013). Computer forensics between the italian legislation and pragmatic questions. *International Journal of Cyber-Security and Digital Forensics*, 2, 9–24.

37. Díaz-Pérez, L. C., Quintanar-Reséndiz, A. L., Vázquez-Álvarez, G. ve Vázquez-Medina, R. (2022). A review of cross-border cooperation regulation for digital

forensics in LATAM from the soft systems methodology. *Applied Computing and Informatics (ahead-of-print)*.

38. Prayudi, Y., Ashari, A. ve Priyambodo, T. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Informations Security*, 7, 1–8.

39. Guo, H. ve Hou, J. (2018). Review of the accreditation of digital forensics in China. *Forensic Sciences Research*, 3, 1–8.

40. Elyas, M., Maynard, S., Ahmad, A. ve Lonie, A. (2014). Towards A Systemic Framework for Digital Forensic Readiness. *Journal of Computer Information Systems*, 54, 97–105.

41. Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W. ve Kim, J. (2018). A comparative study on data protection legislations and government standards to implement digital forensic readiness as mandatory requirement. *Digital Investigation*, 24, S93–S100.

42. Nance, K. ve Ryan, D. J. (2011). Legal Aspects of Digital Forensics: A Research Agenda. In *2011 44th Hawaii International Conference on System Sciences, Kauai, HI, USA*, 1–6.

43. Losavio, M., Pastukov, P., Polyakova, S., Zhang, X., Chow, K. P., Koltay, A. ve Ortiz, M. (2019). The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. *Wiley Interdisciplinary Reviews: Forensic Science*, 1, e1337.

44. Karyda, M. ve Mitrou, L. (2007). Internet Forensics: Legal and Technical Issues. In *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), Karlovassi, Greece*, 3–12.

45. Adams, C. W. (2008). Legal Issues Pertaining to the Development of Digital Forensic Tools. In *2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA*, 123–132.

46. Atalay, N. S., Doğan, Ş., Akbal, E. ve Tuncer, T. (2019). Adli Bilişim Alanında Ağ Analizi. *BEÜ Fen Bilimleri Dergisi*, 8(2), 582–594.

47. Değirmenci, O. (2020). Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi. *Bilişim Hukuku Dergisi*, 2(1), 47–79.

48. Önel, B., ve Irmak, E. (2021). Adli Bilişim ve Dijital Delillerin Windows İşletim Sistemi Üzerinde İncelenmesi. *Politeknik Dergisi*, 24(3), 1187–1196.

49. Gençoğlu, M. T. (2021). Siber Olaylara Müdahale ve Analiz Süreci. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 33(2), 471–479.

50. Yılmaz, F. ve Çakır, H. (2021). Karar Destek Sistemlerinin Mobil Cihaz Adli Bilişimi Süreçlerine Uygulanmasına Yönelik Bir Öneri Çalışması. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 7(1), 24–45.

51. Çakır, H. ve Kılıç, M. S. (2013). Bilişim suçlarına ilişkin delil elde etme yöntemlerine genel bir bakış. *Polis Bilimleri Dergisi*, 15(3), 23–44.

52. Emekci, A., Kuğu, E. ve Temiztürk, M. (2016). Adli Bilişim Ezberlerini Bozan Bir Düzlem : Bulut Bilişim. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(1), 8–14.

53. Akbal, E. ve Güneş, F. (2016). Adli Bilişim Mühendisliği Eğitiminin Kurumlar Açısında Önemi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 4(2), 395–402.

54. Özen, M. ve Özocak, G. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134). *Ankara Barosu Dergisi*, (1), 0.

55. Yılmaz, F. ve Güllüpınar, F. (2020). Türkiye'de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 15(10 Yıl Özel Sayısı).

56. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007). URL: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf, Son Erişim Tarihi: 20.04.2023.

57. İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (2020). URL: https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm, Son Erişim Tarihi: 20.04.2023.

58. Elektronik Haberleşme Kanunu (2008). URL: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf, Son Erişim Tarihi: 20.04.2023.

59. Türk Ceza Kanunu (2004). URL: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf, Son Erişim Tarihi: 20.04.2023.

60. Ceza Muhakemesi Kanunu (2004). URL: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5271.pdf, Son Erişim Tarihi: 20.04.2023.

61. İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik (2007). URL: https://www.resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm, Son Erişim Tarihi: 20.04.2023.

62. Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik (2007). URL: https://www.resmigazete.gov.tr/eskiler/2007/10/20071024-12.htm, Son Erişim Tarihi: 20.04.2023.

63. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik (2007). URL: https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=11746&mevzuatTur=Kur

umVeKurulusYonetmeligi&mevzuatTertip=5, Son Erişim Tarihi: 20.04.2023.

64. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) (2020). Bilgi ve İletişim Güvenliği Rehberi. URL: https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf, Son Erişim Tarihi: 20.04.2023.

65. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) (2021). Bilgi ve İletişim Güvenliği Denetim Rehberi. URL: https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf, Son Erişim Tarihi: 20.04.2023.

66. International Organization for Standardization (ISO) (2022). ISO/IEC 27001 and Related Standarts - Information Security Management Systems.

67. Zaidi, Z., Friderikos, V., Yousaf, Z., Fletcher, S., Dohler, M. ve Aghvami, H. (2018). Will SDN Be Part of 5G?. *IEEE Communications Surveys & Tutorials*, 20(4), 3220–3258.

68. Khan Tayyaba, S. ve Shah, M. A. (2017). 5G cellular network integration with SDN: Challenges, issues and beyond. In *2017 International Conference on Communication, Computing and Digital Systems (C-CODE), Islamabad, Pakistan*, 48–53.

69. Akyildiz, I. F., Wang, P. ve Lin, S.-C. (2015). SoftAir: A software defined networking architecture for 5G wireless systems. *Computer Networks*, 85, 1–18.

70. Guerzoni, R., Trivisonno, R. ve Soldani, D. (2014). SDN-based architecture and procedures for 5G networks. In *1st International Conference on 5G for Ubiquitous Connectivity, Levi, Finland,* 209–214.

71. Abdulghaffar, A., Mahmoud, A., Abu-Amara, M. ve Sheltami, T. (2021). Modeling and Evaluation of Software Defined Networking Based 5G Core Network Architecture. *IEEE Access*, 9, 10179–10198.

72. Kazmi, S. H. A., Qamar, F., Hassan, R., Nisar, K. ve Chowdhry, B. S. (2023). Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions. *Wireless Personal Communications*.

73. Yao, J., Han, Z., Sohail, M. ve Wang, L. (2019). A Robust Security Architecture for SDN-Based 5G Networks. *Future Internet*, 11(4):85, 1-14.

74. Gündüz, S. ve Sağıroğlu, Ş. (2022). SDN/NFV tabanlı 5G ağlarında enerji-etkin güvenlik yönetimi ve trafik yönlendirme için kontrolcü tasarımı ve değerlendirmesi. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 37(1), 1–16.

75. Yousaf, F. Z., Bredel, M., Schaller, S. ve Schneider, F. (2017). NFV and SDN—Key Technology Enablers for 5G Networks. *IEEE Journal on Selected Areas in Communications*, 35(11), 2468–2478.

76. Elbey, N. E., Ayad, S. ve Benhaya, B. (2022). Review on Reinforcement Learning-based approaches for Service Function Chain deployment in 5G networks. In *2022 2nd International Conference on New Technologies of Information and*

Communication (NTIC), Mila, Algeria, 1–8.

77. Farrel, A. (2018). Recent Developments in Service Function Chaining (SFC) and Network Slicing in Backhaul and Metro Networks in Support of 5G. In *2018 20th International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania,* 1–4.

78. Choyi, V. K., Abdel-Hamid, A., Shah, Y., Ferdi, S. ve Brusilovsky, A. (2016). Network slice selection, assignment and routing within 5G Networks. In *2016 IEEE Conference on Standards for Communications and Networking, Berlin, Germany (CSCN),* 1–7.

79. Bouras, C., Kollia, A. ve Papazois, A. (2017). SDN & NFV in 5G: Advancements and challenges. In *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France,* 107–111.

80. Ma, L., Wen, X., Wang, L., Lu, Z. ve Knopp, R. (2018). An SDN/NFV based framework for management and deployment of service based 5G core network. *China Communications*, 15(10), 86–98.

81. Liang, X. ve Qiu, X. (2016). A software defined security architecture for SDN-based 5G network. In *2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), Beijing, China,* 17–21.

82. Ji, X., Huang, K., Jin, L., Tang, H., Liu, C., Zhong, Z. ve Yi, M. (2018). Overview of 5G security technology. *Science China Information Sciences*, 61(8), 81301.

83. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. ve Gurtov, A. (2017). 5G security: Analysis of threats and solutions. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland,* 193–199.

84. Bouras, C., Kollia, A. ve Papazois, A. (2017). Teaching network security in mobile 5G using ONOS SDN controller. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), Milan, Italy,* 465–470.

85. Lal, S., Taleb, T. ve Dutta, A. (2017). NFV: Security Threats and Best Practices. *IEEE Communications Magazine*, 55(8), 211–217.

86. Alnaim, A. K., Alwakeel, A. M. ve Fernandez, E. B. (2022). Towards a Security Reference Architecture for NFV. *Sensors*, 22(10), 3750.

87. Bernardo, D. V. ve Chua, B. B. (2015). Introduction and Analysis of SDN and NFV Security Architecture (SN-SECA). In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications, Gwangju, South Korea,* 796–801.

88. Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A. ve Ylianttila, M. (2019). Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials*, 21(4), 3682–3722.

89. Ryu SDN Framework Community (2021). Ryu Controller, v4.34. URL: https://ryu-sdn.org, Son Erişim Tarihi: 20.04.2023

90. McCauley et al. (2015). POX controller, v0.7.0. URL: https://noxrepo.github.io/pox-doc/html/, Son Erişim Tarihi: 20.04.2023

91. OpenDaylight Project The Linux Foundation. (2016). OpenDaylight Controller, Beryllium release. URL: https://www.opendaylight.org, Son Erişim Tarihi: 20.04.2023.

92. Open Networking Foundation. (2021). ONOS Controller, v2.5.1. URL: https://opennetworking.org/onos/, Son Erişim Tarihi: 20.04.2023.

93. OpenNetworkingFoundation. (2012). ONF White Paper, Software-Defined Networking: The New Norm for Networks. URL: http://opennetworking.wpengine.com/wp-content/uploads/2011/09/wp-sdn-newnorm.pdf, Son Erişim Tarihi: 20.04.2023.

94. ETSI (2012). Network Functions Virtualisation An Introduction, Benefits, Enablers, Challenges & Call for Action. URL: https://portal.etsi.org/nfv/nfv_white_paper.pdf, Son Erişim Tarihi: 20.04.2023.

95. Paolucci, F. (2018). Network Service Chaining Using Segment Routing in Multi-Layer Networks. *Journal of Optical Communications and Networking*, 10, 582.

96. Raynovich, S. (2016). What Is Network Service Chaining? URL: https://www.sdxcentral.com/networking/sdn/definitions/whats-network-virtualization/what-is-network-service-chaining/, Son Erişim Tarihi: 20.04.2023.

97. John, W., Pentikousis, K., Agapiou, G., Jacob, E., Kind, M., Manzalini, A. ve Meirosu, C. (2013). Research Directions in Network Service Chaining. In *2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy*, 1–7.

98. Fang, D., Qian, Y. ve Hu, R. Q. (2018). Security for 5G Mobile Wireless Networks. *IEEE Access*, 6, 4850–4874.

99. Schneider, P. ve Horn, G. (2015). Towards 5G Security. In *2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland*, 1165–1170.

100. Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A. ve Zareei, M. (2022). Towards security automation in Software Defined Networks. *Computer Communications*, 183, 64–82.

101. Achleitner, S., La Porta, T., Jaeger, T. ve McDaniel, P. (2017). Adversarial network forensics in software defined networking. In *Proceedings of the Symposium on SDN Research (SOSR '17). Association for Computing Machinery, New York, NY, USA,* 8–20.

102. Revathi, M., Ramalingam, V. V. ve Amutha, B. (2022). A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework. *Wireless Personal Communications*, 127, 2417–2441.

103. DFWRS (2001). A Road Map for Digital Forensic Research. URL: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf,

Son Erişim Tarihi: 20.04.2023.

104. Bhatt, S., Manadhata, P. K. ve Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*, 12(5), 35–41.

105. Aydeger, A., Saputro, N. ve Akkaya, K. (2019). A moving target defense and network forensics framework for ISP networks using SDN and NFV. *Future Generation Computer Systems*, 94, 496–509.

106. Spiekermann, D. ve Eggendorfer, T. (2016). Towards Digital Investigation in Virtual Networks: A Study of Challenges and Open Problems. In *2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria*, 406–413.

107. Nieto, A. (2018). An Overview of Proactive Forensic Solutions and its Applicability to 5G. In *2018 IEEE 5G World Forum (5GWF), Silicon Valley, CA, USA*, 191–196.

108. Satrya, G. B. ve Shin, S. Y. (2017). Security enhancement to successive interference cancellation algorithm for non-orthogonal multiple access (NOMA). In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada*, 1–5.

109. Khan, H. ve Martin, K. M. (2020). A survey of subscription privacy on the 5G radio interface - The past, present and future. *Journal of Information Security and Applications*, 53, 102537.

110. Dutta, A., Hammad, E., Enright, M., Behmann, F., Chorti, A., Cheema, A. ve Kurt, G. K. (2022). Security and Privacy. In *2022 IEEE Future Networks World Forum (FNWF), Montreal, QC, Canada*, 1–71.

111. Sedaghat, S. (2020). The Forensics of DDoS Attacks in the Fifth Generation Mobile Networks Based on Software-Defined Networks. *International Journal of Network Security*, 22 (1), 41–53.

112. Muragaa, W. H., Seman, K. ve Marhusin, M. F. (2017). A POX Controller Module to Collect Web Traffic Statistics in SDN Environment. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 10(12), 2105–2110.

113. Balarezo, J. F., Wang, S., Chavez, K. G., Al-Hourani, A., Fu, J. ve Sithamparanathan, K. (2020). Low-rate TCP DDoS Attack Model in the Southbound Channel of Software Defined Networks. In *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), Adelaide, SA, Australia*, 1–10.

114. Khan, S., Gani, A., Wahab, A. W. A., Abdelaziz, A., Ko, K., Khan, M. K. ve Guizani, M. (2016). Software-Defined Network Forensics: Motivation, Potential Locations, Requirements, and Challenges. *IEEE Network*, 30(6), 6–13.

115. Khan, S., Gani, A., Wahab, A. W. A., Abdelaziz, A. ve Bagiwa, M. A. (2016). FML: A novel forensics management layer for software defined networks. In *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Noida, India*, 619–623.

116. Mugitama, S. A., Cahyani, N. D. W. ve Sukamo, P. (2020). An Evidence-Based Technical Process for OpenFlow-Based SDN Forensics. In *2020 8th International Conference on Information and Communication Technology (ICoICT), Yogyakarta, Indonesia*, 1–6.

117. Spiekermann, D., Keller, J. ve Eggendorfer, T. (2017). Network forensic investigation in OpenFlow networks with ForCon. *Digital Investigation*, 20, 66–74.

118. Wang, H., Yang, G., Chinprutthiwong, P., Xu, L., Zhang, Y. ve Gu, G. (2018). Towards fine-grained network security forensics and diagnosis in the SDN era. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18). Association for Computing Machinery, New York, NY, USA,* 3–16.

119. Zhang, S., Meng, X. ve Wang, L. (2016). SDNForensics: A Comprehensive Forensics Framework for Software Defined Network. In *Proceedings of the International Conference on Computer Networks and Communication Technology (CNCT 2016)*, 92–99.

120. Hussain, M., Shah, N., Amin, R., Alshamrani, S. S., Alotaibi, A. ve Raza, S. M. (2022). Software-Defined Networking: Categories, Analysis, and Future Directions. *Sensors*, 22(15), 1-47.

121. Mahamat, B. S. ve Çeken, C. (2019). Anomaly Detection in Software-Defined Networking Using Machine Learning. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 7(1), 748–756.

122. Xie, J., Guo, D., Hu, Z., Qu, T. ve Lv, P. (2015). Control plane of software defined networks: A survey. *Computer Communications*, 67, 1–10.

123. Gijrath, S. J. H. (2021). (Re-)defining software defined networks under the European electronic communications code. *Computer Law & Security Review*, 40, 105492.

124. Elektronik İmza Kanunu (2004). URL: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5070&MevzuatTur=1&MevzuatTertip=5, Son Erişim Tarihi: 20.04.2023.

125. Kişisel Verilerin Korunması Kanunu (2016). URL: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf, Son Erişim Tarihi: 20.04.2023.

126. Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik (2017). URL: https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, Son Erişim Tarihi: 20.04.2023.

127. Ujcich, B. E. ve Sanders, W. H. (2019). Data Protection Intents for Software-Defined Networking. In *2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France*, 271–275.

128. Çil, A. ve Demirci, M. (2023). Ağ Adli Bilişimi Süreç Gereksinimlerinin Belirlenmesi ve Yazılım Tanımlı Ağlarda İncelenmesi. *Politeknik Dergisi (erken görünüm)*, 1–1.

129. Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A. ve Ullah, F. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. *International Journal of Advanced Computer Science and Applications*, 12 (5), 879-887.

130. Mininet Project Contributors (2022). Mininet v2.3.0. URL: http://mininet.org/, Son Erişim Tarihi: 20.04.2023.

131. Ubuntu (2020). Ubuntu Desktop 20.04. URL: https://ubuntu.com/download/desktop, Son Erişim Tarihi: 20.04.2023.

132. Oracle (2022). VirtualBox v6.1. URL: https://www.virtualbox.org/, Son Erişim Tarihi: 20.04.2023.

133. Linux Foundation Collaborative Project (2016). OpenvSwitch v2.13.1. URL: https://www.openvswitch.org/, Son Erişim Tarihi: 20.04.2023.

134. Wireshark (2022). Wireshark v3.2.3. URL: https://www.wireshark.org/, Son Erişim Tarihi: 20.04.2023.

135. Kali linux tools (2021). Yersinia, v0.8.2. URL: https://tools.kali.org/vulnerability-analysis/yersinia, Son Erişim Tarihi: 20.04.2023.

136. Kali linux tools (2021). Nikto, v2.1.5. URL: https://tools.kali.org/information-gathering/nikto, Son Erişim Tarihi: 20.04.2023.

137. Iperf (2019). Iperf v2.0.13. URL: https://iperf.fr, Son Erişim Tarihi: 20.04.2023.

138. Nmap: Discover your network, v7.80. (2021). URL: https://nmap.org, Son Erişim Tarihi: 20.04.2023.

139. Hping3 (2021). Hping3 v3.0.0. URL: https://www.kali.org/tools/hping3/, Son Erişim Tarihi: 20.04.2023.

140. Çil, A. ve Demirci, M. (2024). A comparative analysis of software-defined network controllers in terms of network forensics processes and capabilities. *Sigma Journal of Engineering and Natural Sciences (ahead-of-print),* 42(3).

141. Durnagöl, Y. (2011). 5651 Sayılı kanun kapsamında internet aktörlerine getirilen yükümlülükler ile idari ve cezai yaptırımlar. *Türkiye Adalet Akademisi Dergisi*, 0(4), 375–416.

142. International Organization for Standardization (ISO). (2022). Developing standards. URL: https://www.iso.org/developing-standards.html, Son Erişim Tarihi: 20.04.2023.

143. Tatlıgil, İ. S. (2020). *ISO/IEC JTC 1/SC 27 "BT Güvenlik Teknikleri" Standardlarının Siber Güvenliğe Katkısı.* Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi / Fen Bilimleri Enstitüsü, İstanbul, 1–58.

144. International Organization for Standardization (ISO) (2022). ISO Members. URL: https://www.iso.org/members.html, Son Erişim Tarihi: 20.04.2023.

145. Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği (2014).

URL: https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19880&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5, Son Erişim Tarihi: 20.04.2023.

146. Batı Akdeniz İhracatçılar Birliği (2022). ISO/27001 Ek-A Maddeleri. URL: https://www.baib.gov.tr/files/downloads/PageFiles/9d398db4-4a83-41f5-9dc7-002fa6c5248f/Files/27001 ek-a maddeleri.pdf, Son Erişim Tarihi: 20.04.2023.

147. Türk Standartları Enstitüsü - TSE (2023). TS ISO/IEC 27001:2022 Standardı İçin Geçiş Şartları. URL: https://www.tse.org.tr/Icerik/DuyuruDetay?DuyuruID=6355, Son Erişim Tarihi: 20.04.2023.

148. 2019/12 nolu Cumhurbaşkanlığı Genelgesi (2019). Bilgi ve İletişim Güvenliği Tedbirleri. URL: https://www.resmigazete.gov.tr/eskiler/2019/07/20190706-10.pdf, Son Erişim Tarihi: 20.04.2023.

149. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik (2020). URL: https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm, Son Erişim Tarihi: 20.04.2023.

150. ENISA (2016). Forensic analysis Local Incident Response Handbook, Document for teachers. URL: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe1_forensic_analysis_i-handbook, Son Erişim Tarihi: 20.04.2023.

151. ENISA (2016). Forensic Analysis Webserver analysis Handbook, Document for teachers. URL: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe3_forensic_analysis_iii-handbook, Son Erişim Tarihi: 20.04.2023.

152. ENISA (2013). Digital forensics Handbook, Document for teachers. URL: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-handbook, Son Erişim Tarihi: 20.04.2023.

153. ENISA (2016). Forensic analysis Network Incident Response Handbook,Document for teachers. URL: https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe2_forensic_analysis_ii-handbook, Son Erişim Tarihi: 20.04.2023.

154. ENFSI (2022). Expert Working Groups. URL: https://enfsi.eu/about-enfsi/structure/working-groups, Son Erişim Tarihi: 20.04.2023.

155. Özkaya, Ö. ve Toprak, İ. (2022). Türkiye'de Güvenlik Faaliyetleri Kapsamında Kişisel Verilerin İşlenmesi. *MANAS Sosyal Araştırmalar Dergisi*, 11(3), 1291–1305.

156. Volarević, I., Tomić, M. ve Milohanić, L. (2022). Network forensics. In *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia,* 1025–1030.

157. Liyanage, M., Ahmad, I., Okwuibe, J., Ylianttila, M., Kabir, H., Llorente Santos, J. ve Oca, E. (2017). Enhancing Security of Software Defined Mobile Networks. *IEEE Access*, 5, 9422–9438.

158. Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D. ve Maglaris, V. (2014). Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. *Computer Networks*, 62, 122–136.

159. Boussif, M. (2022). On The Security of Advanced Encryption Standard (AES). In *2022 8th International Conference on Engineering, Applied Sciences, and Technology (ICEAST), Chiang Mai, Thailand*, 83–88.

160. Debnath, S., Chattopadhyay, A. ve Dutta, S. (2017). Brief review on journey of secured hash algorithms. In *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India*, 1–5.

161. Ölvecký, M. ve Gabriška, D. (2018). Wiping Techniques and Anti-Forensics Methods. In *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia,* 127–132.

162. Boite, J., Nardin, P.-A., Rebecchi, F., Bouet, M. ve Conan, V. (2017). Statesec: Stateful monitoring for DDoS protection in software defined networks. *2017 IEEE Conference on Network Softwarization (NetSoft), Bologna, Italy*, 1–9.

163. Erokhin, S., Petukhov, A. ve Pilyugin, P. (2019). Critical Information Infrastructures Monitoring Based on Software-Defined Networks. In *Proceedings of the 24th Conference of Open Innovations Association FRUCT (FRUCT'24). FRUCT Oy, Helsinki, Uusimaa, Finland*, 594–598.

164. Nougnanke, K. B., Bruyere, M. ve Labit, Y. (2020). Low-Overhead Near-Real-Time Flow Statistics Collection in SDN. In *2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium*, 155–159.

165. Hamad, D. J., Yalda, K. ve Okumuş, İ. T. (2015). Getting traffic statistics from network devices in an SDN environment using OpenFlow.

166. Tsai, P.-W., Tsai, C.-W., Hsu, C.-W. ve Yang, C.-S. (2018). Network Monitoring in Software-Defined Networking: A Review. *IEEE Systems Journal*, 12(4), 3958–3969.

167. Chowdhury, S., Bari, M. F., Ahmed, R. ve Boutaba, R. (2014). PayLess: A low cost network monitoring framework for Software Defined Networks. In *2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland*, 1–9.

168. Dauer, P., Khondoker, R., Marx, R. ve Bayarou, K. (2015). Security Analysis of Software Defined Networking Applications for Monitoring and Measurement: sFlow and BigTap. In *The 10th International Conference on Future Internet (CFI '15). Association for Computing Machinery, New York, USA*, 51–56.

169. Bhavsar, V., Sahrial, C. ve Goswami, B. (2021). Security and Performance Evaluation of Software Defined Network Controllers Against Distributed Denial of Service Attack. In *2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India*, 1–8.

170. Runze, C., Fangming, R., Yidan, L., Lan, Y., ve Yanli, C. (2021). A Simple DDoS Defense Method Based SDN. In *2021 IEEE 15th International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, China,* 88–92.

171. Mihai-Gabriel, I. ve Victor-Valeriu, P. (2014). Achieving DDoS resiliency in a software defined network by intelligent risk assessment based on neural networks and danger theory. In *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary,* 319–324.

172. Lu, Y. ve Wang, M. (2016). An Easy Defense Mechanism Against Botnet-based DDoS Flooding Attack Originated in SDN Environment Using sFlow. In *Proceedings of the 11th International Conference on Future Internet Technologies (CFI '16). Association for Computing Machinery, New York, USA,* 14–20.

173. Abou El Houda, Z., Khoukhi, L. ve Senhaji Hafid, A. (2020). Bringing Intelligence to Software Defined Networks: Mitigating DDoS Attacks. *IEEE Transactions on Network and Service Management*, 17(4), 2523–2535.

174. Tayfour, O. E. ve Marsono, M. N. (2020). Collaborative Detection and Mitigation of Distributed Denial-of-Service Attacks on Software-Defined Network. *Mobile Networks and Applications*, 25(4), 1338–1347.

175. Hu, D., Hong, P. ve Chen, Y. (2017). FADM: DDoS Flooding Attack Detection and Mitigation System in Software-Defined Networking. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore*, 1–7.

176. Girdler, T. ve Vassilakis, V. G. (2021). Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses. *Computers & Electrical Engineering*, 90, 106990.

177. Neykov, N. (2017). Real-time detection and mitigation of flood attacks in SDN networks.

178. Lawal, B. ve At, N. (2018). Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN). In *2018 26th Signal Processing and Communications Applications Conference (SIU), İzmir, Türkiye,* 1–4.

179. Inmon (2022). sflow-RT (Program). URL: https://sflow-rt.com/, Son Erişim Tarihi: 20.04.2023.

180. Ubuntu (2022). NTP Server. URL: https://ubuntu.com/server/docs/network-ntp, Son Erişim Tarihi: 20.04.2023.

181. Doi, Y. ve Toyama, M. (2019). ToT for CSV: accessing open data CSV files through SQL. In *Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services (iiWAS2019). Association for Computing Machinery, New York, USA,* 423–429.

182. Madani, A., Rezayi, S. ve Gharaee, H. (2011). Log management comprehensive architecture in Security Operation Center (SOC). In *2011 International Conference on Computational Aspects of Social Networks (CASoN), Salamanca, Spain*, 284–289.

183. Saavedra, M. Z. N. L. ve Yu, W. E. S. (2017). A Comparison between Text, Parquet, and PCAP Formats for Use in Distributed Network Flow Analysis on Hadoop. *Journal of Advances in Computer Networks*, 5(2), 59–64.

184. Debinski, M., Breitinger, F. ve Mohan, P. (2019). Timeline2GUI: A Log2Timeline CSV parser and training scenarios. *Digital Investigation*, 28, 34–43.

185. Ubuntu Manuals (2022). Sha3sum. URL: https://manpages.ubuntu.com/manpages/focal/man1/sha3sum.1p.html, Son Erişim Tarihi: 20.04.2023.

186. Ubuntu Manuals (2022). GPG Sign. URL: https://manpages.ubuntu.com/manpages/xenial/man1/gpg.1.html, Son Erişim Tarihi: 20.04.2023.

187. Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W. ve Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1), 56.

188. Chen, S. ve Towsley, D. (1996). A performance evaluation of RAID architectures. *IEEE Transactions on Computers*, 45(10), 1116–1130.

189. Seagate (2022). RAID Modes. URL: https://www.seagate.com/manuals/network-storage/business-storage-nas-os/raid-modes/, Son Erişim Tarihi: 20.04.2023.

190. Janani, A. K., Vetriselvi, V., Parthasarathi, R. ve Subrahmanya, V. R. G. (2019). An Approach to URL Filtering in SDN. In S. Smys, R. Bestak, J. I.-Z. Chen, & I. Kotuliak (Eds.), International Conference on Computer Networks and Communication Technologies, vol 15, Springer Singapore. 217–228.

191. Yürekten, Ö. ve Demirci, M. (2021). Citadel: Cyber threat intelligence assisted defense system for software-defined networks. *Computer Networks*, 191, 108013.

192. Ulusal Siber Olaylara Müdahale Merkezi - USOM (2023). Zararlı Bağlantılar. URL: https://www.usom.gov.tr/adres, Son Erişim Tarihi: 20.04.2023.

193. Read the Docs (2022). Built-in-Ryu Applications. URL: https://ryu.readthedocs.io/en/latest/app/ofctl_rest.html, Son Erişim Tarihi: 20.04.2023.

194. Vitak, J., Crouse, J. ve LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, 27(5), 1751–1759.

195. İşgüzar, S. ve Ayden, C. (2017). Siber Aylaklık Üzerine Değerlendirmeler: Toplu Bir Bakış. In *4th International Regional Development Conference, Tunceli, Türkiye,* 1–18.

196. Tok, M. S. ve Demirci, M. (2021). Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard. *Computers & Security*, 109, 102394.

197. İnternet: Superuser (2017). Why does the same data take more space in a text file than in an Excel file? URL: https://superuser.com/questions/1214933/why-does-the-same-

data-take-more-space-in-a-text-file-than-in-an-excel-file, Son Erişim Tarihi: 20.04.2023.

198. Agile IT (2022). Comparing File Sizes for Data Stored in CSV, Excel, JSON, and XML. URL: https://www.agileit.com/news/comparing-file-sizes-for-data-stored-in-csv-excel-json-and-xml/, Son Erişim Tarihi: 20.04.2023.

199. Adli Tıp Kurumu İhtisas Daireleri (2022). URL: https://www.atk.gov.tr/adli-tip-ihtisas-daireleri.html, Son Erişim Tarihi: 20.04.2023.

200. Özdem, M. ve Alkan, M. (2021). SDN Based Management Platform for Intranet Services. *Journal of Polytechnic*, 24(3), 989–995.

201. Awadh, K. ve Akbaş, A. (2021). Intrusion Detection Model Based on TF.IDF and C4.5 Algorithms. *Journal of Polytechnic*, 24(4), 1691–1698.

202. Utku, A. ve Akcayol, M. A. (2021). Derin Öğrenme Tabanlı Model ile Bir Olayın Sonraki Olma Zamanının Tahmini. *Politeknik Dergisi*, 24(1), 1–15.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: ÇİL, Altuğ
Uyruğu	:
Doğum tarihi ve yeri	:
Medeni hali	:
Telefon	:
e-mail	:

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Doktora	Gazi Üniversitesi / Bilişim Enstitüsü / Adli Bilişim Ana Bilim Dalı	Devam ediyor
Yüksek lisans	Gazi Üniversitesi / Fen Bilimleri Enstitüsü / Elektrik-Elektronik Mühendisliği	2014
Lisans	Gazi Üniversitesi / Mühendislik Fakültesi / Elektrik-Elektronik Mühendisliği	2010
Lise	Ankara Atatürk Lisesi	2005

İş Deneyimi

Yıl	Yer	Görev
2016-Halen	TÜBİTAK / ARDEB-EEEAG	Grup Koordinatörü
2011-2015	Meteoroloji Genel Müdürlüğü	Mühendis

Yabancı Dil

İngilizce

Yayınlar

1. Çil, A., & Demirci, M. (2024). A comparative analysis of software-defined network controllers in terms of network forensics processes and capabilities. *Sigma Journal of Engineering and Natural Sciences (ahead-of-print)*, 42(3).
2. Çil, A., & Demirci, M. (2023). Ağ Adli Bilişimi Süreç Gereksinimlerinin Belirlenmesi ve Yazılım Tanımlı Ağlarda İncelenmesi. *Politeknik Dergisi (erken görünüm)*, 1–1.



GAZİ GELECEKTİR…