ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DOKTORA TEZİ

KABLOSUZ YEREL ALAN AĞLARINDA SALDIRILARIN TESPİT EDİLMESİ VE ANALİZİ

Merve ÖZKAN OKAY

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2022

ÖZET

Doktora Tezi

KABLOSUZ YEREL ALAN AĞLARINDA SALDIRILARIN TESPİT EDİLMESİ VE ANALİZİ

Merve ÖZKAN OKAY

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Refik SAMET

Siber güvenlik, sosyal ağlar, online bankacılık, bulut, web, nesnelerin interneti, kablosuz ve mobil teknolojilerin hızlı gelişmesi ile birlikte önemli bir ihtiyacı karşılayan, büyük ilgi gören ve hızlı büyüyen bir araştırma alanı olmuştur. Kablosuz haberleşme teknolojisinin gelecekte de yaygın bir şekilde kullanılacağı göz önünde bulundurulduğunda son yıllarda araştırmacıların da bu alana ilgisi gittikçe artmaktadır. Kablosuz haberleşme teknolojilerinden en yaygın kullanılanı ise kablosuz yerel alan ağlarıdır ve bu yaygın kullanımın daha da artması beklenmektedir. Özellikle de bu artışın sebebi gelişen IoT teknolojisi ve bu teknolojinin beraberinde getirdiği akıllı ev, akıllı şehir gibi uygulamalarıdır. Ancak, kablosuz yerel alan ağ teknolojilerinin mevcut durumu, ağı pasif gizli dinlemeden aktif müdahaleye kadar değişen saldırılara karşı hassas kılmaktadır. Bir saldırganın ağ kablolarına fiziksel olarak erişmesi veya ağ geçitlerinde birkaç savunma hattından geçmesi gereken kablolu ağların aksine, kablosuz bir yerel alan ağına yapılacak saldırılar her yönden gelebilmekte ve herhangi bir düğümü hedefleyebilmektedir. Bütün bunlar kablosuz bir yerel alan ağının açık bir savunma hattına sahip olamayacağı ve her kullanıcının doğrudan veya dolaylı olarak bir saldırganla karşılaşmak için hazırlanması gerektiği anlamına gelmektedir. Bu nedenlerden dolayı saldırıları önceden tespit edebilen etkili bir saldırı tespit sistemi geliştirilmesi gerekmektedir.

Saldırı tespit sistemleri, bilgileri çalmak, sansürlemek veya ağ protokollerini bozmak gibi kötü niyetli girişimleri tespit etmek için bilgisayar ağını izleyen yazılımlardır. Günümüz saldırı tespit sistemlerinde kullanılan çoğu teknik, bilgisayar ağlarında siber saldırıların dinamik ve karmaşık doğası ile baş edememektedir. Bu saldırıların her gün daha da gelişmesinden dolayı, güncel olarak kullanılan ağ güvenliği sistemleri yetersiz kalmaktadır. Bu sebepler yeni saldırı tespit ve analiz yöntemlerinin geliştirilmesini zorunlu kılmaktadır. Bu tez çalışmasında, son teknolojik gelişmeler kullanılarak kablosuz yerel alan ağları için güvenlik problemlerinin çözümüne katkı sağlanması hedeflenmiştir ve bu kapsamda yeni bir saldırı tespit ve analiz yöntemi önerilmiştir. Tez çalışmasının 4 temel katkısı bulunmaktadır. 1. Saldırı tespit ve sınıflandırma metodolojisi (FSADM) önerilmiştir. 2. Saldırıların hızlı bir şekilde tespit edilebilmesi için öğrenme işleminin de temeli olan yeni özellik seçim yöntemi (FSAP) önerilmiştir. 3. Saldırıların yüksek doğrulukla sınıflandırılması için hibrid bir yöntem (SABADT) önerilmiştir. 4. Önerilen yöntemlerin performans değerlendirmelerini gerçekleştirebilmek için yeni veri seti oluşturulmuştur. Önerilen yöntemler hem geliştirilen veri seti hem de literatürdeki mevcut veri setleri üzerinde uygulanmıştır. Uygulama sonuçlarına göre saldırılar ve türleri %99.17 ile %99.81 arasında değişen doğruluk oranları ile tespit edilmiştir. Elde edilen sonuçlar literatürdeki diğer öncü yöntemler ile karşılaştırıldığında önerilen yöntem ile daha başarılı sonuçlar elde edildiği görülmüştür. Özetle, bu doktora tezi çalışmasında kablosuz yerel alan ağlarındaki trafik davranışları analiz edilerek, saldırılar yüksek doğruluk oranı ile tespit edilmiş ve sınıflandırılmıştır.

Nisan 2022, 160 sayfa

Anahtar Kelimeler: Siber güvenlik, saldırı tespit sistemleri, kablosuz yerel alan ağları, IEEE 802.11 standardı, saldırı tespiti ve analizi, makine öğrenmesi, veri madenciliği

ABSTRACT

PhD Thesis

INTRUSION DETECTION AND ANALYSIS IN WIRELESS LOCAL AREA NETWORKS

Merve ÖZKAN OKAY

Ankara University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Prof. Dr. Refik SAMET

Cyber security has become a rapidly growing research area that meets an important need with the development of social networks, online banking, cloud, web, internet of things, wireless and mobile technologies. Considering that wireless communication technology will be used more widely in the future, the interest of researchers in this field has been increasing. The most widely used wireless communication technologies are wireless local area networks and this usage is expected to increase even more. Especially, the reason for this increase is the developing IoT technology and its applications such as smart home and smart city. However, the current state of wireless local area networking technologies makes the network vulnerable to attacks ranging from passive eavesdropping to active intervention. Unlike wired networks, where an attacker must physically access network cables or pass through several lines of defense at gateways, attacks on a wireless local area network can come from all directions and target any node. All this means that the network cannot have a clear line of defense and every user must be prepared to encounter an attacker directly or indirectly. An effective intrusion detection systems are being developed against these attacks.

Intrusion detection systems are software that monitors computer networks for malicious activities, such as stealing information, censoring or breaking network protocols. Most techniques used in intrusion detection system cannot cope with the dynamic and complex structure of cyber attacks in computer networks. Due to the increasing of these malicious attacks day by day, currently used network security systems are insufficient. For these reasons, it has become necessary to develop new methods. In this thesis, it is aimed to contribute to the solution of security problems for wireless local area networks by using the latest technological developments and a new method is proposed in this context. The thesis work has four main contributions. 1. Intrusion detection and classification methodology is proposed. 2. A new feature selection method (FSAP), which is also the basis of the learning process, is proposed for rapid detection of attacks. 3. A hybrid method (SABADT) is proposed for classification of attacks with high accuracy. 4. A new data set has been developed in order to perform the performance evaluations of the proposed methods. The proposed methods were applied on both the developed dataset and the existing datasets in the literature. According to the results of the application, the attacks and their types were detected with accuracy rates varying between 99.17% and 99.81%. When the results obtained were compared with other pioneering methods in the literature, it was seen that more successful results were obtained with the proposed method. In summary, in this doctoral thesis, the traffic behavior in wireless local area networks was analyzed and attacks were detected and classified with high accuracy.

April 2022, 160 pages

Key Words: Cyber security, intrusion detection systems, wireless local area networks, IEEE 802.11 standard, intrusion detection and analysis, machine learning, data mining

TEŞEKKÜR

Tez çalışmamın her aşamasında bilgi ve deneyimleri ile bana yol gosteren, her durumda desteğini, yardımlarını esirgemeyen, sabrı ve motivasyonu ile her zaman yanımda olan danışman hocam Sayın Prof. Dr. Refik Samet'e,

Tez çalışmalarımı her basamağında inceleyerek değerli yorumları ile katkıda bulunan tez izleme komite hocalarım Sayın Prof.Dr. Suat Özdemir'e, Sayın Doç.Dr. Mehmet Serdar Güzel'e,

Akademik hayatım boyunca değerli fikirlerini benden esirgemeyen, motivasyon kaynağım olan ve her türlü zorlukta yanımda olan sevgili arkadaşlarım Sayın Fethiye Çalışkan'a, Sayın Yeliz Köşker'e, Sayın Dr. Öğretim Üyesi Yılmaz Ar'a, Sayın Dr. Pınar Küllü'ye ve Sayın Dr. Sevgi Yigit Sert'e,

Tez çalışmalarıma fikirleri, deneyimleri ile destek olan ve katkıda bulunan sayın Dr. Öğretim Üyesi Ömer Aslan'a,

Bu tez çalışmasını 2211-E Doğrudan Yurt İçi Doktora Bursu kapsamında destekleyen TÜBİTAK'a,

Hem akademik çalışmalarımda hem de hayatımın her anında yanımda olan, en büyük desteği gördüğüm sevgili eşim Rıza'ya, bu yolda maddi manevi desteklerini esirgemeyen anneme, babama, abime, yengeme, hayatımızın neşe kaynağı olan Alya'ya ve küçücük elleriyle hayatımıza dokunan, en güzel motivasyonum biricik kızım Ada'ya, Sonsuz teşekkürlerimi sunarım.

Merve ÖZKAN OKAY
Ankara, Nisan 2022

İÇİNDEKİLER

KISALTMALAR DİZİNİ

APT	Advanced Persistent Threats	Gelişmiş Kalıcı Tehditler
AWID	Aegean Wi-Fi Intrusion Dataset	Aegean Wi-Fi Saldırı Veri Kümesi
ANN	Artificial Neural Network	Yapay Sinir Ağı
ADFA	Australian Defence Force Academy	Avustralya Savunma Kuvvetleri Akademisi
BNID	Behavior Based Network Intrusion Detection	Davranış Tabanlı Ağ Saldırı Tespiti
CNN	Convolutional Neural Network	Evrişimsel Sinir Ağı
CPDT	Correlation Based Partial Decision Tree	Korelasyona Dayalı Kısmi Karar Ağacı
DM	Data Mining	Veri madenciliği
DTS	Decision Tree Splitting	Karar Ağacı Bölme
DL	Deep Learning	Derin Öğrenme
DNN	Deep Neural Network	Derin Sinir Ağı
DARPA	Defense Advanced Research Project Agency	Savunma İleri Araştırma Projesi Ajansı
DoS	Denial of Service	Hizmet Reddi
DHE	Discrete Hessian Eigenmap	Ayrık Hessian Eigenmap
DDoS	Distributed Denial of Service	Dağıtılmış Hizmet Reddi
DNS	Domain Name System	Alan Adı Sistemi
FFDNNs	Feed Forward Deep Neural Networks	İleri Beslemeli Derin Sinir Ağları
FTP	File Transfer Protocol	Dosya Aktarım Protokolü
GRUs	Gated Repetitive Units	Tekrarlayan Birimler
GST	Generalized Suffix Tree	Genelleştirilmiş Sonek Ağacı
HTTP	Hypertext Transfer Protocol	Üstmetin Transfer Protokolü
HTTPS	Hypertext Transfer Protocol Secure	Köprü Metni Aktarım Protokolü
HIDS	Host-based Intrusion Detection System	Bilgisayar Tabanlı Saldırı Tespit Sistemi
IP	Internet Protocol	İnternet protokolü
IDS	Intrusion Detection System	Saldırı Tespit Sistemi
IDPS	Intrusion Detection Prevention System	Saldırı Tespit Önleme Sistemi
KDD '99	Knowledge Discovery and Data	Bilgi Keşfi ve Veri Madenciliği

	Mining	
KNN	K-Nearest Neighbor	K-en Yakın Komşu
LSTM	Long Short-Term Memory	Uzun Kısa Süreli Bellek
ML	Machine Learning	Makine Öğrenme
MP	Meta Pagging	Meta Sayfalama
NB	Naive Bayes	Naive Bayes
NBC	Naive Bayes Classifier	Naive Bayes Sınıflandırıcısı
NIDS	Network-Based Intrusion Detection System	Ağ Tabanlı Saldırı Tespit Sistemi
NBA	Network Behavior Analysis	Ağ Davranışı Analizi
NN	Neural Network	Sinir Ağı
OSSEC	Open Source Security	Açık Kaynak Güvenliği
OS	Operating System	İşletim Sistemi
OpenWIPS-NG	Open Source Wireless IPS	Açık Kaynak Kablosuz IPS
PID	Pattern Based Intrusion Detection	Örüntü Tabanlı Saldırı Tespiti
RT	Random Tree	Rastgele Ağaç
REPT	Reduced Error Pruning tree	Azaltılmış Hata Budama Ağacı
R2L	Remote to Local	Uzaktan Yerele
SHH	Secure Shell	Güvenli Kabuk
SEM	Security Event Manager	Güvenlik Olay Yöneticisi
SSID	Service Set Identifier	Hizmet Kümesi Tanımlayıcısı
SNR	Signal to Noise Ratio	Sinyal Gürültü Oranı
SMTP	Simple Mail Transfer Protocol	Basit Posta Aktarım Protokolü
SNMP	Simple Network Management Protocol	Basit Ağ Yönetimi Protokolü
SBID	Statistical Based Intrusion Detection	İstatistiksel Tabanlı Saldırı Tespiti
SVM	Support Vector Machine	Destek Vektör Makinesi
TCP	Transmission Control Protocol	Geçiş Kontrol Protokolü
TVM	Tenant Virtual Machine	Kiracı Sanal Makinesi
UNSW	University of New South Wales	New South Wales Üniversitesi
UDP	User Datagram Protocol	Kullanıcı Datagram Protokolü
U2R	User to Root	Kullanıcıdan Çekirdeğe
WIDS	Wireless Intrusion Detection System	Kablosuz Saldırı Tespit Sistemi

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

1.1 Genel Bilgi

Teknolojinin ilerlemesi ile birlikte kablolar hayatımızın büyük bir bölümünden çıkmış, yerini kablosuz cihazlar ve ortamlara bırakmıştır (Deniz ve Samet 2018). Kablosuz ağ teknolojisinin popülerliği ve hızla ilerlemesi günlük yaşamımızı kolaylaştırmıştır. Kablosuz teknolojiler arasında en çok tercih edileni ise WLAN'lardır. WLAN'ların son zamanlarda kullanımı ise özellikle nesnelerin interneti teknolojilerinin (IoT) hayatımızın her alanında karşımıza çıkıyor olmasıdır. Ancak bu hayatımızı kolaylaştıran gelişmelerin yanında güvenlik sorunları da beraberinde gelmiştir (Ethala 2013, Afzal 2016, Chaabouni vd. 2019). Cybersecurity Ventures'ın araştırmalarına göre siber güvenlik alanında 2017-2021 yılları arasında yapılan küresel harcama tutarı 1 trilyon dolara ulaşmış ve siber güvenlik harcamalarının her yıl ortalama yüzde 12-15 seviyesinde artış kaydetmesi beklenmektedir. 2021 yılında ise siber güvenlik suçlarının dünya ekonomisine toplam maliyeti yaklaşık 6 trilyon dolarlık zarara neden olmuştur. Bu sebeplerden dolayı, araştırmacılar arasında ağa izinsiz giriş tespiti sistemlerine ilgi artmıştır (Ozkan-Okay vd. 2021). Saldırı Tespit Sistemleri (IDS'ler), kablosuz ağlarda hem iç hem de dış saldırganlar tarafından gerçekleştirilen hem bilinen hem de bilinmeyen saldırıların tespitinde yaygın olarak kullanılmaktadır. Ek olarak, WLAN için güvenlik standartları hala net olarak ortaya koyulamamıştır. Koruma için kablosuz sensör, Ad-Hoc, MANET gibi benzer kablosuz ağların IDS'leri kabul edilebilirdir, ancak en iyi performansı garanti edememektedir (Ganesh vd. 2017, IEEE Standard 2014).

1.2 Tezde Ele Alınan Araştırma Soruları

Bu çalışmanın amacı kablosuz yerel alan ağlarını hedef alan mevcut ve daha önce görülmemiş saldırıları analiz ve tespit etmektir. Sistemdeki var olan IDS'ler, tespit ederken, ağın gösterdiği davranışları arka planda izleyerek tanıma işlemi yapmaktadır. Bu çalışmanın amacı kablosuz yerel alan ağı IDS problemini olabildiğince farklı açılardan ele alarak yapılan saldırıları azaltmaya çalışmaktır.

WLAN Saldırı Analizi ve Tespiti sırasındaki hedeflerimiz, aşağıdaki araştırma sorularının cevaplarına en verimli ve doğru şekilde ulaşmaktır.

(1) Teorik olarak bütün WLAN saldırılarını tespit etmek mümkün görünmese de pratik olarak tespit etmek ne kadar mümkün?

(2) Saldırıların göstermiş olduğu davranışlar, problemin çözümünde ne kadar etkili olmaktadır?

(3) Var olan ağ saldırılarının davranışları modellenerek, daha sonraki yıllarda ortaya çıkabilecek ağ saldırıları tespit edilebilir mi?

(4) Saldırı kodlarında bazı değişiklikler yapılınca, belirlenmiş olan davranış özellikleri kullanılarak aynı saldırının farklı türevlerini tespit etmek mümkün mü?

(5) Özellikleri belirlenen saldırıların bütün özellikleri değil de belirli özelliklerin kullanılması tespit oranını ve hızını ne derece artırabilir?

(6) Makine öğrenmesi ve veri madenciliği algoritmalarının WLAN saldırılarının tespitinde sınırları ve başarı oranları nedir?

(7) Yakalanmamak için çeşitli teknikler kullanan (gizlenme, şifreleme, vb.) saldırı örnekleri normal davranış modellemesi ile tespit edilebilir mi?

(8) Anomali tabanlı sistemin tespit etme oranı imza tabanlı tanıma yöntemiyle birleştirildiğinde tespit etme oranı artırılabilir mi?

1.3 Tezin Amacı ve Önemi

Kablosuz yerel alan ağlarına olan yoğun ilgiden dolayı, bu ağlara yönelik saldırı türlerinin araştırmaları ve saldırı tespit sistemi çalışmaları da beraberinde artmıştır (Mitchell ve Chen 2014, Pottei ve Parati 2017). Ancak bu çalışmaların hızıyla orantılı olarak saldırıların yoğunlukları da, türleri de aynı hızda artmaktadır (Aslan vd. 2021, Aslan ve Samet 2020). Bu yüzden mevcut saldırı tespit sistemleri bu gelişen dinamik yapıyla yüksek oranda baş edememektedir. Bu tez çalışmasında, ağa yapılan saldırıları ve türlerini yüksek doğruluk oranı ile tespit ederek, saldırı tespit sistemlerin doğruluk oranına katkı yapmak ilk amaçtır. Bunun yanında sadece mevcut saldırı türlerinin değil ağ üzerinden gelen farklı saldırı türlerinin de dinamik olarak belirlenmesi hedeflenmektedir. Bu eksikliklere katkı yapabilecek, WLAN'lara yönelik gittikçe artan

tehdit bilgilerini tanımlayabilen ve raporlayan bir sistem, kablosuz yerel alan ağlarının güvenliğini büyük ölçüde artırabilir ve literatüre büyük katkı sağlayabilir.

1.4 Tezin Katkısı

Saldırı türlerinin her gün daha da çeşitlenmesi ve halen WLAN'lar için başarılı bir şekilde geliştirilmiş, bilinmeyen saldırı türlerini de dinamik bir şekilde, yüksek doğruluk ile tespit edebilen net bir saldırı tespit sisteminin olmaması bu alanda büyük bir eksikliğe sebep olmaktadır. Tez kapsamında yapılan çalışmada bu eksiklikler göz önünde bulundurularak gerekli katkılar yapılmıştır ve WLAN'lara yönelik saldırıların tespit ve doğruluk oranı büyük bir oranda arttırılmıştır. Tez çalışmasının temel katkıları, saldırı tespit ve sınıflandırma için FSADM metodolojisi, saldırıların hızlı bir şekilde tespit edilebilmesi için katkı sağlayan FSAP özellik seçim yöntemi, saldırıların yüksek doğrulukla sınıflandırılması için hibrid SABADT yöntemi, önerilen yöntemlerin performans değerlendirmeleri için geliştirilen yeni veri setidir. Tez kapsamında yapılan katkıların detaylı açıklaması ise şöyle sıralanabilir:

1.Detaylı literatür taraması: WLAN'lara yönelik IDS problemlerinin çözümüne katkı sağlayacak çalışmalara geçmeden önce problemlerin zorluğunu ve sınırlarını belirlemek, daha önce yapılmış çalışmaların ne derece başarılı olup olmadığını görmek ve bu çalışmaları değerlendirerek daha iyi çalışan bir model öne sürebilmek için detaylı bir literatür taraması yapılmıştır. Bu kapsamda, öncelikle bu sistemlerin ne olduğu hakkında bilgilerden ve genel olarak bir IDS'de olması gereken temel özelliklerden bahsedilmiştir. Daha sonra IDS'ler ağ trafiğini izleme, akış verilerini kaydetme, saldırıları tespit etme ve uyarıları raporlama biçimlerine göre kategorilere ayrılmıştır. Bu kapsamdaki tüm IDS teknolojileri, metodolojileri ve yaklaşımları detaylı olarak incelenmiştir. Güçlü ve zayıf yönlerinden bahsedilmiş ve her alanda yapılan çalışmaların kapsamlı bir özeti verilmiştir. Aynı zamanda geliştirilen saldırı tespit sistemlerinin test ve değerlendirme aşamasında yaygın olarak kullanılan veri setleri incelenmiş ve bu veri setleri hakkında detaylı bilgi verilmiştir. Son olarak kişi, kurum ve kuruluşların saldırıları tespit etmek için kullandıkları yaygın saldırı tespit araçlarından bahsedilmiştir. Saldırı tespit araçlarının her birinin kullandığı saldırı tespit yöntemleri, avantajları ve dezavantajları gözden geçirilmiştir.

2. Önerilen FSADM (Feature Selection and Attack Detection Methodology) metodolojisi: WLAN'larda saldırılarının dinamik olarak hızlı ve yüksek doğruluk oranında elde edilebilmesi için FSADM metodolojisi önerilmiştir. Önerilen metodolojide veri analizi, özellik seçimi ve saldırı tespiti işlemleri yapılmıştır. Öncelikle özellik seçimi ve saldırı tespiti için algoritmalar geliştirilirken kullanılacak yöntemlerin belirlenmesi için literatürdeki öncü veri setleri incelenmiştir ve bunların analizi yapılmıştır. Sonrasında bir öğrenme modelinin temel basamağı olan özellik seçimi kapsamında yeni bir yaklaşım (FSAP) sunulmuştur ve bu yaklaşım ile önemli olan özelliklerin seçimi yapılmıştır. Saldırılar yüksek doğruluk oranı ile dinamik olarak tespit edilebilmesi için ise imza tabanlı ve anomali tabanlı yöntemlerinin birleşimi olan (SABADT) hibrid bir model sunulmuştur. Seçilen özelliklerden, literatürde veri setlerinde kullanılan temel özellikler (bilinen veri setlerinde ve araştırmalar kapsamında geliştirilen veri setlerinde ortak olan temel özellikler) ile veriler analiz edilerek kurallar (imzalar) çıkarılmıştır. Temel özellikler dışında kalan, veri setlerine ait özellikler (içerik özellikleri, zamana bağlı özellikler, ek özellikler) kullanılarak ağda görülen davranışlar belirlenmiş, bu davranışlara göre belli kurallar oluşturulmuştur. Önerilen bu yöntemin mevcut IDS'lere eklenmesi saldırıların tespit edilmesinde büyük bir başarı sağlayacaktır.

3. FSAP (Feature Selection Approach) yaklaşımı: Özellik seçimi, makine öğrenmesi modelinin oluşturulmasının en önemli adımlarından biridir. Bu önemli adıma katkı sağlayabilecek, doğru özelliklerin seçimi için FSAP yaklaşımı sunulmuştur. Bu yaklaşım iki aşamadan oluşmaktadır. Öncelikle her bir özellik, karşılık geldiği trafik durumuna (normal/atak) göre gruplandırılmaktır. Gruplama sonucunda çıkan rakamlar kullanılarak bir eşik değeri belirlenmektedir. Bu eşitlik sonucunda eşik değerinin altında kalan özelliklerin önemi düşüktür ve elenmektedir. İkinci aşamada kalan özelliklerin oluşturduğu grupların detaylı analizi yapılmaktadır. Bir özelliğin oluşturduğu gruptaki veri sayısı, eşik değerinin üzerinde olabilir ancak içeriği analiz edildiğinde belirleyiciliği yüksek bir özellik olmayabilir. Bu durumun da önüne geçebilmek için bir algoritma geliştirilmiştir ve bu kapsamda bazı parametreler belirlenmiştir. Bunlar; grubun içerisindeki farklı veri sayısı, grubun veri sayısının sonuç üzerindeki dağılımı, özelliklere göre normal ve atak durumlarının sahip olduğu min,

max ve ortalama gibi değerlerdir. Bu parametrelerin sonucunu sağlayan özellikler ikinci kez elemeden geçirilerek seçilen özellikler listesine eklenmektedir.

4. SABADT (Signature and Anomaly Based Technique) tekniği: Önerilen bu teknik imza ve anomali tabanlı modeli bir arada sunan hibrid bir saldırı tespit eden ve saldırı türünü belirleyen tekniktir. SABADT tekniğinin ilk aşaması imza tabanlı modeldir. Bu modelde öncelikle literatürde bilinen saldırı türlerinin davranışları da (imzaları) göz önünde bulundurulmuştur. Bunların kuralları kaydedilmiştir. Sonrasında hemen hemen her veri setinde ortak olan temel özelliklerden yola çıkılarak kurallar belirlenmiştir. Doğrudan sonuca ulaşılabilen durumlar var ise kurallar çıkarılarak imza listesine eklenmiştir. Modelin ikinci aşamasında veri setinin içerik özellikleri, zamana bağlı trafik özellikleri ve veri setine göre olan ek özellikler kullanılarak trafik davranış analizi yapılmıştır ve kurallar çıkarılmıştır. Anomali tabanlı model sayesinde bilinen saldırılar dışında saldırılar da tespit edilebilmektedir. Anomali tabanlı model oluşturulurken her özellik grubu önce kendi arasında analiz edilmiştir. Sonrasında bütün özellikler beraber analiz edilerek kurallar çıkarılmıştır.

5. Tez kapsamında özgün veri seti oluşturulması: Önerilen modelin uygulanması, test edilmesi ve performans değerlendirmesi için literatürde bilinen veri setleri kullanılmıştır. Ancak bu bilinen veri setleri doğrudan WLAN'lar için oluşturulmuş veri seti olmadığı gibi içerisinde güncel saldırıları da barındıran veri setleri değildir. Bu sebeple tez kapsamında bir WLAN topolojisi oluşturulmuştur. Topolojide bir kurban seçilmiştir ve bu ağ içerisinde özellikle WLAN'lara yönelik yapılan saldırı türleri çoğunlukta olmak üzere çeşitli saldırılar düzenlenmiştir. Düzenlenen bu saldırılar ve normal ağ trafiği kurban bilgisayar üzerine kurulan izleme programı ile kaydedilmiştir. Kaydedilen veriler belirli ön işlemlerden geçirilerek anlamlı bir veri seti haline getirilmiştir.

6. Yeni sonuçların elde edilmesi ve değerlendirme: Bu kapsamda, önerilen yöntemin performansını değerlendirmek amacıyla fazla miktarda veri içeren KDD'99 veri seti, güncel bir veri seti olan UNSW-NB15 ve tez çalışması kapsamında oluşturulan veri seti kullanılmıştır. Veri setleri üzerinde literatürde en çok uygulanan standart makine

öğrenmesi teknikleri (destek vektör makineleri, naive bayes, karar ağaçları, karar tabloları) uygulanmıştır ve sonuçlar hem kendi içerisinde hem de literatürdeki geliştirilen yöntemler ile karşılaştırılmıştır. Önerilen yöntem ve oluşturulan modelin veri setlerine uygulanması ile sırasıyla KDD'99 veri setinde %99.81, UNSW-NB15 veri setinde %99.17 ve tez kapsamında oluşturulan veri setinde %99.79 doğruluk oranları elde edilmiştir.

1.5 Tezin Yapısı

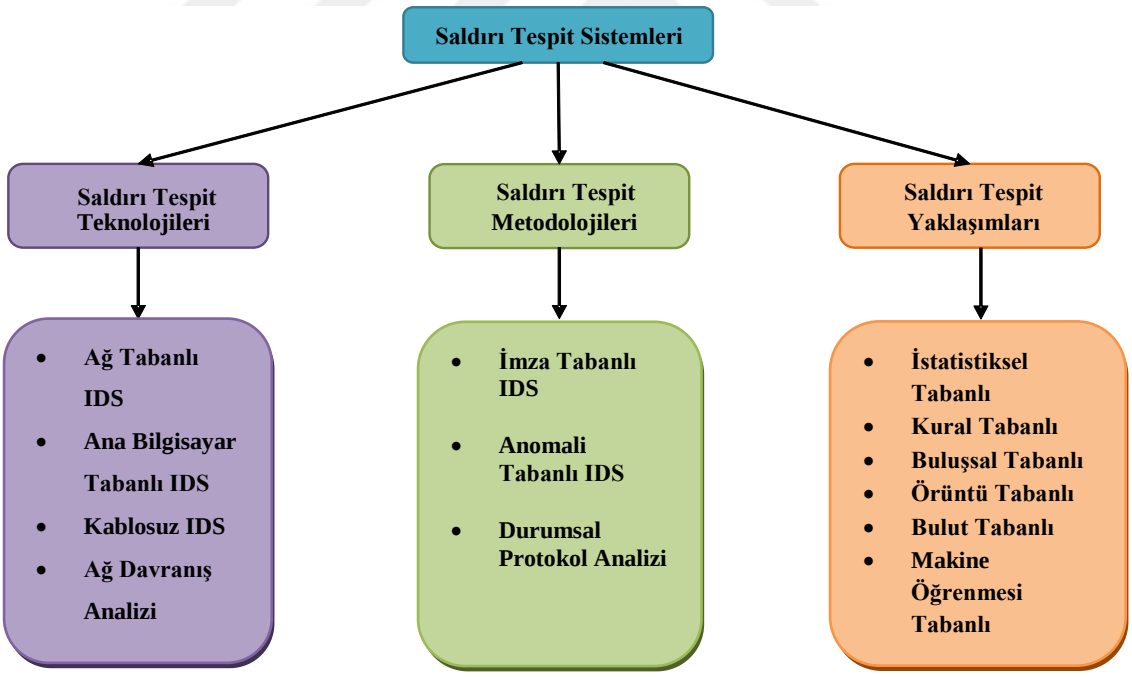
Çalışmanın geri kalan kısmı şu şekilde organize edilmiştir. Bölüm 2'de literatür çalışması kapsamında incelenmiş saldırı tespit sistemlerinin temel kavramları, saldırı tespit teknolojileri, metodolojileri ve yaklaşımları verilmiştir. Saldırı tespit sistemlerinde kullanılan veri setleri açıklanmıştır. Ek olarak, yaygın kullanılan saldırı tespit araçları incelenmiş, avantaj ve dezavantajlarından bahsedilmiştir. Bölüm 3'de WLAN'lara yönelik saldırılar, saldırıların yapılma şekilleri, saldırı imzaları açıklanmıştır ve WLAN'larda saldırı tespit sistemleri incelenmiştir. Bölüm 4'te tez çalışması kapsamında geliştirilen yöntem detaylarıyla açıklanmış ve veri seti oluşturma süreci bütün aşamaları ile birlikte anlatılmıştır. Bölüm 5'te tez çalışması kapsamında geliştirilen yöntemin farklı veri setleri üzerinde uygulanması ve sonuçları verilmiştir. Bölüm 6'da önerilen model ve yöntemlerin sonuçları mevcut öncü yöntemlerle karşılaştırılarak tartışılmıştır. Bölüm 7'de tez çalışmasının sonuçları ve öneriler sıralanmıştır.

2. SALDIRI TESPİT SİSTEMLERİNİN İNCELENMESİ

2.1 Saldırı Tespit Sistemleri Tanımı ve Sınıflandırılması

Saldırı tespiti, bir bilgisayar sisteminde veya ağında meydana gelen olayları izleme ve bu olayları güvenlik uygulamalarının ihlalleri veya yakın tehditleri gibi olası durumları analiz etme ve uyarma işlemidir. Saldırı tespit sistemleri (IDS) öncelikle olası olayları belirlemeye, onlar hakkında bilgi kaydetmeye ve kullanıcılara bildirmeye odaklanır. Ayrıca, kuruluşlar IDS'leri güvenlik politikalarıyla ilgili problemleri tespit etmek, mevcut tehditleri belgelemek ve kişileri güvenlik politikalarını ihlal etmekten alıkoymak gibi başka amaçlar için de kullanırlar.

IDS teknolojilerinin türleri, temel olarak izledikleri olay türleri ve dağıtım şekilleri ile sınıflandırılır (Scarfone ve Mell 2007). Şekil 2.1'de saldırı tespit sistemlerinin sınıflandırılması verilmiştir.



Şekil 2.1 Saldırı tespit sistemlerinin sınıflandırılması

Genel olarak, verimli bir IDS için dikkate alınması gereken bazı önemli kurallar vardır ve bu kurallar aşağıda sıralanmıştır.

- ✓ **IDS bileşenleri uygun şekilde güvence altına alınmalıdır.**

  Bir IDS, kullanıcılar, sensörler, veritabanı sunucuları, yönetim sunucuları ve ağlar dahil olmak üzere çeşitli bileşenlerden oluşur. IDS bileşenlerinin güvenliğini sağlamak çok önemlidir çünkü bu bileşenler, sistemlerin saldırıları tespit etmesini engellemek veya hassas bilgilere erişmek isteyen saldırganlar tarafından doğrudan hedef alınır. Tüm bileşenlerin işletim sistemleri ve uygulamaları güncel olmalı ve yazılım tabanlı tüm IDS bileşenleri tehditlere karşı korunmalıdır.

- ✓ **Saldırıların kapsamlı ve yüksek doğrulukta tespiti için birden fazla IDS teknolojisini kullanmak gerekebilir.**

  Ağ tabanlı, kablosuz ve ana bilgisayar tabanlı gibi kullanılan çeşitli IDS teknolojileri vardır. Her biri temelde farklı bilgi toplama, kaydetme, algılama ve önleme yetenekleri sunar. Ayrıca, her bir teknoloji, belirli olayları daha verimli bir şekilde tespit etme veya daha yüksek doğrulukla tespit etme gibi avantajlar sunar. Örneğin, verimli bir çözüm sağlamak için ana bilgisayar tabanlı ve ağ tabanlı IDS'ler entegre edilebilir. Yani IDS teknolojileri seçilirken her bir teknolojinin farklı özellikleri ve avantajları göz önünde bulundurulmalıdır. Literatürdeki saldırı tespit sistemlerinin en yaygın teknolojileri, yaklaşımları ve metodolojileri Şekil 2.1'de verilmiştir.

- ✓ **IDS'leri değerlendirmeden önce, karşılaması gereken gereksinimler net olarak tanımlanmalıdır.**

  IDS seçilirken, ortamın sistem ve ağ özelliklerinin iyi şekilde anlaşılması gerekmektedir; böylece sistemler veya ağlardaki ilgi olaylarını izleyebilecek uyumlu bir IDS seçilebilir. Ayrıca, bilgi toplama, kaydetme ve tespit etme dahil olmak üzere güvenlik yetenekleri, kapasite ve performans özellikleri, yaşam döngüsü maliyetleri gibi özellikleri göz önünde bulundurulmalıdır.

Özetle IDS'ler, teknoloji ve bilgi sistemlerine olan bağımlılığın artması, saldırıların yaygınlaşması ve potansiyel olarak zarar verici etkileri nedeniyle hemen hemen her kişi, kurum ve kuruluşun güvenliği için gerekli bir sistem haline gelmiştir. Etkili bir güvenlik

sistemi için WLAN'lara yönelik IDS'lerde dahil olmak üzere kablolu veya kablosuz bütün ağlarda kullanılacak IDS'lerde bahsedilen temel özelliklere sahip olmalıdır.

2.1.1 Saldırı tespit ilkeleri

Saldırı tespiti, bir bilgisayar sisteminde veya ağda meydana gelen olayları gözlemleme ve izinsiz girişleri belirlemek için bu olayları analiz etme işlemidir. Kötü amaçlı yazılım, DoS-DDoS saldırıları, yetkisiz erişim, ayrıcalıkların elde edilmesi gibi çeşitli saldırı türleri vardır. Bunlar gibi sistemde zararlı olarak görünen birçok olay aslında saldırı olsa da bazı istisnalar vardır; örneğin kullanıcı bilgisayarın adresini yanlış yazabilir veya bilmeden yanlış sisteme bağlanabilir. Bu yüzden sistem, izinsiz girişleri normal ağ trafiğinden doğru şekilde ayırmalıdır. Sonuç olarak, bir IDS, saldırıları tespit etme sürecini basitleştiren ve otomatikleştiren bir yazılımdır.

IDS teknolojilerini uygularken etkili bir saldırı çözümü için bazı önemli faktörler vardır:
• Sistem dayanıklılığı/güvenilirliği;
• Hızlı tespit;
• Minimum yanlış pozitif;
• Maksimum doğruluk oranı;
• Minimum yazılım/donanım kullanımı;
• İzinsiz girişin yerini doğru bir şekilde tespit etme yeteneği;
• Diğer teknolojilerle çalışabilme.

Özetle, bir IDS, saldırıları tespit etme sürecini basitleştiren ve otomatikleştiren bir yazılımdır. Saldırıların yüksek doğruluk ve zamanında tespiti için yukarıda belirtilen özellikleri sağlamalıdır.

2.1.2 IDS teknolojilerinin temel işlevleri

Öncelikle tanıyabilecekleri saldırı türlerine ve saldırıları tespit etmek için kullandıkları yönteme göre birçok farklı IDS teknolojisi bulunmaktadır. İstenmeyen olayları tespit

etmek için olayları gözlemleme ve analiz etme yeteneğine ek olarak, tüm IDS türleri aşağıda belirtilen işlevleri sağlamalıdır.

Bilgilerin kaydedilmesi: Bilgiler genellikle karşılaştırma için veya normal olarak ayarlanmış profiller oluşturmak için yerel olarak kaydedilir. Ayrıca kaydedilen bilgiler, merkezi kayıt sunucularına, bilgi güvenliği çözümlerine ve yönetim sistemlerine ayrı ayrı gönderilir.

Önemli olayların tespit edilmesi: Düzenli olarak kayıt altına alınan ve normal olarak görülen bilgilerin dışında oluşan bir durumun hızlı ve doğru bir şekilde tespit edilmesi gerekmektedir.

Tespit edilen önemli olayların bildirilmesi: Uyarı adı verilen bu bildirimler, sistemin kullanıcı arayüzünde e-posta, mesaj gibi çeşitli yöntemlerle gerçekleştirilir. Bir mesaj genellikle meydana gelen şüpheli olaylarla ilgili temel bilgileri içerir. Sistem kullanıcılarının daha fazla bilgi edinmek için IDS'ye erişmesi gerekir.

Rapor oluşturma: Oluşturulan sistem raporları, gözlemlenen olayları özetler veya dikkate değer olaylar hakkında ayrıntılı bilgi sağlar. Örneğin, oturumda şüpheli etkinlik tespit edilirse, IDS daha ayrıntılı bilgi toplayabilir. Ayrıca, bir tehdit algılandıktan sonra uyarıların ne zaman verilmesi gerektiği gibi ayarları değiştirebilir.

IDS teknolojilerinin ortak bir özelliği de, tam olarak doğru bir algılama sağlayamıyor olmalarıdır. IDS, normal bir aktiviteyi kötü niyetli olarak tanımladığında, yanlış bir pozitif meydana gelir. Bir IDS kötü niyetli aktiviteyi tespit edemediğinde ise, yanlış bir negatif meydana gelir. Tüm yanlış pozitifleri ve negatifleri ortadan kaldırmak mümkün değildir; Çoğu durumda, birinin oluşumunu azaltmak diğerinin oluşumunu arttırır. Geliştirilen birçok IDS, yanlış pozitifleri artırma pahasına yanlış negatifleri azaltmayı tercih etmektedir.

2.1.3 Saldırı tespit sistemlerindeki eksiklikler

Saldırı tespit sistemleri, bilgisayar sistemlerini ve ağ trafiğini izleyen, bu bilgileri dış saldırıları, sistem ihlallerini veya iç saldırıları belirlemek için kullanan güvenlik sistemleri olarak tanımlanabilir (Moustafa ve Slay 2016, Aslan vd. 2021). Günümüzde IDS'ler kurumsal sistemlerde kullanılması gereken temel güvenlik ürünlerinden biri olarak görülmektedir. IDS'ler, diğer güvenlik ürünleriyle birlikte kullanıldığında katmanlı bir güvenlik mimarisi olarak kullanılabilir. Örneğin, birçok kurum güvenlik duvarları ve antivirüs yazılımları ile birlikte IDS'leri kullanır. Bu şekilde, IDS'ler diğer güvenlik ürünlerinin tespit edemediği saldırıları tespit etmek için kullanılabilir. Ek olarak, WLAN için güvenlik standartları hala net olarak ortaya koyulamamıştır ve WLAN'lara özgü bir saldırı tespit sistemi bulunmamaktadır. WLAN'lara da koruma sağlanması için kablosuz sensör, Ad-Hoc, MANET gibi benzer kablosuz ağların IDS'leri kabul edilebilirdir, ancak bu sistemlerde iyi ve güvenilir bir performansı garanti edememektedir.

IDS'ler saldırıları farklı yöntem ve tekniklerle tespit eder. Sistem çağrılarından anomali tespiti çalışmaları uzun yıllardır devam etmektedir. Bununla birlikte, evrensel veri kümeleri üretmek için bu alanda birçok çalışma yapılmış olmasına rağmen, teorik olarak tüm normal davranışları modellemesi gereken veri kümelerinde hala eksiklikler bulunmaktadır. Aynı zamanda anomali temelli yaklaşımlar bilinen saldırıların yanı sıra bilinmeyen saldırıları da bir ölçüde tespit edebilirken, normal davranışları da saldırı olarak tanımlayabilmektedir. Son kullanıcılar veya sistem yöneticileri, IDS tarafından saldırı olarak algılanan davranışı incelemelidir. Böylece anomali tespit sistemleri aracılığıyla tespit edilen ve analizler sonucunda saldırı olduğu belirlenen uygulama için doğru imzanın çıkarılması mümkün olmaktadır. İmza tabanlı sistemler ise imzaları ile saldırıları doğrudan tespit edebilir, ancak bilinmeyen saldırıları tespit edemezler. Makine öğrenmesi teknikleri ise, son zamanlarda saldırı tespiti alanında yaygın olarak kullanılmaktadır. Örüntü tanıma, görüntü işleme, siber güvenlik ve özellikle saldırı tespiti alanında çok çeşitli sorunların çözümünde etkili olduğu kanıtlanmış birçok sınıflandırma tekniği bulunmaktadır. Ancak, ML teknikleri, belirli bir ağ trafiği için normal veya anormal gibi iki olası sonuç arasında tahmin yapmak için daha

kullanışlıdır. Özetle, mevcut IDS'lerin her birine ait avantajları olsa da şu anda gelişen saldırı türlerinin dinamik doğasıyla baş edememektedirler (Ring vd. 2019, Cordero vd. 2021, Singhrova 2011, Thanthrige vd. 2016, Manzoor and Kumar 2017, Usha ve Kavitha 2017, Primartha ve Tama 2017).

Bu araştırma alanlarında yapılacak çalışmalarda literatüre katkı sağlayacak yeni yöntemlerin geliştirilmesine, yeni veri setlerinin oluşturulmasına ve yeni teknolojilerin uygulanmasına yer verilmelidir. Diğer bir konu ise, IDS türlerinin güçlü yönlerini birleştirerek birbirlerinin zayıf yönlerini kapsayacak şekilde hibrit IDS'lerin oluşturulması ve bu sistemlerin gerçek ortamlarda kullanılması gerektiğidir. Bu çalışmada geliştirilebilecek yeni teknolojilere katkı sağlamak amacıyla IDS türleri, güçlü yönleri ve eksiklikleri için detaylı IDS incelemesi ve analizi yapılmıştır.

2.2 Saldırı Tespit Teknolojileri

Birçok IDS teknolojisi türü vardır. Bu belgenin amaçları doğrultusunda, izledikleri olayların türüne ve dağıtım şekillerine göre aşağıdaki dört gruba ayrılmaktadır: Ağ Tabanlı IDS, Kablosuz IDS, Ağ Davranışı Analizi (NBA), Ana Bilgisayar Tabanlı IDS. Bazı IDS formları diğerlerinden daha gelişmiştir çünkü daha uzun süredir kullanılmaktadır. Ağ tabanlı ve ana bilgisayar tabanlı IDS formları on yılı aşkın süredir piyasada bulunmaktadır. Ağ davranışı analiz yazılımı, kısmen DDoS saldırılarını tespit etmek için, kısmen de iç ağlardaki trafik akışını izlemek için geliştirilen yeni bir IDS formudur. Kablosuz IDS'ler ise, WLAN'ların popülaritesine ve WLAN'lara yönelik artan tehditlere karşı geliştirilen nispeten yeni bir IDS türüdür.

2.2.1 Kablosuz IDS

Kablosuz ağ iletişimi, kablosuz ağ özelliklerine sahip aygıtların, bir ağa fiziksel olarak bağlanmadan bilgi işlem kaynaklarını kullanmasını sağlar. Cihazların, kablosuz ağ altyapısının belirli bir mesafesinde olması gerekir. Kablosuz IDS'ler (WIDS), kablosuz ağ trafiğini izler ve şüpheli etkinliği belirlemek için kablosuz ağ protokollerini analiz eder (Lim vd. 2003, Boob ve Jadhav 2010). Uygulamadaki veya kablosuz ağ trafiğinin

geçtiği üst katman ağ protokollerindeki (örneğin TCP, UDP) şüpheli etkinlikleri tanımlayamazlar. İzleme için kablosuz ağların kapsama alanında yaygın olarak kullanılmaktadırlar.

2.2.1.1 Güvenlik özellikleri

Kablosuz IDS'ler çeşitli güvenlik özellikleri sunar. Kablosuz IDS nispeten yeni bir IDS türü olduğundan, özellikleri şu anda ürünler arasında büyük ölçüde farklılık göstermektedir, ancak zamanla ürün özellikleri daha tutarlı hale gelecektir. Temel olarak üç kategoriye ayrılan ortak güvenlik yetenekleri tanımlanmaktadır: bilgi toplama, kaydetme ve tespit etme.

Bilgi Toplama Özelliği: Kablosuz IDS'lerin çoğu kablosuz cihazlar hakkında bilgi toplayabilir. Bu bilgi toplama yeteneklerinin örnekleri aşağıdaki gibidir:

- ✓ **Cihazları Tanımlama:** Çoğu IDS sensörü, AP'ler ve istemciler dahil olmak üzere gözlemlenen cihazlarının bir grafiğini oluşturur. Grafikler, yeni cihazları tanımlamak ve mevcut cihazların kaldırılmasını sağlamak için bir profil olarak kullanılır.
- ✓ **Kablosuz Ağları Tanımlama:** Çoğu IDS sensörü, izlenen ağları SSID'leriyle tanımlayarak izler. Her biri daha sonra yetkili, normal veya sahte ağ olarak etiketlenir. Bu bilgi, yeni ağları tanımlamak ve ayrıca tanımlanan olaylara verilen yanıtlara öncelik vermek için kullanılır.

Kaydetme Özelliği: Kablosuz IDS'ler genellikle algılanan olaylarla ilgili kapsamlı veri kaydı yapar. Bu veriler uyarıların geçerliliğini doğrulamak, olayları araştırmak ve IDS ile diğer kayıt kaynakları arasındaki olayları ilişkilendirmek için kullanılabilir. Kablosuz IDS'ler tarafından yaygın olarak kaydedilen veri alanları aşağıdakileri gibidir:

- Zaman damgası (genellikle tarih ve saat)
- Etkinlik veya uyarı türü
- Öncelik veya önem derecesi
- Kaynak MAC adresi
- Kanal numarası

- Olayı gözlemleyen sensörün kimliği
- Önleme işlemi (varsa).

Saldırı Tespit Özelliği: Kablosuz IDS'ler, öncelikle IEEE 802.11a, b, g ve i protokol iletişimini inceleyerek WLAN protokolü seviyesindeki saldırıları, yanlış yapılandırmaları ve politika ihlallerini tespit edebilir. Kablosuz IDS'ler iletişimleri daha yüksek seviyelerde incelemez (IP adresleri, uygulama yükleri vb.). Bazı ürünler yalnızca basit imza tabanlı tespit gerçekleştirirken, diğerleri imza tabanlı tespit, anomali tabanlı tespit ve durumsal protokol analizi tekniklerinin bir kombinasyonunu kullanır.

2.2.1.2 Tespit edilebilen saldırılar

Kablosuz IDS'ler tarafından en sık tespit edilebilen olay türleri aşağıdaki gibidir:

Yetkisiz WLAN ve cihazları: Bilgi toplama yetenekleri sayesinde çoğu kablosuz IDS'ler sahte AP'leri, yetkisiz STA'ları ve yetkisiz WLAN'ları algılayabilir.

Olağandışı kullanımlar: Bazı sensörler, olağandışı kullanım modellerini tespit etmek için anomali tabanlı algılama yöntemlerini kullanabilir. Örneğin, normalden çok daha fazla STA (station) belirli bir AP (access point) kullanıyorsa veya bir STA ile AP arasında normalden fazla miktarda ağ trafiği varsa, cihazlardan biri tehlikeye girmiş olabilir veya yetkisiz kişiler ağı kullanıyor olabilir. Birçok sensör, kısa bir süre içinde birkaç başarısız girişimi uyarma gibi ağa katılmak için yapılan başarısız girişimleri tanımlayabilir ve bu da ağa yetkisiz erişim sağlama girişimi olduğunu gösterir. Bazı sensörler, normal kullanım saatleri dışında herhangi bir WLAN aktivitesi tespit edildiğinde de alarm verebilir.

Kablosuz ağ tarayıcılarının kullanımı: Bu tür tarayıcılar, güvenli olmayan veya zayıf şekilde korunan kablosuz ağları tanımlamak için kullanılır. Kablosuz IDS'ler, yalnızca kablosuz ağ trafiği oluşturan aktif tarayıcıların kullanımını algılayabilir. Gözlemlenen trafiği kolayca izleyen ve analiz eden pasif tarayıcıların kullanımını tespit edemezler.

Hizmet reddi (DoS) saldırıları ve koşulları: DoS saldırıları, AP'ye yüksek oranda çok sayıda ileti gönderilmesini içeren sel gibi mantıksal saldırıları ve sıkışma gibi fiziksel saldırıları içerir. Ağı kullanılamaz hale getiren DoS saldırıları, genellikle gözlemlenen aktivitenin beklenen aktivite ile tutarlı olup olmadığını belirleyebilen durumsal protokol analizi ve anomali tespit yöntemleri ile tespit edilebilir. Hizmet reddi saldırılarının çoğu, zaman dilimi boyunca olayların sayılması ve eşik değerlerin aşıldığının uyarılması ile tespit edilir. Örneğin, kablosuz ağ oturumlarının sonlandırılmasını içeren çok sayıda olay DoS saldırısını gösterebilir.

Kimliğe bürünme ve ortadaki adam saldırıları: Bazı kablosuz IDS'ler, bir cihazın başka bir cihazın kimliğini gizlemeye çalıştığını algılayabilir. Bu, çerçevenin belirli değerleri gibi aktivitenin özelliklerinde farklılıklar tanımlanarak yapılır.

2.2.1.3 Kablosuz IDS alanında çalışmalar

Kablosuz IDS yöntemlerinin özeti Çizelge 2.1'de verilmiştir. Çizelge 2.1'de her çalışmanın ana fikri ve önemli yönleri tartışılmaktadır.

Meng ve Li, Bayesian modelini kullanarak güvene dayalı bir saldırı tespit mekanizması geliştirmiş ve bunu kötü niyetli faaliyetleri tespit etme açısından değerlendirmiştir. Bu Bayes modeli sayesinde farklı algılayıcı düğümler arasında bir güven değerleri haritası oluşturulur. Önerilen mekanizmanın performansını değerlendirmek için sabit ve dinamik bir güven eşiğinin etkisini analiz etmişler ve kablosuz bir sensör ortamında değerlendirmişlerdir. Deneysel sonuçlar, Bayes modelinin kötü niyetli faaliyetleri tespit etmede umut verici olduğunu göstermiştir. Bu çalışma birkaç model kullanılarak geliştirilebilir.

Afzal ve diğerlerine göre, kimlik doğrulamasının ve kötü ikiz (evil twin) saldırılarının tespiti için özel ve pratik olarak uygulanan açık kaynaklı bir WIDS çözümü yoktur. Bu çalışmada, OSI katmanı saldırılarını tespit etmek için açık kaynaklı bir WIDS önerilmiştir. Standarda yapılan bu iki yaygın saldırının detaylı incelemesi yapılır. Sonrasında, saldırı davranışını öğrenmek için bu saldırı türleri uygulanır. Son olarak,

yeni saldırı imzaları ve bu saldırıları tespit etmeye yönelik teknikler, bir Kablosuz İzinsiz Giriş Tespit Sistemi (WIDS) olarak tasarlanır ve uygulanır. Önerilen sistemin değerlendirilmesinde iki saldırı için %89 ve %93 doğruluk oranları elde edilmiştir. Yazarlara göre, önerilen saldırı imzaları işe yaramıştır ancak daha da geliştirilebilir.

Kolias vd., kablosuz ağlar için dağıtılmış bir saldırı tespit sistemi olan TermID adlı bir sistem önermiştir. Önerilen sistem, veri alışverişi yapmadan izinsiz giriş tespiti için etkili bir eğitim modeli elde etmek için sürü zekâsı ilkelerine ve sınıflandırma kuralına dayalıdır. Diğer bir özelliği ise önerilen modelin kolay okunabilir olmasıdır. Bunlar önerilen yaklaşımın ana ilkeleridir. Bu yaklaşım AWID veri kümesi üzerinde test edilmiştir. Modern bir WIDS'nin gereksinimleri arasında, bu çalışma, düşük ağ ayak izi ve kullanıcı gizliliği açısından bir model oluşturma görevini yerine getirdi. Bu çalışmalar, doğruluk oranı incelenerek ve bilinmeyen saldırı türleri tespit edilerek geliştirilebilir.

Abdulhammed vd. özellik seçimi, makine öğrenimi sınıflandırıcılarına dayalı gelişmiş bir kablosuz saldırı tespit sistemi için önemli bir faktördür. Bu çalışmanın iki ana katkısı vardır: 1. etkili özellikleri seçme, 2. makine öğrenimi tabanlı bir kablosuz saldırı tespit sisteminin geliştirilmesi. Bu çalışma, sırasıyla 5, 7, 10 ve 32 özellikten oluşan dört etkili özellik seti kullanarak çok sınıflı sınıflandırmayı tartışmaktadır. Elde edilen sonuçlar, seçilen özellik kümesine dayalı olarak iyi bilinen yedi makine öğrenimi sınıflandırıcısının verimliliğini değerlendirmek için AWID veri kümesini kullandı. Önerilen sistem, 32 özellikli bir Rastgele Orman algoritması kullanmış ve maksimum %99.64 doğruluk elde etmiştir. Bu çalışma, önerilen yaklaşımın farklı veri kümeleri üzerinde incelenmesiyle geliştirilebilir.

Kasongo ve Sun derin öğrenmeye dayalı kablosuz bir IDS önermiştir. Önerilen teknik, filtre tabanlı bir özellik seçim algoritması ile birleştirilmiş ileri beslemeli derin sinir ağlarını (FFDNN'ler) kullanır. FFDNN IDS, iyi bilinen veri madenciliği veri seti (NSL-KDD) kullanılarak yorumlanır ve karar ağacı, destek vektör makineleri, Naïve Bayes ve K-Nearest Neighbor gibi literatürdeki mevcut makine öğrenme yöntemleri ile karşılaştırılır. Elde edilen sonuçlar, önerilen FFDNN sisteminin diğer yöntemlere göre

doğruluğu artırdığını göstermiştir. Ancak bu çalışma, küçük saldırı kümeleri olan R2L ve U2R saldırılarının tespit oranlarını artırmak için yeni bir algoritma ile geliştirilebilir.

Kasongo ve Sun'ın bir diğer çalışmasında, bir saldırı tespit sistemi kullanarak çeşitli iletişim altyapılarını korumak için Sarıcı Tabanlı Özellik Çıkarma Birimi (Wrapper Based Feature Extraction Unit-WFEU) kullanan İleri Beslemeli Derin Sinir Ağı (Feed-Forward Deep Neural Network-FFDNN) sistemi önerilmektedir. Önerilen yöntem, optimal bir özellik vektörü oluşturmak için Ekstra Ağaçlar algoritmasını kullanır. WFEU-FFDNN'nin değerlendirmesi, UNSW-NB15 ve AWID veri kümeleri kullanılarak yapılmıştır. Ayrıca WFEU-FFDNN, Random Forest, Decision Tree, SVM, KNN ve Naive Bayes gibi literatürdeki beş farklı standart makine öğrenmesi algoritması ile karşılaştırılmıştır. UNSW-NB15 veri setinde 22 öznitelik kullanılmış ve ikili ve çok sınıflı sınıflandırma şemaları için sırasıyla %87.10 ve %77.16 doğruluk oranı elde edilmiştir. AWID veri setinde 26 öznitelik kullanılmış ve %99.66, %99.77 doğruluk oranı elde edilmiştir. Bu çalışma, kullanılan özelliklerin sayısı daha da azaltılarak geliştirilebilir.

Singh vd., kablosuz ağları saldırılardan korumak ve bu tür etkinlikleri tespit etmek için derin öğrenme tekniğine dayalı yeni bir algoritma önermiştir. Önerilen bu algoritma, özellikleri seçmek amacıyla Özelleştirilmiş Döndürme Ormanı (Customized Rotation Forest) algoritmasını kullanır. Farklı saldırıların sınıflandırılması GRU (Gated Recurrent Units) tarafından gerçekleştirilir. Sunulan model NSL-KDD veri setine uygulanmış ve ikili ve çok sınıflı sınıflandırma için sırasıyla %97.32 ve %97.47 doğruluk oranı elde edilmiştir. Sonuçlara göre önerilen WIDS gerçek zamanlı ağlardaki saldırıları tespit etmek için kullanılabilir. Ancak önerilen model farklı veri setleri üzerinde uygulanarak bu çalışma geliştirilebilir.

Çizelge 2.1 Kablosuz IDS çalışmalarının özeti

Makale	Önerilen Yöntem	Sonuç	Yıl
Meng ve Li	Bayes modeli kullanılarak güvene dayalı bir saldırı tespit mekanizması.	Sabit ve dinamik bir güven eşiğinin etkisi analiz edilmiştir. Deneysel sonuçlar, Bayes modelinin kötü niyetli faaliyetleri tespit etmede umut verici olduğunu gösterdi.	2013
Afzal vd.	Kimlik doğrulamanın ve kötü ikiz saldırılarının tespiti için bir WIDS çözümü.	Önerilen sistemin değerlendirilmesinde iki saldırı türü için %89 ve %93 doğruluk oranları elde edilmiştir.	2016
Kolias vd.	TermID olarak isimlendirilmiş bir WIDS sistemi.	Bu çalışma, düşük iz ve kullanıcı gizliliği açısından bir model oluşturma görevini yerine getirmiştir.	2017
Abdulhammed vd.	Öznitelik seçimi ve çok sınıflı sınıflandırma yöntemleri önerilmiştir.	Rastgele Orman algoritması ve 32 özellik ile %99,64 doğruluk sağlanmıştır. Elde edilen sonuçlar, etkin öznitelik indirgemenin doğruluk oranı ve hız açısından daha iyi sonuçlar verdiğini göstermiştir.	2018
Vijayakumar ve Ganapathy	Makale, WLAN'daki yanlış alarm oranını azaltmak için makine öğrenimi tekniklerinin rolü hakkında kapsamlı bir araştırma yapmıştır ve bir filtreleme tekniği önermiştir.	WLAN saldırılarında daha yüksek doğruluk için akıllı ajanların, hesaplama tekniklerinin ve bulanık kuralların tanıtılmasıyla yeni makine öğrenimi algoritmaları tasarlamayı önermiştir.	2018
Kasongo ve Sun	Derin öğrenmeye dayalı bir kablosuz IDS.	Önerilen FFDNN sistemi, diğer yöntemlere kıyasla doğruluğu artırmaktadır.	2019
Kasongo ve Sun	Sarmalayıcı Tabanlı Özellik Çıkarma Birimi (WFEU) kullanan İleri Beslemeli Derin Sinir Ağı (FFDNN).	UNSW-NB15 veri setinde 22 öznitelik kullanılmış ve ikili ve çok sınıflı sınıflandırma şemaları için sırasıyla %87.10 ve %77.16 doğruluk oranı elde edilmiştir. AWID veri setinde 26 öznitelik kullanılmış ve %99.66 ve %99.77 genel doğruluk elde edilmiştir.	2020
Riyaz ve Ganapathy	Kablosuz ağlardaki davetsiz misafirleri tanımlayarak ve tespit ederek veri iletişiminde güvenlik sağlayan yeni bir IDS.	Önerilen model, algılama doğruluğu (%98.8), daha az eğitim (0.57 s) ve test süresi (0.26 s) açısından daha iyi performans elde etmiştir. Önerilen modelin yanlış alarm oranı, mevcut CNN ile karşılaştırıldığında %1'den azdır.	2020
Satam ve Hariri	Wi-Fi protokolünün normal davranışını modellemek için n-gramları ve Wi-Fi trafik akışlarını sınıflandırmak için makine öğrenimi modellerini kullanan bir WIDS.	Önerilen yaklaşım, düşük yanlış pozitif (0.0174) ve farklı saldırılar için değişen düşük yanlış negatif oranı ile Wi-Fi protokollerine yönelik saldırıları tespit etmiştir.	2020
Singh vd.	Derin öğrenme tekniğine dayalı yeni bir algoritma.	NSL-KDD veri setinde ikili ve çok sınıflı kategorizasyon için sırasıyla %97.32 ve %97.47 doğruluk oranları elde edilmiştir.	2021

2.2.1.4 Kablosuz IDS'lerin değerlendirilmesi

Kablosuz IDS'ler, önce IEEE 802.11a, b, g ve i protokol iletişimini inceleyerek WLAN protokolü düzeyindeki saldırıları, yanlış yapılandırmaları ve ilke ihlallerini tespit edebilir. Ayrıca, hizmet reddi saldırılarına ve fiziksel saldırılara karşı hassastırlar. Bazı kablosuz IDS ürünleri yalnızca imza tabanlı algılama gerçekleştirirken, diğerleri imza tabanlı algılama, anormallik tabanlı algılama ve durumsal protokol analizi tekniklerinin bir entegrasyonunu kullanır. Diğer IDS biçimleriyle karşılaştırıldığında, kablosuz IDS'ler daha yüksek izinsiz giriş algılama doğruluğuna sahiptir. Kablosuz IDS'ler güçlü algılama yetenekleri sunsalar da bazı sınırlamaları vardır: Pasif izleme ve kablosuz trafiğin çevrimdışı işlenmesini içeren saldırılar gibi kablosuz ağlara yönelik saldırı türlerini algılayamazlar.

2.2.2 Ağ tabanlı IDS

Ağ tabanlı bir IDS, belirli ağ bölümleri veya cihazları için ağ trafiğini izler ve şüpheli etkinliği belirlemek için ağ, taşıma ve uygulama protokollerini analiz eder (More vd. 2012). TCP/IP, ağ iletişimi sağlamak için dünya çapında yaygın olarak kullanılmaktadır. TCP/IP iletişimi, birlikte çalışan dört katmandan oluşur. Bir kullanıcı ağlar arasında veri aktarmak istediğinde, veriler en yüksek katmandan en düşük katmana geçirilir ve her katmanda daha fazla bilgi eklenir. En düşük katman toplanan verileri fiziksel ağ üzerinden gönderir; veriler daha sonra katmanlardan hedefine iletilir. Yukarıdan aşağıya doğru dört TCP/IP katmanı aşağıda verilmiştir.

Uygulama Katmanı: Bu katman, DNS, HTTP ve SMTP gibi belirli uygulamalar için veri gönderir ve alır.
İletim Katmanı: Bu katman, uygulama katmanı servislerini ağlar arasında taşımak için bağlantı yönelimli veya bağlantısız servisler sağlar. İletim katmanı isteğe bağlı olarak iletişimin güvenilirliğini sağlayabilir. TCP ve UDP, yaygın olarak kullanılan iletim katmanı protokolleridir.

Ağ Katmanı: Bu katman paketleri ağlar arasında yönlendirir. IPv4, TCP / IP için temel ağ katmanı protokolüdür. Ağ katmanında yaygın olarak kullanılan diğer protokoller IPv6, ICMP ve IGMP'dir.
Veri Bağlantı Katmanı: Bu katman fiziksel ağ bileşenleri üzerindeki iletişimi yönetir. En iyi bilinen veri bağlantı katmanı protokolü Ethernet'tir.

Dört TCP/IP katmanı, ana bilgisayarlar arasında veri aktarmak için birlikte çalışır. Ağ tabanlı IDS'ler genel olarak analizlerinin çoğunu uygulama katmanında gerçekleştirir. Ayrıca, bu katmanlardaki saldırıları belirlemek ve uygulama katmanı etkinliğinin analizini kolaylaştırmak için (örneğin, bir TCP port numarası hangi uygulamanın kullanıldığını gösterebilir), iletim ve ağ katmanlarındaki aktiviteyi de analiz eder. Bazı ağ tabanlı IDS'ler ayrıca donanım katmanında da sınırlı analizler yapar.

2.2.2.1 Güvenlik özellikleri

Ağ tabanlı IDS ürünleri çok çeşitli güvenlik yetenekleri sunar. Genel olarak üç kategoriye ayrılan ortak güvenlik özellikleri aşağıda tanımlanmaktadır: bilgi toplama, kaydetme ve tespit.

Bilgi Toplama Özelliği: Bazı ağ tabanlı IDS'ler sınırlı bilgi toplama özellikleri sunar; ana bilgisayarlar ve ana bilgisayarları içeren ağ etkinliği hakkında bilgi toplayabilirler. Bilgi toplama özelliklerine örnekler aşağıdaki gibidir:

- ✓ **Ana Bilgisayarları Belirleme:** Bir IDS, ağdaki ana bilgisayarların bir listesini oluşturabilir. Bu liste, ağdaki yeni ana bilgisayarları tanımlamak için bir profil olarak kullanılır.

- ✓ **İşletim Sistemlerini Belirleme:** Ana bilgisayarlar tarafından kullanılan işletim sistemlerini ve işletim sistemi sürümlerini çeşitli tekniklerle tanımlayabilir. Örneğin, her bir ana bilgisayarda hangi bağlantı noktalarının kullanıldığını izlenebilir, bu da belirli bir işletim sistemi veya işletim sistemi ailesini (Windows, Unix) gösterebilir. Hangi işletim sistemi sürümlerinin kullanıldığını

bilmek, potansiyel olarak savunmasız ana bilgisayarları belirlemede yardımcı olabilir.

- ✓ **Uygulamaları Tanımlama:** Bazı uygulamalar için, bir IDS sensörü, hangi portların kullanıldığını takip ederek ve uygulama iletişiminin belirli özelliklerini izleyerek kullanımdaki uygulama sürümlerini tanımlayabilir. Örneğin, bir istemci bir sunucuyla bağlantı kurduğunda, sunucu istemciye hangi uygulama sunucusu yazılım sürümünü çalıştırdığını söyleyebilir ve bunun tersi de geçerlidir. Uygulama sürümleriyle ilgili bilgiler, potansiyel olarak savunmasız uygulamaları belirlemek ve bazı uygulamaların izinsiz kullanımını tanımlamak için kullanılabilir.

- ✓ **Ağ Özelliklerinin Belirlenmesi:** Bazı IDS sensörleri, iki cihaz arasındaki atlama sayısı gibi ağ cihazlarının ve ana bilgisayarların yapılandırmasıyla ilgili ağ trafiği hakkında genel bilgi toplar. Bu bilgi ağ yapılandırmasındaki değişiklikleri tespit etmek için kullanılabilir.

Kaydetme Özelliği: Ağ tabanlı IDS'ler genellikle algılanan olaylarla ilgili kapsamlı veri kaydı yapar. Bu veriler uyarıların geçerliliğini doğrulamak, olayları araştırmak ve IDS ile diğer kayıt kaynakları arasındaki olayları ilişkilendirmek için kullanılabilir. Ağ tabanlı IDS'ler tarafından yaygın olarak kaydedilen veri alanları şu şekildedir:

- Zaman damgası (genellikle tarih ve saat)
- Bağlantı veya oturum kimliği
- Etkinlik veya uyarı türü
- Derecelendirme (öncelik, önem, etki, güven)
- Ağ, iletim ve uygulama katmanı protokolleri
- Kaynak ve hedef IP adresleri
- Kaynak ve hedef TCP veya UDP bağlantı noktaları veya ICMP türleri ve kodları
- Bağlantı üzerinden iletilen bayt sayısı
- Uygulama istekleri ve yanıtları gibi veriler
- Önleme işlemi (varsa).

Tespit Özellikleri: Ağ tabanlı IDS'ler genellikle geniş algılama yetenekleri sunar. Çoğu ürün, ortak protokollerin derinlemesine analizini gerçekleştirmek için imza tabanlı algılama, anomali tabanlı algılama ve durumsal protokol analizi tekniklerinin bir kombinasyonunu kullanır. Tespit yöntemleri genellikle iç içe geçmiştir.

2.2.2.2 Tespit edilen saldırı türleri

Ağ tabanlı IDS'ler tarafından yaygın olarak tespit saldırı türleri aşağıdaki gibidir:

Uygulama katmanı keşif ve saldırıları: Arabellek taşmaları, parola tahmini, kötü amaçlı yazılım iletimi gibi saldırılar tespit edilmektedir. Çoğu ağ tabanlı IDS uygulama protokollerini analiz eder. Genellikle analiz edilenler DHCP, DNS, FTP, HTTP, IMAP, IRC, NFS, POP, RPC, SIP, SMB, SMTP, SNMP, Telnet ve TFTP, veritabanı protokolleri, anlık ileti uygulamaları protokolleridir.

İletim katmanı keşif ve saldırıları: Port taraması, olağandışı paket parçalanması, SYN taşması gibi saldırılar tespit edilmektedir. En sık analiz edilen iletim katmanı protokolleri, TCP ve UDP'dir.

Ağ katmanı keşif ve saldırıları: Sahte IP adresleri, geçersiz IP başlık değerleri gibi saldırı türleri tespit edilmektedir. En sık analiz edilen ağ katmanı protokolleri IPv4, ICMP ve IGMP'dir. Birçok ürün IPv6 analizi için de destek sağlamaktadır.

Beklenmeyen uygulama hizmetleri: Arka kapılar, yetkisiz uygulama hizmetleri çalıştıran ana bilgisayarlar gibi saldırı türleridir. Bunlar genellikle, bir bağlantıdaki etkinliğin beklenen uygulama protokolüyle tutarlı olup olmadığını belirleyebilen, ağ trafiğindeki değişiklikleri ve ana bilgisayarlardaki açık bağlantı noktalarını tanımlayabilen bir anormallik algılama yöntemleriyle tespit edilir.

Politika ihlalleri: Uygun olmayan Web sitelerinin kullanımı, yasaklanan uygulama protokollerinin kullanılması gibi saldırılardır. Bazı güvenlik ilkesi ihlali türleri, yöneticilerin TCP veya UDP bağlantı noktası numaraları, IP adresleri, Web sitesi adları

ve tanımlanabilecek diğer veri parçaları gibi izin vermemesi gereken etkinlik özelliklerini belirlemelerine izin veren IDS'ler tarafından tespit edilebilir.

2.2.2.3 Ağ tabalı IDS alanında çalışmalar

Ağ tabanlı IDS'ler kapsamlı algılama yeteneği sunar. Çoğu çalışma, NIDS'ye ek olarak saldırı tespitinde yüksek bir doğruluk oranı elde etmek için farklı saldırı tespit tekniklerinin bir kombinasyonunu kullanır. Yani, saldırı tespit yöntemleri genellikle birbiriyle örtüşür. Bu alanda yapılan çalışmalardan bazıları aşağıda Çizelge 2.2'de özetlenmiştir.

Wattanapongsakorn vd., ağ tabanlı bir Saldırı Tespiti ve Önleme Sistemi (IDPS) önermiştir. Önerilen yaklaşım, farklı makine öğrenme teknikleri ile kullanılabilir ve çevrimiçi bir ağ ortamında test edilebilmektedir. Sonuçlar, önerilen IDPS'nin saldırılardan kaynaklanan normal olayları saniyeler içinde yüksek doğrulukla tanıyabildiğini ve kurbanın bilgisayar ağını saldırılara karşı otomatik olarak engellediğini göstermektedir. Ek olarak, bilinmeyen saldırı türlerini tespit etmek için önerilen bir yaklaşımla C4.5 Karar Ağacı algoritmasını uygulamışlardır ve bu algoritma, bilinmeyen ağ saldırıları ile karşı karşıya kaldığında etkili bir şekilde çalışabilmektedir. Bununla birlikte, bu çalışma, bilinen saldırıların tespitinin yanı sıra bilinmeyen saldırıların tespiti için yaklaşım geliştirilerek daha da geliştirilebilir.

Amaral vd., IPv6 etkin kablosuz sensör ağları için ağ tabanlı bir saldırı tespit sistemi önermiştir. Önerilen sistem, trafik imzalarını ve anormal davranışları kullanarak saldırıları tespit eder. PPPSniffer ve Finger2IPv6 olmak üzere iki bileşenden oluşmaktadır. Önerilen sistemde, gözlemci olarak seçilen ağ düğümleri saldırı tespit sistemi tarafından konumlandırılmaktadır. Bu sayede komşularda değiş tokuş edilen paketler gözlemlenir ve olası saldırı girişimleri tespit edilir. Gözlenen mesajlar, NIDS tarafından oluşturulan kural seti ile karşılaştırılır. Bir eşleşme meydana gelirse, bir alarm oluşturulur ve Olay Yönetim Sistemine gönderilir. Önerilen bu sistem ile önceden tanımlanmış saldırıları tespit etmek yerine olası hatalı davranışlar tespit edilebilmektedir. Ancak, yeni algılama kuralları eklenerek sistem iyileştirilmelidir.

Kumar vd., ağa yönelik tehditleri tespit etmek için makine öğrenimine dayalı ağ tabanlı saldırı tespit sistemi önermiş ve değerlendirmiştir. Bu çalışmada, çeşitli iyi niyetli ve kötü niyetli uygulamalar tarafından oluşan ağ trafiği özelliklerinin etiketli örneklerini içeren veri kümeleri kullanılarak, farklı denetimli makine öğrenimi sınıflandırıcıları oluşturulmuştur. Bu çalışmanın temel amacı, Android tabanlı kötü amaçlı yazılımların tespit edilebilmesidir. Önerilen yaklaşımı test etmek için trafik oluşturulmuştur. Bu trafiği oluşturmak için Premium SMS gönderici, arka kapı, spam gönderici, botlar, fidye yazılımı, bilgi çalma ve sahte antivirüs gibi çeşitli kötü amaçlı yazılım örnekleri kullanılmıştır. Elde edilen sonuçlara göre önerilen yaklaşım, bilinmeyen ve bilinen saldırıları %99,4 doğruluk oranına kadar tespit edebilmiştir. Bu çalışma, oluşturulan veri setinin büyütülmesi ve bahsedilen mevcut saldırı tespit sistemlerine entegre edilmesi ile geliştirilebilir.

Qassim vd., anomali tabanlı saldırı tespit sistemi (AIDS), kötü niyetli olarak algılanan ağ trafiğini tanımlayabilir. Normal davranışlardan farklı bir aktivite tespit ettiğinde her seferinde alarm verir. Bu nedenle, IDS alarmlarını yönetmek ve yanlış pozitifleri gerçek alarmlardan ayırt etmek büyük bir zorluk haline gelir. Bu çalışmada iki adımdan oluşan bir yaklaşım önerilmiştir. İlk olarak, ağdaki anormallikleri tespit etmede en alakalı özellikler olduğu varsayılan bir dizi ağ trafiği özelliği önerilmiştir. İkinci olarak ise, bir paket başlığına dayalı anormallik algılama sistemi tarafından aktiviteleri otomatik olarak sınıflandırmak için AIDS alarm sınıflandırıcısı önerilmiştir. Yazarlara göre, makine öğrenmesi algoritmalarına dayalı önerilen sistem, kötü niyetli faaliyetleri sınıflandırmak açısından etkili ve verimlidir. Bu çalışma, doğruluk oranını artırmak için çeşitli makine öğrenme teknikleri kullanılarak geliştirilebilir.

Mazini vd. , AdaBoost ve yapay arı kolonisi (ABC) algoritmalarını kullanarak anomaliyi tespit etmek için yeni bir hibrit ağ tabanlı IDS yaklaşımı önermektedir. Öznitelik seçimi ABC algoritması kullanılarak yapılmıştır. Seçilen öznitelikleri değerlendirmek ve sınıflandırmak için AdaBoost algoritması kullanılmıştır. Önerilen yaklaşım, yöntemin doğruluğunu değerlendirmek için NSL-KDD ve ISCXIDS2012 veri kümelerine uygulanmıştır. %98,9 doğruluk oranı elde edilmiştir. Yazarlara göre, önerilen yöntem aynı veri kümesindeki diğer IDS'lerden daha iyi performans

göstermiştir. İleride yapılacak çalışmalarda doğruluk daha da geliştirilebilir ve farklı veri setleri üzerinde performans değerlendirmesi yapılabilir.

Meftah et al., UNSW-NB15 veri setini kullanarak anormallik tabanlı bir ağ saldırı tespit yaklaşımı uygulamıştır. Yaklaşımları iki ana aşamadan oluşmaktadır. Makine öğrenimi amaçları için önemli özellikleri seçmek için diğer tekniklerin yanı sıra Özyinelemeli Özellik Eleme (Recursive Feature Elimination) ve Rastgele Orman(Random Forest) algoritmalarını kullanmışlardır. Ardından, Destek Vektör Makinesi, Lojistik Regresyon gibi farklı veri madenciliği tekniklerini kullanarak anormal trafiği tespit etmek için ikili bir sınıflandırma yapılmıştır. Destek Vektör Makinesi ile %82,11 ile en yüksek doğruluk sonucunu elde edilmiştir. Sonrasında saldırı türlerini tespit etme doğruluğunu artırmak için SVM'in çıktısı bir dizi polinom sınıflandırıcı ile beslenmiştir. Özellikle Naive Bayes, Karar Ağaçları ve polinom DVM'nin performansı değerlendirilmiştir. İki aşamalı hibrit sınıflandırmanın uygulanması, sonuçların doğruluğunu %86,04'e kadar artırmıştır. Bu çalışma, yeni bir sınıflandırma algoritması geliştirilerek veya derin öğrenme teknikleri kullanılarak farklı veri kümeleri üzerinde daha da geliştirilebilir.

Kararsız veriler konusunda eğitilmiş NIDS'ler, küçük saldırı sınıflarına karşı yanlış tahminler sunma eğilimi gösterir ve bu da tespit edilmeyen veya yanlış sınıflandırılan izinsiz girişlere neden olur. Bedi vd., bu sınıf dengesizliği sorununu ele almak için iki katmanlı bir Geliştirilmiş Siam-IDS (I-SiamIDS) yaklaşımı önerilmişlerdir. I-SiamIDS, hem azınlık hem de çoğunluk sınıflarını herhangi bir veri seviyesi dengeleme tekniği kullanmadan algoritmalar olarak tanımlar. I-SiamIDS'nin ilk katmanı, girdi örneklerinin filtrelenmesi için Siyam Sinir Ağı, eXtreme Gradient Boosting ve Derin Sinir Ağı ikili kümesini kullanır. Sonrasında, bu saldırılar, çok sınıflı eXtreme Gradient Boosting sınıflandırıcısı (m-XGBoost) kullanılarak farklı saldırı sınıflarına ayrılmak üzere ikinci katmana gönderilir. Benzer çalışmalarla karşılaştırıldığında, I-SiamIDS, hem CIDDS-001 hem de NSL-KDD veri kümeleri üzerinde doğruluk, F1 puanı, kesinlik ve AUC değerlerinde önemli bir gelişme göstermiştir. Sonuçları daha net sunabilmek için önerilen yöntemin hesaplamalı maliyet analizine de yer verilmiştir. Önerilen bu çalışma, farklı veri setleri üzerinde sonuçlar incelenerek geliştirilebilir.

Çizelge 2.2 Ağ tabanlı IDS çalışmalarının özeti

Makale	Önerilen Yöntem	Sonuç	Yıl
Wattanapongsakorn vd.	Ağ tabanlı bir saldırı tespit ve önleme sistemi.	Saldırı türlerinden normal etkinlikleri yüksek doğrulukla algılayabilmekte ve ağı saldırılara karşı otomatik olarak bloke edebilmektedir. Önerilen yaklaşıma sahip C4.5 Karar Ağacı algoritması, bilinmeyen saldırı türlerini algılamaktadır.	2012
Amaral vd.	IPv6 etkin kablosuz sensör ağları için ağ tabanlı bir saldırı tespit sistemi.	Önerilen sistem ile önceden tanımlanmış saldırıları tespit etmek yerine olası hatalı davranışlar tespit edilebilmektedir.	2014
Kumar vd.	Makine öğrenmesini temel alan bir ağ tabanlı bir saldırı tespit sistemi.	Önerilen model, bilinen ve bilinmeyen saldırıları %99,4'e kadar doğrulukla tespit edebilmektedir.	2016
Qassim vd.	Anomali ve ağ tabanlı bir saldırı tespit sistemi.	Makine öğrenmesi algoritmalarına dayalı önerilen sistem, kötü niyetli aktivitelerin sınıflandırılması açısından etkili ve verimlidir.	2016
Karatas ve Sahingoz	Çok katmanlı bir yapay sinir ağında 7 farklı ağ eğitim fonksiyonunun karşılaştırılması.	"trainlm" fonksiyonu, örüntü tanıma problemi olarak gerçekleştirilmiş IDS uygulama alanındaki başarılı algoritmalardandır. "trainr" fonksiyonu da daha az sayıda periyotla(epoch) iyi bir sonuç üretmektedir.	2018
Larijani vd.	Yeni bir Rastgele Sinir Ağı tabanlı Saldırı Tespit Sistemi (RNN-IDS).	NSL-KDD veri setinde farklı sayıda girdi ve gizli katman nöronları öğrenme oranları ile eğitilerek performans değerlendirmesi yapılmıştır. Sonuçlar mevcut sistemlerle karşılaştırılmış ve %94,50 doğruluk elde edilmiştir.	2018
Mazini vd.	Yeni bir anomali ve ağ tabanlı birleşimi hibrit saldırı tespit sistemi.	Önerilen yöntem NSL-KDD ve ISCXIDS2012 veri setleri üzerinde uygulanmış ve %98.9 doğruluk oranı elde edilmiştir.	2019
Meftah vd.	Anomali ağ tabanlı bir saldırı tespit sistemi.	Destek Vektör Makinesi ile %82,11 doğruluk oranı elde edilmiştir. İki aşamalı hibrit sınıflandırmanın uygulanması, sonuçların doğruluğunu %86,04'e kadar artırmıştır.	2019
Devan ve Khare	Özellik seçimi için XGBoost tekniğini kullanan ve ağ izinsiz girişini sınıflandırmak için derin sinir ağını (DNN) kullanan bir XGBoost-DNN modeli önerilmiştir.	NSL-KDD veri seti kullanımıştır. Sonuçlar, LR, NB ve SVM ile karşılaştırılmıştır. DNN, mevcut modellere göre %97 sınıflandırma doğruluğu seviyesi ortaya koymuştur.	2020
Bedi vd.	Dengesiz sınıf sorunu için iki katmanlı bir Siam-IDS yaklaşımı.	Benzer çalışmalarla karşılaştırıldığında, I-SiamIDS, hem CIDDS-001 hem de NSL-KDD veri kümeleri için doğruluk, F1 puanı, kesinlik ve AUC değerlerinde önemli bir gelişme göstermiştir.	2021

2.2.2.4 Ağ tabanlı IDS'lerin değerlendirilmesi

Tarihsel olarak, ağa dayalı IDS'ler, yüksek oranda yanlış pozitif ve yanlış negatif oranlarla ilişkilendirilmiştir. İlk teknolojilerin çoğu, yalnızca göreceli olarak basit bilinen tehditleri tespit etmek için doğru olan, imza temelli tespiti temel almaktadır. Daha yeni teknolojiler, doğruluğu ve tespit genişliğini arttırmak için tespit metotlarının bir kombinasyonunu kullanır ve genel olarak yanlış pozitiflerin ve yanlış negatiflerin oranları azalır. Ağa dayalı IDS'lerin doğruluğuyla ilgili diğer bir yaygın sorun, izlenen ortamın özelliklerini dikkate almak için genellikle önemli miktarda ayarlama ve özelleştirme gerektirmeleridir. Ağ tabanlı IDS'ler kapsamlı algılama yetenekleri sunsa da, bazı önemli sınırlamaları vardır. En önemlileri, şifreli ağ trafiğini analiz etmek, yoğun trafik yüklerini ele almak ve IDS'lerin kendilerine yönelik saldırılara dayanmaktır. Ağ tabanlı IDS'ler, sanal özel ağ (VPN) bağlantıları, SSL üzerinden HTTP ve SSH oturumları dahil olmak üzere şifreli ağ trafiğindeki saldırıları algılayamazlar ve çeşitli saldırı tiplerine karşı hassastırlar.

2.2.3 Ağ davranış analizi sistemi

Bir ağ davranışı analizi (NBA) sistemi, DDoS saldırıları, belirli kötü amaçlı yazılım biçimlerini (solucanlar, arka kapılar) ve politika ihlalleri gibi olağandışı trafik akışlarını belirlemek için ağ trafiğini veya ağ trafiğindeki istatistikleri inceler.

2.2.3.1 Güvenlik özellikleri

NBA ürünleri çeşitli güvenlik yetenekleri sunar. Bunlar sırasıyla bilgi toplama, kaydetme ve tespittir. Bazı NBA ürünleri ayrıca güvenlik bilgileri ve olay yönetimi (SIEM) yetenekleri sağlar.

Bilgi Toplama Özellikleri: NBA sistemleri kapsamlı bilgi toplama yetenekleri sunar, çünkü NBA ürününün tespit tekniklerinin çoğu için ana bilgisayarların özelliklerine ilişkin bilgiye ihtiyaç vardır. NBA sensörleri, izlenen ağlarda iletişim kuran ana bilgisayar listelerini otomatik olarak oluşturabilir ve saklayabilir. Port kullanımını

izleyebilir, pasif parmak izi yapabilir ve ana bilgisayarlar hakkında ayrıntılı bilgi toplamak için diğer teknikleri kullanabilirler. NBA sistemleri saldırıların tespiti için aşağıdaki bilgileri elde etmektedir:

- IP adresi
- İşletim sistemi
- IP protokolleri ve TCP/UDP bağlantı noktaları
- İletişim kurduğu diğer ana bilgisayarlar ve hangi hizmetlerin kullanıldığı

NBA sensörleri, bu bilgilerdeki değişiklikler için ağ etkinliğini sürekli izler. Her sunucunun akışına ilişkin ek bilgiler de sürekli olarak toplanır.

Kaydetme Özellikleri: NBA teknolojileri tipik olarak tespit edilen olaylarla ilgili kapsamlı veri kaydı yapar. Bu veriler, uyarıların geçerliliğini doğrulamak, olayları araştırmak ve NBA çözümü ile diğer günlük kaynakları arasındaki olayları ilişkilendirmek için kullanılabilir. NBA yazılımı tarafından sıkça kaydedilen veri alanları aşağıdakilerdir:

- Zaman damgası (genellikle tarih ve saat)
- Etkinlik veya uyarı türü
- Derecelendirme (örneğin, öncelik, önem, etki, güven)
- Ağ, taşıma ve uygulama katmanı protokolleri
- Kaynak ve hedef IP adresleri
- Kaynak ve hedef TCP veya UDP bağlantı noktaları veya ICMP türleri ve kodları
- Ek paket başlık alanları
- Bağlantı için kaynak ve hedef ana bilgisayarlar tarafından gönderilen bayt ve paket sayısı
- Önleme işlemi (varsa)

Tespit Özellikleri: NBA teknolojileri tipik olarak birkaç tür kötü amaçlı etkinliği tespit etme yeteneğine sahiptir. Çoğu ürün, ağ akışlarını analiz etmek için bazı durumsal protokol analizi teknikleriyle birlikte, öncelikle anomali tabanlı algılama kullanır. NBA

teknolojilerinin çoğu, belirli tehditleri tespit etmek veya durdurmak için esasen imza olan özel filtreleri manuel olarak ayarlamalarına izin vermek dışında, imza tabanlı tespit özelliği sunmaz.

2.2.3.2 Tespit edilen saldırı türleri

NBA sistemleri tarafından en sık tespit edilen olay türleri aşağıdakileri içerir:
Hizmet reddi (DoS) saldırıları: Bu saldırılar normalde önemli ölçüde artmış bant genişliği kullanımını veya normalden çok daha fazla sayıda paket veya bağlantıyı barındırır. Bu özellikleri izleyerek, anormallik tespit yöntemleri, gözlenen aktivitenin beklenen aktiviteden önemli ölçüde farklı olup olmadığını belirleyebilir.

Tarama: Tarama, uygulama katmanındaki, taşıma katmanındaki ve ağ katmanındaki akış düzenleri ile tespit edilebilir.

Solucanlar: Ana bilgisayarlar arasında yayılan solucanlar, birden fazla şekilde tespit edilebilir. Bazı solucanlar hızla yayılır ve çok miktarda bant genişliği kullanır. Solucanlar ayrıca, ana makinelerin normalde kullanmadıkları bağlantı noktalarını kullanmasına neden olabildiği için tespit edilebilmektedir.

Beklenmeyen uygulama hizmetleri: Bunlar genellikle, bir bağlantı içindeki etkinliğin beklenen uygulama protokolüyle tutarlı olup olmadığını belirleyebilen durumsal protokol analizi yöntemleriyle tespit edilir.

Politika ihlalleri: NBA sistemlerinin çoğu, bir sistemin hangi ana bilgisayar veya ana bilgisayar grupları ile iletişim kurabileceği veya temas edemeyeceği ve haftanın belirli saatlerinde veya günlerinde hangi tür etkinliklere izin verilebileceği gibi ayrıntılı politikalar belirlemelerine izin verir. Ayrıca, yeni ana bilgisayarları veya ana bilgisayarlarda çalışan ve yetkisiz olabilecek yeni hizmetleri tespit etmek gibi birçok olası politika ihlalini de otomatik olarak algılar.

2.2.3.3 Ağ davranış analizi alanında çalışmalar

Ağ davranışı analizi çalışmalarının özeti Çizelge2.3'de verilmiştir. Çizelge2.3'de her çalışmanın ana fikri ve makalelerin önemli yönleri tartışılmaktadır.

Youssef ve Emam'ın çalışmasına göre, geleneksel saldırı tespit sistemleri sınırlı yeteneklere sahiptir ve çoğu durumda ağda herhangi bir anormallik olmadığında kötü niyetli davranışları tespit edemez veya alarm (yanlış pozitif) oluşturamazlar. Bu çalışmada, Veri Madenciliği tekniklerinin ağ trafiği verilerine uygulanması ve Ağ Davranışı Analizi sisteminin kullanılmasının daha iyi saldırı tespit sistemlerinin geliştirilmesine yardımcı olacağı düşünülmektedir. Youssef ve Emam, hibrit bir saldırı tespit yaklaşımı önermiştir. Ağ saldırı tespiti için DM ve NBA yaklaşımları incelenmiş ve her iki yaklaşımın bir kombinasyonunun ağ saldırılarını daha etkili bir şekilde tespit edebileceği iddia edilmiştir.

Nitin vd. ağ davranışı analiz sistemi adı verilen bir IDPS teknolojisini analiz etmiş ve değerlendirmiştir. Ağ davranışı analiz sistemi, temel olarak, DDoS saldırıları, belirli kötü amaçlı yazılım türleri gibi olağandışı trafik akışları oluşturan tehditleri belirlemek için ağ trafiğini inceleyen bir saldırı tespit ve önleme sistemi teknolojisidir. Bu makalede NBA teknolojilerinin ayrıntılı bir değerlendirmesi sunulmaktadır. İlk olarak, NBA teknolojilerinin ana bileşenleri ve bileşenlerin dağıtımına yönelik mimarileri açıklanmaktadır. Ayrıca, şüpheli aktiviteyi tespit etmek için kullanılan metodolojiler ile beraber teknolojilerin güvenlik yetenekleri ayrıntılı olarak incelenmiştir. Bölümün geri kalanında, uygulama ve işletim için öneriler de dahil olmak üzere teknolojilerin yönetim yetenekleri tartışılmaktadır.

Srivatav vd., KDD_cup_99 veri seti ile Temel Bileşen Analizi (PCA) ve Ağ Davranışı Analizini (NBA), mevcut saldırıların yanı sıra yeni saldırıları veya izinsiz girişleri tespit etmek için kullanmıştır. Burada PCA, veri setini boyutlandırmak için ve NBA, ağın davranışını analiz etmek için kullanılır. Önerilen yöntemin eğitimi ve testi için KDD_cup_99 veri seti kullanılmıştır. Bu makalenin temel amacı, kötü amaçlı veri kümesini değerlendirmek ve izinsiz girişleri tespit etmektir. Değerlendirme sonuçlarına

göre, önerilen yöntem, literatürdeki önceki sistemlere kıyasla gerçek zamanlı saldırı tespiti için tespit doğruluğu ve hesaplama verimliliği açısından daha umut vericidir. Yöntem ayrıca yeni saldırıları ve en çok bilinen saldırıları tespit etmede oldukça etkilidir. Bu çalışma, bilinen veri kümelerinin yanı sıra çevrimiçi veri kümeleri kullanılarak genişletilebilir.

APT (gelişmiş kalıcı tehditler) saldırıları, ilk izinsiz giriş sırasında kimlik avı gibi basit saldırılar yapar, ancak ilk izinsiz girişten sonraki uzun vadede, bilgi sızdırır, bir arka kapı oluşturur ve kötü amaçlı kod iletmek için ağı analiz eder. Bu makalede, Moon ve diğerleri tarafından sisteme izinsiz girişten sonra değişen APT saldırılarını tespit etmek için davranışsal bilgi analizi gerçekleştiren bir karar ağacı tabanlı saldırı tespit sistemi önerilmiştir. Önerilen sistem önce kötü niyetli kodun davranışını analiz eder ve ardından karar ağacı aracılığıyla kuralı belirler. Değerlendirme sonuçlarına göre önerilen sistem, APT saldırılarına hızlı bir şekilde yanıt verebilir, ilk saldırı olasılığını tespit edebilir ve hasar boyutunu en aza indirebilir. Bu çalışma, süreçte oluşturulan ana davranışların standartlaştırılmasıyla, ağ ve sistemdeki dağıtık APT güvenlik yöntemleri üzerinde farklı çalışmalarla geliştirilebilir.

Bu makalede, Ghansahala vd., bulut ağ katmanında Davranış Tabanlı Ağ Saldırı Tespiti (BNID) adı verilen hafif ve uyarlanabilir bir saldırı tespit yaklaşımı önermektedir. İzinsiz girişleri tespit etmek için Bulut Ağ Düğümü'nde trafik davranışı analizi gerçekleştirilir. BNID'i bulutta dağıtmak için bir güvenlik çerçevesi önerilmiştir. BNID, trafik davranışı analizi için özellik seçimi ve istatistiksel öğrenme tekniklerini kullanır. Önerilen yaklaşımı değerlendirmek için Bilgi Teknolojileri Operasyon Merkezi (ITOC) saldırı veri seti kullanılmıştır. BNID, %1,57 yanlış pozitif ile %98,88 doğruluk oranı elde etmiştir. Bu çalışma, görünmeyen saldırıları tespit etmek için önerilen yaklaşımla geliştirilebilir.

Çizelge 2.3 Ağ davranış analizi çalışmalarının özeti

Makale	Önerilen Yöntem	Sonuç	Yıl
Youssef ve Emam	Ağa izinsiz giriş tespiti için DM ve NBA yaklaşımları.	Her iki yaklaşımın kombinasyonu, ağ izinsiz girişlerini daha etkili bir şekilde tespit edebilmektedir.	2011
Nitin vd.	Ağ davranışı analiz sistemi olarak adlandırılan IDPS teknolojisinin analizi ve değerlendirmesi. .	NBA teknolojilerinin ana bileşenleri ve bileşenlerin dağıtılması için mimarileri açıklanmaktadır. Şüpheli etkinliği tespit etmek için kullanılan metodolojiler de dahil olmak üzere teknolojilerin güvenlik yetenekleri ayrıntılı olarak incelenmiştir.	2012
Srivastav vd.	KDD_cup_99 veri setinde Temel Bileşen Analizi (PCA) ve Ağ Davranış Analizi uygulanmıştır.	Önerilen yöntem, literatürdeki önceki sistemlere kıyasla gerçek zamanlı saldırı tespiti için tespit doğruluğu ve hesaplama verimliliği açısından daha umut vericidir.	2013
Moon vd.	Değişen APT saldırılarını tespit etmek için davranışsal bilgi analizi yapan, karar ağacı tabanlı bir saldırı tespit sistemi.	Önerilen sistem, APT saldırılarına hızlı bir şekilde yanıt verebilir, ilk izinsiz giriş olasılığını tespit edebilir ve hasar boyutunu en aza indirebilir.	2017
Ghanshala vd.	Davranış Tabanlı Ağ Saldırı Tespiti (BNID) adı verilen hafif ve uyarlanabilir bir saldırı tespit yaklaşımı.	BNID, %1,57 yanlış pozitif ile %98,88 doğruluk oranına ulaştı.	2018
Pacheco vd.	Bir IoT ağ düğümünün ne zaman tehlikeye atıldığını algılamak için anormal davranış analizine dayalı bir IDS metodolojisi.	Elde edilen deneysel sonuçlar, önerilen yaklaşımın yanlış kullanımlar veya siber saldırılar nedeniyle bilinen ve bilinmeyen anormallikleri yüksek algılama oranı ve düşük yanlış alarmlarla doğru bir şekilde tespit ettiğini göstermektedir.	2019
Ahn vd.	Hawkware adında yeni bir IDS.	Hawkware, bir Raspberry PI üzerinde konuşlandırılacak kadar hafiftir ve saldırıları oldukça yeterli düzeyde algılayabilir.	2020
Fladby vd.	Mevcut bir NBA çözümünün sağlamlığını değerlendirmek ve iletişim modellerini uyarlamak için çekişmeli tekniklerin kullanımının araştırılması. Ağ akışlarının belirli özelliklerini çıkarmaya, düzenlemeye ve bir yaklaşımı otomatikleştirmeye izin veren bir paket ayrıştırıcı uygulaması.	Elde edilen sonuçlar, ağ akış parametrelerinin, izinsiz giriş tespit modellerinden kaçınmayı sağlamak için gerçekten bozulabileceğini göstermiştir. Ek olarak, ağ akışlarındaki bozulmanın büyüklüğünü en aza indirmeyi amaçlayan optimizasyon problemlerine yönelik tekniklerle kaçınma algılamayı birleştirmenin mümkün olduğunu iddia etmektedir.	2020
Khan	Ağdaki kötü niyetli siber saldırıları tahmin eden ve sınıflandıran derin öğrenme tabanlı bir hibrit IDS çerçevesi oluşturmak için evrişimli tekrarlayan bir sinir ağı kullanılır.	Elde edilen sonuçlara göre, önerilen HCRN NIDS, mevcut IDS metodolojilerinden daha iyi sonuç vererek, 10 kat çapraz doğrulama ile CSE-CIC-IDS2018 verileri için %97,75'e varan yüksek kötü niyetli saldırı tespit doğruluğu elde etmiştir.	2021
Yang	Davranış ve derin öğrenme tabanlı bir IDS.	Önerilen sistem, mevcut ağ ortamında bilinen veya bilinmeyen kötü niyetli davranışları etkili bir şekilde tespit edebilmektedir.	2021

Başka bir çalışmada, Ahn vd., bir IoT cihazında çalışan ve ağ trafiği ile birlikte cihazın çalışma zamanı davranışını analiz eden ANN tabanlı dağıtılmış bir IDS olan Hawkware adlı yeni bir IDS önermektedir. Hawkware sistemi, geleneksel olarak kullanılan pahalı, derin veri analizinin aksine, cihaz davranışını analiz ederek karmaşık saldırıları tespit etmek için tasarlanmıştır. Yapılan değerlendirmelere göre Hawkware'in bir Raspberry PI üzerinde konuşlandırılabilecek kadar hafif olduğu ve saldırıları oldukça yeterli düzeyde algılayabildiği görülüyor. Bu çalışma sadece IoT cihazları için değil, farklı sistemlerde de çalışacak şekilde geliştirilebilir.

Yang, ağdaki kötü niyetli davranışların zamanında tespiti için derin öğrenmeyi kullanan davranışa dayalı bir saldırı tespit sistemi önermektedir. Önerilen sistem, Çift Yönlü Uzun Kısa Süreli Bellek (Bidirectional Long Short Term Memory) mimarisini uygular ve önerilen sistemi test etmek için UNSW-NB15 veri setini kullanır. Yazarlara göre, deneysel testler sonucunda önerilen sistem, mevcut ağ ortamında bilinen veya bilinmeyen kötü niyetli davranışları etkili bir şekilde tespit edebilmektedir. Bu çalışma, dengesiz veri kümesi sınıflandırma problemi çözülerek daha da geliştirilebilir.

2.2.3.4 Ağ davranış analizi sistemlerinin değerlendirilmesi

NBA sistemleri öncelikle normal davranıştan önemli sapmaları algılayarak çalıştığından, kısa sürede büyük miktarda ağ etkinliği oluşturan saldırıları ve olağandışı akış düzenine sahip saldırıları tespit etmekte yüksek doğruluk oranı sağlamaktadırlar. NBA sistemleri küçük çaplı saldırıları tespit etmede hassastır, özellikle yavaş uygulanırsa ve yönetici tarafından belirlenen politikaları ihlal etmiyorlarsa algılama doğruluğu da zamanla değişir. NBA teknolojileri anomaliye dayalı algılama yöntemleri kullandığından, etkinliklerinin beklenenden önemli ölçüde farklı olduğu bir noktaya ulaşana kadar birçok saldırıyı tespit edemezler. Bir DoS saldırısı yavaş başlarsa ve zaman içinde artarsa, algılanması olasıdır. Sensörleri anormal aktiviteye daha duyarlı olacak şekilde yapılandırarak, saldırılar meydana geldiğinde daha hızlı uyarılar üretilecektir, ancak daha fazla yanlış pozitifin de oluşması muhtemeldir. Tersine, eğer sensörler anormal aktiviteye karşı daha az hassas olacak şekilde yapılandırılmışsa, daha

az yanlış pozitif olacaktır, ancak daha uzun süre boyunca saldırıların gerçekleşmesine izin veren uyarılar daha yavaş üretilecektir.

2.2.4 Ana bilgisayar tabanlı IDS

Ana bilgisayar tabanlı bir IDS, ana bilgisayarın özelliklerini ve bu ana bilgisayarın içinde meydana gelen olayları, şüpheli etkinliklerin tespiti için izler. Ana bilgisayar tabanlı bir IDS'nin izleyebileceği özellik türlerine örnek olarak kablolu ve kablosuz ağ trafiği, sistem günlükleri, çalışan işlemler, dosya erişimi/modifikasyonu ve sistem ve uygulama yapılandırma değişiklikleri verilebilir (Gupta ve Mamtora 2012, Deshpande vd. 2018).

Çoğu HIDS, ilgili ana bilgisayarlara yüklenen ajanlar olarak bilinen algılama yazılımına sahiptir. Her ajan, tek bir ana bilgisayardaki etkinliği izler. Ajanlar, verileri veritabanı sunucularını kullanabilen yönetim sunucularına iletir. Konsollar yönetim ve izleme için kullanılır. Bazı ana bilgisayar tabanlı IDS'ler, ajan yazılımını ayrı ana bilgisayarlara yüklemek yerine doğrudan çalıştıran özel cihazlar kullanır. Her cihaz, belirli bir ana bilgisayardaki trafiği izlemek için konumlandırılmıştır. Teknik olarak, bu cihazlar ağ tabanlı IDS'ler olarak kabul edilebilir. Her cihaz, aşağıdakilerden birini korumak için özel olarak tasarlanmıştır:

- **Sunucu:** Ajanlar, sunucunun işletim sistemini gözlemlemeye ek olarak bazı uygulamaları da izleyebilir.
- **İstemci Ana Bilgisayarı:** Kullanıcıların ana bilgisayarlarını izlemek için tasarlanmış ajanlar, genellikle işletim sistemini, e-posta istemcileri ve web tarayıcıları gibi yaygın uygulamaları gözlemler.
- **Uygulama Hizmeti:** Bazı ajanlar, yalnızca web sunucusu programı veya veritabanı sunucusu programı gibi belirli bir uygulamayı gözlemlemek için tasarlanmıştır. Bu tür ajanlar, uygulama tabanlı IDS'ler olarak da bilinir.

2.2.4.1 Güvenlik özellikleri

Ana bilgisayar tabanlı IDS'ler çeşitli güvenlik yetenekleri sunar. Bunlar günlüğe kaydetme ve tespit özellikleridir.

Kaydetme Özellikleri: Ana bilgisayar tabanlı IDS'ler genellikle tespit edilen olaylarla ilgili kapsamlı veri kaydı yapar. Bu veriler, uyarıların geçerliliğini doğrulamak, olayları araştırmak ve ana bilgisayar tabanlı IDS ile diğer günlük kaynakları arasındaki olayları ilişkilendirmek için kullanılabilir. Genel olarak ana bilgisayar tabanlı IDS'ler tarafından kaydedilen veri alanları şunlardır:

- Zaman damgası (genellikle tarih ve saat)
- Etkinlik veya uyarı türü
- Derecelendirme (öncelik, önem, etki, güven)
- IP adresi ve bağlantı noktası bilgileri, uygulama bilgileri, dosya adları/yolları ve kullanıcı kimlikleri
- Önleme işlemi (varsa).

Tespit Özellikleri: Çoğu ana bilgisayar tabanlı IDS, birkaç kötü amaçlı etkinlik türü belirleme özelliğine sahiptir. Bilinen saldırıları tanımlamak için sıklıkla imza tabanlı algılama tekniklerinin bir kombinasyonunu ve önceden bilinmeyen saldırıları tanımlamak için politika veya kural setleriyle anomali tabanlı tespit tekniklerinin bir kombinasyonunu kullanırlar.

2.2.4.2 Tespit edilen saldırı türleri

Ana bilgisayar tabanlı IDS'ler tarafından algılanan olay türleri, kullandıkları algılama tekniklerine bağlı olarak büyük ölçüde değişir. Bazı ana bilgisayar tabanlı IDS ürünleri bu algılama tekniklerinin birçoğunu sunarken, diğerleri birkaç veya bir tanesine odaklanır. Örneğin, bazı ürünler yalnızca ağ trafiğini analiz ederken, diğer ürünler yalnızca ana bilgisayarın kritik dosyalarının bütünlüğünü kontrol eder. Ana bilgisayar tabanlı IDS'lerde yaygın olarak kullanılan spesifik teknikler aşağıdaki gibidir:

Kod Analizi: Aracılar, kod yürütme girişimlerini analiz ederek kötü amaçlı etkinliği tanımlamak için aşağıda listelenen tekniklerden birini veya birkaçını kullanabilir. Bu tekniklerin tümü kötü amaçlı yazılımı durdurmada yardımcı olur ve bazıları yetkisiz erişime, kod yürütülmesine veya ayrıcalıkların artmasına izin verecek diğer saldırıları da önleyebilir.

Ağ Trafiği Analizi: Bu genellikle ağ tabanlı bir IDS'nin çalışma prensibi ile aynıdır; bazı ürünler hem kablolu hem de kablosuz ağ trafiğini analiz edebilir. Ağ, taşıma ve uygulama katmanı protokol analizine ek olarak, popüler e-posta istemcileri gibi yaygın uygulamalar için özel işlem içerebilir. Trafik analizi ayrıca e-posta, web ve dosya paylaşımı gibi uygulamalar tarafından gönderilen dosyaları ayıklamasını da sağlar; bu da daha sonra kötü amaçlı yazılımlara karşı denetlenebilir.

Ağ Trafiği Filtreleme: Genellikle, sistemdeki her uygulama için gelen ve giden trafiği kısıtlayabilen, yetkisiz erişimi ve kabul edilebilir kullanım politikası ihlallerini önleyen ana bilgisayar tabanlı bir güvenlik duvarı vardır. Bu güvenlik duvarlarından bazıları, ana bilgisayarın iletişim kurması gereken bilgisayarların listesini oluşturabilir ve kullanabilir.

Dosya Sistemi İzleme: Dosya sistemi izleme işlemi, dosya bütünlüğü kontrolü, dosya öznitelik kontrolü, dosya erişim girişimleri gibi birkaç farklı teknik kullanılarak yapılabilir. Bu teknikler ile, rootkitler ve truva atları gibi bazı kötü amaçlı yazılım biçimlerinin yüklenmesini önlemek ve dosya erişimi, değiştirilmesi veya silinmesi gibi diğer birçok kötü amaçlı etkinlik türünün önlenmesinde de kullanılabilir. Ancak bu sistemlerde yöneticiler, bazı ürünlerin izleme mantığının dosya adlarına dayandığının farkında olmalıdır; böylece kullanıcılar veya saldırganlar dosya adlarını değiştirirse, dosya sistemi izleme teknikleri etkisiz hale getirilebilir.

Günlük Analizi: Bazı aracılar, kötü amaçlı etkinliği belirlemek için işletim sistemi ve uygulama günlüklerini izleyebilir ve analiz edebilir. Bu kayıtlar sayesinde, sistemi kapatma, bir uygulamayı başlatma ve kapatma, başarılı ve başarısız kimlik doğrulama girişimleri, güvenlik politikası değişiklikleri gibi saldırıların önüne geçilebilmektedir.

Ağ Yapılandırması İzleme: Genellikle, ana bilgisayardaki tüm ağ arabirimleri kablolu, kablosuz, sanal özel ağ (VPN) ve modem dahil olmak üzere izlenir. Önemli ağ yapılandırma değişikliklerinin örnekleri, istem dışı moda geçirilen ağ arabirimleri, ana bilgisayarda ek TCP veya UDP bağlantı noktaları veya IP olmayan protokoller gibi kullanılan ek ağ protokolleridir. Bu değişiklikler, ana bilgisayarın zaten tehlikeye atıldığını ve gelecekteki saldırılarda kullanılmak veya veri aktarmak için yapılandırıldığını gösterebilir.

2.2.4.3 Ağ tabanlı IDS alanında çalışmalar

Ana bilgisayar tabanlı IDS yöntemlerinin özeti Çizelge 2.4'te görülebilir. Çizelge 2.4'te her bir çalışmanın ana fikri ve makalelerin önemli yönleri tartışılmaktadır.

Ou vd., iki tespit teknolojisinden oluşan bir ana bilgisayar tabanlı saldırı tespit sistemi tasarlamış ve uygulamışlardır. Bunlar, günlük dosyası analizi ve geri yayılımlı sinir ağı teknolojisidir. Kötüye kullanım tespiti için günlük dosyası analizi ve anormallik tespiti için geri yayılımlı sinir ağı kullanılmıştır. Bu iki tespit teknolojisinin kombinasyonunun amacı, önerilen HIDS'in izinsiz giriş tespitinin doğruluğunu ve verimliliğini etkin bir şekilde artırabilmesidir. Elde edilen sonuçlar, önerilen sistemin saldırı tespit etkinliğini ve doğruluk oranını iyileştirdiğini göstermektedir.

Creeach vd., semantik bir algoritmaya dayalı yeni bir ana bilgisayar tabanlı anormallik izinsiz giriş tespit yaklaşımı önermiştir. Bu çalışmanın amacı, kesintili sistem çağrı kalıpları kullanarak yanlış alarm oranlarını azaltırken algılama oranlarını arttırmaktır. Temel mantık, anormal davranışları tespit etmeye yardımcı olmak için çekirdek düzeyinde sistem çağrılarına anlamsal bir yapı uygulamaktır. Bu yeni yaklaşımda, çekirdek performansı test etmek için KDD98 ve ADFA-LD veri seti, taşınabilirlik ve sağlamlık testi için UNM veri seti kullanılmıştır. Yazarlara göre, yeni bir semantik tabanlı algoritma, mevcut yöntemlerden önemli ölçüde daha iyi performans göstermiştir. Bu araştırma, eğitim yükünü azaltmak ve anlamsal özelliklerin esnekliğini artırmak için yeni teknikleri araştırabilir.

Catherine vd., mevcut ana bilgisayar tabanlı saldırı tespit sistemlerinin, tüm özellik kümesini kullandıkları için saldırı tespitinde yeterince hızlı olmadıklarını iddia etmiştir. Bahsedilen sorunun bir çözümü olarak, bu makale CPDT (Korelasyon Tabanlı Kısmi Karar Ağacı Algoritması) olarak adlandırılan yeni bir Ana Bilgisayar tabanlı IDS önermiştir. CPDT, özellikleri seçmek için korelasyon özellik seçimini ve trafiği sınıflandırmak için kısmi karar ağacı algoritmasını entegre etmiştir. Algoritma KDD '99 veri seti üzerinde uygulanarak değerlendirilmiş ve %99.94 doğruluk oranı elde edilmiştir. Yazarlara göre CPDT, mevcut algoritmalardan daha iyi sonuçlar vermektedir. Bu çalışma, bilinmeyen saldırıları tespit etmek için yeni bir yöntemle beraber geliştirilebilir.

Subba vd. hesaplama maliyetini ve yoğun kaynak kullanımını azaltmak için yeni bir HIDS çerçevesi önermiştir. Önerilen çerçeve, ilk olarak sistem çağrı izlerini n-gram vektörlerine çevirir ve daha sonra bir boyut indirgemesi uygulayarak öznitelik vektörlerinin boyutunu küçültür. Azaltılmış öznitelik vektörleri, makine öğrenmesine dayalı birkaç sınıflandırıcı modelle analiz edilmiştir. Önerilen modelin performansını değerlendirmek için ADFA-LD veri seti kullanılmıştır. Elde edilen sonuçlar, izinsiz girişleri düşük yanlış pozitif oranı ve yüksek doğrulukla etkili bir şekilde tespit ettiğini göstermiştir. Bu çalışma performansını daha da artırmak için çeşitli parametrelerde ince ayar yapılarak geliştirilebilir.

Chawla vd., sistem çağrılarının sıralarına dayalı olarak bir sistemin normal davranışını belirlemek için yeni bir ana bilgisayar tabanlı IDS önermiştir. Bu çalışma, Tekrarlayan Sinir Ağlarına dayalı, hesaplama açısından verimli bir anomali tabanlı saldırı tespit sistemini açıklamaktadır. Normal LSTM ağları yerine geçitli tekrarlayan birimler (Gated Repetitive Units-GRU) kullanarak eğitim sürelerini kısaltarak önemli sonuçlara ulaşmayı hedeflemişlerdir. Önerilen teknik ADFA veri setlerine uygulanmıştır. Elde edilen sonuçlar, CNN/GRU'nun eğitimdeki daha hızlı yakınsama nedeniyle LSTM'den yaklaşık 10 kat daha hızlı olduğunu göstermiştir. Ayrıca önerilen sistemle %100 doğru tespit oranı ve %60 yanlış alarm oranına ulaştılar. Bu çalışma, eğitim örneklerinin sayısı artırılarak veya farklı veri setleri üzerinde uygulanarak geliştirilebilir.

Çizelge 2.4 Ana bilgisayar tabanlı IDS çalışmalarının özeti

Makale	Önerilen Yöntem	Sonuç	Yıl
Ou vd.	Günlük dosyası analizi ve geri yayılımlı sinir ağı teknolojisi ile ana bilgisayar tabanlı bir saldırı tespit sistemi tasarlanması ve uygulanması.	Önerilen sistem, saldırı tespit sistemlerinin verimliliğini ve doğruluk oranını iyileştirmiştir.	2010
Creech vd.	Anlamsal bir algoritmaya dayalı yeni bir ana bilgisayar tabanlı izinsiz giriş algılama yaklaşımı.	Yeni anlamsal tabanlı algoritma, üç farklı veri kümesinde mevcut yöntemlerden önemli ölçüde daha iyi performans göstermiştir.	2013
Catherine vd.	Korelasyon tabanlı Kısmi Karar Ağacı Algoritması (Correlation based Partial Decision Tree Algorithm-CPDT) olarak adlandırılan yeni bir Ana Bilgisayar tabanlı IDS.	Algoritma KDD '99 veri seti üzerinde uygulanmış ve %99.94 doğruluk oranı elde edilmiştir. CPDT, mevcut algoritmalardan daha iyi sonuçlar vermiştir.	2014
Subba vd.	Yeni bir HIDS çerçevesi önerilmiştir.	Düşük yanlış pozitif oranı ve yüksek doğruluk ile izinsiz girişleri etkili bir şekilde tespit edebilmiştir.	2017
Chawla vd.	Yeni bir ana bilgisayar tabanlı IDS yaklaşımı sunulmuştur.	Yığılmış CNN/GRU, eğitimdeki daha hızlı yakınsama nedeniyle LSTM'den yaklaşık 10 kat daha hızlıdır. Önerilen sistem ile %100 Doğru Tespit Oranı ve %60 yanlış alarm oranı elde edilmektedir.	2018
Deshpande vd.	Uygulama ve analiz ile Bulut ortamı için ana bilgisayar tabanlı bir saldırı tespit modeli önerilmiştir.	Model, altyapı katmanında hizmet olarak güvenlik sağlar. Uygulama sonucu, ortalama %96 saldırı tespit oranı elde edilmiştir.	2018
Byrnes vd.	Güncel Linux çekirdeği 5.7.0-rc1 incelenmiştir.	Modellerin amaçlanan limitlerde çalışması için karşılanması gereken belirli çalışma zamanı ve bellek kısıtlamaları sunulmuştur.	2020
Gassais vd.	Kullanıcı alanı ve çekirdek alanı bilgilerini ve makine öğrenimi tekniklerini birleştiren, IoT'de izinsiz giriş tespiti için yeni bir ana bilgisayar tabanlı otomatik çerçeve sunulmuştur.	Yazarlara göre, sunulan çözüm iyi sonuçlar elde etmiş ve hızlı tespit için optimize edilmiştir.	2020
Liu vd.	Google bulut ortamında Apache Spark kullanan, SCADS olarak adlandırılan sistem çağrılarına sahip ana bilgisayar tabanlı bir saldırı tespit sistemi önerilmiştir.	Yazarlara göre, deney sonuçları izinsiz giriş tespitinin verimliliğinin arttığını göstermiştir. Önerilen yöntem, sistem çağrıları ile yeni nesil ana bilgisayar tabanlı saldırı tespit sistemlerinin tasarımına uygulanabilir.	2021
Park vd.	Leipzig Saldırı Tespiti Veri Kümesine (LID-DS) üzerinde uygulanan yeni bir yaklaşım önerilmiştir.	Doğruluk, kesinlik, geri çağırma ve F1 puanı göstergelerine göre önerilen Siamese-CNN modeli, vanilla-CNN modeline kıyasla yaklaşık %6'lık bir artış göstermiştir.	2021

Byrnes vd.'e göre, işletim sistemlerinin hızlı gelişimi ve bunun sonucunda ortaya çıkan karmaşıklık nedeniyle bazen onlarca yıllık veri kümeleri uzun süre kullanılmamaktadır. Bu çalışmada, en son Linux çekirdeği 5.7.0-rc1'yi inceleyerek teorik modeller ile

uygulama ortamları arasındaki boşluğu kapatmayı amaçlamışlardır. Bu ortam, modern işletim sistemlerinde sistem çağrısı tabanlı HIDS'in uygulanabilirliğini ve HIDS geliştiricisine uygulanan sınırlamaları inceler. Çekirdeğe yönelik son gelişmeler incelenmiştir ve veri üretmek ve algılama modelini geliştirmek için yeni bir yaklaşım önerilmiştir. Ayrıca, modellerin amaçlanan limitlerinde çalışması için karşılanması gereken belirli çalışma zamanı ve bellek kısıtlamalarını da sunmuştur.

Park vd., 2018'de oluşturulan ana bilgisayar tabanlı bir IDS veri kümesi olan Leipzig Saldırı Tespiti Veri Kümesi (LID-DS) üzerinde bir deney gerçekleştirmiştir. Sistemin performansını iyileştirmek için görüntü işleme, eğitim ve test adımları önerilmiştir. Eğitim ve test adımlarında, az miktarda veri kullanılarak yüksek performanslı birkaç adımdan oluşan bir öğrenme tekniği kullanılarak Siyam Evrişimli Sinir Ağı (Siamese-CNN) oluşturulmuştur. Siamese-CNN, görüntüye dönüştürülen her bir saldırı örneğinin benzerlik puanına göre saldırı türünü belirler. Performans değerlendirmesi için Vanilla Convolutional Neural Network (Vanilla-CNN) ve Siamese-CNN'nin performansı karşılaştırılmıştır. Doğruluk, kesinlik, F1 puanı göstergelerine göre önerilen Siyam-CNN modeli, vanilya-CNN modeline kıyasla yaklaşık %6'lık bir artış göstermiştir. Önerilen model, hiper parametre değerlerinin optimize edilmesiyle bilinen veya bilinmeyen siber saldırılar için saldırı tespit doğruluğunun artırılması üzerinde çalışılarak geliştirilebilir.

2.2.4.4 Ana bilgisayar tabanlı IDS'lerin değerlendirilmesi

Ana bilgisayar tabanlı IDS'ler tarafından algılanan saldırı türleri, sistemde kullanılan algılama tekniklerine bağlı olarak değişiklik gösterir. Bazı ana bilgisayar tabanlı IDS ürünleri, bu algılama tekniklerini birleştirirken, diğerleri birkaçına veya bir tanesine odaklanır. Ana bilgisayar tabanlı IDS'ler, ana bilgisayarların özellikleri ve yapılandırmaları hakkında ayrıntılı bilgiye sahip olduklarından, bir IDS aracısı, genellikle, bir ana bilgisayara yönelik bir saldırının durdurulmaması durumunda başarılı olup olmayacağını belirleyebilir.

Diğer IDS teknolojilerinde olduğu gibi, ana bilgisayar tabanlı IDS'ler de sıklıkla yanlış pozitiflere ve negatiflere neden olur. Ancak, tespitin doğruluğu, ana bilgisayar tabanlı IDS'ler için daha zor olabilir. Çünkü çoğu IDS, günlük analizi ve dosya sistemi izleme gibi algılanan olayların gerçekleştiği bağlamı bilmez. Örneğin, bir ana bilgisayar yeniden başlatılabilir veya yeni bir uygulama yüklenebilir ve bu eylemler kötü niyetli faaliyetler olabilir. Olayların kendileri doğru bir şekilde tespit edilir, ancak çoğu zaman ek bilgi olmadan normal mi yoksa saldırı mı oldukları belirlenemez. Birkaç algılama tekniğinin bir kombinasyonunu kullanan ana bilgisayar tabanlı IDS'ler, genellikle tek bir teknik kullananlardan daha doğru bir algılama oranı sağlayabilir. Her teknik, sunucunun farklı yönlerini izleyebildiğinden, daha fazla teknik kullanmak, gerçekleşen faaliyetler hakkında daha fazla bilgi toplamayı sağlar. Bu, olayların daha eksiksiz bir profilini sağlar ve ayrıca olayların amacının değerlendirilmesine yardımcı olacak ek bilgiler sağlayabilir.

2.3 Saldırı Tespit Metodolojileri

Saldırı tespit metodolojileri kullandıkları tespit yöntemlerine göre temel olarak üç farklı model olarak incelenmektedir:

1. İmza tabanlı model;
2. Anomali tabanlı model;
3. Durumsal protokol analizi.

Her IDS metodolojisi, ağ saldırılarını tanımlamak için farklı bir teknik kullanır. Bilinen saldırı türleri için imza tabanlı model oldukça hızlı ve etkilidir, ancak sıfır gün saldırılarını tanıyamaz. Anomali tabanlı model, daha önce görülmemiş ağ tabanlı saldırıları tespit etmede etkilidir, ancak yanlış alarmlara neden olur. Başka bir deyişle, normal trafiği saldırı olarak sınıflandırır. Durumsal protokol analizi yeni saldırıların bir kısmını tespit edebilirken, kaynak kullanımı yoğundur, karmaşıktır ve akıllı saldırıları tespit edemez. Her bir metodolojinin detayları aşağıda verilmiştir.

2.3.1 İmza tabanlı tespit (Signature-based detection)

İmza, bilinen bir saldırıya karşılık gelen bir kalıptır. İmza tabanlı tespit, potansiyel saldırıları tespit etmek için imzaları gözlemlenen olaylarla karşılaştırma sürecidir (Farshchi 2003). Karşılaştırma işleminde eşleşme olması durumunda sistem uyarı veya ek rapor verecektir. Bazı imza örnekleri şunlardır: Ağın güvenliğini tehdit eden "root" kullanıcı adıyla saldırı girişimi veya bilinen ve yaygın kötü amaçlı yazılımların ortak özelliği olan "Ücretsiz programlar" konulu bir e-posta.

İmza tabanlı algılama, en basit algılama yöntemidir, çünkü gözlemlenen olaylar, bir karşılaştırma işlemi kullanılarak bir imza listesine göre kontrol edilir. Listede daha önce tanımlanmış bir saldırı durumu varsa uyarı üretilir. İmza tabanlı IDS'ler bilinen tehditleri tespit etmede çok etkilidir, ancak bilinmeyen tehditleri veya bilinen tehditlerin türevlerini tespit etmede büyük ölçüde etkisizdir. Örneğin, bir saldırgan "prog.exe" adlı kötü amaçlı dosyayı "prog2.exe" adıyla değiştirirse, "prog.exe"yi arayan bir imza eşleşmeyecektir.

2.3.1.1 İmza tabanlı tespit alanında çalışmalar

İmza tabanlı IDS yöntemlerinin özeti, önerilen yöntemin ana fikri ve her bir çalışmanın başarısı Çizelge 2.5'de görülebilir.

Kumar ve Sangwan'ın çalışmasında, Snort kullanılarak imza tabanlı saldırı tespiti gerçekleştirilmiştir. Snort üzerinden Saldırı Tespiti yapılırken, DARPA Veri Kümesi ağ üzerinden aktarılmış ve iletim sırasında tespit edilen anormal bağlantıların analizine odaklanılmıştır. Snort, ağ paketlerini incelemek ve bunları bilinen saldırı imzalarından oluşan bir veritabanıyla karşılaştırmak için kullanılan popüler bir NIDS'dir. Ayrıca Snort saldırı imza veritabanı zaman zaman güncellenebilir. Bu IDS sistemi, gerçek zamanlı ağ trafiğindeki izinsiz girişleri tespit edip analiz edebildiğini göstermiştir. Yazarlara göre bu çalışma, yeni kullanıcıların Snort tabanlı IDS kavramını anlamalarına yardımcı olacaktır. Bu çalışma, farklı saldırı tespit araçları uygulanarak ve analiz edilerek de geliştirilebilir.

İmza tabanlı IDS'ler için en büyük zorluklardan biri, her paketin veritabanındaki her imzayla karşılaştırılması gerektiğinde büyük hacimli gelen trafiğin nasıl ele alınacağıdır. Uddin vd., mobil aracıları kullanan yeni bir İmza Tabanlı Çok Katmanlı IDS modeli önermiştir. Önerilen model, küçük ve çoklu veri tabanlarını dinamik ve otomatik olarak oluşturup kullanarak yüksek başarı oranıyla tehditleri tespit edebilmektedir. Ayrıca, mobil aracıları kullanarak bu küçük imza veritabanlarını periyodik olarak güncellemek için bir mekanizma sağlar. Önerilen model, çoklu IDS sistemlerinin veri tabanları arasında imza dağıtabilen, ekleyebilen ve kaldırabilen otomatik bir sistem olarak geliştirilebilir.

Hubbali ve Suryanarayanan imza tabanlı Ağ İzinsiz Giriş Tespit Sisteminde (NIDS) yanlış alarm oranını en aza indirmek için olası teknikler incelenmiştir. İmza tabanlı IDS'de yanlış alarm minimizasyon tekniklerinin bir sınıflandırması, avantajları ve dezavantajları verilmiştir. Ayrıca, performanslarıyla birlikte bu teknikleri uygulayan önde gelen Güvenlik Bilgileri ve Olay Yönetimi araçlarından birkaçı gözden geçirilir. Yazarlara göre, bilinen tüm tekniklere rağmen, hala ele alınması gereken sorunlar vardır. Bu çalışma, güvenlik araştırmacılarının IDS uyarıları için yeni işlem sonrası teknikleri uygulamalarına yardımcı olabilir. Gelecekteki araştırmalar, önerilen tekniklerin kullanılabilirliğini artıracak farklı araştırma konularını da ele almalıdır.

Rai vd. tarafından C4.5 karar ağacı yaklaşımına dayalı bir karar ağacı algoritması geliştirilmiştir. Özellik seçimi ve bölünmüş değer, bir karar ağacı oluşturmak için önemli hususlardır. Bu çalışmada, geliştirilen algoritma bu iki konuyu ele almak için tasarlanmıştır. Önerilen yöntem NSL-KDD veri seti üzerinde uygulanmış ve özellik sayısına göre deneye bağlı kalınmıştır. Modeli oluşturmak için geçen süre ve elde edilen doğruluk metrik olarak kullanılmıştır. Yazarlara göre, önerilen Karar Ağacı Bölme (DTS) algoritması, imza tabanlı saldırı tespiti için etkili bir yöntemdir. Bu çalışma, bölme değeri iyileştirilerek ve kullanılan özellik sayısı azaltılarak geliştirilebilir.

Aldwairi vd., imza tabanlı modelin eşleştirme yükünü azaltmayı ve imza eşleştirme algoritmasını çok çekirdekli bir CPU üzerinde paralel hale getirerek algoritmayı hızlandırmayı amaçlamaktadır. Bu yazıda, bir vektör algoritması olan Myers

algoritması, MapReduce çerçevesi altında çok çekirdekli bir CPU üzerinde paralelleştirilmiştir. Çok çekirdekli uygulama ile yaklaşık dört kat hızlanma sağlanmıştır. Ayrıca Myers algoritmasını paralelleştirmek için iki MapReduce uygulaması kullanılmıştır. Önerilen yöntemin uygulanması, algoritmanın bir önceki mesaj geçiş arayüzü (MPI) tabanlı uygulaması ile karşılaştırılır. Elde edilen sonuçlara göre Phoenix++ ve MAPCG MapReduce uygulamaları MPI'ye göre sırasıyla 1.3 ve 1.7 kat iyileşme göstermiştir.

Malek vd., bir dizi kural kullanarak saldırıları tespit etmek için yeni bir sistem önermiştir. Daha önce uygulanan SBID (İstatistiksel Tabanlı Saldırı Tespiti) modelini doğrulayan bir PBID (Pattern Based Intrusion Detection) modeli kullandılar. Önerilen model, çalışma kapsamında üretilen veri seti üzerinde test edilmiştir. %75 doğruluk oranı elde edilmiştir. Yazarlara göre, SBID ve PBID yaklaşımlarının kombinasyonu saldırıların tespiti için kapsamlı bir sistem sağlar. Ancak sadece imza tabanlı saldırı tespiti ile etkili bir sonuç alınamaz. Bu nedenle, bu çalışma, anomali tabanlı saldırı tespiti entegre edilerek daha da geliştirilebilir.

Otoum ve Nayak, IoT ağlarındaki bilinen ve bilinmeyen saldırıları tespit etmek için iki yaklaşımı birleştiren AS-IDS olarak isimlendirilmiş bir saldırı tespit modeli önermektedir. Önerilen model üç aşamadan oluşmaktadır: trafik filtreleme, ön işleme ve hibrit IDS. İlk aşamada, ağ trafiği, IoT ağ geçidinde paket özellikleri eşleştirilerek filtrelenir, ardından ön işleme aşamasında sırasıyla bir Hedef Kodlayıcı, Z-skor ve Ayrık Hessian Eigenmap (DHE- Discrete Hessian Eigenmap) uygulanmıştır. Son aşamada, imza tabanı ve anomali tabanlı model birleştirilmiştir. İmza tabanlı sistem kısmında, Genelleştirilmiş Sonek Ağacı (Generalized Suffix Tree-GST) algoritması kullanılmıştır ve saldırıların normal veya bilinmeyen olarak sınıflandırılması için imzalar eşleştirilir. Anomali tabanlı sistem bölümünde, bilinmeyen saldırıları belirlemek için Derin Q-öğrenme yöntemi uygulanmıştır ve saldırıları sınıflandırmak için Sinyal Gürültü Oranı (SNR) ve bant genişliği kullanılmıştır. Önerilen AS-IDS modeli, NSL-KDD veri seti ile gerçek zamanlı trafikte uygulanmış ve test edilmiştir. %96,9'luk bir saldırı tespit oranı elde edilmiştir. Bu çalışma farklı veri kümeleri üzerinde uygulanarak daha kapsamlı deneysel sonuçlar elde edilebilir.

Çizelge 2.5 İmza tabanlı IDS çalışmalarının özeti

Makale	Önerilen Yöntem	Sonuç	Yıl
Kumar ve Sangwan	Snort kullanılarak imza tabanlı saldırı tespiti yapılmıştır.	Bu sistem, gerçek zamanlı ağ trafiğindeki saldırıları tespit ve analiz edebilmektedir. Bu çalışma, yeni kullanıcıların Snort tabanlı IDS kavramını anlamalarına yardımcı olmaktadır.	2012
Uddin vd.	Mobil ajanları kullanan yeni bir İmza Tabanlı Çok Katmanlı IDS modeli önerilmiştir.	Önerilen model, yüksek bir başarı oranı ile tehditleri tespit edebilmektedir. Ayrıca, küçük imza veritabanlarını periyodik olarak güncellemek için mekanizma sağlamaktadır.	2013
Hubbali ve Suryanarayanan	İmza tabanlı, ağ saldırı tespit sistemlerinde yanlış alarm oranını en aza indirmek için olası teknikler incelenmiştir.	Bilinen tüm tekniklere rağmen, hala ele alınması gereken sorunlar vardır.	2014
Rai vd.	C4.5 karar ağacı yaklaşımına dayalı bir karar ağacı algoritması sunulmuştur.	Önerilen Karar Ağacı Bölme algoritması, imza tabanlı saldırı tespiti için etkili bir yöntemdir.	2016
Aldwairi vd.	MapReduce çerçevesi altında çok çekirdekli bir CPU üzerinde bir vektör algoritması paralelleştirilmiştir.	Phoenix++ ve MAPCG MapReduce uygulamaları MPI'ye göre sırasıyla 1.3 ve 1.7 kat iyileştirme göstermiştir.	2017
Baykara ve Das	Saldırı tespit/önleme sistemleri için bal küpü tabanlı bir yaklaşım önerilmiştir.	Geliştirilen sistem sunucular üzerindeki ağ trafiğini gerçek zamanlı animasyon ile görsel olarak gösterebilmektedir. Sıfır gün saldırısını tespit edebilir. Aynı zamanda IDS'lerdeki yanlış pozitif seviyenin azaltılmasına da yardımcı olur.	2018
Baykara ve Das	Merkezileştirilmiş bir bal küpü tabanlı yaklaşım önerilmiştir.	Önerilen sistem GNS3 simülasyon yazılımında çalıştırılmış ve yanlış alarm seviyesi, ağ trafiği ve siber güvenlik maliyeti düşürülerek iyi sonuçlar elde edilmiştir.	2019
Gunduz ve Das	IoT tabanlı akıllı şebekenin amaçları, gereksinimleri, tehditleri ve potansiyel çözümleri analiz edilmiştir.	Makale, IoT tabanlı akıllı şebeke uygulamaları üzerindeki tehditlere özel çözümler sunar ve araştırmacıların gelecekteki araştırma yönergelerini sağlamaları için olası araştırma fırsatlarını vurgular.	2020
Malek vd.	İzinsiz girişleri tespit etmek için bir dizi kural çıkarımı yapan, pattern tabanlı yeni bir sistem önerilmiştir.	SBID ve PBID yaklaşımlarının kombinasyonu, saldırı tespiti için kapsamlı bir sistem sağlamaktadır.	2020
Otoum ve Nayak	AS-IDS olarak isimlendirilmiş bir saldırı tespit modeli önerilmiştir.	NSL-KDD veri setinde %96,9 saldırı tespit oranı elde edilmiştir.	2021

2.3.1.2 İmza tabanlı IDS'lerin değerlendirilmesi

İmza tabanlı tespit, en basit tespit yöntemidir ve anlaşılması kolaydır. Sistem, paketler veya günlük girişleri gibi etkinlikleri bir kayıtlı imza listesiyle karşılaştırır. Böylece

kullanıcılar imza veritabanını kontrol edebilir ve sistem yöneticisi hangi saldırı türlerinin alarma neden olacağını kolaylıkla anlayabilir. İmza tabanlı IDS'ler bilinen saldırıları tespit etmede çok etkilidir, ancak önceden bilinmeyen tehditleri, gizlenen tehditleri ve bilinen tehditlerin herhangi bir çeşidini tespit etmede etkili bir şekilde başarılı değildir. Başarı oranının yüksek olması için bir saldırganın yapabileceği tüm saldırılar için ayrı bir imza tanımlanmalı ve imza veritabanının güncel tutulması gerekmektedir.

2.3.2 Anomali tabanlı tespit (Anomaly-Based detection)

Anomali tabanlı tespit, anormal olayları tanımlamak için gözlemlenen aktiviteleri normal kabul edilen tanımlarla karşılaştırma sürecidir (Samrin ve Vasumathi 2017). Anomali tabanlı algılama sistemi kullanan bir IDS, kullanıcıların, ana bilgisayarların, ağ bağlantılarının veya uygulamaların normal davranışını temsil eden kurallara sahiptir. Bu kurallar, belirli bir süre boyunca olağan faaliyetlerin özellikleri takip edilerek geliştirilir. Örneğin, iş günü saatlerinde web etkinliğinin ortalama kullanım süresidir bir kuraldır. IDS, web etkinliğinin beklenenden önemli oranda yüksek kullanımını tespit etmek ve mevcut etkinliğin özelliklerini kurallarla karşılaştırırken uyarılar oluşturmak için istatistiksel yöntemler kullanır. Bir kullanıcı tarafından gönderilen e-postaların sayısı, başarısız oturum açma girişimlerinin sayısı ve belirli bir zaman diliminde aktarılan paketlerin sayısı gibi birçok davranışsal nitelik için kurallar geliştirilebilir. Anomali tabanlı tespit yöntemlerinin en önemli avantajı, önceden bilinmeyen saldırı tiplerini tespit etmede etkili olmalarıdır. Örneğin, bir bilgisayara yeni bir tür kötü amaçlı yazılım bulaştığını varsayalım. Kötü amaçlı yazılım, bilgisayarın işleme kaynaklarını tüketebilir, çok sayıda e-posta gönderebilir, birçok ağ bağlantısı başlatabilir ve bilgisayar için oluşturulan normal profillerden önemli ölçüde farklı olabilecek diğer davranışlarda bulunabilir.

Anomali tabanlı tespit için oluşturulan kurallar iki türdür: statik ve dinamik. Bir kez oluşturulduktan sonra, IDS yeni bir kural oluşturmaya yönlendirilmedikçe statik kural listesi değişmez. Dinamik liste ise ek olaylar gözlemlendikçe sürekli olarak güncellenir. Sistemler ve ağlar zamanla değiştikçe, karşılık gelen normal davranış ölçüleri de

değişir. Statik bir liste sonunda sona erer, bu nedenle periyodik olarak yenilenmesi gerekir. Dinamik profillerde bu sorun yoktur, ancak saldırganlar tarafından ele geçirme girişimlerine karşı hassastırlar. Örneğin, bir saldırgan az miktarda kötü amaçlı etkinlik gerçekleştirebilir, ardından etkinlik sıklığını ve miktarını yavaş yavaş artırabilir. Değişim hızı yeterince yavaşsa, IDS kötü niyetli etkinliği normal davranış olarak görebilir ve profiline dahil edebilir. Kuralın bir parçası olarak kötü niyetli etkinliklerin yanlışlıkla dahil edilmesi, anomali tabanlı IDS ürünlerinde yaygın bir sorundur.

Anormali tabanlı IDS'lerle ilgili bir diğer sorun, bazı durumlarda kuralları doğru belirlemenin zor olabilmesidir. Örneğin, büyük dosya aktarımları gerçekleştiren bir olay ayda yalnızca bir kez meydana gelirse, bu davranış sürekli olarak gözlemlenmez, bu nedenle anormal bir durum olarak kabul edilebilir ve bir uyarı tetiklenebilir. Anomali tabanlı IDS ürünleri, özellikle farklı veya dinamik ortamlarda, kurallardan önemli ölçüde sapan iyi huylu etkinlik nedeniyle çoğu zaman birçok yanlış pozitif üretir.

2.3.2.1 Anomali tabanlı tespit alanında çalışmalar

Anomali tabanlı tespit yöntemlerine ilişkin literatür taraması Çizelge 2.6'da özetlenmiştir. Her bir makalenin ana fikri, artıları ve eksileri özetlenmiştir.

Geramiraz vd., yanlış alarmların sayısını azaltmak ve verimliliği artırmak için anomali tabanlı bir saldırı tespit sistemi sunmuştur. Bulanık kural tabanlı modelleme ve bulanık denetleyici, sırasıyla oluşturma ve test aşamasında modeli güncellemek için kullanılmıştır. Ayrıca sistem tahminlerinin sonuçları sistem kullanıcısına sunulmaktadır. Ardından sistem kullanıcısı kararları doğrular ve bulanık denetleyici, sistem kullanıcısının geri bildirimini kullanarak algılama modelini ayarlar. Sistemin değerlendirilmesinde NCL veri seti kullanılmıştır. Veri kümesi, KDD'99 veri kümesinin bir alt kümesidir. Yazarlara göre, test sonuçları, uyarlanabilir IDS kullanarak sistemin performansını yaklaşık %20 oranında iyileştirmiştir. Ek olarak, önerilen anomali tabanlı saldırı tespiti, sistemin doğruluğunu yaklaşık %15 oranında iyileştirmiştir.

Yasin vd., yanlış alarmı en aza indirirken algılama ve doğruluğu en üst düzeye çıkarmak için K-Means kümelemesine ve Naive Bayes Sınıflandırıcısına (Naive Bayes Classifier -NBC) dayalı, KMC+NBC olarak isimlendirilmiş entegre bir makine öğrenme algoritması önermektedir. Etiketleme işlemine K-Means kümelemesi uygulanmıştır. Tüm veriler K-Means ile davranışlarına göre normal ve saldırı olarak kümelerinde toplanırken, Naive Bayes Sınıflandırıcısı yanlış sınıflandırılan verileri doğru kategorilere yeniden kategorize etmek için kullanılır. KMC+NBC ve NBC'nin performans değerlendirmeleri ISCX-2012 veri seti üzerinde yapılmıştır. Elde edilen sonuçlara göre KMC+NBC, doğruluğu ve algılama oranını sırasıyla %99 ve %98,8'e kadar artırırken, yanlış alarmı %2,2'ye indirmiştir. Bu çalışma, öznitelik seçim yöntemlerini içerecek şekilde daha da genişletilebilir.

Narsingyani ve Kale, ağ saldırı tespiti için makine öğrenmesinde en etkili evrimsel tekniklerden biri olan Genetik algoritma (GA) tabanlı anomali tespit tekniğini uygulamışlardır. Yanlış pozitif oranının azalması aynı zamanda doğruluğu ve performansı da artıracağından, bu çalışma özellikle yanlış pozitif oranının optimizasyonuna odaklanmıştır. Yanlış pozitif oranları için diğer doğruluk tekniklerinin sınırlaması bu yazıda tartışılmaktadır. Deneyler için KDD99cup veri seti kullanıldı. Elde edilen sonuçlara göre uygun özellik seçimi kullanılarak Yanlış Pozitif alarm oranı düşürülebilir ve algılama hızı arttırılabilir. Bu çalışma, daha önemli özelliklerin seçimi için dinamik özellik seçim teknikleri kullanılarak geliştirilebilir.

Harish ve Kumar, bulanık kümelemeye dayalı ağdaki anormallikleri tespit etmek için anomali tabanlı bir yöntem önermiştir. Önerilen yöntem üç aşamadan oluşmaktadır: Ön İşleme, Özellik Seçimi ve Kümeleme. Ön işleme aşamasında, veri setinden tekrarlı veriler elimine edilmiştir. Daha sonra ayırt edici özellikleri seçmek için temel bileşenler analizi uygulanmıştır. Kümeleme adımında ağ örnekleri, RSKFCM (Robust Spatial Kernel Fuzzy C-Means) algoritması kullanılarak kümelenmiştir. RSKFCM, komşuluk bilgisini hesaba katan ve çekirdek mesafesi metriğini kullanan standart Bulanık C-Ortalamaların bir varyasyonudur. Önerilen yöntemi değerlendirmek için KDD veri setinin bir varyantı olan EDA veri seti kullanılmış ve literatürdeki standart tekniklerle karşılaştırılmıştır. Performans ölçütleri olarak doğruluk, yanlış pozitiflik oranı ve küme

geçerlilik indeksleri kullanılmıştır. %86,3 doğruluk ve %17,04 yanlış alarm oranı elde edilmiştir. Yazarlara göre önerilen yöntem diğer yöntemlere göre daha iyi sonuçlar vermiştir. Ancak bu çalışma Evrimsel algoritma gibi farklı yöntemler kullanılarak geliştirilebilir.

Aljawarneh vd., izinsiz giriş kapsama eşiğini tahmin etmek için ağ işlem verilerinin optimal özelliklerine dayanan yeni bir hibrit model geliştirmiştir. Önerilen modelin değerlendirilmesinde %20 test veri seti ve ikili ve çok sınıflı bir problem olan NSL-KDD veri seti kullanılmıştır. Elde edilen sonuçlara göre, öznitelik ilişkilendirme etki ölçeğini belirlerken hesaplama ve zaman maliyetini en aza indirmede hibrit yaklaşım önemli bir etkiye sahiptir. Çift sınıflı ve çok sınıflı NSL-KDD veri setleri için sırasıyla %99.81 ve %98.56 doğruluk oranı elde edilmiştir. Bunun yanında yüksek yanlış negatif ve yanlış pozitif oranı problemleri vardır. Bu sorunların ele alınmasında iki ana bölümden oluşan hibrit bir yaklaşım önerilmiştir. İlk olarak, önerilen modelin doğruluğunu artıracak önemli özniteliklerin seçimi için olasılık dağılımlarını birleştiren Bilgi Kazancı ve Oylama (Information Gaind and Vote) algoritması kullanılmıştır. Daha sonra hibrit algoritmada AdaBoostM1, REPTree, J48, Random Tree, Naïve Bayes, Meta Pagging ve Decision Stump sınıflandırma algoritmaları kullanılmıştır. Sonuç olarak, artan doğruluk, yüksek yanlış negatif oranı ve düşük yanlış pozitif durumu gözlemlendi. Önerilen yöntemin farklı veri kümeleri üzerinde farklı optimizasyon teknikleri ile uygulanmasıyla bu çalışma daha da geliştirilebilir.

Tama vd., ilgili özniteliklerin seçimi için bir yöntem ve iki seviyeli sınıflandırıcılar topluluğuna dayalı bir saldırı tespit sistemi önerilmiştir. Eğitim veri setlerinin öznitelik boyutunu azaltmak için parçacık sürü optimizasyonu (particle swarm optimization), and, karınca kolonisi algoritması (ant colony algorithm) ve genetik algoritma (genetic algorithm) olmak üzere 3 farklı yöntem kullanılmıştır. Özellikler, azaltılmış bir hata budama ağacı (REPT- reduced error pruning tree) kullanılarak sınıflandırma performansına göre seçilir. Daha sonra iki seviyeli bir sınıflandırıcı grubu olan döndürme ormanı (rotation forest) ve torbalama yöntemleri (bagging methods) uygulanmıştır. Önerilen sistemi değerlendirmek için NSL-KDD ve UNSW-NB15 veri setleri kullanılmıştır. NSL-KDD veri setinde %85,8 ve UNSW-NB15 veri setinde

%91,3 doğruluk oranı elde edilmiş ve yazarlara göre yakın zamanda önerilen diğer sınıflandırma tekniklerini önemli ölçüde geride bırakmıştır. Bu çalışma, daha az özellik kullanarak daha yüksek doğruluk elde edebilen yeni yaklaşımlarla daha da geliştirilebilir.

Çizelge 2.6 Anomali tabanlı IDS çalışmalarının özeti

Makale	Önerilen Yöntem	Sonuç	Yıl
Geramiraz vd.	Anomali tabanlı saldırı tespit sistemi önerilmiştir.	Ssistemin performansı yaklaşık %20 oranında iyileştirilmiştir. Önerilen anomali tabanlı saldırı tespiti, sistemin doğruluğunu yaklaşık %15 oranında iyileştirmiştir.	2012
Yassin vd.	K-Means kümelemeye ve Naive Bayes Sınıflandırıcısına (KMC+NBC) dayalı entegre bir makine öğrenimi algoritması sunulmuştur.	ISCX-2012 veri seti üzerinde performans değerlendirmeleri yapılmıştır. KMC+NBC, yanlış alarm oranını %2,2'ye düşürürken, doğruluğu ve algılama oranını sırasıyla %99 ve %98,8'e çıkarmıştır.	2013
Narsingyani ve Kale	Genetik algoritma tabanlı anomali tespit tekniği önerilmişir.	KDD99cup veri seti kullanılmış ve sonuçlara göre yanlış pozitif alarm oranı düşürülebilir ve algılama hızı arttırılabilir.	2015
Harish ve Kumar	Bulanık kümelemeye dayalı anomali tabanlı bir yöntem önerilmişir.	KDD veri setinin bir varyantı olan EDA veri seti kullanılmıştır.%86,3 doğruluk ve %17,04 yanlış alarm oranı elde edilmiştir.	2017
Aljawarneh vd.	Yeni hibrit bir model önerilmişir.	İkili ve çok sınıflı NSL-KDD veri setleri için sırasıyla %99.81 ve %98.56 doğruluk oranı elde edilmiştir.	2018
Tama vd.	İlgili özelliklerin seçimi için bir yöntem ve iki seviyeli sınıflandırıcılar topluluğuna dayalı bir saldırı tespit sistemi önerilmiştir.	NSL-KDD veri setinde %85,8 ve UNSW-NB15 veri setinde %91,3 doğruluk oranı elde edilmiştir.	2019
Viegas vd.	Büyük paket hızlarına ölçeklenebilen, gelişen ağ trafiğini işleyebilen BigFlow isimli bir IDS yaklaşımı önerilmiştir.	Tam bir yılı kapsayan bir ağ trafiği veri seti üzerinde deneyler yapılmıştır. BigFlow, zaman içinde yüksek doğruluğu koruyabilmiştir. Diğer yaklaşımlarla karşılaştırıldığında, %4 kadar az depolama ve %0,05 ile %4 arasında eğitim süresi gerektirmiştir.	2019
Dwivedi vd.	EFSAGOA olarak adlandırılan, Özellik Seçimi ve Uyarlanabilir Optimizasyon Algoritmalarını birleştiren yeni bir teknik önerilmiştir.	EFSAGOA, ISCX 2012 veri seti üzerinde değerlendirilmiştir. %99,23 tespit oranı, %99,13 doğruluk ve 0,067 yanlış alarm oranı elde edilmiştir.	2020
Eskandari vd.	Passban adı verilen anomali tabanlı akıllı saldırı tespit sistemi önerimiştir.	Passban, saldırıları düşük yanlış pozitif ve yüksek doğruluk oranlarıyla tespit edebilir.	2020
Kumar vd.	Mevcut bulut tabanlı güvenlik mimarisini yerel fog düğümlerine dağıtan, anomali tabanlı bir saldırı tespit sistemi önerilmiştir.	Önerilen model, gerçek bir IoT tabanlı veri kümesi kullanılarak test edilir. Temel yaklaşımın değerlendirilmesi, Random Forest algoritması kullanılarak yüksek algılama doğruluğu ve düşük yanlış alarm oranı açısından iyi performans göstermiştir.	2021

İskenderiye vd., Passban adı verilen ve kendisine doğrudan bağlı olan IoT cihazlarını koruyabilen, anormallik tabanlı bir akıllı saldırı tespit sistemi önermektedir. Önerilen sistemin özelliği, doğrudan uygun maliyetli IoT ağ geçitlerine dağıtılabilmesidir. Bu özellik sayesinde, siber tehditleri veri kaynaklarına mümkün olduğunca yakın tespit etmek için uç bilgi işlem paradigmasından tam olarak yararlanabilir. Passban değerlendirme aşamasında iki farklı senaryo uygulanmıştır. İlk senaryoda Passban, IoT cihazlarından ve internetten veri alan ağ geçidinde doğrudan çalışan bir IDS olarak kullanılmıştır. İkinci senaryoda, altyapı öğesi olarak internetten ve yerel ağ geçidinden trafik alan özel bir cihaz olan "kutudaki güvenlik (security in the box)" kullanılır. Değerlendirme sonuçlarına göre Passban birçok saldırı türünü düşük yanlış pozitif ve yüksek doğruluk oranları ile tespit edebilmektedir.

2.3.2.2 Anomali tabanlı IDS'lerin değerlendirilmesi

Anomali tabanlı algılama, farklı durumları belirlemek için trafiği normal kabul edilenlerle karşılaştırma ilkesine dayanır. Anomali tabanlı saldırı tespit sistemleri, bir saldırıyı tespit etmek için önceden saldırı imzası bilgisi gerektirmediğinden, imza tabanlı sistemlerden daha iyi bir seçenek olarak kabul edilir. Ancak aynı zamanda, bu sistem tarafından üretilen alarmları yönetmek, imza tabanlı saldırı tespit sistemlerine göre daha zordur. Bunun nedeni, imza tabanlı IDS'nin bildirilen alarmlarla birlikte bilgi üretmesi ve anomali tabanlı IDS'nin kötü amaçlı olarak algılanan trafik akışını tanımlaması olabilir.

Anormallik tabanlı IDS, normal davranışın temel modelinden sapan bir aktivite tespit ettiğinde bir alarm üretir, ancak anormalliğin nedeni izinsiz giriş tespit sistemi tarafından bilinmez. Bu, alarmları yönetmede ve yanlış pozitifleri gerçek alarmlardan ayırt etmede büyük bir zorluk haline gelir. Bu nedenle anomali tabanlı tespit sistemleri bilinmeyen saldırıları tespit edebilirken, tespit edilen bir saldırının sınıflarını belirlemek de önemlidir.

2.3.3 Durumsal protokol analizi

Durumsal protokol analizi, her bir protokol durumu için genel kabul görmüş normal (benign) protokol aktivite tanımlarının, önceden belirlenmiş profillerden sapmalarını tanımlamak için gözlenen olaylarla karşılaştırılmasıdır. Ana bilgisayar veya ağa özgü profilleri kullanan anomali tabanlı tespitin aksine, durum bilgisi protokolü, belirli protokollerin nasıl kullanılması ve kullanılmaması gerektiğini belirten, sağlayıcı tarafından geliştirilen evrensel profillere dayanır. Durumsal protokol analizindeki, "durum bilgisi", IDS'nin ağın, ulaşım ve uygulama protokollerinin durumunu anlama ve takip etme yeteneğine sahip olduğu anlamına gelir. Örneğin, bir kullanıcı bir Dosya Aktarım Protokolü (FTP) oturumu başlattığında, oturum başlangıçta doğrulanmayan durumda olur. Kimliği doğrulanmamış kullanıcılar, bu durumda yalnızca yardım bilgilerini görüntüleme veya kullanıcı adlarını ve şifrelerini sağlama gibi birkaç komut gerçekleştirmelidir. Anlama durumunun önemli bir kısmı, istekleri cevaplarla eşleştirmedir, bu nedenle bir FTP kimlik doğrulama girişimi gerçekleştiğinde, IDS, karşılık gelen yanıtta durum kodunu bularak başarılı olup olmadığını belirleyebilir. Kullanıcı başarıyla doğrulandıktan sonra, oturum doğrulanmış durumdadır ve kullanıcıların komutlardan herhangi birini gerçekleştirmesi beklenir. Bu komutların çoğunun doğrulanmayan bir durumda gerçekleştirilmesi şüpheli kabul edilirken, kimliği doğrulanmış durumda bunların çoğunun gerçekleştirilmesi normal kabul edilir.

Durumsal protokol analizi yöntemleriyle gerçekleştirilen "protokol analizi" genellikle bağımsız komutlar için minimum ve maksimum uzunluklar gibi denetimler içerir. Bir komutun tipik olarak bir kullanıcı adı argümanı varsa ve kullanıcı isimleri maksimum 20 karakter uzunluğundaysa, 1000 karakter uzunluğunda bir argüman şüphelidir. Durumsal protokol analizi yöntemleri, genellikle yazılım sağlayıcılarının ve standart kuruluşlarının standartlarına dayanan protokol modelleri kullanır. Protokol modelleri ayrıca her protokolün uygulanmasındaki değişiklikleri de dikkate alır. Pek çok standart, uygulamalar arasında değişikliklere neden olan protokolün detaylarını tam olarak açıklayamamıştır. Ayrıca, özel protokoller için, protokoller hakkında eksiksiz bilgi çoğu zaman mevcut değildir ve bu durum IDS teknolojilerinin kapsamlı ve doğru analizler yapmasını zorlaştırır.

2.3.3.1 Durumsal protokol analizi alanında çalışmalar

Durumsal protokol analizinin özeti Çizelge 2.7'de verilmiştir. İlgili çalışmalar, ana fikir, önerilen yöntem, her bir tespit yönteminin artıları ve eksileri göz önünde bulundurularak incelenmiştir.

Mudzingwa vd. saldırı tespit ve önleme sistemlerinde kullanılan dört ana tekniğin ayrıntılı bir incelemesini sunmuştur. Bunlar anomali tabanlı, imza tabanlı, durumsal protokol analizi ve hibrit tabanlı tekniklerdir. Her metodolojinin ayrıntılı bir açıklaması ve bu metodolojilerin bir karşılaştırması verilmiştir. Bu karşılaştırmaların sonuçlarına göre, anomali tabanlı metodoloji, kullanıcılar için herhangi bir güncelleme veya girdi olmaksızın yeni tehditleri tespit etmede diğer tekniklerden üstündür, ancak mevcut IDPS'lerin çoğu, ana metodolojilerin bir kombinasyonunu kullanır. Yöntemlerin bir kombinasyonunu kullanan sistemlerde, uygun metodoloji ve sistemi seçmeye çalışırken bazı karışıklıklar olabilir. Özetle, yazarlar piyasada IDPS ürünleri tarafından kullanılan metodolojilerini ve karşılaştırmalarını sundular. Ayrıca bu çalışmayı geliştirmek için piyasada kullanılan sistemlerin testleri de verilebilir.

Son zamanlarda birçok mobil VoIP uygulaması piyasaya sürüldü ve saldırganlar için çekici hedefler haline geldiler. Özellikle çağrı prosedürlerini ve sistem kaynaklarını hedef alan saldırılar üzerine yoğunlaşmışlardır. Seo vd., hatalı biçimlendirilmiş SIP (Session Initiation Protocol) mesajlarını ve SIP sel saldırılarını tespit etmek için optimize edilmiş, SIPAD olarak adlandırılmış durum bilgisi olan bir inceleme mekanizması önermişlerdir. Mevcut duruma ve mesaj tipine bağlı olarak SIPAD durum bilgisi olan kural ağacından ilgili dallar belirlenir ve bir SIP mesajının yapısı dallarla karşılaştırılır. Optimize edilmiş kural ağacı mevcut yaklaşımlardan daha yüksek algılama doğruluğu ve hız sağlar. Geleneksel SIP şemaları, kural eşleştirme mekanizmalarının karmaşıklığı nedeniyle maliyetlidir. Yazarlara göre, önerilen optimize edilmiş yaklaşım, işletim maliyetini önemli ölçüde azaltır ve akıllı telefonlar gibi kaynak kısıtlı ortamlarda bile kullanılabilir. Bu çalışma sadece iki saldırı tipi için değil, farklı saldırı tiplerinin tespiti için de geliştirilebilir.

Denetleyici Kontrol ve Veri Toplama (SCADA-Supervisory Control and Data Acquisition) sistemlerindeki siber tehditler, güç sisteminin çalışmasına fiziksel olarak zarar verme ve kesintiye uğratma potansiyeline sahiptir. SCADA gereksinimlerini karşılayacak sağlam bir saldırı tespit sisteminin nasıl geliştirileceği, ortaya çıkan sorunlardan biridir. Yang vd., IEC 60870-5-104 protokolünü kullanarak SCADA sistemlerinin güvenliğini artırmak için Derin Paket Denetimi yöntemini kullanan durum bilgisi olan bir Saldırı Tespit Sistemi önermiştir. IEC 608705-104 protokolü için özel olarak tasarlanmış, durum bilgisi olan bir protokol analizi yaklaşımı sunulmuştur. Son olarak, yeni saldırı tespit yaklaşımı test edilmiş ve doğrulanmıştır.

Akıllı şebeke sistemleri, cihazları ve hizmetleri için bir dizi uygulama protokolü kullanır. Bu uygulama protokollerindeki bilgiler, önemli güvenlik çözümleri olan saldırı tespit sistemleri için kullanışlıdır. Durum analizine dayalı saldırı tespit sistemlerinde ağ ve sistem davranışları izlenir ve tespit kararlarının verilebilmesi için olay kayıtları tutulur. Akıllı şebeke sistemlerinde bu davranışların izlenmesi, uzman bilgisi ve özel uygulama protokolleri için adaptasyon gerekir. Bu çalışmada, Kang vd., Suricata'da çalıştırılabilen akıllı şebeke saldırılarını tespit etmek için durum bilgisi olan kuralları tanımlamasına izin veren bir çerçeve sunar. Durum bilgisi olan bir kural, akıllı şebeke cihazlarının durumunu tanımlar ve herhangi bir eşleşme bulmak için gelen ağ trafiğini inceler. Ayrıca, önerilen çerçevenin uygulanmasını göstermek ve IEC 61850 durum bilgisi analizi için bir uygulama geliştirilmiştir. Sunulan test ortamı ile yapılan deneyde, tehlikeli durumlar yaratabilecek saldırıların önerilen çerçeve tarafından tespit edilebileceği iddia edilmektedir. Bu çalışma, akıllı şebeke sistemleri için diğer uygulama protokolleri işlevleri eklenerek geliştirilebilir.

Boite vd., uç ana bilgisayarları DDoS saldırılarından korumak için durum bilgisi olan paradigmayı temel alır. DDoS saldırılarını tespit etmek ve azaltmak için, anahtar içi işleme yeteneklerine dayanan StateSec adlı yeni bir yaklaşım önerilmiştir. StateSec, yapılandırılabilir trafik özellikleri sayesinde denetleyiciye danışmadan eşleşen paketleri izleyebilmektedir. StateSec, entropi tabanlı bir algoritmayı bu şekilde izleme özellikleriyle besleyerek, DDoS ve port taramaları gibi çeşitli saldırıları yüksek doğrulukla tespit eder ve azaltır. StateSec'in uygulanması, SDN'deki trafiği izlemeye

yönelik yeni bir teknoloji yaklaşımı olan sFlow ile karşılaştırılmıştır ve yazarlara göre StateSec daha verimlidir. Ayrıca çok hassas bir algılama düzeyine sahiptir. Bu çalışma, farklı saldırı türlerinin tespiti için geliştirilebilir.

Çizelge 2.7 Durumsal protokol analizi çalışmalarının özeti

Makale	Önerilen Yöntem	Sonuç	Yıl
Mudzingwa ve Agrawal	Saldırı tespit ve önleme sistemlerinde kullanılan ana tekniklerin ayrıntılı bir incelemesi yapılmıştır.	Anomali tabanlı teknik, diğer tekniklerden üstündür, ancak IDPS'lerin çoğu, ana metodolojilerin bir kombinasyonunu kullanır. Ancak yöntemlerin bir kombinasyonu için uygun metodoloji ve sistemi seçmeye çalışırken bazı karışıklıklar olabilmektedir.	2012
Seo vd.	SIPAD adı verilen durum bilgisi olan bir SIP inceleme mekanizması önerilmiştir.	Önerilen yaklaşım, maliyeti önemli ölçüde azaltmaktadır. Akıllı telefonlar gibi kaynakları kısıtlı ortamlarda bile kullanılabilmektedir.	2013
Yang vd.	Derin Paket Denetimi yöntemini kullanan, durum bilgisi olan bir Saldırı Tespit Sistemi önerilmiştir.	IEC 60870-5-104 protokolü için özel olarak tasarlanmış bir yaklaşımdır. Bu saldırı tespit yaklaşımı test edilmiş ve doğrulanmıştır.	2014
Kang vd.	Akıllı şebeke saldırılarını tespit etmek için bir yöntem önerilmiştir.	Tehlikeli durumlar yaratabilecek saldırılar etkin bir şekilde tespit edilebilmiştir.	2016
Boite vd.	StateSec olarak adlandırılan durum bilgisi olan paradigma önerilmiştir.	StateSec, DDoS ve port taramaları gibi çeşitli saldırıları yüksek doğrulukla algılamakta ve azaltmaktadır.	2017
Lewis vd.	P4ID olarak adlandırılan bir filtreleme yaklaşımı sunulmuştur.	Bu sistem, CICS2017 veri seti ve Emerging Threats kural seti birleştirilerek değerlendirilmiştir. Önerilen IDS tarafından işlenen trafikte önemli bir azalma sağlanabilmiştir.	2019
Sharma vd.	IoT'ye gömülü siber-fiziksel sistemler için davranış tabanlı bir saldırı algılama sistemi (BRIoT) önerilmiştir.	Önerilen yaklaşım, insansız bir hava aracına gömülü bir sistem tarafından doğrulanmıştır. Önerilen modelin uygulanabilirliği, mevcut kural tabanlı çözümlere kıyasla yüksek güvenilirlik, düşük işletme maliyeti, düşük yanlış pozitif, düşük yanlış negatif ve yüksek doğru pozitif ile gösterilmiştir.	2019
Rashid vd.	NSL-KDD ve CIDDS-001 veri kümelerinin kapsamlı ve karşılaştırmalı bir analizi sunulmuştur.	k-NN, SVM, NN ve DNN sınıflandırıcıları NSL-KDD veri setinde yaklaşık %100 doğruluğa; k-NN ve Naïve Bayes sınıflandırıcıları CIDDS-001 veri setinde yaklaşık %99 doğruluğa sahiptir.	2020
Sbai ve Elboukhari	DDoS'un alt sınıfı olan sel saldırılarını tespit etmek için derin sinir ağı tabanlı bir teknoloji önerilmiştir.	Önerilen model, CICDDoS2019 veri kümesi üzerinde değerlendirilmiştir. Elde edilen sonuçlara göre, önerilen mimari model iyi bir performans (Doğruluk, Kesinlik, Geri Çağırma ve F1-puanı açısından) göstermiştir.	2020
Choudhary ve Kesswani	IoT ağındaki çok sınıflı saldırıları tespit etmek için hibrit bir sınıflandırma yaklaşımı önerilmiştir.	UNSW-NB15 ve NSL-KDD veri setinde sırasıyla %81.02 tespit oranı, %2.22 yanlış alarm oranı ve %92.85 tespit oranı, %2.99 yanlış alarm oranı elde edilmiştir.	2021

Lewis vd., izinsiz giriş tespit sistemlerinin dağıtımı ve ölçeklenebilirliği zorluklarına bir çözüm olarak P4ID'yi tanıtmıştır. P4ID, trafiğin, izinsiz giriş tespit sistemine iletilmesi gerekip gerekmediğini dinamik olarak belirlemek için P4 durum bilgisi olan bir veri düzlemi kullanan filtreleme yaklaşımıdır. P4ID sisteminde, P4 kural ayrıştırıcısı kullanılır ve durumsuz paket işleme birleştirilir. Bu sistem, CICS2017 veri seti ve Emerging Threats kural seti birleştirilerek değerlendirilmiştir. Yazarlara göre, önerilen teknikle beraber, IDS tarafından işlenen trafikte önemli bir azalma sağlanabilir. Bu çalışma, IDS'ye gelen trafiği sınırlamak için öğeler eklenerek daha da geliştirilebilir.
Rashid vd., NSL-KDD ve CIDDS-001 veri setlerinin kapsamlı ve karşılaştırmalı bir analizini gerçekleştirmiştir. İdeal sonuçları elde etmek için, Neural Networks, Naive Bayes, SVM k-NN, DAE ve DNN gibi sınıflandırma yaklaşımlarını uygulamadan önce hibrit özellik seçimi ve sıralama yöntemlerini (imza tabanlı, anomali tabanlı ve durum bilgisi olan protokol analizinin kombinasyonu) kullanmıştır. IDS'nin performansı, kesinlik, doğruluk ve f1-skoru gibi metrikler kullanılarak değerlendirilmiştir. Deneysel sonuçlar, k-NN, SVM, NN ve DNN sınıflandırıcılarının NSL-KDD veri setinde yaklaşık %100, k-NN ve Naïve Bayes sınıflandırıcılarının CIDDS-001 veri setinde yaklaşık %99 doğruluğa sahip olduğunu göstermiştir. Çalışmanın sonuçlarına göre, son teknoloji sınıflandırıcıların daha iyi performans göstermesi için hibrit yöntemler tercih edilmelidir. Bu çalışma, CIC-IDS 2017, CIC-IDS 2018 gibi güncel veri kümeleri üzerinde farklı derin öğrenme yaklaşımları uygulanarak geliştirilebilir.

2.3.3.2 Durumsal protokol analizi değerlendirilmesi

Durumsal protokol analiz yöntemleri genellikle standart protokol modellerini kullanır ve her bir protokolün uygulanmasındaki değişiklikleri hesaba katar. Böylece beklenmedik bir komut dizisini algılayabilir ve hem ağ katmanında hem de uygulama katmanlarında belirtilen profilleri takip edebilir. Ancak birçok standart, protokollerin ayrıntılarını tam olarak açıklamamıştır.

Durumsal protokol analiz yöntemlerinin bir dezavantajı, birçok oturumun aynı anda izlenmesi nedeniyle analiz sürecinin karmaşık ve kaynak kullanımının yüksek olmasıdır. Diğer bir sorun, protokol davranışının özelliklerini ihlal etmeyen saldırı

türlerinin tespit edilememesidir. Örneğin, hizmet reddine neden olmak için kısa sürede birçok normal eylem gerçekleştirilmesi. Başka bir sorun, bir IDS tarafından kullanılan protokol modelinin belirli işletim sistemleri sürümlerinde veya farklı istemciler/sunucular üzerinde uygulanma biçiminin farklılık gösterebilmesidir.

2.4 Saldırı Tespit Yaklaşımları

İstatistiksel, kural, buluşsal, örüntü, bulut, makine öğrenimi ve derin öğrenme tabanlı olmak üzere bilgisayar ağlarındaki saldırıları tespit etmek için çeşitli yaklaşımlar vardır. Bu yaklaşımların isimleri, saldırı tespit etme işlemi sırasında kullandığı tekniklere ve platformlara göre değişmektedir.

2.4.1 İstatistiksel tabanlı yaklaşım

İstatistiksel tabanlı saldırı tespit sistemi, normal bir profil oluşturmak için olası işlemleri izler (Khraisat vd. 2019). Gözlenen olayların normal olarak belirlenen profillerden farklı olması saldırıların göstergesidir. Her işlem için, izinsiz girişimleri normal trafikten ayırmak için bir puan atanır. Ölçülen puan belirlenen eşik değerinden büyük olduğunda alarm tetiklenir. Eşik değeri, belirtilen zaman aralığında meydana gelen olay sayısına göre belirlenir. Normal profil oluşturulurken ortalama, mod, medyan, varyans ve standart sapma gibi istatistiksel metrikler kullanılır (Ye vd. 2002). İstatistik tabanlı teknikler değişiklik gösterir. Temel olarak üç kategoride sınıflandırılabilir: tek değişkenli, çok değişkenli ve zaman serisi modeli. Bu istatistiksel tabanlı teknikler ayrıca operasyonel model, markov süreç modeli, parametrik ve parametrik olmayan modeller, eşik metriği, istatistiksel momentler ve çok değişkenli model gibi alt kategorilere ayrılabilir.

İstatistik tabanlı IDS, aşağıdaki gibi sıralanabilecek bazı avantajlar içerir:

1. Saldırı imzasına gerek olmadığı için sıfır gün saldırılarını tanıyabilir.
2. Güncellemeye gerek olmadığı için bakımı kolaydır.
3. DoS ve DDoS saldırılarını algılayabilir.

Öte yandan istatistik temelli yaklaşımın sakıncaları ise şu şekilde sıralanabilir:

1. Normal bir profil oluşturmak zaman alır.
2. Normal profil zamanla değişebilir.
3. Kullanılan istatistiksel dağılımların etkili ve doğru olması gerekir.

2.4.2 Kural tabanlı yaklaşım

Kural tabanlı IDS, ağ trafiğindeki olası saldırıları tespit ederken kuralları kullanır (Han ve Cho 2003). Kurallar, bir kalıp olarak tanımlanabilir. Kurallar çıkarıldığında, saldırı modellerinden kurallar türetmek için yapay zeka kullanılmaktadır. Tek bir kuralla, birçok saldırı tanımlanabilir. Aynı tür ve sayıda saldırıyı tanımak için, kural tabanlı yaklaşım sadece birkaç kural gerektirirken, imza tabanlı yaklaşım binlerce imza gerektirir. Kural tabanlı IDS'yi devam ettirmek kolaydır. İlk kurallar tanımlandıktan sonra sisteme kolayca ek kurallar eklenebilir. Kural tabanlı tespit sistemleri yeni saldırıları tespit edebilir çünkü saldırıdaki basit değişiklikler izinsiz giriş modellerini tamamen değiştiremez. Ancak, ağdaki olası tüm saldırıları tespit etmek için çok fazla kural gerektirir.

2.4.3 Sezgisel tabanlı yaklaşım

Sezgisel tabanlı IDS, kötü niyetli davranışlara dayalı izinsiz girişleri arar. Sezgisel tabanlı IDS, kabul edilebilir davranışları belirten ve diğer davranışları iptal eden bir algılama modeli oluşturmaktadır (Qureshi vd. 2019). Normal davranışlardan saldırı davranışlarını doğru bir şekilde ayırt etmek için sezgisel yaklaşım bilgi ve deneyim gerektirir. Sezgisel yaklaşımda, toplanan izler herhangi bir şüpheli davranış için analiz edilir. Herhangi bir şüpheli davranış kalıbı bulunursa, uyarı verilir. Ağ saldırılarında yeni davranış türleri tespit edildiğinde, kötü niyetli davranışlar listesi genişletilir. Sezgisel tabanlı yaklaşımlar ile iyi bilinen ve sıfır gün saldırıları tespit edilebilir. Ancak bazı saldırı türleri, buluşsal algılama motorundan kaçmak için gizleme tekniklerini kullanabilir.

2.4.4 Örüntü tabanlı yaklaşım

Örüntü tabanlı yaklaşım, toplanan verilerdeki anlamlı kalıpları çıkarmak için karakterleri, dizileri ve formları tanımlar ve bu kalıplara dayalı saldırıları bulur (Lia vd. 2013). Örüntü tabanlı yaklaşım, saldırılardaki kötü niyetli talimat dizilerini belirler. Bilinen saldırıları hızlı ve verimli bir şekilde tespit edebilir, ancak imzaları (kalıpları) henüz bilinmediği için sıfır gün saldırılarının çoğunu tespit edemez. Örüntü tabanlı bir algılama sistemi uygulamak kolaydır. Örüntü eşleme algoritmaları, tekli ve çoklu desen eşleme olmak üzere iki türe ayrılır. Çoklu eşleştirme algoritması, paketi birkaç kez taramaktan kaçındığı için IDS'ler için daha verimlidir (Lia vd. 2013). Ancak, daha fazla bellek ve işlem süresi gerektirir.

2.4.5 Bulut tabanlı yaklaşım

Bulut bilişim, çeşitli hizmetleri çevrimiçi olarak verimli bir şekilde destekleyen umut verici teknolojilerden biridir (Aldwairi vd. 2017, Aslan ve Samet 2020, Aslan vd. 2021, Gupta vd. 2020, Yassin vd. 2012). Bulut bilişim, kullandığın kadar öde, 7/24 veri erişimi, daha düşük maliyetli sınırsız hizmetler ve daha fazla hesaplama gücü gibi birçok avantaj sağlar. Bulut ortamları üç tür hizmet sağlar: SaaS (hizmet olarak yazılım), PaaS (hizmet olarak platform) ve IaaS (hizmet olarak altyapı) (Gupta vd 2020). SaaS, kullanıcılara internet üzerinden karmaşık faaliyetler yürütmeleri için büyük faydalar sağlar. PaaS, kullanıcıların çeşitli algoritmaları ve teknikleri kolayca uygulayabilmeleri için devasa bir yazılım platformu sunar. IaaS, ağ, temel bilgi işlem cihazları ve depolama kaynakları dahil olmak üzere şirketlerin yanı sıra kullanıcılara da altyapı imkanı sunar. IDS'yi bulut ortamının üzerine inşa etmek çeşitli avantajlar sağlar. Bulut ortamları, kötü niyetli ağ aktivitelerinin farklı açılardan tanımlanmasını sağlar ve klasik saldırı tespit sistemlerindeki eksiklikleri tamamlar (Yassin vd. 2012).

Bulut tabanlı IDS, kullanıcı veri toplayıcı, bulut hizmeti ve bulut saldırı algılama dahil olmak üzere üç farklı bileşenden oluşur (Yassin vd. 2012). Kullanıcı veri toplayıcı, ağ paketlerini toplayan, filtreleyen, standartlaştıran ve bulut hizmetine gönderen bağımsız bir sunucudur. Bulut hizmeti, kullanıcı veri toplayıcısından alınan verileri analiz eder,

doğrular ve verileri, bulut saldırı algılama bileşeni için ortak bir biçime dönüştürür. Bulut saldırı algılama bileşeni, bulut saldırı tespit sisteminin ana parçasıdır. Bulut hizmeti bileşeninden verileri alır, paketleri analiz eder ve saldırıları belirtir. Bulut saldırı algılama bileşeni, bir imza veritabanı, hizmet konsolu ve analiz motorundan oluşur. Bulut tabanlı IDS yaklaşımı hala erken aşamadadır. Bu yaklaşım, model performanslarını artırmak için gelecekte saldırı tespit sistemlerinde daha fazla kullanılmalıdır.

2.4.6 Makine öğrenmesi tabanlı yaklaşım

Makine öğreniminin amacı, insan müdahalesi olmadan analiz sürecini otomatikleştirmektir. Başka bir deyişle, verileri tanımlamanın algoritmik bir yoludur. Makine öğrenimi yaklaşımı, denetimli (etiketli/etiketsiz veri), denetimsiz (etiketsiz veri) ve yarı denetimli (birkaç etiketli, birkaç etiketsiz veri) dahil olmak üzere farklı öğrenme tekniklerini kullanabilir. Saldırı tespiti için kullanılan yeni bir yaklaşımdır. Bayes algoritmaları, k-en yakın komşu, destek vektör makineleri, karar ağaçları, sinir ağları, genetik algoritmalar ve bulanık mantık dahil olmak üzere IDS'lerde kullanılan geniş bir teknik ve algoritma kategorisi vardır. Son zamanlarda, IDS'ler için makine öğrenimi yaklaşımını uygulayan çalışmalar yayınlanmıştır (Tsai vd. 2009, Vinchurkar ve Reshamwala 2012, Musa vd. 2020).

ML yaklaşımının başlıca avantajları, uyarlanabilirlik, yüksek performans, esneklik ve yeni saldırı türlerini tespit edebilmedir. Öte yandan, ML tabanlı IDS'nin aşağıdaki gibi sıralanabilecek bazı dezavantajları vardır:

1. ML algoritmaları veriler hakkında varsayımda bulunur.
2. Aykırı değerlerle her zaman başa çıkamaz.
3. Bilinmeyen saldırıların tespiti ve önlenmesi zordur.
4. Büyük veri boyutu (milyonlarca ağ bağlantısı).
5. Veri ön işlemesi zordur (İzleme sisteminden gelen verileri analiz için uygun formata dönüştürmek)
6. Yalnızca IP adreslerine değil, bağlamsal özelliklere de ihtiyaç duyulmaktadır.
7. Algoritmalar alan bilgisini hesaba katmaz.

2.4.7 Derin öğrenme tabanlı yaklaşım

Derin öğrenme, son zamanlarda popüler hale gelen yeni bir öğrenme yöntemidir. Örneklerden öğrenen ve çoğu zaman özellik mühendisliği adımını ortadan kaldıran bir makine öğrenimi alt alanıdır. Derin öğrenme, öğrenme işlemi sırasında birden çok ardışık katman kullanır. Katmanlar birbirine bağlıdır ve önceki katmanın çıktısı, sonraki katmanın girişidir. Özellikler hiyerarşik bir şekilde çıkarılır. Her katmanda, özellikler daha net bir şekilde tanımlanır. Derin öğrenme, görüntü işleme, insan tanıma, yüz tanıma, sürüş güvenliği ve kötü amaçlı yazılım tespiti gibi birçok farklı alanda kullanılmıştır (Aslan ve Yılmaz 2021). Son zamanlarda saldırı tespit sistemlerinde de kullanılmaya başlanmıştır. Derin öğrenme tabanlı IDS, sınıflandırma ve boyut küçültme avantajlarından yararlanarak anormallikleri tespit edebilir. Ayrıca derin öğrenme, büyük ölçekli ve çok boyutlu verileri tanıyabilir (Aldweesh vd. 2020). Derin öğrenme yaklaşımı, değişen dinamik verileri işleyebilir. Derin öğrenme modeli, yeni trafiği normal veya saldırı olarak sınıflandırır. Ayrıca saldırı türlerini belirterek daha fazla sınıflandırma yapabilir (Bovenzi vd. 2020, Mirsky vd. 2018).

Saldırıları tespit etmede derin öğrenme yaklaşımının avantajları şu şekilde sıralanabilir:

1. Otomatik özellik çıkarma.
2. Çok büyük veri kümelerini işleme.
3. Güçlüdür, etkilidir ve özellik alanını önemli ölçüde azaltır.

DL tabanlı IDS yaklaşımının dezavantajları şu şekilde sıralanabilir:

1. Anlamlı özellikler tasarlamak için verilerin zor anlaşılması
2. Uygulamayı kontrol edecek iyi eğitimli alan uzmanlarının ve veri bilimcilerinin olmaması
3. Yeterli etiketli veri olmaması
4. Gizli bir katman oluşturmak zaman almaktadır ve ekstra gizli katmanlar eklemek nadiren model performansını artırır.
5. Kaçınma saldırılarına karşı dayanıklı değildir

2.4.8 Saldırı tespit yaklaşımlarının değerlendirilmesi

Bu bölümde IDS yaklaşımlarında kullanılan teknikler, her bir yaklaşımının ana fikri, avantajları ve dezavantajları verilmiştir. Her bir yaklaşımın değerlendirilmesi aşağıdaki gibi özetlenebilir:

- ✓ **İstatistik tabanlı yaklaşım,** bilinen saldırıların yanı sıra sıfır gün saldırılarını da tespit edebilir. Her seferinde güncellemeye ihtiyaç duymaz. Çok çeşitli saldırı türlerini tespit edebilir. Ancak normal bir profil oluşturmak zaman alır.

- ✓ **Kural tabanlı yaklaşım**, binlerce saldırıyı tespit etmek için yalnızca birkaç kural gerektirir. Saldırı kodlarındaki basit değişiklikler izinsiz giriş modellerini tam olarak değiştiremeyeceğinden, yeni saldırı türevlerini tanır. Ancak, ağdaki tüm olası saldırıları tanımlamak için birden fazla kural gerektirir.

- ✓ **Sezgisel tabanlı yaklaşım**, yeni saldırıların davranışlarını tespit ederken kötü niyetli davranışlar listesini genişletebilir. Sezgisel tabanlı bir yaklaşımla hem bilinen hem de bilinmeyen saldırılar tespit edilir. Bununla birlikte, bazı saldırı türleri, iletişim ağlarında ve ana bilgisayarlarda yakalanmamak için kaçma teknikleri kullanır.

- ✓ **Örüntü tabanlı yaklaşım**, bilinen saldırıları hızlı ve verimli bir şekilde tespit eder, ancak imzaları henüz mevcut olmadığı için bilinmeyen saldırıların çoğunu tespit edemez. Örüntü tabanlı bir yaklaşımın uygulanması hızlı ve kolaydır.

- ✓ **Bulut tabanlı yaklaşım**, daha düşük maliyetli sınırsız hizmetler, 7/24 veri erişimi, daha fazla hesaplama gücü vb. gibi birçok avantaj sağlar. Bulutun üzerine farklı IDS teknikleri uygulanabilir. Bulut tabanlı IDS, bir imza veritabanı, hizmet konsolu ve analiz motorundan oluşur. IDS performansını artırırken analiz süresini kısaltır. Bulut tabanlı IDS yaklaşımı hala erken aşamadadır ve yakın gelecekte IDS'lerde daha fazla kullanılmalıdır.

- ✓ **Makine öğrenmesi tabanlı yaklaşım**, saldırıları tespit etmek için analiz sürecini otomatikleştirir. Denetimli, denetimsiz ve yarı denetimli olmak üzere çeşitli öğrenme tekniklerinin yanı sıra karar ağaçları, k-en yakın komşu, destek vektör makineleri, sinir ağları, genetik algoritmalar ve bulanık mantık gibi farklı algoritmalar kullanır. Makine öğrenimi yaklaşımının temel avantajları, yüksek performansı, uyarlanabilirliği, esnekliği desteklemesi ve sıfır gün saldırılarını tespit etmesidir. Ancak, ML tabanlı IDS'nin büyük verileri işlemenin zor olması, veri ön işlemesinin zor olması ve algoritmaların alan bilgisini hesaba katmaması gibi çeşitli dezavantajları vardır.

- ✓ **Derin öğrenmeye tabanlı yaklaşım**, öğrenme süreci sırasında birden çok ardışık katman kullanır. Verilerdeki anormallikleri algılayabilir, büyük ölçekli ve çok boyutlu verileri tanıyabilir ve zamanla değişen dinamik verileri işleyebilir. Öte yandan, akışlar içinde yeterli bilgi bulunmaması, uygulamayı kontrol etmek için iyi eğitimli alan uzmanlarının olmaması, yeterli etiketli veri olmaması gibi dezavantajları vardır.

Özetlemek gerekirse, her tespit yaklaşımının kendi avantajları ve dezavantajları vardır ve farklı veri kümelerinde daha iyi performans gösterir. IDS yaklaşımlarının performanslarını değerlendirmek için verinin boyutu, mevcut öznitelik sayısı, veri dağılımı vb. gibi çeşitli özellikler kullanılabilir. Mevcut IDS'lerde istatistiksel, sezgisel ve örüntü tabanlı yaklaşımların yeterince kullanıldığı görülmüştür. Bu nedenle, araştırmacıların bulut, makine öğrenimi ve derin öğrenme tabanlı yaklaşımlara daha fazla odaklanması gerekmektedir. Ayrıca, bir saldırı tespit sistemi oluştururken, araştırmacılar ve geliştiriciler, adres dolandırıcılığı, örüntü değişikliğinden kaçınma ve parçalanma gibi çeşitli kaçınma tekniklerinin farkında olmalıdır.

3. WLAN SALDIRI TESPİT SİSTEMLERİNİN İNCELENMESİ

Kablosuz yerel alan ağlarına yönelik tehditler çok fazla sayıdadır ve potansiyel olarak yıkıcıdır. Yanlış yapılandırılmış kablosuz erişim noktalarından (WAP) oturum kaçırmaya ve sunucuların hizmet dışı bırakılmasına (DoS) kadar değişen güvenlik sorunları bir WLAN'ı zedeleyebilmektedir. Kablosuz ağlar, yalnızca kablolu ağlara özgü TCP/IP tabanlı saldırılara duyarlı değildir, aynı zamanda 802.11'e özgü çok çeşitli tehditlere maruz kalmaktadırlar. Bu potansiyel tehditlerden kaçınılması ve tespit edilmesine yardımcı olmak için, WLAN'lar izinsiz giriş tespit sistemi (IDS) içeren bir güvenlik çözümü kullanmalıdır.

Kablosuz yerel alan ağlarına olan yoğun ilgiden dolayı, saldırı tespit sistemleri alanında çalışmalarda artmıştır. Ancak bu çalışmaların hızıyla orantılı olarak saldırıların yoğunlukları da türleri de aynı hızda artmaktadır. Bu yüzden mevcut saldırı tespit sistemleri bu gelişen dinamik yapıyla yüksek oranda baş edememektedir. Bu eksikliklere katkı yapabilecek, WLAN'lara yönelik gittikçe artan tehdit bilgilerini tanımlayabilen ve raporlayan bir sistem ihtiyacı kaçınılmaz hale gelmiştir.

3.1 WLAN'lara Yönelik Saldırılar ve Yapılma Şekilleri

Bu bölümde, 802.11 güvenlik mekanizmasının çeşitli sürümlerine (yani WEP, WPA, WPA2) yönelik saldırılar açıklanmıştır. Burada, pratik olarak gerçekleştirilen ve penetrasyon test araçlarıyla uygulanan saldırılara ağırlık verilmiştir. Saldırılar benzer amaç gruplarına göre düzenlenmiştir.

3.1.1 Anahtar çalma saldırıları (Key retrieving attacks)

Bu alt bölüm, gizli anahtarları ortaya çıkarmaya çalışan saldırılara odaklanmaktadır. Bu saldırılarda, saldırganın belirli paketleri izlemesi ve ardından anahtar kırma işlemine çevrimdışı olarak devam etmesi yeterlidir. Bu pasif uygulama, en gelişmiş IDS'ler tarafından bile tamamen izlenemezken, saldırgan ağa bir takım paketlerin enjeksiyonuna

dayanan (çoğu zaman büyük miktarda) saldırıları kullanmayı seçecektir ve yüksek ihtimalle kendini açığa çıkaracaktır.

FMS Saldırısı (Fluhrer, Mantin and Shamir Attack) : FMS saldırısı (Fluhrer vd. 2001), RC4 şifrelemenin (stream cipher) anahtar programlama algoritmasındaki bir güvenlik açığından yararlanarak, WEP anahtarı türetmek için yapılan ilk belgelenmiş başarılı girişimdir. Bu saldırı zayıf IV (Initializing Vector)'lerin teorisine dayanmaktadır (Bittau 2003, Berghel ve Uecker 2005). Böyle zayıf bir IV bir paketi şifrelemek için kullanıldığında, saldırgan şifreleme anahtarının sadece ilk n baytını bilerek, n + 1'in değeri hakkında doğru varsayımlarda bulunabilmektedir. Bu durumda, giriş koşullarının elde edilmesi kolaydır çünkü düz metnin ilk baytı tahmin edilebilirdir. Bu işlemi tamamladıktan sonra saldırgan n + 1 baytın olası değerine sahip olacaktır. Bu yüzden saldırgan, zayıf IV koşulunu sağlayan çoklu mesajlar için bu işlemi tekrarlamayı seçebilir. Bu noktadan itibaren, aynı döngü anahtarın geri kalan baytları için tekrarlanabilir.

KoreK Saldırıları: KoreK takma adını taşıyan bir kriptanalist, WEP anahtarını çalmayı amaçlayan on yedi saldırının uygulanmasını (Netstumpler formunda) yayınlamıştır. Bu saldırıların her biri, FMS ile aynı matematiksel ilkelere dayanmaktadır, ancak farklı korelasyonları kullanmaktadır (Kore 2004).

Her durumda, WEP anahtarını alabilmesi için saldırganın elinde önemli miktarda IV toplanması gerekir. Aslında, hem FMS hem de KoreK saldırıları, sınırlı sayıda olası anahtarın başlangıç alanını oluşturmak için birlikte kullanılmaktadır ve daha sonra doğru olanı etkin bir şekilde ortaya çıkarmak için kaba kuvvet (brute-force) saldırısı ile devam edilmektedir.

PTW Saldırısı (Pyshkin, Twes ve Weinmann Attack): PTW saldırısı (Tews vd. 2007), Pyshkin, Twes ve Weinmann'ın araştırmalarıyla tanımlanmıştır ve Klein'ın RC4'ün kapsamlı versiyonunu hedef alan saldırısına dayanmaktadır (Klein 2008). PTW saldırısı, WEP anahtarını istatistiksel yöntemlerden çok daha etkili bir şekilde (daha az

IV/veri çerçevesi) kırmaya çalışır. Günümüzde, pek çok WEP kırma aracı bu saldırıyı, verimliliği nedeniyle varsayılan kırma yöntemi olarak görmektedir.

ARP Enjeksiyonu: ARP enjeksiyonu aslında bir saldırı yöntemi değildir, ancak anahtar kırma atakları için ilk adım olarak kullanılabilmektedir (Tews vd., 2007). Bu saldırının amacı, ağı bu şekilde manipüle etmektir, böylece ağda gerçek bir trafik olmamasına rağmen, yeni IV'lerin sürekli olarak üretilmesi sağlanır. Zorla oluşturulmuş bu IV'ler daha sonra saldırgan tarafından yakalanacak ve sonraki bir çevrimdışı adımda ilgili anahtar kırma algoritmalarına beslenecektir.

Sözlük Saldırısı: Sözlük Saldırısı, zayıf WPA/WPA2 (Moskowitz 2003) ve WEP anahtarlarını çalmak için yaygın olarak kullanılan bir kaba kuvvet saldırı şeklidir. Bugünün standartlarına göre, WPA/WPA2 kırma işlemlerinde en güvenilir yöntem olarak görülmektedir. Sözlük saldırısı, önceden düzenlenmiş bir listedeki tüm dizeleri denemeye dayanır. Bu tür saldırılar, başlangıçta bir sözlükte bulunan sözcükleri kullanır; ancak artık internet ortamında geçmişteki veri ihlallerinden kurtarılan yüz milyonlarca şifreyi içeren çok daha büyük listeler vardır. Ayrıca, bu tür listeleri kullanabilen ve sayıları benzer görünen harflerle değiştirmek gibi yaygın varyasyonlar üretebilen kırma yazılımları da vardır. Bir sözlük saldırısı, yalnızca başarılı olma olasılığı en yüksek olan olasılıkları dener ve bu saldırılar genellikle başarılı olur. Çünkü birçok kişi sıradan kelimeler veya yaygın şifreler olan kısa şifreleri seçme eğilimine sahiptir veya sadece bir rakam veya noktalama işareti ekleyerek veryantlarını elde ederler. Ancak, parola sözlükte bulunmuyorsa bu saldırı başarısız olur (Liu vd. 2010). Bu saldırılara karşı daha güvenli bir ortam için bir parola yöneticisi programı kullanmak, parolayı manuel olarak yazmak, rastgele uzun bir parola belirlemek(15 karakter veya daha fazla) veya çok sözcüklü bir parola oluşturmak, doğru bir yaklaşım olacaktır.

3.1.2 Anahtar akışı çalma saldırıları (Keystream retrieving attacks)

WEP korumalı ağlarda bir saldırganın yalnızca anahtar akışı bilgisinden bile faydalanması mümkündür. Örneğin, saldırganlar saldırılarını düzenlerken ağa paketler

oluşturmak ve enjekte etmek için anahtar akışlarını kullanmaktadırlar. Başka bir seçenek de paketlerin bölümlerinin şifresini çözmektir. Burada saldırgan kritik bölümlerin şifresini çözerek bir ağın topolojisini öğrenebilir veya dolaylı olarak kapsamlı bir anahtar/IV çiftleri veritabanı oluşturarak tüm trafiğin şifresini çözebilir.

ChopChop Saldırısı: ChopChop saldırısı, KoreK tarafından önerilmiştir (Kore 2004). ChopChop saldırısı genellikle anahtar akışının büyük bölümlerini türetmek amacıyla gerçekleştirilmektedir. Bu anahtar akışı, sonraki adımda ağdaki çerçeveleri oluşturmak ve enjekte etmek için kullanılmaktadır. Daha az sıklıkla karşılaşılan bir senaryo olsa da, bazen bu saldırı, özellikle saldırganın WEP anahtarını bilmediği durumlarda, paketlerin şifresini çözmek için kullanılmaktadır.

Parçalanma Saldırısı: Parçalanma saldırısı (Bittau 2005), ChopChop saldırısından çok daha az mesaj göndererek, anahtar akışının önemli bir bölümünü ortaya çıkarmayı amaçlamaktadır. Anahtar akışı daha sonra diğer saldırıların bir parçası olarak ağa paket üretmek ve enjekte etmek için kullanılabilmektedir. Verimliliğinden dolayı bazen saldırganlar tarafından IV'lerin farklı değerleri için tam bir keystream sözlüğü oluşturmayı amaçladıklarında kullanılır.

Caffe Latte Attack: Bu saldırı, bir saldırganın hedef ağın menzili içinde kalmasına gerek kalmadan WEP anahtarını almak için kullanılan ilk saldırıdır. Ahmad ve Ramachandran (2007), artık yakınında olmasa bile, bir zamanlar hedef ağda kimliği doğrulanmış yalıtılmış bir istemciye saldırarak WEP anahtarını almanın mümkün olduğunu göstermiştir. Saldırgan bu saldırıyı gerçekleştirirken, (a) istemcilerin genellikle bilinen anahtar kelimelerle birlikte bilinen ESSID'lerin bir listesini tuttukları; (b)çoğu istemcinin kimliği doğrulanmayan bir durumdayken bu tür ağlar için aktif olarak araştırma yaptığını ve bu şekilde geçmişte ilişkilendirildikleri ağların bir listesini ortaya çıkardığını; (c) söz konusu ağın herhangi bir probu ile aynı ESSID'ye sahip olması durumunda, istemcinin bir ağa otomatik olarak bağlanmaya çalıştığı durumlarından yararlanmaktadır.

Hirte Attack: Hirte Attack, sadece bir istemci kullanarak WEP anahtarını almak ve ağın AP (Access Point)'sine ihtiyaç duymayan bir yöntemdir. Caffe Latte'ye benzer şekilde çalışır ancak parçalanma saldırısında bulunan yöntemleri içermektedir. Tipik bir saldırı senaryosunda, saldırgan Caffe Latte saldırısına benzer şekilde bir Honeypot kurduktan sonra şifreli bir paket edinir. Daha sonra, bu paketi parçalara ayırarak ve sıralarını değiştirerek IP adres alanını yeniden yerleştirir. Birleştirilmiş paket sonunda bir ARP isteği haline gelir ve bu andan itibaren mesaj seli (flooding), kırma (cracking) gibi saldırılar gerçekleşebilir.

3.1.3 Kullanılabilirlik saldırıları (Availability attacks)

Yaygın olarak Hizmet Reddi (DoS) saldırıları olarak adlandırılan, hizmet kullanılabilirliği kaybına neden olan saldırılar bu bölümde verilmiştir. Burada anlatılan saldırıların çoğu, sahte 802.11 yönetim mesajlarının yayınlanmasına dayanmaktadır. Bu tür saldırılar, yönetim mesajları korunmadan iletildiğinden, standardın 802.11n'e (IEEE 2007) kadar olan sürümlerine entegre edilmesinin önemsiz olduğu düşünülmektedir. Her durumda, olumsuz sonuçların, saldırı yapıldığı sürece geçerli olduğunu unutmamalıdır. Bu, pratik olarak (a) DoS saldırılarının etkisinin kalıcı olmadığı ve (b) saldırganın saldırısı sırasında fiziksel olarak ağın aralığında bulunması gerektiği anlamına gelir (Bicakci ve Tavli 2009).

Kimlik Doğrulama Saldırısı (Deauthentication Attack): Sadeliği ve etkinliği nedeniyle 802.11 ağlarında en güçlü DoS saldırısı olarak kabul edilmektedir. Bu saldırı, kimlik doğrulama paketlerinin korumasız olarak iletilmesi ve saldırgan tarafından kolayca kandırılabilmeleri temeline dayanmaktadır.

Saldırgan, belirli bir istemciyle ve AP ile ilişkili MAC adreslerini belirlemek için ağdaki trafiği izler. Daha sonra bir kimlik doğrulama yönetim çerçevesi oluşturur ve bunu AP adına istemciye gönderir. Alternatif olarak, istemci adına AP'ye de gönderebilir, böylece ağ bu istemcinin kimliğini doğrulamayı düşünerek durur. İstemci ağ ile olan bağlantısını hemen kaybeder ve kimlik doğrulama prosedürünü otomatik olarak yeniden başlatır. Bu

döngü genellikle çok kısadır, ancak servis istemcisi daha uzun süre servis dışı bırakılarak saldırı tekrar tekrar yapılabilir (Bicakci ve Tavli 2009).

Ayrışma Saldırısı (Disassociation Attack): Ayrışma saldırısı, kullanımının kolay olması ve gösterdiği etkiler ile Kimlik Doğrulama saldırısına çok benzerdir. Teorik olarak, bu tür saldırılar daha az etkilidir çünkü istemcinin ilişkili olmayan durumdan ilişkili duruma dönmesi için daha az sayıda prosedür vardır. Bu nedenle, hizmet kaybı süresinin daha kısa olması beklenmektedir.

Kimlik Doğrulama Yayını Saldırısı (Deauthentication Broadcast Attack): Kimlik Doğrulama Yayını Saldırısı, basit Kimlik Doğrulama saldırısı ile aynı şekilde çalışır, ancak ilgili alandaki bir istemci adresi yerine saldırgan yayın adresini girer. Bu durum, tüm istemcilerin bu mesajı almasına ve kimlik doğrulaması yapmasına neden olur. Ağdaki bağlı tüm istemciler aynı anda doğrulama işlemi başlatmaya çalışacaklarından, sistem çalışamaz hale gelecektir (Nguyen vd. 2008).

Ayrışma Yayını Saldırısı (Disassociation Broadcast Attack): Bu saldırı, Kimlik Doğrulama saldırısı ile aynı şekilde çalışır ancak bunun yerine Ayrışma mesajını kullanır. Bu saldırının etkileri benzerdir, ancak yeniden birleşme süreci daha kısa ve daha az hesaplama yoğunluğu olduğu için daha az etkisi olması beklenmektedir (Nguyen vd. 2008).

ACK taşmasını engelleme (Block ACK flood): Bu saldırı AP'nin belirli bir istemciden kaynaklanan tüm paketleri kendi isteğiyle düşürmesine neden olmaktadır. 802.11n ağlarına karşı etkilidir ve standardın bu versiyonunda tanıtılan Add Block Acknowledgement (ADDBA) mekanizmasından yararlanarak sonuçlarına ulaşır. Daha spesifik olarak, bu mekanizma bir istemcinin birkaç küçük parça yerine tek bir büyük çerçeve bloğu aynı anda iletmesine izin verir (Tinnirello ve Choi 2005). Bu tür bir işlemi yapma isteğini AP'ye bildirmek için istemci adına bir ADDBA mesajı gönderilmelidir. Bu mesaj, bloğun boyutu ve karşılık gelen sıra numaraları gibi bilgileri içerir. Böyle bir mesajı aldıktan sonra, AP yalnızca belirtilen sıraya giren çerçeveleri

kabul eder ve gerisini bırakır. Bu saldırı, ağa çok düşük miktarda trafik enjekte edildiğinde bile etkili olduğu için tespit edilmesi zordur.

Kimlik Doğrulama İsteği Sel Saldırısı (Authentication Request Flooding Attack): İstemci ilişkileri tablosunda taşmaya neden olarak AP'nin kaynaklarını tüketmeye çalışan saldırı türüdür. İstemci AP'nin ilişkilendirme tablosunda tutulabilecek maksimum istemci sayısının sınırlı olması temeline dayanmaktadır. İstemci kimlik doğrulama işlemini tamamlamamış olsa bile, bir Kimlik Doğrulama İsteği iletisinin alınmasından sonra AP'nin istemci ilişkilendirme tablosuna bir giriş eklenir. Genel olarak, saldırganın çok sayıda sahte istemci taklit etmesi ve her biri adına bir kimlik doğrulama çerçevesi göndermesi gerekir. AP'nin istemci ilişkilendirme tablosu sahte girdilerle dolduktan (overflow) sonra, AP yasal STA'ları artık ilişkilendiremez (Liu vd. 2010).

Sahte Güç Tasarrufu Saldırısı (Fake Power Saving Attack): Bu, yönetim çerçevelerine dayanmayan daha çok boş veri çerçeveleri aracılığıyla uygulanan tek DoS saldırısıdır. Sahte güç tasarrufu saldırısı amacına ulaşmak için daha az sayıda çerçeve gerektirme avantajına sahiptir (Meiners 2009). Bu saldırı, güç tasarrufu mekanizmasını kötüye kullanarak, AP'yi belirli bir STA'nın uyku moduna geçtiğini düşünmeye zorlar. 802.11'deki Güç Yönetimi mekanizması, ağ adaptörlerini güç tasarrufu moduna ayarlayarak bir STA'nın güç tüketimini azaltmaya yardımcı olmaktadır. Bu duruma ayrıca doze modu da denir (genel olarak uyku modu olarak bilinir). Uyku moduna geçiş genellikle istemci iletişim olmadan zaman harcadığında yapılır. Uyku moduna geçmek için, istemcinin önce AP'ye Güç Tasarrufu biti 1 olarak ayarlanmış olan boş bir veri çerçevesi aracılığıyla isteğini bildirmesi gerekir. Uyku modundayken, istemci çerçeveleri alamaz veya iletemez ve AP, kendisine gönderilen tüm çerçeveleri geçici olarak saklar.

CTS Sel Saldırısı (CTS Flooding Attack): The Request to Send (RTS), Clear to Send (CTS) ileti çifti, RF ortamına erişimi kontrol eden bir mekanizmadır. Bu mekanizma etkinleştirildiğinde ve bir STA kuyruğunda aktarım için veri bulunduğunda, önceden belirlenmiş bir süre boyunca RF ortamına erişmek için bir RTS çerçevesi gönderir. Bu

ayrıcalık aslında CTS çerçevesini aldıktan sonra verilir. CTS Sel Saldırısında, saldırgan CTS çerçevelerini sürekli olarak kendisine veya başka bir STA'ya iletebilir, böylece ağdaki diğer STA'lar iletimlerini sürekli olarak ertelemeye zorlayacaktır.

RTS Sel Saldırısı (RTS Flooding Attack): Bir RTS Sel Saldırısı, RTS/CTS mekanizmasından yararlanır, ancak CTS sel saldırısından zıt bir şekilde çalışır. Kablosuz ortam, kalan STA'ların aktarımdan geri çekilmesini zorlayacak şekle getirilmesi için çok sayıda sahte RTS çerçevesini iletir (Malekzadeh vd. 2009, Sawwashere ve Nimbhorkar 2014).

Beacon Sel Saldırısı (Beacon Flooding Attack): Beacon Sel saldırısı, bir saldırganın yeni istemcilerin ağa girmesinin engellenmesi veya tamamen reddedilmesi için uygulanan bir DoS saldırısı şeklidir (Martinez vd. 2008). Burada, saldırgan var olmayan ESSID'lerin yayınını yapan sabit bir sahte beacons akımı iletir. Bu, mevcut ağlar listesine taşmaya neden olacak ve bu da kullanıcının tercih ettiği ağı bulmasını zorlaştıracaktır.

Prob İsteği Sel Saldırısı (Probe Request Flooding Attack): Bir Prob İsteği Sel Saldırısı (Ferreri vd. 2004) bir AP'nin kaynaklarına baskı yapmayı ve sonunda durdurmaya yol açmayı amaçlamaktadır. Bu saldırı, 802.11 standardına göre bir AP'nin her Probe Talebi (Probe Request) mesajına Probe Yanıtı (Probe Response) ile cevap vermek zorunda olduğu durumu kullanmaktadır. Saldırgan, sürekli sahte Probe İstek paketi akışı gönderebilir. Bu, yüksek hacimde ve uzun bir süre boyunca yapılırsa AP, var olmayanların problara cevap vermeye uğraşacağından, esas istemcilere hizmet veremeyecektir.

Prob Yanıtı Sel Saldırısı (Probe Response Flooding Attack): Bu saldırı, AP yerine istemciyi hedef alarak tersine çalışmasına rağmen, Prob mekanizmasından da yararlanır. Saldırgan, geçerli istemcilerden gelen probe istek mesajlarını izler ve bir AP gibi davranarak STA'lara sahte ve yanlış probe yanıtları iletir. Bu mesajlar ağ hakkında sahte bilgiler içerir, böylece STA'nın geçerli AP'den yanıt almasını yanlış yönlendirir ve herhangi bir AP'ye bağlanmasını engeller.

3.1.4 Ortadaki adam saldırıları (Man-in-the-Middle attacks)

Honeypot: Honeypots (Al-Gharabally vd. 2009), kullanıcıları çekmek ve daha sonra onlara farklı saldırılar yapmak için kötü niyetli yöneticiler tarafından oluşturulan ve kontrol edilen ağlardır. Genellikle, bu tür ağlar kendilerine bağlı olan istemci sayısını en üst düzeye çıkarmak için ESSID'lerin (Ücretsiz İnternet, Ücretsiz WiFi, Açık Erişim Noktası vb.) yayınını yapar. Kullanıcılar bağlandığında ve şifreleme uygulanmadığından tüm trafik saldırgan tarafından görülebilir. Bir Honeypot kendi başına bir saldırı sayılmaz, yalnızca güvenilir ağlara bağlanmak kullanıcının sorumluluğundadır.

Evil Twin: Evil Twin, kullanıcıları geçerli ağ yerine, bağlantı kurmaya zorlamak için mevcut bir ESSID'nin yayınını yapan özel bir Honeypot'tur (Song vd. 2010). Evil Twin AP'ler, (a) aynı ESSID'ye sahip birden fazla AP'nin aynı alanda bulunmasına izin verilmesi ve (b) böyle durumlarda müşterinin yasal AP'nin BSSID'sini göz ardı ederek en güçlü sinyale bağlanmayı tercih etmesi nedeniyle oluşmaktadırlar. Normal bir Honeypot'da olduğu gibi, saldırgan o noktadan itibaren daha yüksek seviyelerde saldırılar başlatabilir veya sadece trafiği izleyebilir.

Sahte Erişim Noktası (Rogue Access Point): Sahte AP'ler, şirket, ev veya ofis içindeki o ağın içerisinden biri tarafından etkinleştirilen yetkisiz erişim noktalarıdır. Bu ayarlar, ağ yöneticisinin izni olmadan disiplinsiz kullanıcılar tarafından güvenlik politikasını kendileri için daha uygun hale getirmek veya saldırganların gizli amaçları için arka kapıyı açık bırakmak amacıyla oluşturulabilir (Beyah ve Venkatamaran 2011, Patel vd. 2014).

3.1.5 Saldırı imzaları

Bu bölümde, yaygın olarak bilenen WLAN saldırılarının teorik ve pratik açıdan analizi ele alınmıştır.

3.1.5.1 Sel saldırıları(Flooding attacks)

Sel saldırıları, genellikle birim zaman başına yönetim çerçevelerinde ani bir artış yaratır. Bu, bir sel saldırısını normal trafikten ayırt etmeyi kolaylaştırsa da, diğer saldırı türlerinden ayırmak her zaman kolay değildir. Benzer olarak bazı saldırılar da, belirli yönetim çerçevelerinde geçici bir artışa neden olabilir. Genellikle ilave ipuçları ve izler vardır, ancak bunların her saldırı sırasında kullanılan araçlara bağlı oldukları unutulmamalıdır. Bir saldırganın kullandığı araç tarafından üretilen izleri maskelemek için yapabileceği bazı işlemler olabilir, ancak tüm sel saldırılarının temeli yönetim çerçevelerinin sayısındaki artışa dayadığından, bunu gizlemek için yapılabilecek çok şey yoktur.

Kimlik Doğrulama Sel saldırısı, kablosuz ağlardaki en güçlü DoS saldırılarından biri olarak kabul edilmektedir, aynı zamanda doğru bir şekilde tanımlanması en zor olan saldırılardan biridir. Bu saldırı sırasında, aşırı sayıda kimlik doğrulama çerçevesi üretilir. Bununla birlikte, bu gibi çerçeveler Ayrılma, Güç Tasarrufu, Kimlik Doğrulama İsteği Sel saldırılarında da izlenebilir.

Kimlik Doğrulama İsteği Sel saldırısı sırasında, Kimlik Doğrulama çerçevelerinin önemli bir artış göstermesi beklenmektedir. Kimlik Doğrulama Sel saldırılarında olduğu gibi artan sayıda kimlik doğrulama talebi görülebilir, ancak kimlik doğrulama isteği seli durumunda, biriken hacim çok daha yüksektir. Bu saldırı genellikle, statik bir Dinleme Aralığı (Listen Interval) alanı (0x0000) olan Kimlik Doğrulama çerçevelerini ileten MDK3 aracıyla başlatılır. Ek olarak, Tagged Parametreleri alanı daima sayıların normalden daha az olduğu aynı tür parametreleri içerir. Son olarak, sıra numarası (sequence number) her zaman 0 sabit değerine sahiptir.

Bir Beacon Sel saldırısı, Beacon çerçevelerinin miktarında kuvvetli bir artışa neden olur. Tipik olarak, yayınlanan ESSID'ler yeni ve kısa ömürlüdür, anlaşılamaz ve rastgele oluşturulmuş isimlere sahiplerdir. Beacon çerçevelerinde artış, tüm kimliğe bürünme saldırılarında da doğal olarak meydana gelir, ancak bu gibi durumlarda ESSID, civarda zaten var olan bir ağın değerini taşır. MDK3 aracı bu saldırının

uygulanmasını sunan tek araçtır. Kimlik Doğrulama İsteği Sel saldırısına benzer şekilde, oluşturulan çerçevelerin statik değerinde bir zaman damgası (timestamp) alanı vardır (0x0000000000000000). Ayrıca, sıra numarası artmaz ve tüm çerçeveler için 0 kalır. Son olarak, Kısa Başlangıç (short preamble) ve Kısa Slot Süresi (short slot time) işaretleri (flag) eşzamanlı olarak 0 olarak ayarlanmıştır.

Prob Yanıt Sel saldırısı, Prob Yanıt çerçevelerinin aşırı şekilde artışıyla sonuçlanır. Kimliğe bürünme saldırılarında bu tür çerçevelerde bir artış gözlenmektedir, ancak genellikle daha hafiftir. Metasploit aracı, saldırganın bu tür saldırıları gerçekleştirmesini sağlayan bir saldırı moduna sahiptir. Metasploit ile hazırlanmış prob yanıt çerçeveleri tamamen rastgele gönderici bir adrese sahiptir.

3.1.5.2 Enjeksiyon saldırıları (Injection attacks)

Enjeksiyon saldırıları genellikle geçerli bir şekilde şifrelenmiş veri çerçevelerinin bozulmasına (deluge) neden olmaktadır.

ARP Enjeksiyon saldırılarında saldırgan, ağdan uygun yanıtı alacağını umarak, çok sayıda küçük veri çerçevesini önemli bir süre boyunca iletme isteği vardır. DS Durum (DS Status flag) işaretçisi 1 olarak ayarlanmıştır ve bu da bir ARP Enjeksiyon saldırısının bir başka göstergesidir.

Parçalanma saldırısı sırasında saldırgan, bir dizi kısa, parçalanmış veri çerçevesi enjekte eder. Başarılı olursa, bu işlem genellikle bir saniyeden fazla zaman almaz, ancak başarılı olmazsa aynı işlem tekrarlanır. Aireplay bu saldırının düzenlenmesinde kullanılan bir araçtır. Ürettiği paketleri incelendiğinde hepsinin hedef adresinde (Destination Address) (ff: ff: ff: ff: ff: ed) statik, geçersiz bir değer vardır. DS durum işaretçisi 1 olarak ayarlanır, çerçevenin uzunluğu küçüktür (ancak sabit değildir).

3.1.5.3 Kimliğe bürünme saldırıları (Impersonation attacks)

Kimliğe bürünme saldırıları, önceden var olan geçerli bir ağın yayınını yapan Beacon çerçevelerini yayınlayan komşulukta ek bir AP sağlar. Tüm kimliğe bürünme saldırılarının ortak paydası, mağdur ağının Beacon çerçevelerinin sayısının yaklaşık iki katına çıkmasıdır. Bu saldırılar ilk adım olarak kısa bir Deauthentication çerçeve seliyle birleştirilir, böylece saldırgan STA'ları, kendi hileli AP'lerine bağlanmaya zorlayabilir. Saldırganlar, **Evil Twin** saldırılarını başlatmak için Aircrack takımının Airbase aracını kullanmaktadırlar. Beklendiği gibi, ilave Beacon çerçeveleri yayınlanır, ancak bu durumda önemli ölçüde farklı özelliklere sahiptirler. Örneğin, Times-tamp alanı tüm sahte beacon çerçeveleri için sabit bir değere sahiptir (0x0000000000000000) ve Etiketli Parametreler (Tagged-Parameter) alanı sürekli farklı sayıda parametre içerir.

Caffe Latte saldırıları daha karmaşıktır. Kimliğe bürünme saldırıları kategorisine girdiklerinden, hepsi kurban ağının ESSID'sine sahip ek Beacon çerçeveleri sunacaklardır. Bu çerçeveler ayrıca Airbase aracı kullanıldığında Evil Twin saldırısı sırasında iletilenlerle aynı imza özelliklerini taşıyacaktır. Bununla birlikte, Caffe Latte saldırıları, normal bir enjeksiyon saldırısı gibi küçük boyutlu şifrelenmiş veri çerçevelerini enjekte eder ve bu da ARP Enjeksiyonu veya Evil Twin saldırısından açık bir şekilde ayırt edilmesini zorlaştırmaktadır.

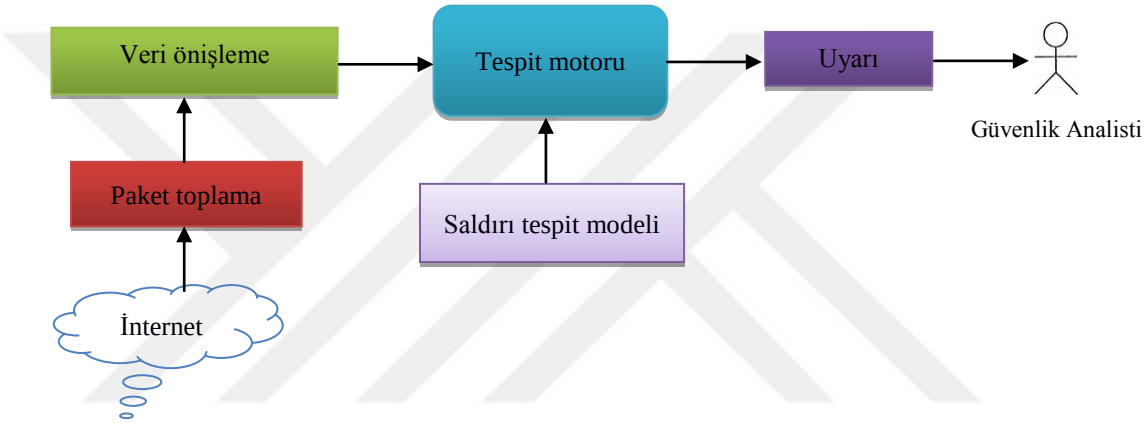
WLAN'lara yönelik yaygın olarak gerçekleştirilen saldırı türleri ve imzaları Çizelge 3.1' de verilmiştir. Yukarıda açıklanan tüm durumlarda, tüm sahte çerçevelerden alınan Sinyal Gücü, muhtemelen geçerli olarak oluşturulanlardan farklı bir değer aralığında (genellikle sahte çerçevelerde daha yüksek sinyal gücü vardır) olacaktır. Bu durum net bir gösterge değildir, ancak istatistiksel bir araç olarak kullanıldığında ve diğer faktörlerle birleştirildiğinde, genellikle bir saldırının göstergesidir.

Çizelge 3.1 WLAN'lara yönelik yapılan yaygın saldırı türleri ve imzaları

Saldırı Kategorileri	**Saldırı Türleri**	**Saldırı İmzaları**
Sel Saldırıları	Kimlik Doğrulama Sel Saldırıları	Bu saldırı sırasında, aşırı sayıda kimlik doğrulama çerçevesi üretilir.
	Kimlik Doğrulama İsteği Sel Saldırıları	Artan sayıda kimlik doğrulama talebi görülebilir. Tagged Parametreleri alanı daima sayıların normalden daha az olduğu aynı tür parametreleri içerir. Sıra numarası her zaman 0 sabit değerine sahiptir.
	Beacon Sel Saldırıları	Yayınlanan ESSID'ler yeni ve kısa ömürlüdür, anlaşılamaz ve rastgele oluşturulmuş isimlere sahiplerdir. Oluşturulan çerçevelerin statik değerinde bir zaman damgası alanı vardır. Kısa Başlangıç ve Kısa Slot Süresi işaretleri eşzamanlı olarak 0 olarak ayarlanmıştır.
	Prob Yanıt Sel Saldırıları	Prob Yanıt çerçevelerinin aşırı şekilde artışıyla sonuçlanır. Bu saldırı türü genellikle Metasploit aracı ile gerçekleştirilir.
Enjeksiyon Saldırıları	ARP Enjeksiyon Saldırıları	Çok sayıda küçük veri çerçevesini önemli bir süre boyunca iletme isteği vardır. DS Durum işaretçisi 1 olarak ayarlanmıştır.
	Parçalanma Saldırıları	Bir dizi kısa, parçalanmış veri çerçevesi enjekte edilir. Bu saldırı türü genellikle Aireplay aracı ile gerçekleştirilir. Ürettiği paketleri incelendiğinde hepsinin hedef adresinde statik, geçersiz bir değer vardır. DS durum işaretçisi 1 olarak ayarlanmıştır.
Kimliğe Bürünme Saldırıları	Evil Twin Saldırıları	Bu saldırı türü genellikle Aircrack takımının Airbase aracı ile gerçekleştirilir. İlave Beacon çerçeveleri yayınlanır. Times-tamp alanı tüm sahte beacon çerçeveleri için sabit bir değere sahiptir. Etiketli Parametreler alanı sürekli farklı sayıda parametre içerir.
	Caffe Latte Saldırıları	Kurban ağının ESSID'sine sahip ek Beacon çerçeveleri sunarlar. Küçük boyutlu şifrelenmiş veri çerçevelerini enjekte eder.

3.2 WLAN İncelemesinde Yaygın Olarak Kullanılan Araçlar

İletişim ağlarındaki izinsiz girişleri tespit etmek için birçok farklı IDS araçları vardır. Kategorik olarak IDS araçları ikiye ayrılmaktadır: açık kaynaklı ve ticari. Açık kaynak IDS araçlarının basit lisans yönetimi, daha düşük donanım ve yazılım maliyetleri, çok sayıda destek ve satıcı kısıtlaması olmaması gibi çeşitli avantajları vardır. Öte yandan, ticari IDS araçlarının net kullanım politikası, yüksek kaliteli yazılımları, geliştirme ve bakım için daha fazla fonu, zamanında güncellemeleri ve sorunlar için yardımı vardır. IDS araçlarının genel çalışma prensibi Şekil 3.1'de görülebilir.



Şekil 3.1 Saldırı tespit araçlarının genel çalışma prensibi

Antivirüs programından ağ trafiğini izleyen hiyerarşik sistemlere kadar çok çeşitli IDS araçları bulunmaktadır. En yaygın olan araçlar aşağıda detaylı olarak açıklanmıştır.

3.2.1 SolarWinds Security Event Manager

Log yöneticisi olan bu sistem, ana bilgisayar tabanlı izinsiz giriş algılama sistemidir. Bununla birlikte, bir paket dinleyicisi olan Snort tarafından toplanan verileri ağ tabanlı saldırı tespit sisteminin bir parçası yaparak da yönetir. Security Event Manager'ın NIDS olarak kullanabilmek için Snort'u bir paket yakalama aracı olarak kullanmak ve toplanan verileri analiz için Security Event Manager'a yönlendirmek gerekmektedir.
SolarWinds ürünü bir izinsiz giriş önleme sistemi olarak da çalışabilmektedir, çünkü izinsiz giriş tespiti üzerindeki eylemleri tetikleyebilmektedir. Araç, şüpheli faaliyetlerin tespit edilmesini ve otomatik olarak düzeltme etkinliklerinin uygulanmasını sağlayan

700'den fazla olay korelasyon kuralına sahiptir. Bu eylemler Aktif Yanıtlar (ekran mesajları veya e-posta yoluyla uyarılar, kullanıcı hesabının askıya alınması veya silinmesi, IP adresi engelleme, işlem sonlandırma, sistem kapatma veya yeniden başlatma vb.) olarak adlandırılmaktadır (Administrator Guide 2021).

3.2.2 Snort

Snort, NIDS'te endüstri lideri olarak adlandırılmaktadır ve açık kaynak kodlu bir araçtır. Windows' da çalışabilen az sayıdaki IDS aracından biridir. 1998 yılında Martin Roesch tarafından geliştirilmiştir. Snort kullanmanın temel avantajı, gerçek zamanlı trafik analizi ve ağda paket loglama yeteneğidir. Protokol analizi, içerik arama ve çeşitli ön işlemcilerin işlevselliği ile Snort, çeşitli solucanlar, istismarlar, port taraması ve diğer zararlı tehditleri tespit etmek için kullanılan yaygın bir araç olarak kabul edilmektedir. İzleme, paket kaydetme ve saldırı tespiti olmak üzere üç ana modda yapılandırılmıştır. İzleme modunda, program sadece paketleri okumakta ve bilgileri konsolda göstermektedir. Paket kaydetme modunda, paketler diske kaydedilmektedir. Saldırı tespit modunda, program gerçek zamanlı trafiği izlemekte ve kullanıcı tarafından tanımlanan kurallarla karşılaştırmaktadır (Bhosale ve Mane 2015, KR ve Indra 2010, Timofte 2008).

3.2.3 OSSEC

OSSEC, log analizi, bütünlük kontrolü, kayıt defteri izleme, rootkit tespiti, zamana dayalı uyarı ve aktif cevaplama gibi çeşitli görevleri yerine getiren açık kaynak kodlu bir HIDS güvenlik aracıdır. Ana bilgisayar tabanlı saldırı tespit sistemi olan program, yüklenilen bilgisayardaki log dosyalarına odaklanmaktadır. Olası girişimi bulmak için tüm log dosyalarının sağlama toplamı imzalarını (checksum signature) izler. Windows'ta, kayıt defterinde yapılan değişiklikler üzerindeki sekmeleri tutar. Unix benzeri sistemlerde, root hesaba ulaşma girişimlerini izler (KR ve Indra 2010).

OSSEC sistemi aşağıdaki üç ana bileşenden oluşmaktadır:
Ana uygulama: Bu kurulumlar için temel bir gerekliliktir. OSSEC Linux, Windows, Solaris ve Mac ortamları tarafından desteklenmektedir.

Windows aracısı: Bu, yalnızca Windows tabanlı bilgisayarlara/istemcilere ve sunuculara OSSEC yükleneceği zaman gereklidir.
Web arayüzü: Kuralları ve ağ izlemeyi tanımlamak için web tabanlı GUI uygulamasıdır.

OSSEC'in log dosyaları FTP, posta ve web sunucusu verilerini içermektedir. Ayrıca işletim sistemi loglarını, trafik loglarını, güvenlik duvarı ve antivirüs loglarını ve tablolarını izlemektedir. OSSEC'in davranışı, üzerine kurulan politikalar tarafından kontrol edilir. Bir politika bir uyarı koşulunu (alert condition) tanımlar. Bu uyarılar konsolda görüntülenebilir veya e-posta yoluyla bildirim olarak gönderilebilir.

3.2.4 Suricata

Suricata, Open Information Security Foundation tarafından geliştirilen açık kaynak kodlu, hızlı ve oldukça sağlam bir ağ saldırı tespit sistemidir. Suricata, gerçek zamanlı saldırı tespiti, önleme ve ağ güvenliği izleme özelliğine sahiptir. Suricata, Yakalama, Toplama, Kod Çözme, Algılama ve Çıktı gibi birkaç modülden oluşur. Suricata hem imza hem de anomali tabanlı yöntemler kullanır. Suricata, Snort'un ana alternatifidir. Snort'a göre önemli bir avantajı vardır, o da uygulama katmanında veri toplamasıdır. Snortun, birkaç TCP paketine bölünmüş imzalara sahip olma zorunluluğu eksikliğini ortadan kaldırmaktadır. Suricata, paketlerdeki tüm verilerin, bilgileri analiz etmeye başlamadan önce toplanmasını bekler. Sistem uygulama katmanında çalışsa da, protokol etkinliğini IP, TLS, ICMP, TCP ve UDP gibi düşük seviyelerde izleyebilir. FTP, HTTP ve SMB dahil olmak üzere farklı ağ uygulamaları için gerçek zamanlı trafiği inceler. Yalnızca paket yapısına bakmaz, TLS sertifikalarını inceleyebilir, HTTP isteklerine ve DNS çağrılarına odaklanabilir. Dosya çıkarma özelliği ile virüs özellikli şüpheli dosyaları incelenmesine ve izole edilmesine olanak sağlar (Bhosale ve Mane 2015).

3.2.5 Bro

Bro, saldırı tespitinin ötesine geçen ve diğer ağ izleme işlevlerini sağlayabilen bir ağ tabanlı IDS'dir. Bro saldırı tespit fonksiyonu iki aşamada gerçekleştirilir: trafik kaydı ve analizi. Suricata gibi Bro da uygulama katmanında çalıştığından Snort'a karşı büyük bir

avantaja sahiptir. Bro analiz modülünün hem imza analizi hem de anomali tespitinde çalışan iki unsuru vardır (Resmi ve Manicka 2017).

Bro Event Engine: Ağda olağandışı bir şey olduğunda uyarı oluşturmak için anlık veya kaydedilmiş ağ trafiği paketlerini analiz eder. Yeni bir TCP bağlantısı veya bir HTTP isteği gibi olayları izler. Her olay kaydedilir, bu nedenle sistemin bu kısmı politika açısından tarafsızdır.

Bro Policy Scripts: Bunlar, uyarı oluşturmak için olayları analiz eder. Uyarılar, e-posta göndermek, alarm vermek, sistem komutlarını uygulamak ve hatta acil durum numaralarını aramak gibi politika komutları kullanılarak gerçekleştirilir.
Bro, HTTP, DNS ve FTP etkinliklerini ve ayrıca SNMP trafiğini izleyebilir ve cihaz yapılandırma değişikliklerinin kontrol edilebilmesini sağlar. Düşük seviyelerde, DDoS saldırılarına dikkat edebilir ve bağlantı noktası taramaları tespit edilebilir. Bro, Unix, Linux ve MacOS işletim sistemlerine yüklenebilir.

3.2.6 Sagan

Sagan, ana bilgisayar tabanlı izinsiz giriş tespit sistemidir, bu yüzden OSSEC'e bir alternatiftir. HIDS olmasına rağmen, program bir NIDS sistemi olan Snort tarafından toplanan verilerle uyumludur. Bro ve Suricata'dan gelen veri kaynakları da Sagan'a beslenebilir. Bu araç Unix, Linux ve Mac OS işletim sistemlerine yüklenebilmektedir. Sagan, Windows'ta çalışmasa da, Windows olay günlüklerini içine yüklenebilmektedir.
Sagan bir log analiz aracıdır. Tek başına bir NIDS olabilmesi için sahip olmadığı unsur, paket dinleme modülüdür. Ancak, olumlu olarak, bu, Sagan'ın özel bir donanım gerektirmediği ve hem ana bilgisayar günlüklerini hem de ağ trafiği verilerini analiz etme esnekliğine sahip olduğu anlamına gelmektedir. Analiz modülü hem imza hem de anomali tabanlı metodolojileri ile çalışmaktadır. Sagan, bir log analiz aracı olduğundan dolayı herkesin en iyi IDS aracı listesine girememektedir. Ancak, NIDS olabilme özelliğine sahip bir HIDS olması, onu hibrit IDS analiz aracı olarak ilginç bir öneri haline getirmektedir. Sagan'ın farklı bir özelliği ise, şüpheli etkinlik olarak algılanan IP adreslerinin coğrafi konumunun görülmesini sağlayan bir IP konumlandırıcı

içermesidir. Bu, bir saldırı oluşturmak için uyumlu olarak görünen IP adreslerinin eylemlerinin bir araya getirilmesine olanak sağlar (Gassais vd. 2020).

3.2.7 Security Onion

IDS araçlarının çoğu açık kaynak kodlu projelerdir. Security Onion geliştiricisi bu durumdan faydalanarak, Snort, Suricata, OSSEC ve Bro'un kaynak kodundan elementler alınmıştır ve Linux tabanlı NIDS&HIDS olan hibrit bir IDS oluştumuştur. Security Onion Ubuntu'da çalışacak şekilde yazılmıştır ve Snorby, Sguil, Squert, Kibana, ELSA, Xplico ve NetworkMiner gibi analiz araçlarından unsurlar da entegre edilmiştir (Lupari 2021).

Her ne kadar Security Onion, NIDS olarak sınıflandırılsa da, HIDS fonksiyonlarını da içermektedir. Logları ve yapılandırma dosyalarını şüpheli etkinliklere karşı izler ve beklenmedik değişiklikler için bu dosyaların sağlama toplamlarını (checksum) kontrol eder. Security Onion'un ağ izlemeye yönelik kapsamlı yaklaşımının bir dezavantajı karmaşık olmasıdır. Birkaç farklı işletim yapısına sahiptir ve ağ yöneticisinin aracın tüm yeteneklerine hakim olabilmesi için çevrimiçi ya da paketlenmiş yeterli öğrenme materyali yoktur.

3.2.8 AIDE

AIDE (Advanced Intrusion Detection Environment), Unix ve benzeri işletim sistemleri için rootkit tespiti ve dosya imza karşılaştırmalarına odaklanan bir HIDS'tir. AIDE, config dosyalarından bulduğu düzenli ifade kuralları ile bir veritabanı oluşturur. Araç hem imza hem de anomali tabanlı izleme yöntemlerini içerir. Sistem kontrolleri talep üzerine yapılır ve sürekli çalışmaz, bu da HIDS ile ilgili bir eksikliktir. Bu bir komut satırı işlevi olsa da, cron gibi bir işletim yöntemiyle periyodik olarak çalışacak şekilde zamanlanabilmektedir. Gerçek zamanlı verilerle çalışmak istendiğinde, çok sık çalışacak şekilde programlanabilmektedir (Lai vd. 2021).

3.2.9 Open WIPS-NG

Aircrack-NG'yi ile aynı girişimci tarafından geliştirilmiştir. Open WIPS-NG kablosuz ağları savunmak için tasarlanmıştır ve yalnızca Linux'ta çalışmaktadır. “WIPS” adı “kablosuz izinsiz giriş önleme sistemi” anlamına gelmektedir, bu nedenle bu NIDS, hem izinsiz girişi algılar hem de engeller. Sistem algılayıcı (sensor), sunucu (server), arayüz (interface) olmak üzere üç bileşenden oluşur. Sensör, orta akışta (mid-flow) kablosuz yayınları değiştirme yeteneğine sahip olan bir paket algılayıcıdır. Böylece sensör, sistemin alıcı-vericisi olarak hareket eder. Sensör tarafından toplanan bilgiler, olayın gerçekleştiği sunucuya iletilir. Sunucu izinsiz girişleri algılayacak analiz motorunu içerir. Algılanan izinsiz girişleri engellemeye yönelik müdahale ilkeleri de sunucuda üretilir. Ağı korumak için gerekli eylemler sensöre talimat olarak gönderilir. Sistemin arayüz modülü, sistem yöneticisine olayları ve uyarıları gösteren görsel bir panodur. Aynı zamanda ayarların yapılabileceği ve savunma eylemlerinin ayarlanabileceği/geçersiz kılınabileceği modüldür (Resmi ve Manicka 2017).

3.2.10 Samhain

Almanya'da Samhain Design Labs tarafından üretilen Samhain, ana bilgisayar tabanlı bir saldırı tespit sistemidir. Her makinede çalışan ajanlar tarafından tespit edilen olaylarla ilgili merkezi veri toplama olanağı sunar ve tek bir bilgisayarda veya birçok ana bilgisayarda çalıştırılabilir (Wang vd. 2013).

Her ajan tarafından gerçekleştirilen görevler dosya bütünlüğü kontrolü, günlük dosyası izleme ve port izlemedir. İşlemler rootkit virüslerini, sahte SUID'leri (kullanıcı erişim hakları) ve gizli işlemleri arar. Sistem, çoklu ana bilgisayar (multi-host) uygulamalarında aracılar ve merkezi denetleyici arasındaki iletişimlere şifreleme uygular. Samhain tarafından toplanan veriler ağdaki aktivitelerin analizini sağlar, saldırılara yönelik uyarı işaretleri verir, ancak, izinsiz girişleri engelleyemez. Ek olarak bu araç, işlemlerini gizli tutmak için gizli bir teknoloji kullanmaktadır ve böylece davetsiz misafirlerin IDS'yi manipüle etmelerini engellemektedir. Bu gizli yönteme “steganografi” adı verilmektedir. Merkezi log dosyaları ve yapılandırma yedekleri, davetsiz misafirlerin müdahalesini önlemek için bir PGP anahtarıyla işaretlenmektedir.

3.2.11 Fail2Ban

Fail2Ban, başarısız oturum açma girişimleri gibi log dosyalarında kaydedilen şüpheli olayları tespit etmeye odaklanan ana bilgisayar tabanlı bir saldırı tespit sistemidir. Sistem, şüpheli davranış gösteren IP adreslerini engeller. Bu yasaklar genellikle sadece birkaç dakika sürer, ancak standart bir kaba kuvvet şifre kırma senaryosunu bozmak için yeterli olabilmektedir. IP adres yasağının gerçek uzunluğu bir yönetici tarafından ayarlanabilmektedir (Ford vd. 2016).

Fail2Ban aslında bir izinsiz giriş önleme sistemidir, çünkü şüpheli bir etkinlik tespit edildiğinde harekete geçebilir ve sadece kaydetme yapmaz, olası izinsiz girişleri vurgular. Bu nedenle, sistem yöneticisinin yazılımı kurarken erişim politikaları konusunda dikkatli olması gerekir, çünkü çok sıkı bir önleme stratejisi iyi niyetli kullanıcıları kolayca kilitleyebilir. Fail2Ban ile ilgili bir sorun, tek bir adresten tekrarlanan eylemlere odaklanmasıdır. Bu, dağıtılmış parola kırma eylemleri veya DDoS saldırılarıyla başa çıkma yeteneği vermez.

3.2.12 Bölüm değerlendirmesi

Bu alt bölümde, IDS araçları çalışma prensibi, saldırıları tespit etme stratejisi, desteklenen platformlar, avantajlar ve dezavantajlar temelinde incelenmiştir. Mevcut IDS araçlarının karşılaştırması Çizelge 3.2'de özetlenmiştir. Çizelge 3.2'den de görüleceği gibi IDS tipleri HIDS ve NIDS olabilir. IDS araçlarından bazıları çoklu platformları desteklerken diğerleri tek platformu destekler. Snort IDS, birden fazla platformu destekleyen, imzalara ve anormalliklere dayalı olarak izinsiz girişleri tespit etmek için birçok kuralı olan ilk araçlardan biridir. Ancak Snort, parçalanmış paketleri etkili bir şekilde algılayamaz ve büyük ağlarda paketleri izlemek zordur. Suricata IDS aracı, birden çok işletim sistemi ortamını desteklemenin yanı sıra daha yüksek ve daha düşük seviyeli protokolleri de destekler. Öte yandan, Suricata için CPU kullanımı yüksektir ve kurulum süreci karmaşıktır.

Bro, ağdaki anormallikleri algılamanın yanı sıra imza analizini kullanır. Uygulama düzeyinde inceleme, analiz gerçekleştirir ve SNMP, FTP, DNS ve HTTP dahil olmak

üzere çeşitli protokolleri destekler. Ancak, Bro IDS aracında kullanılabilirlik, GUI'ler ve kurulumla ilgili bazı zorluklar vardır. OSSEC, çapraz platformları destekler, güçlü bir analiz motoru, rootkit algılama, Windows kayıt denetimi, gerçek zamanlı uyarı ve yanıt sağlar. Ancak OSSEC, Windows'ta yalnızca sunucu-aracı modunu destekler ve OSSEC IDS araçlarının kurulumu ve yönetimi alan bilgisi gerektirir. OpenWIPS-NG, özellikle kablosuz ağlar için tasarlanmış bir IDS ve IPS aracıdır. Linux işletim sistemi üzerinde, izinsiz giriş dedektörü ve Wi-Fi paket dinleyicisi olarak çalışır. DoS saldırılarını algılar, eklentileri destekler ve paketleri birleştirir. Öte yandan, OpenWIPS-NG, her kurulum için bir sensör gerektirir ve bir NIDS olarak bazı sınırlamaları vardır. SolarWinds Security Event Manager, çeşitli işletim sistemleri tarafından oluşturulan mesajları günlüğe kaydedebilen ticari bir ağ güvenlik aracıdır. HIDS olarak kategorize edilebilir, ancak Snort tarafından toplanan ve NIDS olarak da kabul edilen verileri yönetir. Davranış profili oluşturmayı, uygulama ve kullanıcı izlemeyi, raporlama ile günlük yönetimini destekler ve dosya bütünlüğü izleme sağlar.

Security Onion, Linux dağıtımı için günlük yönetimi ve kurumsal güvenlik izlemenin yanı sıra bir IDS aracıdır. Ön uç analizinden farklı bileşenleri birleştirir. Security Onion, NIDS olarak kategorize edilmesine rağmen, birkaç HIDS işlevine sahiptir. Öte yandan, Security Onion'un dezavantajları, ağ izleme için karmaşık bir yöntem kullanması ve aracın öğrenme eğrisinin zorlu olmasıdır. Samhain dosyayı günlüğe kaydeder, bağlantı noktalarını izler, dosya bütünlüğü denetimi sağlar ve rootkit'i algılar. Samhain, merkezi günlük kaydı, merkezi güncellemelerle depolama ve web tabanlı yönetim konsolu sağlar. Samhain, bütünlüğünü korumak için gizli mod, yapılandırma dosyaları ve steganografi dahil olmak üzere çeşitli özellikler uygular. Ancak, pahalı bütünlük denetleyicileri nedeniyle Samhain çok fazla işlemci gücü kullanır. Fail2ban, günlük dosyalarını izleyen, kötü niyetli IP'lerden gelen trafiği önleyen, saniye başına istek sayısını sınırlayan ve araştırma girişimlerini durduran bir IDS/IPS yazılım çerçevesidir. Fail2ban IDS aracında bir filtre ve eylem kombinasyonuna hapishane adı verilir. Hapishane, kötü niyetli ana bilgisayarları tespit etmek ve bu ana bilgisayarların belirtilen ağ hizmetlerine erişmesini engellemek için kullanılır.

Çizelge 3.2 Yaygın kullanılan saldırı tespit araçları özeti

Araç İsmi	IDS Türü	Desteklenen Platform	Temel Özellikler
Snort	NIDS	Unix, Linux, MacOs, Windows, FreeBSD	Saldırıları gerçek zamanlı olarak tespit etmek için yakalanan trafiği analiz eder. Dos, DDos, port taramaları, nmap taramaları, SBM probları, CGI saldırıları, NetBIOS sorguları dahil olmak üzere çeşitli saldırıları tespit edebilir.
Suricata	NIDS	Unix, Linux, MacOs, Windows, FreeBSD	SMB, HTTP, FTP dahil olmak üzere çok iş parçacıklı, daha yüksek seviyeli protokolleri ve TLS, UDP, TCP, ICMP gibi daha düşük seviyeli protokolleri destekler.
Bro	NIDS	Unix, Linux, MacOs	İmza analizini kullanır ve anormallikleri tanımlar. Uygulama düzeyinde inceleme, ve analiz gerçekleştirir. çeşitli protokolleri destekler: SNMP, FTP, DNS ve HTTP.
OSSEC	HIDS	Unix, Linux, MacOs, Windows	Güçlü bir analiz motoru, rootkit algılama, Windows kayıt denetimi ve gerçek zamanlı uyarı ve yanıt sağlar.
OpenWIPS-NG	NIDS	Linux	OpenWIPS-NG aracı, bir izinsiz giriş dedektörü ve Wi-Fi paket dinleyicisi olarak çalışır. Dos saldırılarını algılar, eklentileri destekler ve paketleri birleştirir.
SolarWinds Security Manager	HIDS	Linux ve Windows	Tehdit algılama ve yanıtlarını otomatikleştiren ticari bir ağ güvenlik aracıdır. Davranış profili oluşturmayı, uygulama ve kullanıcı izlemeyi, raporlama ile günlük yönetimini destekler ve dosya bütünlüğü izleme sağlar.
Security Onion	NIDS ve HIDS	Linux, MacOs	ELSA, Kibana, NetworkMiner, Sguil, Snorby ve Xplico gibi ön uç analiz araçlarından farklı bileşenleri entegre eder.
Samhain	HIDS	Linux, bütün POSIX/UNIX sistemleri	Dosyayı ve bağlantı noktası izlemeyi günlüğe kaydeder, dosya bütünlüğü denetimi sağlar ve rootkit'i algılar. Samhain, merkezi günlük kaydı, merkezi güncellemelerle depolama ve web tabanlı yönetim konsolu sağlar.
Fail2Ban	HIDS	Unix benzeri sistemler	Günlük dosyalarını izler, kötü niyetli IP'lerden gelen trafiği önler, saniye başına istek sayısını sınırlar ve araştırma girişimlerini durdurur.
Sagan	HIDS log analizör	Unix, Linux, MacOs	Açık kaynak ve çok iş parçacıklı mimariyi destekleyen gerçek zamanlı bir günlük analizörüdür. Sagan aracı, analiz, raporlama, olay algılama ve günlük normalleştirme için çeşitli çıktı biçimlerini destekler. Sagan'ın dezavantajı, gerçek bir IDS olmamasının yanı sıra zor kurulum sürecidir.
AIDE	HIDS	Unix, Linux, MacOS	Dosya içeriğindeki değişiklikleri, kayıt özetlerini, izinleri, değişiklik zamanlarını vb. algılayabilen dosya bütünlüğü denetleyicisidir.

Genel olarak, farklı durumlar ve platformlar için bir IDS aracının diğerinden daha iyi performans gösterebileceği söylenebilir. Bunun nedeni, şirketlerin isteklerinin ve ihtiyaçlarının değişkenlik göstermesidir. Ağların bant genişliği, IDS araçlarının ölçeklenebilirliği, IDS'nin performansı, şirketin büyüklüğü ve kurban sistemin karmaşıklığı, hedef için en uygun IDS seçilirken dikkate alınması gereken kriterlerdir.

3.3 WLAN Saldırı Tespitinde Kullanılan Veri Setleri

İzinsiz giriş tespit sistemlerinin etkinliğini değerlendirmek için önerilen IDS'nin iyi bilinen veri kümeleri üzerinde test edilmesi gerekir. Güvenilir bir IDS veri seti oluşturmak için, ilk olarak, paket analiz araçları kullanılarak ağ akışları toplanır. Ardından, önemli ağ özelliklerini toplamak için toplanan ağ akışları manuel olarak veya otomatik olarak analiz edilir. Ağ akışları, kaynak ve hedef IP adreslerinden, kaynak ve hedef bağlantı noktalarından, paket uzunluğundan, ağ hizmetleri türünden, başarısız oturum açma girişimi gibi bilgilerden oluşur (Verma vd. 2020). Veri kümesi oluşturulduktan sonra, saldırı tespit sistemleri ağ saldırılarını tespit etmek ve sınıflandırmak için saldırı kalıplarını çıkarır. Bu çalışmada, izinsiz giriş tespit sistemleri için KDD '99, CAIDA, NSL-KDD, ADFA-LD ve ADFA-WD, AWID, UNSW-NB15 ve CICIDS dahil olmak üzere kullanıma açık çeşitli veri kümeleri incelenmiştir. Tez çalışması kapsamında faydalanılan veri setleri ise uygulama kısmında (bkz. Bölüm 5) daha detaylı analiz edilmiştir. Bu veri kümeleri, ağ saldırı tespiti için iyi bilinir ve birçok bilimsel ve ticari çalışmada kullanılmaktadır. Literatürdeki birçok veri seti değerli sonuçlara ve değerlendirmelere imza atmış olsalar da zamanla güncelliklerini kaybettikleri görülmektedir. Bu nedenle IDS'ler için yeni, gerçeğe uygun ve güncel saldırıları da kapsayan veri kümelerinin oluşturulması gerekmektedir. Aynı zamanda, ağ saldırı türleri zamanla değiştiğinden, mevcut ihtiyaçları karşılamak için IDS'lerin veri kümeleri ve özellikleri güncellenmelidir (Thakkar ve Lohiya 2020).

3.3.1 KDD'99 veri seti

Ağ trafiği akışlarını içeren ilk veri seti DARPA'dır (Defense Advanced Research Project Agency) (Siddique vd. 2019). DARPA veri seti, 1998 yılında MIT Lincoln LAB'de oluşturulmuştur ve ham veri TCP paket akışından oluşmaktadır. DARPA veri seti ham verilerden oluştuğu için makine öğrenmesi sınıflandırma algoritmalarının yapılması mümkün olmamıştır. Makine öğrenmesi sınıflandırıcılarını gerçekleştirmeden önce özniteliklerin çıkarılması gerekmekteydi. 1999 yılında DARPA veri setinin öznitelik çıkarımlı versiyonu olan Bilgi Keşfi ve Veri Madenciliği (KDD '99) veri seti önerilmiştir. KDD'99 veri seti, DoS (hizmet reddi) saldırısı, uzaktan yerel (R2L) saldırı, kullanıcıdan uzak (U2R) saldırı, prob saldırısı ve normal olmak üzere beş gruba ayrılan

etiketli bir sınıfa sahiptir. Eğitim için veri kümesi 24 farklı saldırı türü içerir ve test veri kümesi eğitimden farklı olarak 14 farklı bilinmeyen saldırı türü içerir. KDD'99 veri setinde saldırı türleri ve normal sınıf etiketleri eşit olarak dağılmamaktadır. Ayrıca oldukça büyük bir veri setidir, birçok yedekli özellik içerir ve son ağ saldırılarını içermez.

3.3.2 CAIDA veri seti

CAIDA veri seti, 2007'de bir saatlik anonim ağ trafiği izlerinden oluşmaktadır (Hick vd. 2007). Bu veri kümesi, meşru kullanıcıların hedeflenen sunuculara erişmesini engellemeye çalışan DDoS saldırılarını içerir. CAIDA veri setinin dezavantajı, içerdiği ağ saldırı çeşidinin az olması ve tüm ağ verilerini içermemesidir. Ayrıca CAIDA veri seti etiketlenmemiştir ve 20 özellikten oluşmaktadır.

3.3.3 AWID veri seti

AWID veri seti, büyük paket kümesinden (F) ve daha küçük bir paketten (R) oluşur. Bu iki versiyon ilişkili değildir, yani küçük olan paket büyükten üretilmemiştir. Aslında, farklı zamanlarda, farklı ekipmanlarla ve farklı ortamlarda yakalanmışlardır (Kolias vd. 2015). Her versiyonda bir eğitim seti (Trn) ve bir test seti (Tst) vardır. Enjeksiyon, taşma, kimliğe bürünme ve normal dahil olmak üzere 4 etiket içerir. Eğitim veri seti, arp, authentication request, amok, cafe latte, beacon, evil twin, probe yanıtı, deauthentication, parçalanma ve normal olmak üzere 10 sınıftan oluşur. Test veri seti 17 sınıf içerir. AWID'in geniş veri kümesi, eğitim için 162.375.247 kayıt ve test için 48.524.866 kayıt içerir (Thanthrige vd. 2016). Azaltılmış veri kümesinde eğitim için 1.795.575 kayıt ve test için 575.643 kayıt bulunur. AWID veri seti, mevcut IDS testleri için önemlidir, çünkü bu veri setinde özellik mühendisliği yapmak ve makine öğrenme algoritmalarını uygulamak kolaydır. Her bir kayıt, bir saldırı sırasında kaydın normal mi yoksa aktarılmış mı olduğunu gösteren sınıf niteliği dahil olmak üzere 155 nitelik içerir. Bu özelliklerden bir kısmı saldırıları tespit etmek için yararlıdır, bazıları yanıltıcı olabilirken bazıları sadece gürültüdür.

3.3.4 NSL-KDD veri seti

NSL-KDD, KDD'99 veri setinin geliştirilmiş bir versiyonudur. KDD veri setinde birkaç özellik tekrarlanmıştır. Yinelenen kayıtların büyük bir yüzdesi nedeniyle, makine öğreniminin performansı etkilenmektedir. Ayrıca, KDD veri setinin boyutu çok büyüktür ve bu da ML analizini zorlaştırmaktadır. Öte yandan, 2009 yılında Tavalaee vd. (2009), KDD veri kümesindeki yinelenen kayıtları kaldıran ve veri kümesinin boyutunu azaltan bir NSL-KDD veri kümesi oluşturmuştur. NSL-KDD eğitim veri seti 125.973 ve test veri seti 22.544 örnekten oluşmaktadır. Ayrıca NSL-KDD, 41 özellik ile eğitim için 22 farklı saldırı etiketine sahiptir. NSL-KDD veri seti, mevcut IDS'leri test etmek için uygundur. ML performanslarını daha da artırmak için, ML algoritmalarını gerçekleştirmeden önce NSL-KDD veri setinde özellik mühendisliği uygulanabilir.

3.3.5 ADFA-LD ve ADFA-WD veri seti

2014 yılında, Avustralya Savunma Kuvvetleri Akademisi'nde (ADFA) çalışan araştırmacılar, iki modern saldırı tespit veri seti oluşturdu: ADFA-LD (Linux veri seti) ve ADFA-WD (Windows veri seti) (Creech 2014). Bu veri kümeleri hem Windows hem de Linux işletim sistemlerinden örnekler içermektedir. Aynı zamanda, ana bilgisayar tabanlı saldırı tespit sistemi (HIDS) sistem çağrısı izlerini içerir. Veriler, eğitim, doğrulama ve saldırı olmak üzere üç farklı veri kümesinden oluşur. Saldırı veri kümesi, normal ve sıfır gün saldırılarını içerir.

3.3.6 UNSW-NB15 veri seti

Kapsamlı ağ trafiğinden oluşan UNSW-NB15 veri seti 2015 yılında üretilmiştir. Ham ağ trafiği, IXIA aracı (Moustafa ve Slay 2015) ile oluşturulur. Oluşturulan trafik tcpdump ile yakalanır. Veri kümesi 49 özellik, 9 farklı saldırı türü ve 2,540,044 kayıt içerir. Veri kümesi, UNSW-NB15_1.csv,UNSW-NB15_2.csv, UNSW-NB15_3.csv ve UNSW-NB15_4.csv dahil olmak üzere 4 farklı csv dosyasından oluşur. Eğitim seti 175.341 kayıt, test seti ise 9 farklı saldırı ve normal kategorilerinden oluşan 82.332 kayıt içermektedir. UNSW-NB15 veri seti, kapsamlı özelliklerin yanı sıra yeni saldırı türleri içerdiğinden, modern IDS'leri test etmek için oldukça uygun olabilir.

3.3.7 CICIDS 2017 veri seti

CICIDS veri seti modem, anahtarlar, yönlendiriciler, güvenlik duvarı ve Windows, Linux ve macOS'un farklı sürümleri gibi çeşitli işletim sistemlerinden toplanan veriler ile 2017 yılında oluşturulmultur. Veri setinde kaba kuvvet (FTP, SSH), Sızma, DoS, DDoS, Heartbleed, Botnet ve Web saldırısı gibi farklı saldırı profilleri bulunmaktadır (Sharafaldin vd. 2018). CICIDS veri seti 80 özellikten oluşur.

3.3.8 CIC-DDoS2019 veri seti

CIC-DDoS2019 veri kümesi, normal trafiği ve çeşitli DDoS saldırı türlerini içerir. Veri kümesi, yüz binlerce kayıtla 88 özelliğe sahiptir. NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN ve TFTP dahil olmak üzere kullanılan protokole göre farklı DDoS türlerini gösteren birkaç ayrı .csv dosyası vardır. Bu veri kümesi bilinmeyen saldırılardan oluşan yeni bir veri kümesidir ve mevcut IDS'lerin etkinliğini ölçmek için kullanılabilir (Kousar vd. 2021).

3.3.9 BoT-IoT veri seti

BoT-IoT veri kümesi, IoT ağlarından gelen ağ trafiğini içerir. Veri kümesinin kaynak dosyaları, pcap, oluşturulan argus ve csv dosyaları dahil olmak üzere farklı biçimlerdedir. Veri kümesi herkese açıktır ve 49 özellik içerir. Veri setinde 72.000.000 kayıt bulunmaktadır. Veri kümesi, işletim sistemi ve hizmet taraması, DoS, DDoS, keylogging ve veri hırsızlığı gibi farklı türde saldırılara sahiptir. BoT-IoT veri seti, üzerinde mevcut IDS'leri test etmek için etkili olabilecek çeşitli saldırı senaryolarının yanı sıra gerçekçi ağ trafiğinden oluşur (Koroniotis vd. 2019).

3.3.10 Saldırı tespit sistemlerinde kullanılan veri setlerinin değerlendirilmesi

Mevcut IDS'lerin etkinliğini değerlendirmek için literatürde yaygın olarak kullanılan veri setleri incelenmiştir. Her veri kümesinin kendi artıları, eksileri vardır ve farklı durumlar için daha iyi çalışır. Mevcut saldırı tespit veri kümelerinin karşılaştırmalı tablosu Çizelge 3.2'de görülebilir. KDD'99 veri kümesi, IDS'ler için en büyük ve en çok kullanılan veri kümesidir, ancak bu veri kümesi, ML sınıflandırma sürecini zorlaştıran

özelliklere sahiptir. NSL-KDD veri seti, KDD'nin bir modifikasyonudur. Modern IDS'leri NSL-KDD veri kümesinde test etmek oldukça etkilidir, ancak bu veri kümesinde modern ağ saldırıları yoktur.

Çizelge 3.3 Yaygın veri setlerinin karşılaştırılması

Veri seti	Yıl	Özellik sayısı	Atak tipleri	Etiketli/ Etiketsiz	Veri sayısı
DARPA	1998	-	Dos, U2R, R2L, Probe	Etiketsiz	-
KDD '99	1999	41	Dos, U2R, R2L, Probe, Normal	Etiketli	4,900,000
CAIDA	2007	20	DDoS, Normal	Etiketsiz	-
NSL-KDD	2009	41	Dos, U2R, R2L, Probe, Normal	Etiketli	125,973 eğitim 22, 544 test
ADFA-LD ve ADFA-WD	2014	26	Stealth, Webshell, Zero-day, Dydra, Meterpreter, Adduser	Etiketli	13,675 traces
AWID	2015	155	Injection, Flooding, Impersonating, Normal	Etiketli	162,375,247 eğitim 48,524,866 test
UNSW-NB15	2015	49	Analysis, Backdoors, DoS, Exploits, Generic, Fuzzers, Reconnaissance, Shell code, Worms	Etiketli	2,540,044
CICIDS	2017	80	Brute force, Infiltration, DoS, DDoS, Heartbleed, Botnet, ,Web attack	Etiketli	-
CIC-DDoS2019	2019	88	Benign, Various DDoS attacks	Etiketli	Yüzbinlerce kayıt
BoT-IoT	2021	49	OS and service scan, DoS, DDoS, keylogging, data exfiltration attacks	Etiketli	72.000.000

CAIDA, ADFA-LD ve ADFA-WD, AWID, UNSW-NB15 ve CICIDS gibi diğer veri kümelerinin farklı eksiklikleri vardır. CIC-DDoS2019 ve BoT-IoT veri kümeleri, mevcut IDS'lerin etkinliğini ölçmek için kullanılabilecek ağ trafiğindeki son izinsiz girişleri içerir. Bu veri kümeleri, ağ saldırı tespit sistemleri için popülerdir ve birçok bilimsel çalışmada kullanılmaktadır. Ağ saldırıları zamanla geliştiğinden, gelecekteki ağ saldırılarının doğruluğunu değerlendirmek için IDS veri kümeleri ve özellikleri zaman zaman güncellenmelidir.

3.4 Bölüm Değerlendirmesi

Teknolojinin ilerlemesi ile birlikte kablolar hayatımızın büyük bir bölümünden çıkmış, yerini kablosuz cihazlar ve ortamlara bırakmıştır. Bu olumlu ilerleme ile birlikte

kablosuz ortamlar farklı güvenlik problemlerini de beraberinde getirmiştir. Günlük hayatta insanların büyük bir çoğunluğu kablosuz ağları kullanmaktadır. Ek olarak, neredeyse bütün kurum ve kuruluşlarda, evlerde, ofislerde kablosuz yerel alan ağları kullanılmaktadır. Ağ üzerinden yapılan bütün işlemlerde güvenliği sağlamak, kişisel olan ve olmayan bütün verileri korumak ve donanımların sorunsuz çalışmasını sağlamak için gelişmiş bir saldırı tespit sistemi büyük önem arz etmektedir.

Kablosuz yerel alan ağlarına olan yoğun ilgiden dolayı, saldırı tespit sistemleri alanında çalışmalarda artmıştır. Gelişmiş 802.11 WLAN güvenlik protokolüne rağmen, ne yazık ki güvenlik açıkları hala devam etmektedir ve ağlar bir dizi saldırıya karşı savunmasız kalmaktadır. Tüm WLAN açıklarını gidermek için önlemlerin alınmaması, güvenlik ihlalleri, saldırılar ve izinsiz girişlerin engellenebilmesi için sürekli WLAN'ları izlemenin zorunlu olduğunu görülmektedir. Bununla birlikte, IEEE 802.11 WLAN'larındaki olası tüm saldırıları güvenilir ve doğru bir şekilde tespit edebilen bir kablosuz saldırı tespit sistemi (WIDS) eksikliği vardır. Günümüzde kullanılan anomali tabanlı, imza tabanlı ve davranış tabanlı saldırı tespit sistemlerine karşılık, saldırılar da form değiştirmektedir. Daha önce anomali olarak belirlenen bir saldırı türü farklı bir şekilde davranarak tanımlanamamaktadır. Sonuç olarak, günümüz saldırı tespit sisteminde kullanılan çoğu teknik, bilgisayar ağlarında siber saldırıların dinamik ve karmaşık doğası ile baş edememektedir.

Tez çalışmasının bu bölümünde öncelikle kablosuz yerel alan ağlarına yönelik saldırı türleri, bu saldırıların yapılma şekillerinin araştırılmış ve bu çalışmada anlatılmıştır. Mevcut çalışmalarda kablosuz yerel alan ağlarına yapılan saldırıların tespit edilmesi ve saldırı tipinin belirlenmesi için kullanılan yöntemler (yaygın kullanılan IDS teknikleri) derinlemesine incelenmiştir. Kablosuz yerel ağlarında saldırı tespiti için kullanılan analiz araçları araştırılmıştır ve yaygın olarak kullanılan araçlar anlatılmıştır. Son olarak WLAN saldırı tespit sistemlerinde kullanılan yaygın veri setleri araştırılmış ve açıklanmıştır. Böyle bir detaylı araştırma yapılmasının nedeni çözüme yönelik çalışmalara geçmeden önce problemin zorluğunu ve sınırlarını belirlemek, daha önce yapılmış çalışmaların ne derece başarılı olup olmadığını görerek ve değerlendirerek daha iyi çalışan bir model öne sürebilmektir.

4. ÖNERİLEN METODOLOJİ

WLAN'larda saldırıların yüksek doğrulukla ve dinamik bir şekilde tespit edilebilmesi için tez kapsamında aşağıdaki üç aşamalı metodoloji önerilmiştir:

1. IDS veri setinin oluşturulması;
2. WLAN'larda saldırıların tespiti;
3. WLAN'larda tespit edilen saldırıların türlerinin belirlenmesi.

Önerilen metodolojinin aşamaları aşağıdaki bölümlerde detaylı olarak açıklanmıştır.

4.1 IDS Veri Seti Oluşturma

Genel olarak saldırıların gerçekleştirebilmesi için ilk adım, saldırı elemanları ile kurban olarak seçilen cihaza erişim sağlanmasıdır. İlgili adrese ve arabirime erişimler sağlandıktan sonra, saldırı trafiği kurban cihaza yönlendirilebilir. Saldırıların etkisi gelen paket sayısına ve paketlerin kurban cihaza ulaşma sürelerine göre değişmektedir. Aynı zamanda bu etki kullanılan cihazların sayısına, yapılan saldırının boyutuna ve amacına göre de değişmektedir. Kurban cihazların fiziksel katmandan uygulama katmanına kadar tüm bilgileri, çeşitli yazılım ve araçlar kullanarak, izlenebilmektedir.
Ancak bu saldırı araçlarına karşın ağ trafiğini izlemek için kullanılan araçlar sayesinde gelen paketlerin kaynak IP adresleri, gelen paketlerin sayısı, gönderilmeye başlandığı zaman, saldırının süresi, vb. gibi bilgiler elde edilebilmektedir. Bu bilgiler paketin her bir özelliğini temsil etmektedir. Bütün özellikler saldırı çeşitlerinin bulunması için, uygulanması gereken işlemler hakkında ipucu vermektedirler. Saldırgan cihazlar tarafından bir kurban cihaza yönlendirilen saldırılar çeşitlerine göre kaydedilerek, eğitim verisi olarak kullanılacaktır. Bu işlemlerin gerçekleştirilebilmesi için WLAN'larda en yaygın kullanılan saldırı araçları, yaygın yapılan saldırı türleri ve izleme araçları belirlenmelidir. Bu kapsamda öncelikle, saldırgan cihazlar ve kurban cihaz belirlemek gerekmektedir. Daha sonra saldırı paketlerinin gönderilmesi için farklı saldırı türlerine göre saldırı yazılım araçları belirlenmektedir. Saldırıları gerçekleştirmek için kullanılan test amaçlı birçok saldırı aracı bulunmaktadır. Bu saldırı araçları amaçlarına yani gerçekleştirmek istedikleri saldırı çeşidine göre farklılık göstermektedir. Veri seti oluşturmak için saldırgan olarak belirlenen cihazlardan gelen

farklı saldırılar, kurban bilgisayar tarafından ağ izleme sistemi kullanılarak izlenebilir, bu sayede gerekli olan özelliklerden oluşan veri setleri kolaylıkla oluşturulabilir.

4.1.1 Saldırı türlerinin belirlenmesi

WLAN'lara karşı aktiften pasife birçok saldırı türü bulunmaktadır. Saldırı türleri belirlenirken günümüzde yaygın olarak karşılaşılan ve literatürdeki veri setlerinde bulunan saldırı türleri incelenmiştir. Bunların başında ise son yıllarda popüler olan ve yüksek oranda maddi kayıplara sebep olan DoS saldırıları gelmektedir. DoS saldırıları genelde TCP/IP protokol yapısındaki açıklardan faydalanarak veya bir sunucuya çok sayıda istek göndererek çalışamaz hale gelmesine sebep olan saldırılardır. Veri seti oluşturulurken de DoS saldırı türlerine ağırlık verilmiştir.

DoS saldırılarının iki genel yöntemi vardır: sel veya hizmetleri devre dışı bırakma (flooding services or crashing services). Sel saldırıları, sistem sunucunun arabelleğe alması için çok fazla trafik aldığında meydana gelir ve bu da sunucunun yavaşlamasına ve sonunda durmasına neden olur. Popüler sel saldırıları şunları içerir:

Tampon taşması (Buffer overflow) saldırıları – en yaygın DoS saldırısıdır. Konsept, bir ağ adresine, programcıların sistemi işlemek için oluşturduğundan daha fazla trafik göndermektir. Belirli uygulamalara veya ağlara özgü hatalardan yararlanmak için tasarlanmıştır.

ICMP taşması – yalnızca belirli bir cihaz yerine hedeflenen ağdaki her bilgisayara ping gönderen sahte paketler göndererek yanlış yapılandırılmış ağ cihazlarından yararlanır. Ağ daha sonra trafiği yükseltmek için tetiklenir. Bu saldırı aynı zamanda smurf saldırısı veya ölüm pingi (death of ping) olarak da bilinir.

SYN taşması – bir sunucuya bağlanmak için bir istek gönderir, ancak el sıkışmayı asla tamamlamaz. Tüm açık bağlantı noktaları isteklerle dolana ve meşru kullanıcıların bağlanabileceği hiçbir bağlantı kalmayana kadar devam eder. Örneğin neptune saldırısı.
DoS saldırılarına ek olarak bir cihazın geçerli IP adreslerini, aktif portlarını veya işletim sistemini öğrenmek için yapılan saldırı türleri de vardır. Bu tür probe saldırılarına da

veri setinde yer verilecektir. Bahsedilen saldırılar kadar yoğun olmasa da kullanıcı haklarına sahip olunmadığı durumda misafir ya da başka bir kullanıcı olarak bilgisayar sistemine izinsiz erişim yapılması veya bilgisayar sistemine girme izni olan fakat yönetici olmayan bir kullanıcının yönetici izni gerektirecek işler yapmaya çalışması gibi saldırı türleri de vardır. Bu saldırı türlerinden hepsini içerecek bir veri seti hazırlanması hedeflenmiştir.

4.1.2 Saldırı araçlarının belirlenmesi

Saldırı oluşturmak için kullanılacak olan araçlar belirlenirken ise WLAN'lara yönelik saldırılar gerçekleştirilirken kullanılan popüler saldırı araçları araştırılmıştır. Bu araçlar genel olarak kablosuz ağların tümünde yaygın olarak kullanılan araçlardır. Aynı zamanda, Windows ve Ubuntu işletim sistemi ile uygun çalışabilecek saldırı araçları incelenmiştir. Veri seti oluşturma kapsamında kullanılmaya karar verilen saldırı araçlarının özeti Çizelge 4.1'de verilmektedir. DoS saldırı türlerinden yaygın olanları ise sel saldırılarıdır. SYN flood saldırısı için Tor's Hammer saldırı aracı kullanılmıştır. Bu araç TOR ağı üzerinden çalışan rasgele kaynak IP adresi kullanan saldırı aracıdır. HTTP flood saldırısı için HULK ve PyLoris araçları kullanılabilir. HULK, web sunucusunda büyük miktarda belirsiz trafik oluşturmaktadır. Ancak kimlik gizlemede başarısız olabilmektedir.

PyLoris komut dosyası tabanlı bir araçtır ve doğrudan sunucuya saldırı yapmaktadır. Sunucuya yetkili HTTP trafiği gönderir. Saldırı HTTP, FTP, SMTP, IMAP ve Telnet üzerinden yapılabilir. Kullanımı kolay bir GUI'ye sahiptir. Geleneksel DoS saldırı araçlarının aksine, bu araç doğrudan hizmete girer.

UDP flood saldırısı için ise LOIC ve XOIC saldırı araçlarından yararlanılmıştır. LOIC, kolayca elde edilebilen popüler DoS saldırı araçlarından biridir. Bu araç, geçtiğimiz yıllarda birçok büyük firmanın ağına karşı bilgisayar korsanları tarafından kullanılmıştır. Küçük sunucularda bir DoS saldırısı gerçekleştirmek için yalnızca tek bir kullanıcı tarafından kullanılabilir. Saldırı yapmak için yalnızca sunucunun IP adresinin URL'sini bilmek yeterli olmaktadır, bu yüzden acemi saldırılar yapan kişiler için dahi kullanımı kolaydır. Bu araç, kurban sunucusuna UDP, TCP veya HTTP istekleri

göndererek bir DoS saldırısı gerçekleştirir. Yalnızca sunucunun IP adresinin URL'sini bilmek yeterlidir ve bu araç geri kalan işlemleri yapmaktadır. Bu özelliklerin yanında LOIC saldırı IP adreslerini gizlemek için özellik bulundurmamaktadır.

XOIC ise bir başka DoS saldırı aracıdır. IP adresi, kullanıcı tarafından seçilen bir bağlantı noktası ve kullanıcı tarafından seçilen protokol içeren herhangi bir sunucuda bir DoS saldırısı gerçekleştirir. XOIC aracı da LOIC gibi kolay kullanımlı bir GUI'ye sahiptir, web sitelerine veya sunuculardaki saldırıları gerçekleştirmek için bu araç kolaylıkla kullanabilir. Genel olarak, araç üç saldırı moduyla birlikte gelir. Birincisi, test modu olarak bilinmektedir ve basittir. İkincisi normal DoS saldırı modudur. Sonuncusu, bir TCP/HTTP/UDP/ICMP iletisiyle birlikte gelen bir DoS saldırı modudur. Bu saldırı aracı etkili bir araçtır ve küçük web sitelerine karşı kullanılabilir.

DoS saldırılarına ek olarak yukarıda bahsedilen zayıflıkların taranması (Vulnerability scanning) hem saldırganlar için hem de güvenlik uzmanları için önemlidir. Bu taramanın amacı zayıf servisleri ve işlemleri bulmayı amaçlar. Zayıflık taraması için çok sayıda araç vardır. En basit örneği Nmap aracıdır. Bu araç bir "port scanner"dır. Host üzerindeki çalışan servisleri listeler ve işletim sisteminin türünü döndürür.

Parola çalma, sisteme izinsiz giriş gibi kaba kuvvet saldırı türleri için de Brutus ve Medusa saldırı araçları kullanılmıştır. Brutus, şifre kırma için en çok kullanılan uzaktan çevrimiçi araçlardan biri ve piyasada mevcut olan en hızlı ve en esnek şifre kırma aracı olduğunu iddia edimektedir. Brutus, yalnızca Windows istemcileri için kullanılabilen ücretsiz bir hizmettir ve HTTP, Telnet, Pop3, IMAP, vb. gibi bir dizi kimlik doğrulamasını destekler. Ayrıca, kullanıcıların kendi kimlik doğrulama türlerini oluşturmalarına olanak tanıyan ek işlevler içerir. Brutus uzun süredir güncellenmemesine rağmen hala şifre kırmak için oldukça kullanışlı bir araçtır.

Medusa, şifre kırma için bir başka popüler komut satırı tabanlı araçtır ve ubuntu işletim sistemi üzerinde çalışmaktadır. MS SQL, MYSQL, HTTP, FTP, CVS, SMTP, SNMP, SSH ve daha birçok protokolü desteklemektedir. Medusa'nın farklı sistemlerde aynı anda paralel saldırılar gerçekleştirme gibi bir özelliği vardır, bu da sadece hedefler

hakkında bilgi vererek birden fazla uygulamanın aynı anda kırılabileceği anlamına gelmektedir.

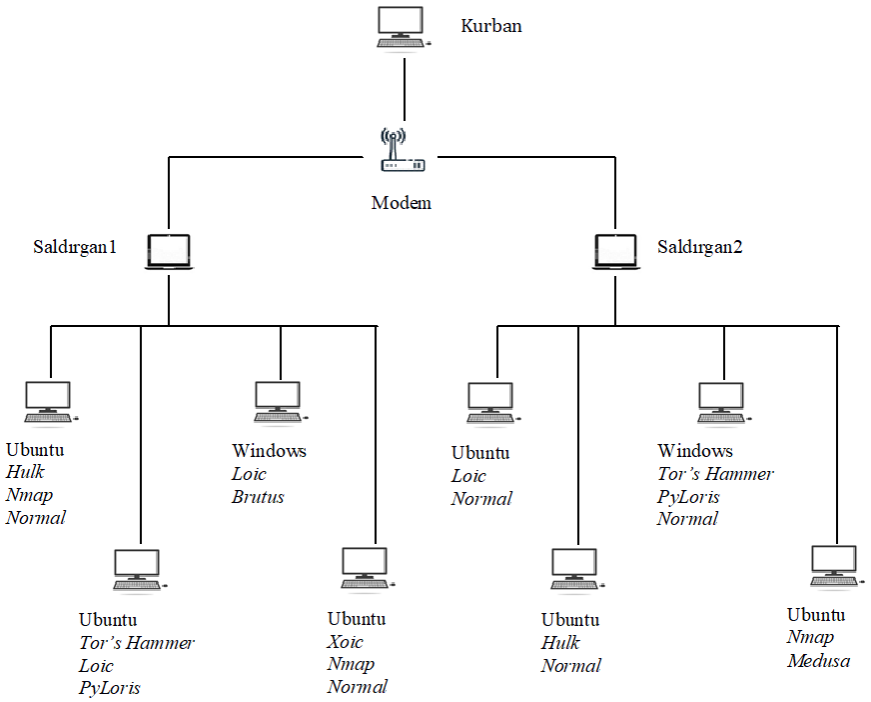
Çizelge 4.1 Veri seti oluşturmak için kullanılan araçlar ve özellikleri

Kullanılan araç	**Saldırı Türü**	**Özellikleri**
Tor's Hammer	syn flood	TOR ağı üzerinden çalışır. Rasgele kaynak IP adresi kullanır.
HULK	http flood	Web sunucusunda büyük miktarda belirsiz trafik oluştur ur. Kimlik gizlemede başarısız olabilmektedir.
PyLoris	http flood	Komut dosyası tabanlı bir araçtır. Doğrudan sunucuya saldırı yapmaktadır.
LOIC	udp flood	Saldırı için yalnızca sunucunun IP adresinin URL'sini bilmek yeterlidir. Kullanımı kolaydır.
XOIC	udp flood	Web sitelerine veya sunuculardaki saldırıları gerçekleştirmek için kullanılır. Kullanımı kolaydır.
Nmap	port scanner	Zayıflıkların taranması için kullanılır. Zayıf servisler ve işlemler belirlenir.
Brutus	brute force	Şifre kırma için en çok kullanılan uzaktan çevrimiçi araçlardan biridir. Yalnızca Windows işletim sistemi ile çalışır.
Medusa	brute force	Komut tabanlı bir araçtır. Yoğunlukla şifre kırma işlemleri için kullanılır.

Yukarıda anlatılan saldırı araçları, kablosuz yerel alan ağlarında karşılaşılan saldırılar hakkında araştırma yapan birçok kişiye yardımcı olmaktadır. Anlatılan bu saldırı araçları tasarladığımız topolojide uygun saldırı cihazları üzerine kurulmuştur.

4.1.3 Veri seti oluşturma topolojisi

Yukarıda belirlenen saldırı tipleri ve bu saldırıların düzenlenmesinde kullanılacak araçlar göz önünde bulundurularak, çeşitli saldırı tiplerini içeren bir veri seti oluşturmak ve sonrasında bu saldırıları geliştirilen algoritma ve literatürde yaygın kullanılan makine öğrenmesi algoritmaları ile tespit edebilmek için oluşturulan topoloji Şekil 4.1'de verilmiştir.



Şekil 4.1 Veri seti oluşturma topolojisi

Topoloji incelendiğinde, bir adet masaüstü ve iki adet dizüstü bilgisayar modem cihazı ile birbirine bağlanmıştır. Topolojinin üst kısmında yer alan masaüstü bilgisayar kurban cihaz olarak belirlenmiştir. Saldırgan cihazlar üzerinde Windows 10 işletim sistemi ve işlemci olarak Intel i5 ve i7 bulunmaktadır. Cihaz sayısını artırmak için saldırgan cihazların her birinin üzerine VMware 4 adet sanal makine kurulmuştur. Bu sanal makineler Windows ve Ubuntu işletim sistemine sahiptir. Hem her iki işletim sisteminden de faydalanmak hem de her saldırı aracının uygulanabilir olduğu işletim sistemi farklı olduğu için iki işletim sistemine de sahip sanal makineler kurulmuştur.

Cihazlar üzerine araçların kurulumu yapılırken öncelikle veri setinin homojen olması, gruplama oluşturabilecek davranışların olmaması bakımından, yani hangi cihazdan hangi saldırı türünün gelebileceğin belli olması gibi, araç kurulumları rastgele dağıtılmaya çalışmıştır. Ek olarak, bazı saldırı araçları sadece Ubuntu işletim sisteminde, bazıları Windows'ta bazıları ise her ikisi üzerinde de çalışabilmektedir. Bu yüzden dağılım yapılırken bu da göz önünde bulundurulmuştur. Örneğin, XOIC saldırı aracı sadece Ubuntu ile uyumlu iken LOIC her ikisinde de çalışabilmektedir.

4.1.4 Veri setinin oluşturulması

Veri seti oluşturmak için gerekli altyapı işlemler, tamamlandıktan sonra kurulan araçlar ile saldırı işlemleri gerçekleştirilmiştir. Aynı zamanda bu sanal makinelerde saldırı yanında normal trafik davranışları da oluşturulmuştur. Bu oluşturulan aktif ağ trafiği Wireshark ağ izleme programı ile izlenmiştir ve ".pcap" dosyaları elde edilmiştir.
Gelen ağ trafiği bilgileri incelendiğinde kaynak IP adres bilgisi, paketlerin hangi IP üzerinden geldiği, aynı kaynaktan kaç tane paket alındığı vb. gibi ayırt edici özelliklerin olabileceği görülmüştür. Bu veriler analiz edilerek özellik çıkarımı işlemi yapılmıştır. Sonrasında .pcap formatındaki veriler .csv formatına dönüştürülmüştür. İlgili olan özellikler seçildikten ve veriler üzerinde filtreleme yapıldıktan sonra saldırı çeşitlerine göre etiketleme işlemi yapılmıştır. Şekil 4.2'de veri seti oluşturma aşamaları verilmiştir ve aşağıda detaylı olarak açıklanmıştır.

Şekil 4.2 Veri seti oluşturma aşamaları

1. Önerilen metodolojinin ilk adımında saldırganlar tarafından kurban cihaza farklı saldırı çeşitlerinden oluşan ağ trafiği ve normal ağ trafiği gönderilmiştir.
2. Gönderilen ağ trafiği, kurban cihaz üzerine kurulu olan ağ trafik izleme programı aracılığı ile kaydedilmiştir.
3. İzlenen ağ trafik kaydedilmiştir ve veri seti oluşturma işlemi tamamlanmadan önce tekrar eden veriler gibi durumları elemek için önişleme yapılmıştır.
4. Son olarak veriler saldırı tiplerine göre etiketlenerek veri seti oluşturulmuştur.

Oluşturulan veri seti özellikleri aşağıda Çizelge 4.2'de verilmiştir.

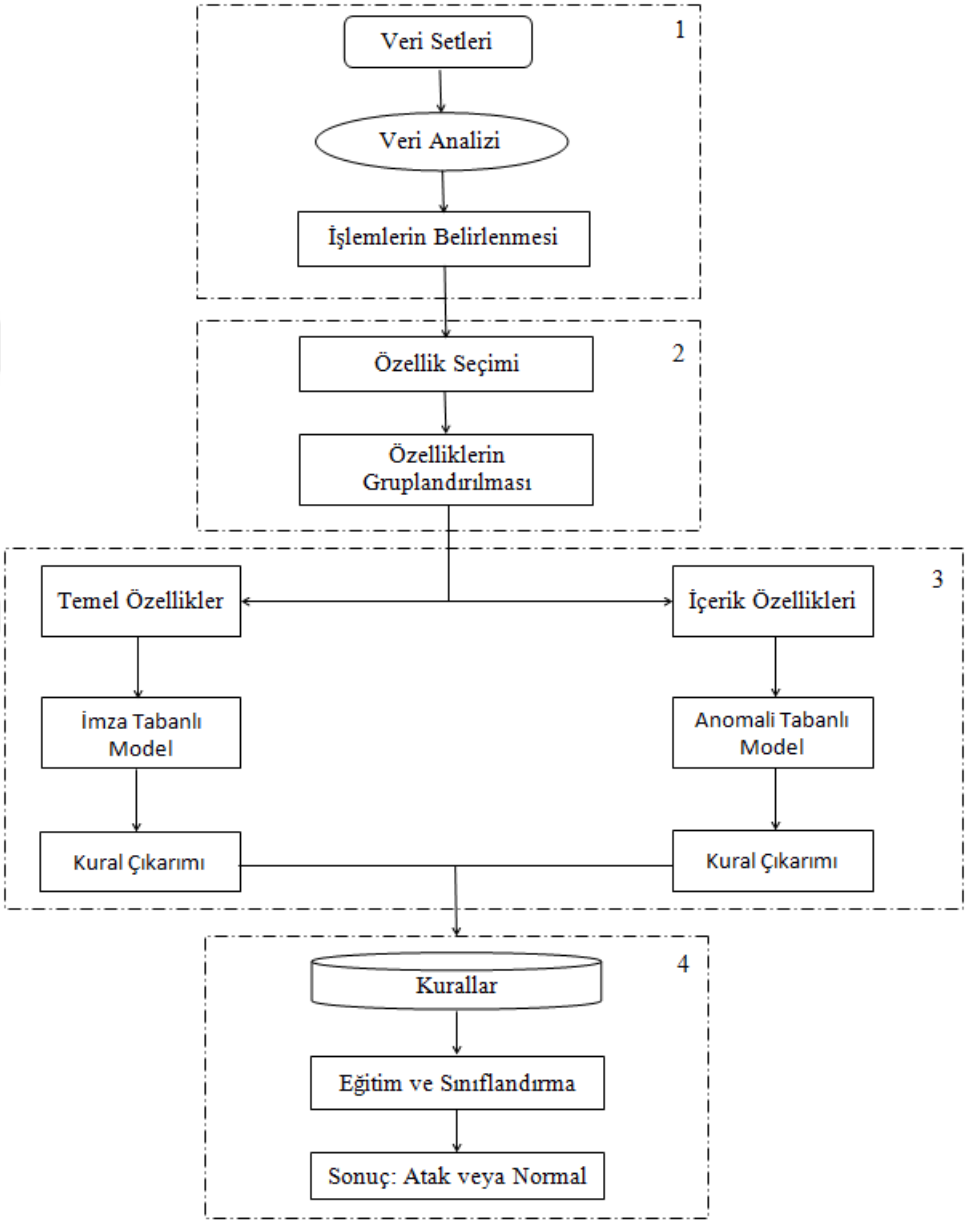
Çizelge 4.2 Veri seti özellikleri

Özellik	**Açıklama**
time	Toplam geçen zaman için başlangıç noktası
source_id	Kaynak IP adresi
destination_id	Hedef IP adresi
duration	Toplam bağlantı süresi
protocol	Protokol tipi
service	Servis tipi
src_port	Paketin geldiği arabirim numarası
dst_port	Paketin gönderildiği arabirim numarası
src_bytes	Kaynaktan hedefe gönderilen veri boyutu
capt_bytes	Yakalanan veri boyutu
counts	Kaynağa yapılan bağlantı sayısı
login	Yanlış giriş durumu
frame_len	Çerçeve uzunluğu
frame_status	Çerçevenin işaretlenmesi veya yok sayılması durumu
header_len	TCP başlığı uzunluğu
total_len	Paketin uzunluğu
urgent	Acil paket sayısı
flag	Bayrak
fragment	Parçalanma sayısı
root	Root a ulaşma durumu
result	Saldırı etiketi

Çizelge 4.2'de verilen özellikler ve görevleri incelendiğinde; "time", "duration" gibi bağlantının başlama ve süresi hakkında bilgi vermektedir. Uzun süredir devam eden bağlantı istekleri, sistemler tarafından tehlike anlamına gelmektedir. Ayrıca aynı kaynaktan tekrar tekrar gelen paketler için süre bilgisi saldırıların tespit edilmesinde kolaylık sağlamaktadır. "length", "frame_len", "header_len" özellikleri ile alınan uzunluk bilgileri saldırı tespitinde özellikle DoS saldırılarının tespiti için önemlidir. "count" gibi sistemde yetki almaya çalışma gibi özellikler ise yetki elde etme saldırılarının tespitinde önemli rol oynamaktadır. Özetlenecek olursa, Çizelge 4.2'de verilen özellikler anlatılan yol gösterici sebepler göz önünde bulundurularak seçilmiştir. Saldırı çeşitlerine göre etiketlenen veriler tek bir veri seti haline getirilmiştir. Gelecekte bu veri setinin, topolojiye IoT cihazları eklenerek daha da geliştirilmesi planlanmaktadır.

4.2 WLAN'larda Saldırıların Tespiti

WLAN'larda saldırılarının dinamik olarak hızlı ve yüksek doğruluk oranında elde edilebilmesi için tez çalışmasının bu aşamasında FSADM yöntemi önerilmiştir. Önerilen yöntemin blok diyagramı Şekil 4.3'de verilmiştir.



Şekil 4.3 Önerilen yöntemin blok diyagramı

Önerilen yöntem temel olarak 6 basamaktan oluşmaktadır:

- ✓ Verilerin Analizi
- ✓ Özellik Seçimi
- ✓ Özelliklerin Gruplandırılması
- ✓ İmza Tabanlı Yöntem (Kural Çıkarımı)
- ✓ Anomali Tabanlı Yöntem (Kural Çıkarımı)
- ✓ Eğitim ve Sınıflandırma

Önerilen blok diyagramda, blok 1'de Bölüm 3.3'de bahsedilen ve literatürde yer alan veri setleri ve analiz yöntemleri kullanılmıştır. Blok 2'de tez çalışması kapsamında katkı yapılmıştır ve bir modelin temel basamağı olan özellik seçimi konusunda FSAP yaklaşımı sunulmuştur. Blok 3'de saldırılar tespit edilirken, eğitim ve sınıflandırılma için imza tabanlı ve anomali tabanlı yöntemler birleşimi olan (SABADT) hibrid bir model sunulmuştur, Blok 4'de ise eğitim ve sınıflandırma işlemi hem sunulan yöntem hem de literatürdeki yöntemler ile gerçekleştirilmiştir.

4.2.1 Özellik seçimi

Özellik seçimi, makine öğrenmesi modelinin oluşturulmasının en önemli adımlarından biridir. Her bir özelliğin trafiğin sonucunu belirlemede etkisi vardır, ancak bu özelliklerden bazıları daha önemli rol oynamaktadır (Abdulhammed vd. 2018, Ullah ve Mahmoud 2017). Özellik seçimi için sunulan FSAP yaklaşımımız iki aşamadan oluşmaktadır. Öncelikle her bir özellik trafiğin durumuna göre gruplandırılmaktır. İlk aşamada, özelliklerin oluşturduğu grup sayıları temelinde aşağıdaki eşitlik kullanılarak, oluşturacağımız modelimizde bize ayırt edici durumlar sunabilecek özellikler seçiminin ilk aşaması gerçekleştirilmiştir.

$$t = \frac{\sum_{n=1}^{f} g_n - std(g)}{g} \tag{4.1}$$

Burada, t (threshold) özellik seçimi için hesaplanan eşik değeri, f veri setindeki toplam özellik sayısı, g her bir özellik için oluşan grup sayısıdır.

Bu eşitlik sonucunda eşik değerinin altında kalan özellikler elenmiştir. İkinci aşamada kalan özelliklerin oluşturduğu grupların analizi yapılmıştır. Bir özelliğin oluşturduğu gruptaki veri sayısı, eşik değerinin üzerinde olabilir. Ancak, değer aralığı geniş olduğundan veya her değerin bir normal bir de atak karşılığı olabilme ihtimalinden dolayı grup fazla sayıdan oluşmuş olabilir. Örneğin bir ağdaki kullanım süresi özelliğinin 1 saniyeden 100 saniyeye kadar 100 farklı değerden (1,2,..100) oluştuğunu varsayalım. Burada, her bir saniyede hem atak hem normal durum var ise 200 farklı durumdan oluşan bir grup ortaya çıkabilir. Bu haliyle, bu özelliğin oluşturduğu grup sayısı eşik değerinin üzerinde kalabilir ancak içeriği analiz edildiğinde atak durumunun belirlenmesinde belirleyiciliği yüksek bir özellik olmaz. Çizelge 4.3'de bir grubun oluşma şekli verilmiştir.

$F = \{ f_1, f_2, f_3, \ldots , f_L \}$ - özellik listesi.

$f = \{ x_1, x_2, x_3, \ldots , x_K \}$ - her özellik K adet farklı veriden oluşur.

$\beta = \{0, 1\}$ - 0 normal durumu ve 1 atak durumunu gösterir.

$r = \{ r_1, r_2, r_3, \ldots , r_N \}$ - (x_k, β) gruplamasında karşılık gelen normal ve atak durumlarının sayısıdır. Bu değerlerin toplamı, toplam veri sayısını vermektedir.

$g = \{f_l(x_1, \beta), f_l(x_2, \beta), f_l(x_3, \beta), \ldots , f_l(x_{K-1}, \beta), f_l(x_K, \beta) \}$ - her bir özelliğin oluşturduğu grubu göstermektedir.

Çizelge 4.3 Özellik grubu

$f_l(x_k, \beta)$	r
x_1 , β	r_1
x_2 , β	r_2
x_3 , β	r_3
x_4 , β	r_4
. . .	. . .
x_{K-1} , β	r_{N-1}
x_K , β	r_N

Özellik seçiminin ikinci aşamasında bazı parametreler belirlenmiştir. Bunlar; grubun içerisindeki farklı veri sayısı, grubun veri sayısının sonuç üzerindeki dağılımı, özelliklere göre normal ve atak durumlarının sahip olduğu min, max ve ortalama değerlerdir. Özellik seçilirken kullanılan algoritma Şekil 4.4'de verilmektedir.

Algoritma: Özellik Seçimi

Girdi: g: *Özellik Grupları Listesi*
Çıktı: f: *Seçilen Özellikler Listesi*
Tanımlamalar:
r: *gruptaki veriye karşılık gelen sonuç sayısı*
tN: gruptaki veriye karşılık gelen sonuç sayısının toplamı
tA: gruptaki veriye karşılık gelen sonuç sayısının toplamı
β: *gruptaki veriye karşılık gelen durum*
ψ: *gruptaki aynı veri sayısı*
μ: *aynı veriye ait normal/atak sonuçlarının oranı*
mN: *özelliğe ait normal durumdaki max değer*
miN: *özelliğe ait normal durumdaki min değer*
mA: *özelliğe ait atak durumdaki max değer*
miA: *özelliğe ait atak durumdaki min değer*

```
1.      g1← grup1, g2← grup2, …, gn← grupN s← u(g(j))
2.       for i← 1 to n
3.          for j← 1 to s-1
4.                if β(g(j))==’normal’
5.                     tN=tN+ r(g(j))
6.                    if (g(j+1)<miN)
7.                         miN=g(j+1)
8.                   if (g(i+1)>mN)
9.                        mN=g(i+1)
10.               else
11.                      tA=tA+ r(g(i))
12.                     if (g(j+1)<miA)
13.                          miA=g(j+1)
14.
15.                     if (g(j+1)>mA)
16.                         mA=g(j+1)
17.               end if
18.               if g(j)==g(j+1)
19.                      μ =r(g(i))/ r(g(i+1))
20.                     μt=μt+ μ
21.                     ψ ++
22.           end for
23.
24.           if  μt/ψ>= A/N
25.               ekle.f()
26.           else
27.              özellik ele
28.           end if
29.           if miN<mA or mA<mN
30.               özellik ele
31.           elif miN<miA or mAa<mN
32.              özellik ele
33.           else
34.             ekle.f()
35.           end if
36.      end for
```

Şekil 4.4 Özellik seçimi algoritması

Bu algoritma ile belirtilen parametrelerin sonucunu sağlayan özellikler, seçilen özellikler listesine eklenmektedir.

4.2.2 İmza tabanlı model

Modelin bu aşamasında ilk olarak literatürde bilinen WLAN saldırı türlerinin davranışları da (imzaları) göz önünde bulundurulmuştur. Bunların kuralları kaydedilmiştir. Bu kuralların detayları Bölüm 3.1.5'de verilmiştir. Sonrasında literatürde yaygın kullanılan veri setleri incelenmiştir. Oluşturulan her veri setinin kendi içerik özellikleri bulunmasının yanı sıra hepsinde ortak olarak kullanılan temel özellikler vardır. Bu temel özelliklerden yola çıkılarak kurallar belirlenmiştir.

İlk olarak, seçilen temel özelliklerin her biri ayrı analiz edilmiştir. Bu analiz sonucundan parametreler belirlenmiştir (ortalama/max/min normal süre, aktarılan paket sayısı, kullanılan protokoller vb.). Doğrudan sonuca ulaşılabilen durumlar var ise kurallar çıkarılarak imza listesine eklenmiştir. Örneğin, bir ağın normal durumda kullanılan maksimum süre belirlenmiştir ve atak durumundaki minimum süre ile karşılaştırılarak bir kural çıkarılmıştır. İkinci olarak, seçilen temel özelliklerin hepsi birlikte analiz edilmiştir. Bunun sebebi belirlenen parametrelerin dışındaki durumların göz ardı edilmesini engellemektir. Örneğin, atak durumunda da ağın kullanım süresi normal aralıkta olabilir. Bu süre özelliğinin yanına aktarılan veri miktarı özelliği de eklenerek incelendiğinde, normal trafik süresi gibi görünen atak durumunda aktarılan veri miktarı normalin çok üzerindedir. Modelin ilk aşamasının amacı doğrudan ulaşılabilen sonuçlara hızlı bir şekilde erişerek, saldırının belirlenme hızının artırılmasıdır. İkinci aşamasında ise gözden kaçırılabilecek bütün durumların incelenerek yüksek doğruluk oranı elde etmek hedeflenmektedir. Şekil 4.5'de imza tabanlı modelin algoritması verilmiştir (Belirlenen parametre ve kural sayısı fazla olduğundan dolayı her birinin hesaplanma detayı verilmemiştir, temel fonksiyonlar şeklinde yazılmıştır).

Algoritma: İmza Tabanlı Model

Girdi: *f* : *Seçilen temel özellikler*
Çıktı*: s*: *Belirlenen imzalar*
Tanımlar:
β: ağda karşılık gelen durum
NDP: *Normal durum parametreleri*
ADP: *Atak durum parametreleri*
r: *çıkarılan kurallar*

```
1.    f1← özellik1, ..., fn← özellikN    n← u(f(i))
2.     for i← 1 to n
3.         if β(f(i))==’normal’
4.                  yaz.NDP()
5.         else
6.                  yaz.ADP()
7.         end if
8.    end for
9.         kıyasla(NDP,ADP)
10.                belirle.r()
11.                yaz.s(r)
12.   analiz.f()
13.        belirle.r()
14.        yaz.s(r)
```

Şekil 4. 5 Saldırıların tespitinde imza tabanlı model algoritması

Genel olarak özetlenecek olursa, hem literatürde bilinen saldırı imzaları hem de yaygın kullanılan veri setlerinde ortak olarak kullanılan temel özelliklerden yola çıkılarak belirlenen imzalar kaydedilmiştir. İlk olarak, seçilen temel özelliklerin her biri ayrı analiz edilmiştir ve analiz sonucunda parametreler belirlenmiştir. Doğrudan sonuca ulaşılabilen durumlar var ise kurallar çıkarılarak imza listesine eklenmiştir. İkinci olarak seçilen temel özelliklerin hepsi birlikte analiz edilmiştir. Bu model ile birlikte doğrudan sonuca ulaşılan kurallar ile atağın belirlenme hızı ve özelliklerin bir arada detaylı analizi ile doğruluk oranının artırılması amaçlanmaktadır.

4.2.3 Anomali tabanlı model

Modelin ikinci aşamasında veri setinin içerik özellikleri, zamana bağlı trafik özellikleri ve veri setine göre olan ek özellikler kullanılarak trafik davranış analizi yapılmıştır ve kurallar çıkarılmıştır. Anomali tabanlı model sayesinde bilinen saldırılar dışında saldırılar da tespit edilebilmektedir. İmza tabanlı modele göre zaman ve bellek kullanımı fazla olsa da önceden tanımlanmayan saldırıları da tespit edebilmesi sayesinde yüksek doğruluk oranı sağlamaktadır (Yu vd. 2016). Anomali tabanlı model

oluşturulurken her özellik grubu önce kendi arasında analiz edilmiştir. Sonrasında bütün özellikler beraber analiz edilerek kurallar çıkarılmıştır. Şekil 4.6'da anomali tabanlı modelin algoritması verilmiştir (Belirlenen parametre ve kural sayısı fazla olduğundan dolayı her birinin hesaplanma detayı verilmemiştir, temel fonksiyonlar şeklinde yazılmıştır.).

Algoritma: Anomali Tabanlı Model

Girdi: fc: *Seçilen içerik özellikleri*
ft: *Seçilen zaman özellikleri*
fa: *Seçilen ek özellikler*
f: *Seçilen özellikler*
Çıktı: s: *Belirlenen kurallar*
Tanımlar:
β: *ağda karşılık gelen durum*
NDP: *Normal durum parametreleri*
ADP: *Atak durum parametreleri*
r: *çıkarılan kurallar*

```
1.    f_c1← icerikf.1, ...,   f_cn← icerikf.N   n← u(f_c(i))
2.    f_t1← zamanf.1,...,   f_tn← zamanf.N   n← u(f_t(i))
3.    f_a1← ek.f.1, ...,      f_an← ek.f.N        n← u(f_a(i))
4.    for i← 1 to n
5.        if β(fc(i))==’normal’
6.                yaz.NDP()
7.        else
8.                yaz.ADP()
9.        end if
10.   end for
11.   for i← 1 to n
12.       if β(ft(i))==’normal’
13.               yaz.NDP()
14.       else
15.               yaz.ADP()
16.       end if
17.   end for
18.   for i← 1 to n
19.       if β(fa(i))==’normal’
20.               yaz.NDP()
21.       else
22.               yaz.ADP()
23.       end if
24.   end for
25.   kıyasla(NDP,ADP)
26.       belirle.r()
27.       yaz.s(r)
28.   analiz.f()
29.       belirle.r()
30.       yaz.s(r)
```

Şekil 4.6 Saldırıların tespitinde anomali tabanlı model algoritması

Anomali tabanlı modelde, çıkarılan kural sayısı fazla ve detayları oldukça karmaşıktır. Modelin uygulanması aşamasında zaman kullanımı fazla olsa da atakların belirlenmesinde doğruluk oranı yüksektir. Ayrıca azaltılan özellikler sayesinde zaman bakımından iyileşme elde edilmektedir.

4.2.4 Eğitim ve sınıflandırma

Eğitim ve sınıflandırma işlemi yapılırken hem önerilen yöntem hem de literatürde yaygın bilinen makine öğrenmesi teknikleri kullanılmıştır. Makine öğrenmesi algoritmaları uzun yıllardır birçok farklı alanda kullanılmasına rağmen kablosuz yerel alan ağlarında saldırıların analizinde ve tespitinde son yıllarda kullanılmaya başlanmıştır. Bundan dolayı bu çalışmada bu algoritmalardan uygun olanlar kullanılacaktır. Bu algoritmalara örnek olarak Bayesian Ağı (Bayesian network- BN), J48 karar ağacı (decision tree variant- J48), k-en yakın komşular algoritması (k-nearest neighbor- KNN), basit logistik regresyon (simple logistic regression- SLR), çok katmanlı algılayıcı (multi-layer perceptron-MLP), naive bayes (NB), rastgele orman karar ağacı (random forest tree- RF), destek vektör makinesi (support vector machine-SVM) gösterilebilir (Ghanem vd. 2017, Primartha ve Tama 2017, Shabtai vd. 2009, Shapoorifard ve Shamsinejad 2017).

Genel olarak hiçbir algoritmanın diğerinden daha iyi olduğu söylenememekle birlikte her algoritmanın kendine göre avantajları ve dezavantajları bulunmaktadır. Verinin dağılışına, özellik sayısına, özellikler arasındaki bağımlılıklara göre bir algoritma diğer algoritmalara göre daha iyi performans gösterebilmektedir. Bu konuyla ilgili analiz Çizelge 4.4'de mevcuttur.

Çizelge 4.4 Sınıflandırma algoritmaları avantaj ve dezavantajları

Sınıflandırıcı	Avantaj	Dezavantaj
RF	Mantık tabanlı algoritma kullanan bir sınıflandırıcıdır. Tahmin performansı yüksektir.	Genellikle analiz edilmesi zor olan çıktılar üretir.
J48	Mantık tabanlı algoritma kullanan bir sınıflandırıcıdır. Karar ağacı anlaşılırlığının hızlı ve ölçeklenebilir bir sınıflandırıcısıdır.	Sürekli sınıf özelliklerinin tahmininde çok etkili bir algoritma değildir.
BN	İstatistiksel tabanlı bir sınıflandırıcıdır. Hızlı ve verimli hesaplama yeteneğine sahiptir. Veri eğitimi de oldukça hızlıdır.	Çok fazla özelliğe sahip veri setleri için uygulaması etkili değildir.
KNN	İstatistiksel tabanlı bir sınıflandırıcıdır. Veri hakkında bilgi sahibi olunmadığı durumlarda etkili sonuç üretir.	Sınıflandırma için zaman ve depolama maliyeti yüksektir.
MLP	Algılama tabanlı sınıflandırıcıdır. Öğrenme süreci paralelleştirilebilir ve doğru tahmin oranı yüksektir.	Sınıflandırma için hesaplama maliyeti yüksektir.
SVM	Yüksek boyutlu verilerde başarılıdır. Sınıfların ayrılabilir olduğu durumda en başarı algoritmalardandır. Aykırı (outliers) değerlerin etkisi diğer algoritmalara göre daha azdır.	Zaman maaliyeti yüksektir. Örtüşen(overlapped) sınıflarda iyi performans göstermez. Uygun çekirdek işlevini seçmek zor olabilir.
NB	Hızlı bir algoritmadır ve gerçek zamanlı olarak kullanılabilir. Çok sınıflı tahminleri etkin bir şekilde yapabilmektedir. Yüksek boyutlu veriler üzerinde iyi performans göstermektedir.	Bir sınıf etiketinin ve belirli bir öznitelik değerinin bir arada bulunmadığı durumlarda iyi sonuç vermez.
SLR	Tahmine dayalı çalışan bir algoritmadır. Uygulaması basit ve etkilidir. Özellik ölçeklendirmesi gerekli değildir.	Doğrusal olmayan verilerde performansı düşüktür İyi çalışması için tüm önemli değişkenler/özellikler tanımlanmalıdır.

4.2.5 Model performanslarının değerlendirilmesi

Algoritmaların performanslarını karşılaştırmak için bazı metrikler kullanılmıştır: Tespit oranı (recall), yanlış pozitif, yanlış negatif, kesinlik (precision), f-ölçümü (f-measure) ve doğruluk, vb. Bu değerler karışıklık matrisi (confusion matrix) kullanılarak hesaplanmaktadır (Çizelge 4.5).

Çizelge 4.5 Karmaşıklık matrisi

Gerçek	**Tahmin Edilen**		
		Pozitif	**Negatif**
	Pozitif	TP	FN
	Negatif	FP	TN

Bu değerler TP (saldırıların atak olarak işaretlenme sayısı), TN (normal durumların normal olarak işaretlenme sayısı), FP (normal durumun yanlışlıkla atak olarak işaretlenme sayısı), FN (saldırıların yanlışlıkla normal olarak işaretlenme sayısı) olarak gösterilmektedir. Bu değerler kullanılarak tespit oranı, yanlış pozitif, kesinlik, f-ölçümü ve doğruluk değerleri hesaplanmıştır.

$$Detection\,rate = TP/(TP + FN), \quad (4.2)$$

$$False\,positive = FP/(FP + TN), \quad (4.3)$$

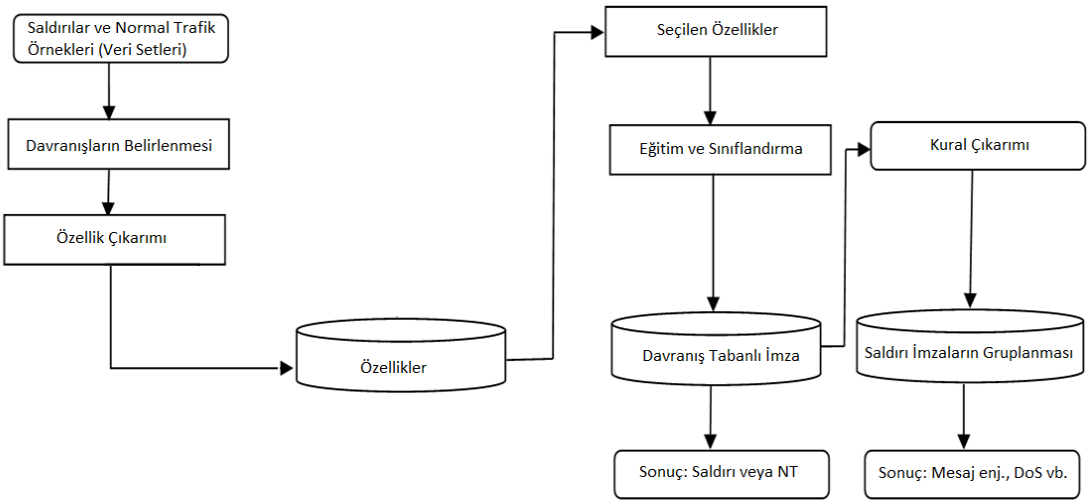
$$Precision = TP/(TP + FP), \quad (4.4)$$

$$F - Measure = (2 * precision * recall)/(precision + recall), \quad (4.5)$$

$$Accuracy = TP + TN/(TP + TN + FP + FN), \quad (4.6)$$

4.3 WLAN'larda Saldırı Türlerinin Tespiti

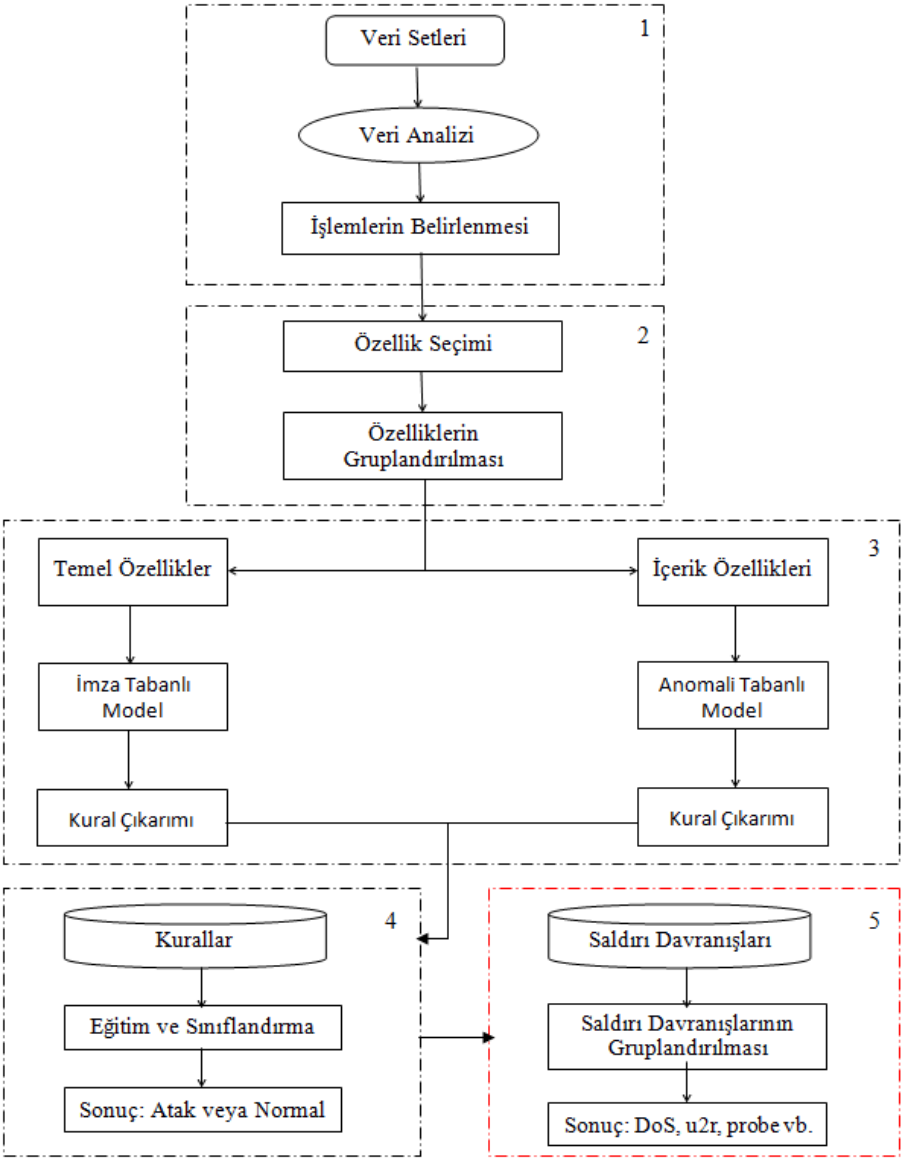
Tez çalışmasının bu bölümünde saldırıların tespitine ek olarak saldırı türlerinin de belirlenmesine yönelik çalışma yapılmıştır. Aynı zamanda, daha az özellik kullanılarak yüksek doğruluk oranı elde etmek için yeni algoritma geliştirilmiştir ve mevcut algoritmalar da güncellenmiştir. Önerilen yöntemin genel mimarisi Şekil 4.7'de verilmektedir.



Şekil 4.7 Önerilen yöntemin genel mimarisi

Bu mimariye göre öncelikle tez kapsamında oluşturulan veri setinin ve literatürde yaygın kullanılan veri setlerinin analizi yapılmış, özellik çıkarımı yapılmış ve özellik seti oluşturulmuştur. Oluşturulan özellik seti içerisinden ise geliştirilen özellik seçim yöntemi ile önemli olan özellikler seçilmiştir. Ardından imzalar ve kurallar belirlenerek saldırıların tespiti yapılmıştır. Eğer bir saldırı durumu var ise ve saldırının türü de öğrenilmek isteniyorsa saldırıların göstermiş olduğu davranışlar da kendi aralarında gruplandırılarak türleri belirlenmiştir.

Genel olarak mimarisi anlatılan yöntemin blok diyagramı ile her basamağı Şekil 4.8'de verilmiştir.



Şekil 4.8 Önerilen yöntemin blok diyagramı

Önerilen yöntem temel olarak 6 basamaktan oluşmaktadır:

- Verilerin Analizi
- Özellik Seçimi
- Özelliklerin Gruplandırılması
- İmza Tabanlı Yöntem (Kural Çıkarımı)
- Anomali Tabanlı Yöntem (Kural Çıkarımı)
- Eğitim ve Sınıflandırma

Blok 5 tez çalışmasının bu bölümünde, saldırı türlerinin tespiti ile tezin yeni katkısı olmuştur. Burada, trafik sonucunun saldırı çıkması durumunda saldırı türlerinin davranışları belirlenmiştir ve davranışlar türlerine göre gruplandırılmıştır. Diğer blokların detaylı anlatımı ise önceki bölümde (bkz. Bölüm 4.2) verilmiştir.

4.3.1 Özellik seçimi

Çalışmanın bu aşamasında, saldırı türleri belirlenirken özellik seçimi yaklaşımı mecvut algoritma güncellenerek ve yeni bir algoritma daha eklenerek geliştirilmiştir. Özellik seçimi için sunulan FSAP yaklaşımımız üç aşamadan oluşmaktadır. Öncelikle her bir özellik saldırı sonucuna göre gruplandırılmaktır. İlk aşamada, özelliklerin oluşturduğu grup sayıları temelinde geliştirilen eşitlik kullanılarak, oluşturacağımız modelimizde bize ayırt edici durumlar sunabilecek özellikler seçiminin ilk aşaması gerçekleştirilmiştir (detaylar için bkz. Bölüm 4.1).

Özellik seçiminin ikinci aşamasında normal/atak durumlarının özelliklerden oluşturulan gruplar içerisindeki dağılımlarına bakılmıştır. Bir grup içerisinde homojen bir dağılım varsa bu özellik seçici değildir, heterojen bir dağılım olması gerekmektedir. Örneğin, bir DoS saldırısı var ise özellik içerisinde belirli bir değer aralığında olmalıdır. Özelliğin içerdiği her değere karşılık gelebiliyorsa homojen dağılım oluşmuştur ve bu özellik durum tespitinde bir gösterge olamaz. Bu durumdan yola çıkılarak bir algoritma geliştirilmiştir. Geliştirilen algoritma Şekil 4.9'da verilmektedir.

Algoritma Özellik Seçimi I

Girdi: *g: Özellik Grupları Listesi*
Çıktı: *f: Seçilen Özellikler Listesi*
Tanımlamalar:
β: gruptaki veriye karşılık gelen durum
γ : trafik durum sayılarının toplam veri sayısına oranlarını tutan liste
c: trafik durum dağılım sayacı

```
1.    g1← grup1, g2← grup2, ..., gn← grupN    s← u(g(j))
2.     for i← 1 to n
3.         for j← 1 to si-1
4.             if β(g(j))=='normal'
5.                 cNormal++
6.              elif β(g(j))== 'attackType 1'
7.                 cType1++
8.             elif β(g(j))== 'attackType 2'
9.                 cType2++
10.                  ...
11.            else
12.                cTypek++
13.            end if
14.        end for
15.        if cNormal/ si<= γ normal
16.           p++
17.        end if
18.        if cType1/ si <= γ type1
19.           p++
20.        end if
21.        if cType2/ si <= γ type2
22.           p++
23.        end if
24.           ...
25.        if cTypek/ si <= γ typek
26.           p++
27.        end if
28.        if p>k/2
29.           ekle.f()
26.        else
27.           özellik ele
28.        end if
36.    end for
```

Şekil 4. 9 Özellik seçimi algoritması I

Özellik seçiminin sonraki aşamasında ise belirlenen parametreler kulanılarak belirli özellikler seçilmektedir. Bu aşamada, Bölüm 4.2.1'de anlatılan Şekil4.4'deki özellik seçimi algoritması, saldırı türlerinin belirlenmesine yönelik olarak güncellenmiştir ve özellik seçiminde kullanılmıştır.

4.3.2 İmza tabanlı model

Önerilen saldırı tespit tekniğinin ilk aşaması olan imza tabanlı model saldırıların tespit edilebilmesinin yanında (detaylar için bkz. Bölüm 4.2.2) saldırı türlerinin de tespitine göre yeniden düzenlenmiştir. Düzenleme sonucunda oluşturulan güncellenmiş algoritma

Şekil 4.10'da verilmiştir (Belirlenen parametre ve kural sayısı fazla olduğundan dolayı her birinin hesaplanma detayı verilmemiştir, temel fonksiyonlar şeklinde yazılmıştır.).

Algoritma İmza Tabanlı Model

Girdi: f : *Seçilen temel özellikler*
Çıktı: s: *Belirlenen imzalar (kurallar)*
Tanımlamalar:
β: *ağda karşılık gelen durum*
NDP: *Normal durum parametreleri*
ADP_1: *Atak tip*1 *durum parametreleri*
ADP_2: *Atak tip*2 *durum parametreleri*
ADP_n: *Atak tipn durum parametreleri*
r: *çıkarılan kurallar*

```
1.    f1← feature1, ..., fn← featureN    n← u(f(i))
2.     for i← 1 to n
3.        if β(f(i))=='normal'
4.                  yaz.NDP()
5.        else
6.                   if β(f(i))=='type1'
7.                        yaz. ADP1()
8.                   elif β(f(i))=='type2'
9.                        yaz. ADP2()
10.                  elif β(f(i))=='type3'
11.                       yaz. ADP3()
12.                  else
13.                       yaz. ADPn()
14.        end if
15.    end for
16.       kıyasla(NDP, ADP1, ADP2,..., ADPn)
17.             belirle.r()
18.             yaz.s(r)
19.   analiz.f()
20.      belirle.r()
21.      yaz.s(r)
```

Şekil 4. 10 Saldırı türlerinin tespitinde imza tabanlı model algoritması

Genel olarak özetlenecek olursa, hem literatürde bilinen saldırı imzaları hem de yaygın kullanılan veri setlerinde ortak olarak kullanılan temel özelliklerden yola çıkılarak belirlenen imzalar kaydedilmiştir. Bu model ile birlikte doğrudan sonuca ulaşılan kurallar ile atağın belirlenme hızı ve özelliklerin bir arada detaylı analizi ile doğruluk oranının artırılması amaçlanmaktadır.

4.3.3 Anomali tabanlı model

Önerilen saldırı tespit tekniğinin ikinci aşaması olan anomali tabanlı model saldırıların tespit edilebilmesinin yanında (detaylar için bkz. Bölüm 4.2.3) saldırı türlerinin de tespitine göre düzenlenmiştir.

Algoritma: Anomali Tabanlı Model

Girdi: fc: *Seçilen içerik özellikleri (content features)*
ft: *Seçilen zamana bağlı özellikler (time features)*
fa: *Seçilen ek özellikler (additional features)*
f: *Seçilen özellikler*
Çıktı: s: *Belirlenen kurallar*
Tanımlamalar:
β: *ağda karşılık gelen durum*
NDP: *Normal durum parametreleri*
ADP_1: *Atak tip*1 *durum parametreleri*
ADP_2: *Atak tip*2 *durum parametreleri*
ADP_n: *Atak tipn durum parametreleri*
r: *çıkarılan kurallar*

```
1.    f_c1← contentf.1, ..., f_cn← contentf.N   n← u(f_c(i))
2.    f_t1← timef.1, ...,    f_tn← timef.N      n← u(f_t(i))
3.    f_a1← add.f.1, ...,    f_an← add.f.N      n← u(f_a(i))
4.    for i← 1 to n
5.        if β(fc(i))=='normal'
6.                yaz.NDP()
7.        else
6.                 if β(f(i))=='type1'
7.                      yaz. ADP_1()
8.                 elif β(f(i))=='type2'
9.                      yaz. ADP_2()
10.                elif β(f(i))=='type3'
11.                     yaz. ADP_3()
12.                else
13.                     yaz. ADP_n()
14.       end if
15.   end for
16.   for i← 1 to n
17.       if β(ft(i))=='normal'
18.              yaz.NDP()
19.       else
20.                if β(f(i))=='type1'
21.                     yaz. ADP_1()
22.                elif β(f(i))=='type2'
23.                     yaz. ADP_2()
23.                elif β(f(i))=='type3'
25.                     yaz. ADP_3()
26.                else
27.                     yaz. ADP_n()
28.       end if
29.   end for
30.   for i← 1 to n
31.       if β(fa(i))=='normal'
32.              yaz.NDP()
33.       else
34.                if β(f(i))=='type1'
35.                     yaz. ADP_1()
36.                elif β(f(i))=='type2'
37.                     yaz. ADP_2()
38.                elif β(f(i))=='type3'
30.                     yaz. ADP_3()
40.                else
41.                     yaz. ADP_n()
42.       end if
43.   end for
44.   kıyasla(NDP, ADP_1, ADP_2,..., ADP_n)
45.       belirle.r()
46.       yaz.s(r)
47.   analiz.f()
48.       belirle.r()
49.       yaz.s(r)
```

Şekil 4.11 Saldırı türlerinin tespitinde anomali tabanlı model algoritması

Düzenleme sonucunda oluşturulan güncellenmiş algoritma Şekil 4.11'de verilmiştir (Belirlenen parametre ve kural sayısı fazla olduğundan dolayı her birinin hesaplanma detayı verilmemiştir, temel fonksiyonlar şeklinde yazılmıştır.). Anomali tabanlı modelde, çıkarılan kural sayısı fazla ve detayları oldukça karmaşıktır. Modelin uygulanması aşamasında zaman kullanımı fazla olsa da atakların belirlenmesinde doğruluk oranı yüksektir. Ayrıca azaltılan özellikler sayesinde zaman bakımından iyileşme elde edilmektedir.

5. ÖNERİLEN METODOLOJİNİN UYGULANMASI

Önerilen metodolojinin performans ve doğruluğunu değerlendirmek için veri miktarı yüksek olan KDD'99 veri seti, güncel veri seti olan UNSW-NB15 veri seti ve tez çalışması kapsamında üretilen veri seti kullanılmıştır. Veri setleri üzerinde yapılan uygulamaların detayları aşağıdaki bölümlerde verilmiştir.

5.1 Önerilen Metodolojinin KDD'99 Veri Seti Üzerinde Uygulanması

Bölüm 3.3'de bahsedilen KDD'99 veri setinin detayları bu bölümde uygulama kapsamında incelenmiştir. Veri setinde, 9 temel ve 32 adet türetilmiş olmak üzere toplamda 41 tane özellikten oluşan bir özellik haritası çıkarılmıştır. Bu 41 özellik dört temel kategoriye ayrılarak ifade edilmiştir:

• Temel özellikler (based features);
• İçerik özellikleri (content features);
• Sunucu tabanlı trafik özellikleri (host-based traffic features);
• Zamana bağlı trafik özellikleri (time-based traffic features).

Çizelge 5.1'de, sırasıyla bu 4 kategori ve kategoriler içerisindeki veri özellikleri gösterilmiştir.

İçerik özellikleri, sadece TCP bağlantılarından alınan temel özelliklerdir. Bu özelikleri elde etmek, ağ trafiği verileri üzerinde önişlem yapılması gerekmediğinden, diğer kategorilere göre daha kolaydır. Sunucu tabanlı trafik özellikleri, etki alanı (domain) bilgisi ile ortaya çıkan bağlantı içerik özellikleridir. Zamana bağlı trafik özellikleri, "aynı sunucu" ve "aynı servis" özellikleri kullanılarak çıkarılan özelliklere verilen isimdir. "Aynı sunucu" özellikleri, son iki saniye içerisinde aynı sunucuya yapılan bağlantıların gözden geçirilmesi ile elde edilir. Benzer olarak "aynı servis" özellikleri son iki saniye içerisinde aynı servise yapılan bağlantıların gözden geçirilmesi ile elde edilir.

Çizelge 5.1 KDD’99 veri seti temel özellikleri

Özellik	Tanım
Temel Özellikler	
Duration	Bağlantı uzunluğu
protocol_type	Protokol tipi
service	Servis tipi
flag	Bayrak
src_bytes	Kaynaktan hedefe veri boyutu
dst_bytes	Hedeften kaynağa veri boyutu
land	Kaynak ve hedef IP aynı ise 1 değilse 0
wrong_fragment	Yanlış parçalama
urgent	Acil paket sayısı
İçerik Özellikleri	
hot	“hot” göstergesi
num_failed_logins	Hatalı giriş sayısı
logged_in	Giriş başarılı ise 1 değilse 0
num_compromised	Gizliliğin ihlal edilme sayısı
root_shell	“root shell” elde edildiyse 1 değilse 0
su_attempted	“su root” komutu girildiyse 1 değilse 0
num_root	“root” erişim sayısı
num_file_creations	“dosya oluşturma işlemleri sayısı”
num_shells	Shell istemi sayısı
num_access_files	Kontrol dosyalarına erişim sayısı
num_outbound_cmds	ftp oturumunda giden komut sayısı
is_host_login	Giriş “host” listesindeyse 1 değilse 0
is_guest_login	Giriş “guest” ise 1 değilse 0
Sunucu tabanlı trafik özellikleri	
count	son iki saniye içinde mevcut bağlantıyla aynı ana bilgisayara yapılan bağlantıların sayısı
srv_count	son iki saniye içinde mevcut bağlantıyla aynı servise yapılan bağlantıların sayısı
serror_rate	“SYN” hata bağlantılarının yüzdesi (aynı ana bilgisayar bağlantıları)
srv_serror_rate	“SYN” hata bağlantılarının yüzdesi (aynı servis bağlantıları)
rerror_rate	“REJ” hata bağlantılarının yüzdesi (aynı ana bilgisayar bağlantıları)
srv_rerror_rate	“REJ” hata bağlantılarının yüzdesi (aynı servis bağlantıları)
same_srv_rate	Aynı servise bağlantıların yüzdesi
diff_srv_rate	Farklı servislere bağlantıların yüzdesi
srv_diff_host_rate	Farklı ana bilgisayarlara bağlantıların yüzdesi
Zamana bağlı trafik özellikleri	
dst_host_count	aynı hedef ana bilgisayara sahip bağlantıların sayısı
dst_host_srv_count	aynı hedef ana bilgisayara sahip ve aynı servisi kullanan bağlantı sayısı
dst_host_same_srv_rate	aynı hedef ana bilgisayara sahip ve aynı servisi kullanan bağlantıların yüzdesi
dst_host_diff_srv_rate	mevcut ana bilgisayardaki farklı servislerin yüzdesi
dst_host_same_src_port_rate	Aynı bağlantı noktasına sahip olan mevcut ana bilgisayara bağlantıların yüzdesi.
dst_host_srv_diff_host_rate	farklı ana bilgisayarlardan gelen aynı servise olan bağlantıların yüzdesi
dst_host_serror_rate	S0 hatası bulunan mevcut ana bilgisayara olan bağlantıların yüzdesi
dst_host_srv_serror_rate	S0 hatası bulunan mevcut ana bilgisayara ve belirtilen servise bağlantıların yüzdesi
dst_host_rerror_rate	RST hatası bulunan mevcut ana bilgisayara olan bağlantıların yüzdesi
dst_host_srv_rerror_rate	RST hatası bulunan mevcut ana bilgisayara ve belirtilen servise bağlantıların yüzdesi

DARPA veri setlerinin, belirli önişlemlerden geçirilmesi ile oluşturulan KDD'99 veri seti toplamda 38 farklı saldırı içerir (Kayacik vd. 2007). Bunlardan 23 tanesi eğitim veri setinde iken, test veri seti, eğitim veri setinde bulunmayan 15 farklı saldırı tipini daha içerir. KDD'99 eğitim ve test veri setinde bulunan saldırılar ve bu saldırıların ait oldukları saldırı tipleri Çizelge 5.2'de verilmiştir.

Çizelge 5. 2 KDD'99 eğitim ve test veri setindeki saldırılar ve türleri

KDD'99 eğitim veri seti saldırı türleri		**KDD'99 test veri seti saldırı türleri**	
Saldırı	**Kategori**	**Saldırı**	**Kategori**
smurf	dos	apache2	dos
neptune	dos	httptunnel	r2l
back	dos	mailbomb	dos
teardrop	dos	mscan	probe
pod	dos	named	r2l
land	dos	processtable	dos
normal	normal	saint	probe
satan	probe	sendmail	r2l
ipsweep	probe	snmpgetattack	r2l
portsweep	probe	snmpguess	r2l
nmap	probe	sqlattack	u2r
warezclient	r2l	udpstorm	dos
guesspasswd	r2l	worm	r2l
warezmaster	r2l	xclock	r2l
imap	r2l	xterm	u2r
ftp_write	r2l		
multihop	r2l		
phf	r2l		
spy	r2l		
buffer_overflow	u2r		
rootkit	u2r		
loadmodule	u2r		
perl	u2r		

Saldırıların tespiti için önerilen yöntem iki aşamadan oluşmaktadır. Birincisi özellik seçimi için geliştirilen yaklaşım (FSAP) ikincisi ise eğitim ve sınıflandırma için önerilen hibrid SABADT modelidir.

Eğitim ve sınıflandırma için modelimiz oluşturulurken %10KDD'99 veri seti kullanılmıştır. Problemimizin ilk aşaması olan saldırı veya normal olarak sonucu belirlemek için saldırı tipleri "dos", "probe", "u2r", "r2l" normal durumlar ise "normal" olarak etiketlenmiştir. Öncelikle önerdiğimiz özellik seçimi yöntemleri ile önemli olan özellikler seçilmiştir. Sonrasında, doğrudan sonuca ulaşabildiğimiz durumlardan (imza

tabanlı) ve trafiğin davranışlarından (anomali tabanlı) kurallar çıkarılarak modelimiz oluşturulmuştur. Modelimizin testi aşamasında ise bütün KDD'99 veri seti kullanılmıştır.

İlk olarak veri setinde sunulan her bir özellik trafik durumu sonucu (normal/dos/probe/u2r/r2l) ile gruplandırılmıştır (service-result, count-result, duration-result vb.). Her bir özelliğin oluşturduğu grup sayısı yani sonuç üzerindeki etkisi hesaplanan eşik değeri ile karşılaştırılmıştır. Bu değer üzerinde kalan özellikler sonuç için belirgin özelliklerdir ve bu özellikler seçilmiştir.

Şekil 5.1'de seçilen özellikler arasına giremeyen, elenen özelliklere örnek olarak "root_shell" özelliği verilmiştir.

root_shell, β	r
(0, 'dos.')	391458
(0, 'normal.')	97255
(0, 'probe.')	4107
(0, 'r2l.')	1120
(0, 'u2r.')	26
(1, 'normal.')	23
(1, 'r2l.')	6
(1, 'u2r.')	26

Şekil 5.1 "root_shell" özelliği gruplama sonucu

"root_shell" özelliği içerdiği değerler ile saldırı durumuna göre ayrıştırıldığında, 8 farklı grup ((0,dos), (0,normal)…(1,u2r)) oluşturmuştur ve belirleyiciliği düşüktür. Rakamlara bakıldığında aynı durumda (0-1) atak türlerinin sayısı da normal sayısı da göz ardı edilebilecek miktarda değildir. Örneğin, "root_shell" özelliğinin 0 olduğu durumda 391458 adet dos saldırısı varken aynı zamanda 97255 normal durum vardır. Her ikisininde miktarı oldukça yüksektir. Yani "root_shell" özelliğinin 0 olduğu durumda dos saldırısı vardır veya normal bir durum vardır diyebilmek için belirleyicilik yüksek değildir. Diğer durumlar ile birlikte bakıldığında belirleyici bir yanı olma ihtimali tabi ki vardır ancak bizi zaman açısından daha hızlı sürede sonuca

ulaştırabilecek farklı özellikler bulunmaktadır. Bu yüzden özellik seçimi yapılırken, eşik değerinin altında kalan bu özellik elenmiştir.

service, β	r
('IRC', 'normal.')	42
('IRC', 'probe.')	1
('X11', 'normal.')	9
('X11', 'probe.')	2
('Z39_50', 'dos.')	91
('Z39_50', 'probe.')	1
('auth', 'dos.')	108
('auth', 'normal.')	220
...	
('echo', 'dos.')	111
('echo', 'probe.')	1
('eco_i', 'normal.')	389
('eco_i', 'probe.')	1253
('ecr_i', 'dos.')	281049
('ecr_i', 'normal.')	345
('ecr_i', 'probe.')	6
('efs', 'dos.')	102
('efs', 'probe.')	1
('exec', 'dos.')	99
('finger', 'dos.')	197
...	

Şekil 5.2 “service” özelliği gruplama sonucu

Şekil 5.2’de “service” özelliği içerdiği değerler ile saldırı durumuna göre ayrıştırıldığında, 140 farklı grup oluşturmuştur. Bağlantı yapılan servis tiplerine ve saldırı türlerine bakıldığında genellikle heterojen bir dağılım mevcuttur. ‘IRC’ servisi üzerinde 2 farklı durum mevcuttur ve “normal durum” oldukça belirgindir. ‘ecr_i’ servis tipinde 3 farklı durum mevcuttur. Burada içerdiği saldırı türü de çoğalmıştır ancak sayısal dağılımlar arasında yine belirgin fark vardır. “service” özelliğinin gruplandırılması sonucunda “probe” saldırısı 48, “dos” saldırısı 56, “r2l” saldırısı 7,

“u2r” saldırısı 4, “normal” durum ise 25 farklı servis tipinde dağılım göstermiştir. “ service” özelliği geliştirilen algoritma sonucunda 5 farklı durum içeren veri setinde 4 durum için algoritmayı sağlamaktadır. Aynı zamanda önerilen özellik seçimi II yönteminde belirtilen parametreler de bu özellikte sağlanmaktadır. Sonuç olarak hem eşik değerinin üzerinde kalmasıyla hem de özellik seçimi yöntemlerini sağlamasıyla “service” özelliği özellik listesine eklenmiştir.

Özetle, önerilen özellik seçim yöntemi sonucunda (Eşitlik1’e ve özellik seçim algoritmaları) modelimizde kullanılmak üzere seçilen özelliklerin listesi Çizelge 5.3’de verilmiştir. Tez çalışmasının ilk aşaması olan saldırıların tespiti bölümünde geliştirilen özellik seçimi yaklaşımıyla 41 özellikten 22 özellik seçilirken, çalışmanın sonrakı aşaması olan saldıtıların ve türlerinin belirlenmesi bölümünde geliştirilen yaklaşımla 10 özellik seçilmiştir.

Çizelge 5.3 Seçilen özellikler

Yaklaşım I	**Yaklaşım II**
Duration	duration
Service	service
src_bytes	src_bytes
dst_bytes	dst_bytes
Count	count
srv_count	srv_count
serror_rate	same_srv_rate
rerror_rate	dst_host_same_srv_rate
srv_rerror_rate	dst_host_rerror_rate
same_srv_rate	dst_host_srv_rerror_rate
diff_srv_rate	
srv_diff_host_rate	
dst_host_count	
dst_host_srv_count	
dst_host_same_srv_rate	
dst_host_diff_srv_rate	
dst_host_same_src_port_rate	
dst_host_srv_diff_host_rate	
dst_host_serror_rate	
dst_host_srv_serror_rate	
dst_host_rerror_rate	
dst_host_srv_rerror_rate	

Çizelge 5.1’de belirtilen KDD’99 veri setinin temel özelliklerinden özellik seçim algoritmasından sonra kalan özellikler kullanılarak, imza tabanlı model için doğrudan

saldırı sonucuna ulaşılabilen kurallar çıkarılmıştır. Bazı basit kurallar ile trafik durumunun sonucu kolaylıkla berirlenebilmektedir. Bunlar "normal/dos/probe/u2r/r2l" olarak etiketlenerek kaydedilmiştir. Bu aşama ile veri setinin yaklaşık %30'luk kısmının sonucuna doğrudan ulaşılabilmiştir. Bu durumda bize zaman açısından ve bellek açısından tasarruf sağlamaktadır. Bu imza durumlarından bazıları şu şekildedir; verideki trafik analizine göre bağlantı süresinin, normal minimum trafik süresinin altında veya maksimumun üzerinde olması, iletilen veri miktarının normal trafikteki veri miktarının üzerinde olması veya süre miktarı normal iken hiçbir veri alışverişinin olmaması vb. Bu imzalardan bir kısmı Çizelge 5.4'de verilmiştir.

Çizelge 5.4 Temel özelliklerden çıkarılan imzalar (Liste kısaltılmıştır)

min("normal_duration")<duration<max("normal_duration")	normal
service="auth", count>avg(normal)	dos
min("normal_src_bytes")<src_bytes<max("normal_src_bytes")	normal
service="efs", same_srv_rate=1	probe
service="ftp_data", dst_bytes>max(other_situations)	r2l
service="telnet",max("normal_duration")<duration< max(other_situations_duration)	u2r
service="ecr_i", count<=1	normal

Anomali tabanlı modelin oluşturulması aşamasında içerik özellikleri, sunucu tabanlı trafik özellikleri, zamana bağlı trafik özelliklerinden seçilmiş olanlar kullanılarak trafik davranış analizi yapılmıştır ve kurallar çıkarılmıştır. Analiz yapılırken önce içerik özellikleri, ardından sunucu tabanlı özellikler, sonrasında ise zamana bağlı özellikler sırasıyla kendi içlerinde incelenmiştir. Son olarak ise bu özellikler bir arada analiz yapılmıştır. Anomali tabanlı model sayesinde bilinen saldırılar dışındaki saldırılar da tespit edilebilmektedir. İmza tabanlı modele göre zaman ve bellek kullanımı fazla olsa da önceden tanımlanmayan saldırıları da tespit edebilmesi sayesinde yüksek doğruluk oranı sağlamaktadır. Çıkarılan kurallardan bazıları şu şekildedir; 1.private servis tipi üzerinden bağlantı yapılırken aynı zamanda hiçbir veri akşının görülmemesi ve hatalı bağlantı sayısının 0'dan farklı olması, 2. trafik süresi normal görünürken hiçbir veri akışının olmaması aynı zamanda son 2 saniye içerisinde aynı ana bilgisayara yapılan bağlantı sayısının yoğun miktarda olması vb. Bu kuralların bir kısmı Çizelge 5.5'de verilmiştir.

Çizelge 5.5 KDD'99 veri setinden seçilen özelliklerden çıkarılan durumlar (Liste kısaltılmıştır)

service=private, duration=0, src_btyes=0, dst_btes=0	atak	dos
service=private, duration>max("normal"), src_btyes=0, dst_btes=0	atak	probe
service=eco_i, srv_diff_host_rate=1	atak	probe
service=http , src_bytes>max("normal_src_bytes")	atak	dos
service=finger, count>= ort("normal_count"), dst_host_srv_serror_rate >=0.1	atak	probe
service=ssh, src_btyes=0, dst_btes=0	atak	dos
service=ftp_data, duration>max("normal_dur"), dst_host_same_srv_rate=1	atak	r2l
service=telnet, count >= ort("normal_count"), srv_count >= ort("normal_srv_count")	atak	u2r

Son aşamada ise, %10_KDD'99 veri seti kullanılarak çıkarılan kurallar KDD'99 veri setinin tamamına uygulanmıştır. Çıkarılan kurallar ile oluşturulan modelin performanslarını karşılaştırmaları ve sonuçları Bölüm 6.1'de detayı olarak açıklanmıştır.

5.2 Önerilen Metodolojinin UNSW-NB15 Veri Seti Üzerinde Uygulanması

UNSW-NB15 veri setinin ham ağ paketleri, Avustralya Siber Güvenlik Merkezi'nin (ACCS) Siber Menzil Laboratuvarında IXIA PerfectStorm aracı tarafından gerçek normal faaliyetler ve yapay saldırı davranışlarının bir karmasını elde etmek için oluşturulmuştur. Tcpdump aracı, 100 GB ham trafiği (örneğin, Pcap dosyaları) yakalamak için kullanılımıştır. Bu veri setinde Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode ve Worms olmak üzere dokuz tür saldırı vardır. Toplam 49 özellikten oluşmaktadır (Çizelge 5.6).

Çizelge 5.6 UNSW-NB15 veri seti özellikleri

Akış özellikleri	**Temel özellikler**	**İçerik özellikleri**	**Zaman özellikleri**	**Üretilen ek özellikler**	**Etiketli özellikler**
srcip	state	swin	sjit	ct_state_ttl	attack_cat
sport	dur	dwin	djit	ct_flw_http_mthd	label
dstip	sbytes	stcpb	Stime	is_ftp_login	
dsport	dbytes	dtcpb	dtime	ct_ftp_cmd	
proto	sttl	smeansz	sintpkt	ct_srv_src	
	dttl	dmeansz	dintpkt	ct_srv_dst	
	sloss	trans_depth	tcprtt	ct_src_ltm	
	dloss	res_bdy_len	synack	ct_dst_ltm	
	service		ackdat	ct_src_dport_ltm	
	sload		is_sm_ip_ports	ct_dst_sport_ltm	
	dload			ct_dst_src_ltm	
	spkts				
	dpkts				

UNSW-NB15 veri seti özellikleri aşağıdaki gibi altı grupta sınıflandırılır:

Akış özellikleri: Bu özellikler, istemciden sunucuya veya sunucudan istemciye gibi ana bilgisayarlar arasında tanımlayıcı özniteliklere sahiptir.

Temel özellikler: Protokol bağlantılarını temsil eden özelliklerdir.

İçerik özellikleri: TCP/IP'nin özelliklerini ve ayrıca http hizmetlerinin bazı özelliklerini içerirler.

Zaman özellikleri: Bu grup, örneğin paketler arasındaki varış zamanı, paket başlangıç/bitiş zamanı ve TCP protokolünün gidiş-dönüş zamanı gibi zaman özelliklerini içerir.

Ek oluşturulan özellikler: Bu grup ayrıca iki gruba ayrılabilir: (1) Protokol hizmetlerini korumak için her özelliğin kendi amacına sahip olduğu genel amaçlı özelliklerdir. (2) Bağlantı özellikleri, son zaman özelliğinin sıralı sırasına göre 100 kayıt bağlantısının akışından oluşturulur.

Etiketli Özellikler: Bu kategori her kaydın etiketini temsil eder.

Çizelge 5.7 UNSW-NB15 veri seti saldırı örnekleri

Saldırı Tipleri	Açıklama
fuzzers	Saldırganın bir uygulama, işletim sistemi veya ağdaki güvenlik boşluklarını, çökmesini sağlamak için büyük miktarda rastgele veri girişi ile besleyerek yaptığı bir saldırıdır.
analysis	Bağlantı noktaları (örneğin bağlantı noktası taramaları), e-postalar (örneğin istenmeyen postalar) ve web komut dosyaları (örneğin HTML dosyaları) aracılığıyla web uygulamalarına sızan bir tür izinsiz giriş türüdür.
backdoors	Gizli bir normal kimlik doğrulamasını atlama, cihaza yetkisiz uzaktan erişimi güvence altına alma, gözlemlenmeden devam etmek için mücadele ederken düz metin girişi bulma tekniğidir.
dos	Yetkili isteklerin cihaza erişmesini engellemek için aşırı işlere neden olacak şekilde bellek üzerinden bilgisayar kaynaklarını bozan bir saldırıdır.
exploits	Bir ana bilgisayar veya ağ üzerinden şüphelenilmeyen bir davranışa neden olan bir aksaklık, hata veya güvenlik açığından yararlanan bir talimat dizisidir.
generic	Blok şifrelemenin konfigürasyonuna bakılmaksızın bir çarpışmaya neden olmak için bir karma işlevi kullanarak her blok şifresine karşı kurulan bir tekniktir.
reconnaissance	güvenlik kontrollerinden kaçmak için bir bilgisayar ağı hakkında bilgi toplayan bir saldırıdır.
shellcode	Saldırganın, tehlikeye atılan makineyi kontrol etmek için bir kabuktan başlayarak küçük bir kod parçasına girdiği kötü amaçlı yazılımdır.
worms	Saldırganın kendini kopyalayarak diğer bilgisayarlara yaydığı bir saldırıdır. Genellikle, kendisine erişmek için kullanılan hedef bilgisayarın güvenlik arızalarına bağlı olarak, kendisini yaymak için bir bilgisayar ağı kullanır.

Önerilen yöntemin uygulanması iki aşamadan oluşmaktadır. Birincisi özellik seçimi için geliştirilen yaklaşım (FSAP), ikincisi ise eğitim ve sınıflandırma için önerilen hibrid SABADT modelidir.

Eğitim ve sınıflandırma için model oluşturulurken UNSW-NB15_training-set veri seti kullanılmıştır. Problemimizin ilk aşaması olan saldırı veya normal olarak sonucu belirlemek için saldırı tipleri "attack" normal durumlar ise "normal" olarak etiketlenmiştir. Öncelikle önerdiğimiz özellik seçimi yöntemleri ile önemli olan özellikler seçilmiştir. Sonrasında, doğrudan sonuca ulaşabildiğimiz durumlardan (imza tabanlı) ve trafiğin davranışlarından (anomali tabanlı) kurallar çıkarılarak modelimiz oluşturulmuştur. Modelimizin testi aşamasında ise UNSW-NB15_testing-set veri seti kullanılmıştır.

İlk olarak veri setinde sunulan her bir özellik trafik durumu sonucu (normal/attack) ile gruplandırılmıştır (service-attack_cat, proto- attack_cat, sttl- attack_cat vb.). Her bir özelliğin oluşturduğu grup sayısı yani sonuç üzerindeki etkisi hesaplanan eşik değeri ile karşılaştırılmıştır. Bu değer üzerinde kalan özellikler sonuç için belirgin özelliklerdir ve bu özellikler seçilmiştir. Şekil 5.3'de "ct_ftp_cmd" özelliğibib gruplama sonucu verilmiştir.

ct_ftp_cmd , β	num_of_res
(0, 'Attack')	45021
(0, 'Normal')	36631
(1, 'Attack')	307
(1, 'Normal')	363
(2, 'Attack')	4
(2, 'Normal')	6

Şekil 5.3 "ct_ftp_cmd" özelliği gruplama sonucu

"ct_ftp_cmd" özelliği 0, 1 ve 2 değerlerinden oluşmaktadır. İçerdiği değerler ile saldırı durumuna göre ayrıştırıldığında, 6 farklı grup oluşturmuştur ve belirleyiciliği düşüktür. Gruplandırma sonucu oluşan sayılarak bakıldığında, örneğin, ct_ftp_cmd özelliğinin 0 olduğu durumda 45021 adet atak, 36661 adet normal durum vardır. Yani her iki

durumdan da yüksek miktarda sonuç mevcuttur. Diğer durumlar ile birlikte bakıldığında belirleyici bir yanı olma ihtimali tabi ki vardır ancak bizi zaman açısından daha hızlı sürede sonuca ulaştırabilecek farklı özellikler bulunmaktadır. Bu yüzden özellik seçimi yapılırken, eşik değerinin altında kalan bu özellik elenmiştir.

spkts , β	num_of_res
(1, 'Attack')	90
(1, 'Normal')	894
(2, 'Attack')	28997
(2, 'Normal')	7985
(3, 'Attack')	15
(3, 'Normal')	14
(4, 'Attack')	276
(4, 'Normal')	1544
...	
(716, 'Attack')	1
(730, 'Attack')	3
(742, 'Attack')	1
(752, 'Attack')	1
(764, 'Attack')	1
(772, 'Attack')	2
...	
(8424, 'Attack')	1
(8669, 'Attack')	1
(9392, 'Attack')	1
(9416, 'Attack')	1
(10200, 'Attack')	1
(10646, 'Attack')	1

Şekil 5.4 “spkts” özelliği gruplama sonucu

Şekil 5.4’de “spkts” özelliği içerdiği değerler ile saldırı durumuna göre ayrıştırıldığında, 572 farklı grup oluşturmuştur. Bağlantı yapılan servis tiplerine ve saldırı türlerine

bakıldığında genellikle heterojen bir dağılım mevcuttur. Örneğin gelen paket sayısı 2 iken 2 farklı durum mevcuttur ve "atak" sayısı normalden belirgin bir şekilde daha fazladır. Belirli bir değerden sonra ise yani gelen paket miktarı arttıkça saldırı durumu belirginleşmiştir. Önerilen özellik seçimi II yönteminde belirtilen parametreler de bu özellikte sağlanmaktadır. Sonuç olarak hem eşik değerinin üzerinde kalmasıyla hem de özellik seçimi yöntemlerini sağlamasıyla "spkts" özelliği özellik listesine eklenmiştir.

Özetle, önerilen özellik seçim yöntemi sonucunda (Eşitlik 1'e ve özellik seçim algoritmaları) modelimizde kullanılmak üzere seçilen özelliklerin listesi Çizelge 5.8'de verilmiştir. Geliştirilen özellik seçimi yaklaşımı ile 49 özellikten 13 adet özellik seçilmiştir.

Çizelge 5.8 Seçilen özellikler

service
proto
duration
sttl
spkts
dkpts
sbytes
dbytes
ct_dst_src_ltm
ct_dst_sport_ltm
ct_src_dport_ltm
sloss
response_body_len

Çizelge 5.6'da belirtilen UNSW-NB15 veri setinin temel özelliklerinden özellik seçim algoritmasından sonra kalan özellikler kullanılarak, imza tabanlı model için doğrudan saldırı sonucuna ulaşılabilen kurallar çıkarılmıştır. Bunlar "normal/atak" olarak etiketlenerek kaydedilmiştir. Bu aşama ile veri setinin %40'lık kısmının sonucuna ulaşılabilmektedir. Bu durumda bize zaman açısından ve bellek açısından tasarruf sağlamaktadır. Çıkarılan bu imza durumlarından bazıları Çizelge 5.9'da verilmiştir.

Çizelge 5.9 Temel özelliklerden çıkarılan imzalar (Liste kısaltılmıştır)

min(“normal_duration”)<duration<max(“normal_duration”)	normal
service=”-”, protocol=”tcp”, dur< max(“normal_duration”)	normal
service=”http”, protocol=”tcp”, dur > max(“normal_duration”)	atak
min(“normal_src_bytes”)<sbytes <max(“normal_src_bytes”)	normal
service=”dns”, protocol=”udp”, dur > max(“normal_duration”)	atak
duration=0, spkts>max(normal_spkts)	atak
service=”smtp”, protocol=”tcp”, dur > max(“normal_duration”)	atak

Anomali tabanlı modelin oluşturulması aşamasında içerik özellikleri, akış özellikleri, zamana bağlı özellikler ve üretilmiş ek özelliklerden seçilmiş olanlar kullanılarak trafik davranış analizi yapılmıştır ve kurallar çıkarılmıştır. Analiz yapılırken önce içerik özellikleri, ardından akış özellikleri, sonrasında ise zamana bağlı özellikler sırasıyla kendi içlerinde incelenmiştir. Son olarak ise bu özellikler bir arada analiz yapılmıştır. Çıkarılan bu imza durumlarından bazıları Çizelge 5.10’da verilmiştir.

Çizelge 5.10 UNSW-NB15 veri setinden seçilen özelliklerden çıkarılan durumlar (Liste kısaltılmıştır)

sttl>=max(normal_dest_time) & response_body_len>0	atak
sttl>=max(normal_dest_time) &ct_dst_src_ltm<min(normal) &sbytes<avg(normal)	atak
sttl>=max(normal_dest_time)& min(normal)<ct_dst_src_ltm<max(normal) & min(normal)<sbytes<avg(normal)	normal
ct_dst_src_ltm>max(normal) | response_body_len >max(normal) | ct_src_dport_ltm>max(normal)	atak
Dur>min(normal) & response_body_len==0 & tcprtt<min(normal)	atak

Son aşamada ise, eğitim veri seti kullanılarak çıkarılan kurallar test veri setine uygulanmıştır. Çıkarılan kurallar ile oluşturulan modelin performans değerlendirmeleri Bölüm 6.2’de verilmiştir.

5.3 Önerilen Metodolojinin Tez Kapsamında Oluşturulan Veri Setine Uygulanması

Tez çalışması kapsamında üretilen veri kümesinin ham ağ paketleri, günümüzde yaygın kullanılan saldırı araçları kullanılarak normal faaliyetler ve güncel saldırı davranışlarının bir karmasını elde etmek için oluşturulmuştur. Wireshark aracı, ham trafiği (örneğin, Pcap dosyaları) yakalamak için kullanılmıştır. Bu veri setinde DoS

(Smurf, neptune, buffer_of), probe (nmap, portscan, ipscan) ve bruteforce (guess_passw, imap) olmak üzere 3 farklı kategori 7 farklı saldırı tipi vardır. Toplam 21 özellikten oluşmaktadır.

Çizelge 5. 11 Üretilen veri setinin özellikleri

Temel Özellikler	**İçerik Özellikleri**
Time	counts
source_id	login
destination_id	frame_len
Duration	frame_status
Protocol	header_len
Service	total_len
src_port	urgent
dst_port	flag
src_bytes	fragment
capt_bytes	root
	result

Önerilen yöntemi çalışma kapsamında oluşturulan veri seti üzerinde denerken öncelikle önerilen özellik seçimi yöntemleri ile önemli olan özellikler seçilmiştir. Sonrasında, doğrudan sonuca ulaşabildiğimiz durumlardan (imza tabanlı) ve trafiğin davranışlarından (anomali tabanlı) kurallar çıkarılarak modelimiz oluşturulmuştur. İlk olarak veri setinde sunulan her bir özellik trafik durumu sonucu (normal/dos/probe/bruteF) ile gruplandırılmıştır (service-result, protocol-result, duration-result vb.). Her bir özelliğin oluşturduğu grup sayısı yani sonuç üzerindeki etkisi hesaplanan eşik değeri ile karşılaştırılmıştır. Bu değer üzerinde kalan özellikler sonuç için belirgin özelliklerdir ve bu özellikler seçilmiştir. Şekil 5.5'de "login" özelliği gruplama sonucu verilmiştir.

login, β	num_of_res
(0, 'dos.')	985
(0, 'normal.')	537
(0, 'probe.')	322
(0, 'bruteF.')	128
(1, 'normal.')	14
(2, 'normal.')	11
(3, 'bruteF.')	3

Şekil 5.5 “login” özelliği gruplama sonucu

“login” özelliği 0, 1, 2 ve 3 değerlerinden oluşmaktadır. İçerdiği değerler ile saldırı durumuna göre ayrıştırıldığında, 7 farklı grup oluşturmuştur ve belirleyiciliği düşüktür. Gruplandırma sonucu oluşan sayılarak bakıldığında, örneğin, login özelliğinin 0 olduğu durumda 985 adet dos, 537 adet normal, 322 adet probe 128 adet bruteF durumu vardır. Yani her durumda sonuç miktarı önemli seviyededir. Diğer durumlar ile birlikte bakıldığında belirleyici bir yanı olma ihtimali tabi ki vardır ancak bizi zaman açısından daha hızlı sürede sonuca ulaştırabilecek farklı özellikler bulunmaktadır. Bu yüzden özellik seçimi yapılırken, eşik değerinin altında kalan bu özellik elenmiştir.

duration, β	num_of_res
(0, 'dos.')	748
(0, 'normal.')	381
(0, 'probe.')	184
(0, 'bruteF.)	78
(1, 'dos.')	7
(1, 'normal.')	112
(1, 'probe.')	92
(1, 'bruteF.')	23
(2, 'dos.')	3
...	
(220, 'normal.')	2
(221, 'normal.')	3
(222, 'normal.')	1
(223, 'normal.')	1
...	
(971, 'probe.')	1
(973, 'probe.')	4
(974, 'probe.')	2
(975, 'probe.')	3
(977, 'probe.')	1

Şekil 5.6 “duration” özelliği gruplama sonucu

Şekil 5.6’da “duration” özelliği içerdiği değerler ile saldırı durumuna göre ayrıştırıldığında, 142 farklı grup oluşturmuştur. Bağlantı yapılan servis tiplerine ve saldırı türlerine bakıldığında genellikle heterojen bir dağılım mevcuttur. Örneğin gelen 0. Saniye de saldırı adetleri arasında belirgin farklılıklar vardır. Ek olarak, belirli değer aralıklarında normal durum mevcutken, maksimum normal sürenin üzerine çıkıldığında saldırı durumları görünmeye başlamıştır. Sonuç olarak hem eşik değerinin üzerinde kalmasıyla hem de özellik seçimi yöntemlerini sağlamasıyla “duration” özelliği özellik listesine eklenmiştir.

Özetle, önerilen özellik seçim yöntemi sonucunda (Eşitlik1’e ve özellik seçim algoritmaları) modelimizde kullanılmak üzere seçilen özelliklerin listesi Çizelge 5.12’de

verilmiştir. Geliştirilen özellik seçimi yaklaşımı ile 20 özellikten 9 adet özellik seçilmiştir.

Çizelge 5. 12 Seçilen özellikler

Service
Protocol
Duration
src_bytes
capt_bytes
Counts
total_len
Urgent
Root

Çizelge 5.11'de belirtilen veri setinin temel özelliklerinden özellik seçim algoritmasından sonra kalan özellikler kullanılarak, imza tabanlı model için doğrudan saldırı sonucuna ulaşılabilen kurallar çıkarılmıştır. Bunlar "normal/dos/probe/bruteF" olarak etiketlenerek kaydedilmiştir. Bu aşama ile veri setinin %30'luk kısmının sonucuna ulaşılabilmektedir. Bu durumda bize zaman açısından ve bellek açısından tasarruf sağlamaktadır. Bu imzalardan bir kısmı Çizelge 5.13'de verilmiştir.

Çizelge 5. 13 Temel özelliklerden çıkarılan imzalar (Liste kısaltılmıştır)

min("normal_duration")<duration<max("normal_duration")	normal
service="icmp", count>avg(normal)	dos
min("normal_src_bytes")<src_bytes<max("normal_src_bytes")	normal
service="private", src_bytes=0	probe
service="ftp_data", dst_bytes>max(other_situations)	bruteF
service="tcp", count<=1	normal

Anomali tabanlı modelin oluşturulması aşamasında temel özellikler ve içerik özelliklerinden seçilmiş olanlar kullanılarak trafik davranış analizi yapılmıştır ve kurallar çıkarılmıştır. Anomali tabanlı model sayesinde bilinen saldırılar dışındaki saldırılar da tespit edilebilmektedir. İmza tabanlı modele göre zaman ve bellek kullanımı fazla olsa da önceden tanımlanmayan saldırıları da tespit edebilmesi sayesinde yüksek doğruluk oranı sağlamaktadır. Bu kuralların bir kısmı Çizelge 5.14'de verilmiştir.

Çizelge 5.14 İçerik özelliklerden çıkarılan durumlar (Liste kısaltılmıştır)

service=private, duration=0, src_btyes=0, dst_btes=0	dos
service=private, duration>max(“normal”), src_btyes=0, dst_btes=0	probe
service=http , src_bytes>max(“normal_src_bytes”)	dos
service=finger, count>= ort(“normal_count”), root!=0	probe
service=ssh, src_btyes=0, dst_btes=0	dos
service=telnet, count >= ort(“normal_count”)	bruteF

Son aşamada çıkarılan kurallar veri setine uygulanmıştır. Çıkarılan kurallar ile oluşturulan modelin performans değerlendirmeleri Bölüm 6.3’de detaylı olarak verilmiştir.

5.4 Bölüm Değerlendirmesi

Bu bölümde, önerilen yöntemin, yöntemin içerdiği yaklaşım ve tekniğin uygulaması anlatılmıştır. FSADM kullanılarak özellik seçimi yapılmış ve saldırılar tespit edilmiştir. Önerilen FSAP yaklaşımı ile ağ trafiğinin durumu sınıflandırılmadan önce önemli olan özelliklerin seçimi yapılmış ve özellik sayısı azaltılarak model performansı artırılmıştır. SADABT ise saldırıları tespit ederken imza ve anomali tabanlı yöntemleri entegre ederek çalışmakta olup, hızı ve doğruluk oranını artırmaktadır.

6. BULGULAR VE TARTIŞMA

Bu bölümde tez kapsamında WLAN'larda saldırıların tespiti için geliştirilen yöntemin uygulanması sonucu elde edilen test sonuçları ve bu sonuçların yorumları yer almaktadır. Elde edilen sonuçlar literatürde yapılan öncü çalışmalarla karşılaştırılarak tartışılmıştır.

6.1 KDD'99 Veri Seti Bulguları

Önerilen yöntemin KDD'99 veri seti üzerinde uygulanması ve değerlendirme için kullanılan metriklerin sonuçları Çizelge 6.1 ve Çizelge 6.2'de verilmiştir.

Çizelge 6.1 KDD'99 veri seti üzerinde elde edilen sonuçlar

Kullanılan Yöntem	TespitOranı	YanlışPozitif	Kesinlik	f-Ölçümü	Doğruluk
Önerilen Yöntem	**99,8**	**0,013**	**99,79**	**99,93**	**99,81**
Naive Bayes	86,1	0,028	97,5	90,6	86,13
DecisionTree	99,7	0,02	99,8	99,8	99,75
DecisionTable	99,5	0,08	98,7	94,65	99,5
SMO	96,8	0,056	91,6	61,95	96,83
AdaBoost	97,6	0,023	95,25	96,95	97,61

Önerilen yöntemin test edilmesi işleminin sonucunda saldırıların tespit edilmesinde %99.81 doğruluk oranı elde edilmiştir. Decision Table ve Decision Tree teknikleri de yakın sonuçlar vermiştir. Ancak araştırmalar esnasında geliştirilen yöntemlerin performansının ve hafıza kullanımının mevcutlara göre daha da iyileştirildiği gözlemlenmiştir. Ek olarak Decision Table ve SMO algoritmaları veri setindeki "u2r" saldırısını, AdaBoost algoritması ise "u2r" ve "r2l" saldırılarını tespit edememiştir. Bu saldırıları veri setinde diğer saldırı türlerine göre çok daha az miktardadır. Bu yüzden dağılımın homojen olmadığı durumlarda bu algoritmalar etkili performans gösterememektedir.

Çizelge 6.2 Elde edilen sonuçların literatürdeki yöntemler ile karşılaştırılması

Makale	Özellik Seçimi	Sınıflandırma Tekniği	Kullanılan Özellik Sayısı	Doğruluk Oranı (%)
Xiao ve Liu 2009	Gereksiz özelliklerin silinmesi	SVM	21	86,3
Araújo vd. 2010	Hibrid yaklaşım: k-means ve gain ratio	K-means	14	90,00
Amiri vd. 2011	Üç farklı seçim yönteminin kıyaslanması	Least squares SVM	FFSA: 29 MMIFS: 22 LCFS: 36	97,92
Li vd. 2012	Kademeli olarak özellik kaldırma yöntemi	SVM	19	98,62
Karimi vd. 2013	Hibrit filtreleme özelliği seçimi	Naive Bayes	16	98,28
Saxena ve Richariya 2014	Information gain	Hibrid PSO-SVM Yaklaşımı	18	99.4
Olusola vd. 2015	Bağımlılık oranı	-	34	-
Hasan vd. 2016	Permütasyon önem ölçüsü	Random Forest	25	82,36
Manzoor ve Kumar 2017	Information gain ve korelasyon	Yapay Sinir Ağları tabanlı teknik	25	97,91
Babirye ve Mwebaze 2018	Information gain	Genetik algoritma	21	99,64
Kaur ve Singh 2019	-	Derin öğrenme tabanlı D-Sign	-	99,14
Iwendi vd. 2020	Korelasyona dayalı özellik seçimi	Bagging ve Adaboost sınıflandırma	13	99,4
Önerilen Yöntem	**FSAP**	**SABADT**	**10**	**99,81**

Bazı çalışmaların katkıları, yöntemleri, kullanılan özellik sayıları ve doğruluk oranları Çizelge 6.2'de verilmiştir. Literatürdeki yöntemlere bakıldığında hem özellik seçimi hem de saldırı tespiti için algoritma geliştiren çok fazla çalışma bulunmamaktadır. Mevcut olanlara kıyasla Babirye ve Mwebaze'nin çalışması önerilen yönteme en yakın doğruluğu vermiş ancak önerilen yöntem hem kullanılan öznitelik sayısı hem de elde edilen doğruluk oranı açısından daha başarılıdır. Bununla birlikte, Iwendi vd. kullanılan özellik sayısı açısından iyi gibi görünse de, önerilen yöntem doğruluk oranı açısından daha başarılıdır.

6.2 UNSW-NB15 Veri Seti Bulguları

Önerilen yöntemin UNSW-NB15 veri seti üzerinde uygulanması ve değerlendirme için kullanılan metriklerin sonuçları Çizelge 6.3 ve Çizelge 6.4'de verilmiştir.

Çizelge 6.3 UNSW-NB15 veri seti üzerinde elde edilen sonuçlar

Kullanılan Yöntem	TespitOranı	YanlışPozitif	Kesinlik	f-Ölçümü	Doğruluk
Önerilen Yöntem	**99,1**	**0,02**	**99,11**	**99,2**	**99,17**
Naive Bayes	76,1	0,2	78,7	76,0	76,13
DecisionTree	97,0	0,03	97,0	97,0	96,9
DecisionTable	93,3	0,06	93,3	93,3	93,29
SMO	91,6	0,08	91,7	91,6	91,63
AdaBoost	88,6	0,12	88,9	88,5	88,56

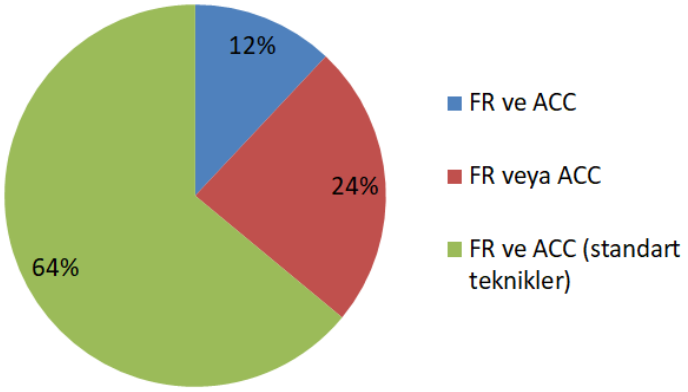
Önerilen yöntemin test edilmesi işleminin sonucunda saldırıların tespit edilmesinde %99.17 doğruluk oranı elde edilmiştir. Decision Table ve Decision Tree teknikleri de yakın sonuçlar vermiştir. Ancak araştırmalar esnasında geliştirilen yöntemlerin performansının ve hafıza kullanımının mevcutlara göre daha da iyileştirildiği gözlemlenmiştir. Ek olarak sonuçlara bakıldığında, Naive Bayes ve AdaBoost algoritmaları saldırı izlerinin belirgin olmadığı veri setlerinde başarılı sonuçlar verememektedir.

UNSW-NB15 veri seti üzerinde yapılan bazı çalışmaların katkıları, yöntemleri, kullanılan özellik sayıları ve doğruluk oranları Çizelge 6.4'de verilmiştir. Literatürdeki yöntemlere bakıldığında hem özellik seçimi hem de saldırı tespiti için algoritma geliştiren çok fazla çalışma bulunmamaktadır. Mevcut olanlara kıyasla Moustafa ve Slay'in çalışması kullanılan özellik bakımından önerilen yönteme yakındır ancak doğruluk oranına kıyasla çok geride kalmıştır. Bununla birlikte, Mousta vd. doğruluk oranı bakımından önerilen yöntemle yakındır ancak bu çalışmada da hem özellik azaltımı yönünde bir çalışma yoktur büyün özellikler kullanılmıştır hem de sınıflandırma için de standart yöntemler kullanılmıştır.

Çizelge 6.4 Elde edilen sonuçların literatürdeki yöntemler ile karşılaştırılması

Makale	Özellik Seçimi	Sınıflandırma Tekniği	Kullanılan Özellik Sayısı	Doğruluk Oranı (%)
Moustafa & Slay 2015	Gereksiz özelliklerin silinmesi hibrid yaklaşım	Expectation Maximization (EM) clustering, Naive Bayes (NB) and Logistic Regression (LR)	11	77.2-83
Bhamare vd. 2016	-	Logistic Regression	43	89,26
Baig vd. 2017	-	boosting based ANN AdaBoost	43	86.4
Belouch vd. 2017	Ranker algorithm	RepTree	20	88,95
Anwer vd. 2018	Filter and Wrapper	J48 and Naïve Bayes	18	88
Aravind & Kalaiselvi 2017	-	Ensemble classifier	-	90
Idhammad vd. 2017	Relevant features	FNN ADDM	-	97.1
Nguyen vd.2018	PCA	Derin Öğrenme	-	95.84
Moustafa vd.2018	-	AdaBoost, DT, NB, ANN	-	99.54
Belouch vd. 2018	-	NB, DT, RF, SVM	43	97,49
Hassine vd. 2019	İmportance-based özellik seçimi	Random Forest	18	97,24
Rajagopal vd. 2020	İlgili özelliklerin seçimi	Sinir Ağları	23	97
Önerilen Yöntem	**FSAP**	**SABADT**	**13**	**99,17**

Şekil 6.1'de verilen dağılımda mavi alan literatürdeki çalışmalarda hem özellik azaltımı hem de sınıflandırma alanında özgün katkı sağlayan çalışmaları, kırmızı alan bu alanlardan sadece birinde özgün katkı sağlayan çalışmaları, yeşil alan bu alanlarda çalışma yapan ancak bilinen standart teknikleri kullanan çalışmaları göstermektedir.



Şekil 6.1 Araştırma katkılarının dağılımı

Şekilde de görüldüğü gibi, hem KDD'99 veri setinde hem UNSW-NB15 veri setinde incelenen çalışmaların sadece %12'si hem özellik seçimi hem de sınıflandırma alanında katkı sağlamış, %24'ü ise ya özellik azaltımı ya da sınıflandırma alanlarından sadece birinde katkı sağlamıştır. Kalan kısım her iki alanda da çalışma yapmış ancak alanlardan en az birinde literatürdeki mevcut yöntemleri kullanmıştır. Bu tez çalışmasında bahsedilen alanlardan her birine özgün yöntemler ile katkı yapılmıştır ve dolayısıyla bu tez çalışması da %12'lik dilimde yer almaktadır.

6.3 Oluşturulan Veri Seti Bulguları

Önerilen yöntemin tez çalışması kapsamında üretilen veri seti üzerinde uygulanması ve değerlendirme için kullanılan metriklerin sonuçları Çizelge 6.5'de verilmiştir.

Çizelge 6. 5 Oluşturulan veri seti üzerinde elde edilen sonuçlar

Kullanılan Yöntem	TespitOranı	YanlışPozitif	Kesinlik	f-Ölçümü	Doğruluk
Önerilen Yöntem	**99,7**	**0,01**	**99,75**	**99,83**	**99,79**
Naive Bayes	85,7	0,10	89,6	85,9	85,71
DecisionTree	99,1	0,013	99,2	99,2	99,18
DecisionTable	98,7	0,015	98,5	98,4	98,77
SMO	97,6	0,017	97,8	97,6	97,61
AdaBoost	98,3	0,021	97,4	97,95	98,37

Önerilen yöntemin test edilmesi işleminin sonucunda saldırıların tespit edilmesinde %99.79 doğruluk oranı elde edilmiştir. Decision Table, Decision Tree ve AdaBoost teknikleri de yakın sonuçlar vermiştir. Ancak araştırmalar esnasında geliştirilen yöntemlerin performansının ve hafıza kullanımının mevcutlara göre daha da iyileştirildiği gözlemlenmiştir. Ek olarak veri seti daha da geliştirilerek daha net sonuçlar da elde edilebilir.

6.4 Bölüm Değerlendirmesi

Bu bölümde önerilen FSADM metodolojisi altında FSAP ve SABADT yöntemlerinin performansları ve literatürdeki öncü yöntemlerle karşılaştırmaları anlatılmıştır. Önerilen metodoloji ikisi literatürde en çok kullanılan veri setleri ve diğeri çalışma kapsamında geliştirilen veri seti olmak üzere toplamda üç farklı veri seti üzerinde uygulanmış ve test edilmiştir. Önerilen yöntem hem saldırıların farklı türlerini hem de yeni ve daha önce bilinmeyen saldırıları başarılı bir şekilde tespit etmiştir. Test edilen bütün veri setleri üzerinde en yüksek doğruluk oranları önerilen metodoloji ile elde edilmiştir. Sonuç olarak, önerilen metodoloji amacına ulaşmıştır ve literatüre katkısı kanıtlanmıştır.

7. SONUÇ

Teknolojinin ilerlemesi ile birlikte kablolar hayatımızın büyük bir bölümünden çıkmış, yerini kablosuz cihazlar ve ortamlara bırakmıştır. Bu olumlu ilerleme ile birlikte kablosuz ortamlar farklı güvenlik problemlerini de beraberinde getirmiştir. Günlük hayatta insanların büyük bir çoğunluğu kablosuz ağları kullanmaktadır. Neredeyse bütün kurum ve kuruluşlarda, evlerde, ofislerde ise kablosuz yerel alan ağları kullanılmaktadır. Son yıllarda IoT teknolojilerinin akıllı evler, iş yerleri, şehirler gibi uygulamalarıyla hayatımızın her alanını çevrelemiş olması da WLAN'ların kullanımını fazlasıyla artırmıştır. Ağ üzerinden yapılan bütün işlemlerde güvenliği sağlamak, kişisel olan ve olmayan bütün verileri korumak ve donanımların sorunsuz çalışmasını sağlamak için gelişmiş bir saldırı tespit sistemi büyük önem arz etmektedir.

Kablosuz yerel alan ağlarına olan yoğun ilgiden dolayı, saldırı tespit sistemleri alanında çalışmalarda artmıştır. Gelişmiş 802.11 WLAN güvenlik protokolüne rağmen, ne yazık ki güvenlik açıkları halen devam etmektedir. Bununla birlikte, IEEE 802.11 WLAN'larındaki olası tüm saldırıları güvenilir ve doğru bir şekilde tespit edebilen bir kablosuz saldırı tespit sistemi eksikliği vardır. Günümüzde kullanılan saldırı tespit sistemlerine karşılık, saldırılar da davranışlarını değiştirmektedir. Daha önce anomali olarak belirlenen bir saldırı türü farklı bir şekilde davranarak tanımlanamamaktadır. Yaygın IDS'lerde kullanılan çoğu teknik, bilgisayar ağlarında siber saldırıların dinamik ve karmaşık doğası ile baş edememektedir. Özetle buradaki temel eksiklikler, imza tabanlı tespit yöntemlerde kullanılan imzaların tespitte yetersiz kalması, anomali tabanlı tespit yöntemlerinde kuralların net bir şekilde belirlenememesi ve mevcut IDS'lerin yeni nesil saldırı türlerinin tespitinde yetersiz kalmaları şeklindedir.

Bu tez çalışmasında, saldırı tespit sistemlerinin doğruluk oranına katkı yapmak ilk amaçtır. Bunun yanında ağ üzerinden gelen çeşitli saldırı türlerinin de dinamik olarak belirlenmesi hedeflenmektedir. Bu kapsamda yeni bir saldırı tespit ve analiz yöntemi önerilmiştir. Tez çalışmasının 4 temel katkısı bulunmaktadır. 1. Saldırı tespit ve sınıflandırma işlemleri için bir metodoloji (FSADM) önerilmiştir. 2. Saldırıların hızlı bir şekilde tespit edilebilmesi için öğrenme işleminin de temeli olan yeni özellik seçim yöntemi (FSAP) önerilmiştir. 3.Saldırıların yüksek doğrulukla sınıflandırılması için

hibrid bir yöntem (SABADT) önerilmiştir. 4. Önerilen yöntemlerin performans değerlendirmelerini gerçekleştirebilmek için yeni veri seti geliştirilmiştir.

Bu metodoloji ve yöntemler geliştirilirken ve uygulanırken yapılan çalışmalar adım adım aşağıda özetlenmiştir:

1. Problemin zorluğunu ve sınırlarını belirlemek, daha önce yapılmış çalışmaların ne derece başarılı olup olmadığını görmek ve daha iyi çalışan bir model öne sürmek için aşağıdaki çalışmalar yapılmıştır.
    - Kullanılacak veri setleri belirlenmesi,
    - Özellik çıkarımı için mevcut veri madenciliği tekniklerinin araştırılması,
    - Ağ üzerindeki işlemlerin sınıflandırılması için mevcut makine öğrenmesi algoritmalarının araştırılması ve uygulanması,
    - Yapılan işlemlerin raporlandırılmasıdır.

2. Var olan problemlerin çözümüne katkı sağlamak ve ağdaki saldırıların tespiti için algoritmalar geliştirilerek yeni yaklaşımlar sunulmuştur. Bu adımı gerçekleştirebilmek için aşağıdaki çalışmalar yapılmıştır.
    - Özellik seçimi için bir yaklaşım önerilmesi ve önerilen yaklaşıma göre önemli özelliklerin seçiminin yapılması,
    - Seçilen özelliklerden, veri setlerinde kullanılan temel özellikler ile veriler analiz edilerek imzalar çıkarılması,
    - Temel özellikler dışında veri setlerine ait diğer özellikler kullanılarak ağda görülen davranışların belirlenmesi, bu davranışlara göre belirli kurallar oluşturulması,
    - Önerilen yöntemin performans karşılaştırmaları.

3. Çalışmanın önceki aşamasında önerilen algoritmaları geliştirerek saldırıların tespit edilmesinin yanı sıra saldırıların türünün de belirlenmesine yönelik yeni yaklaşımlar sunulmuştur. Bu adımı gerçekleştirebilmek için aşağıdaki çalışmalar yapılmıştır.
    - Özellik seçimi için önerilen yaklaşıma yeni bir algoritma daha eklenmesi,
    - Önerilen yaklaşıma göre özelliklerin daha da azaltılarak seçiminin yapılması
    - Temel özellikler kullanılarak imza çıkarma algoritmasının saldırı ve türlerinin tespitine yönelik güncellenmesi,
    - Temel özellikler dışında veri setlerine ait diğer özellikler kullanılarak davranışlara göre kurallar çıkarma algoritmasının saldırı ve türlerinin tespitine yönelik güncellenmesi,
    - Önerilen yöntemin performans karşılaştırmaları.

4. Tez kapsamında yeni bir veri seti oluşturulmuştur. Önerilen yöntemler oluşturulan veri seti ve literatürdeki mevcut veri setleri üzerinde uygulanmıştır. Bu adımı gerçekleştirebilmek için aşağıdaki çalışmalar yapılmıştır.
    - Veri toplama işlemi için topoloji tasarlanması, tasarlanan topolojiye göre kurban bilgisayara belirli aralıklar ile saldırılar düzenlenmesi ve normal trafik davranışlarında bulunulması,
    - Toplanan verilerin analiz edilmesi, özellik çıkarımı yapılması ve veri setinin oluşturulması,
    - Önerilen yöntemin veri setlerine uygulanması ve sonuçların mevcut makine öğrenmesi teknikleri ve literatürdeki öncü çalışmalar ile karşılaştırılması.

Tez çalışması kapsamında geliştirilen bu yöntemin performansını değerlendirmek amacıyla KDD'99, UNSW-NB15 ve oluşturulan veri seti kullanılmıştır. Yöntemin test edilmesi işleminin sonucunda saldırıların tespit edilmesinde KDD'99 veri setinde %99.81, UNSW-NB15 veri setinde %99.17 doğruluk oranı ve çalışma kapsamında üretilen veri setinde %99.79 doğruluk oranı elde edilmiştir. Elde edilen sonuçlar, bilinen makine öğrenmesi yöntemleri ile karşılaştırıldığında değerlendirme metriklerine göre en iyi sonuçlar elde edilmiştir. Diğer taraftan, hem özellik azaltımı hem de saldırı tespit yaklaşımını bir arada sunan fazla çalışma bulunmamaktadır. Ek olarak, araştırmalar esnasında geliştirilen yöntemlerin performansının ve hafıza kullanımının mevcutlara göre daha da iyileştirildiği gözlemlenmiştir. Bir sonraki çalışmalarda geliştirilen yöntemlerin performansının çalışma süresi, hafıza kullanımı gibi metriklere göre de değerlendirilmesi planlanmaktadır. Aynı zamanda geliştirilen veri setinin oluşturulma topolojisine IoT cihazları eklenerek de veri setinin geliştirilmesi hedeflenmektedir.

Bu tez çalışması ile birlikte, literatürdeki eksiklere katkı sağlayabilecek, daha az özellik kullanarak yüksek doğruluk ile bilinmeyen saldırıları da tespit edebilen bir yöntem önerilmiştir. Geliştirilen birçok başarılı çalışmanın yanında siber saldırılar da her geçen gün artmaya devam edecektir. Bu sebeple bu saldırıların önüne geçebilmek için en önemli adım kişilerin ve kurumların güvenlik alanında bilinçlendirilmesidir. Aynı zamanda, gelecekte yapılacak çalışmalarda, saldırı imzalarının güncel tutulması, doğru özelliklerin kullanılması ve doğru kural çıkarabilen yöntemlerin geliştirilmesi, mevcut IDS yöntemlerinin başarılı yanlarının kullanılabilmesi için iki veya daha fazla yöntemin entegre edilmesi gibi adımlar ile başarılı sonuçlar elde edilebilecektir.

KAYNAKLAR

Abdulhammed, R., Faezipour, M., Abuzneid, A., & Alessa, A. 2018. Effective features selection and machine learning classifiers for improved wireless intrusion detection. In 2018 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.

Administrator Guide, "Security Event Manager," Version 2021.2, Available: https://documentation.solarwinds.com/en/success_center/sem/content/sem_administrator_guide.htm, Accessible: 30 June 2021.

Afzal, Z., Rossebø, J., Talha, B., & Chowdhury, M. (2016, March). A wireless intrusion detection system for 802.11 networks. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 828-834). IEEE.

Ahmad, M. S., & Ramachandran, V. (2007). Cafe latte with a free topping of cracked wep retrieving wep keys from road warriors. In Proc. Conf. ToorCon.

Ahn, S., Yi, H., Lee, Y., Ha, W. R., Kim, G., & Paek, Y. (2020, July). Hawkware: network intrusion detection based on behavior analysis with ANNs on an IoT device. In 2020 57th ACM/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE.

Aldwairi, M., Abu-Dalo, A. M., & Jarrah, M. (2017). Pattern matching of signature-based IDS using Myers algorithm under MapReduce framework. EURASIP Journal on Information Security, 2017(1), 1-11.

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189, 105124.

Al-Gharabally, N., El-Sayed, N., Al-Mulla, S., & Ahmad, I. (2009, March). Wireless honeypots: survey and assessment. In Proceedings of the 2009 conference on Information Science, Technology and Applications (pp. 45-52).

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152-160.

Amaral, J. P., Oliveira, L. M., Rodrigues, J. J., Han, G., & Shu, L. (2014, June). Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks. In 2014 IEEE international conference on communications (ICC) (pp. 1796-1801). IEEE.

Amiri, F., Yousefi, M. R., Lucas, C., Shakery, A., & Yazdani, N. (2011). Mutual information-based feature selection for intrusion detection systems. Journal of Network and Computer Applications, 34(4), 1184-1199.

Anwer, H. M., Farouk, M., & Abdel-Hamid, A. (2018, April). A framework for efficient network anomaly intrusion detection with features selection. In 2018 9th International Conference on Information and Communication Systems (ICICS) (pp. 157-162). IEEE.

Araújo, N., de Oliveira, R., Shinoda, A. A., & Bhargava, B. (2010, April). Identifying important characteristics in the KDD99 intrusion detection dataset by feature selection using a hybrid approach. In 2010 17th International Conference on Telecommunications (pp. 552-558). IEEE.

Aravind, M. M., & Kalaiselvi, V. K. G. (2017, March). Design of an intrusion detection system based on distance feature using ensemble classifier. In 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN) (pp. 1-6). IEEE.

Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE Access, 8, 6249-6271.

Aslan, Ö., Ozkan-Okay, M., & Gupta, D. (2021). Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. IEEE Access.

Aslan, Ö., Ozkan-Okay, M., & Gupta, D. (2021). A Review of Cloud-Based Malware Detection System: Opportunities, Advances and Challenges. European Journal of Engineering and Technology Research, 6(3), 1-8.

Aslan, Ö., & YILMAZ, A. A. (2021). A New Malware Classification Framework Based on Deep Learning Algorithms. IEEE Access.

Babirye, C.,& Mwebaze, E. (2018). Signature-based Denial of Service and Probe Detection, a Machine Learning approach. International Journal of Technology and Management, 3(2), 11-11.

Baig, M. M., Awais, M. M., & El-Alfy, E. S. M. (2017). A multiclass cascade of artificial neural network for network intrusion detection. Journal of Intelligent & Fuzzy Systems, 32(4), 2875-2883.

Baykara, M., & Das, R. (2018). A novel honeypot based security approach for real-time intrusion detection and prevention systems. Journal of Information Security and Applications, 41, 103-116.

Baykara, M., & DAŞ, R. (2019). SoftSwitch: a centralized honeypot-based security approach using software-defined switching for secure management of VLAN networks. Turkish Journal of Electrical Engineering & Computer Sciences, 27(5), 3309-3325.

Bedi, P., Gupta, N., & Jindal, V. (2021). I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems. Applied Intelligence, 51(2), 1133-1151.

Belouch, M., El Hadaj, S., & Idhammad, M. (2017). A two-stage classifier approach using reptree algorithm for network intrusion detection. International Journal of Advanced Computer Science and Applications, 8(6), 389-394.

Belouch, M., El Hadaj, S., & Idhammad, M. (2018). Performance evaluation of intrusion detection based on machine learning using Apache Spark. Procedia Computer Science, 127, 1-6.

Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2016, December). Feasibility of supervised machine learning for cloud security. In 2016 International Conference on Information Science and Security (ICISS) (pp. 1-5). IEEE.

Bovenzi, G., Aceto, G., Ciuonzo, D., Persico, V., & Pescapé, A. (2020, December). A hierarchical hybrid intrusion detection approach in iot scenarios. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-7). IEEE.

Berghel, H. and Uecker, J. 2005. "WiFi attack vectors". In: Communications of the ACM 48.8, pp. 21–28.

Beyah, R., & Venkataraman, A. (2011). Rogue-access-point detection: Challenges, solutions, and future directions. IEEE Security & Privacy, 9(5), 56-61.

Bicakci, K., & Tavli, B. (2009). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. Computer Standards & Interfaces, 31(5), 931-941.

Bittau, A. (2003). Additional weak IV classes for the FMS attack. Department of Computer Science, University College London, 226-238.

Bittau, A. (2005, September). The fragmentation attack in practice. In IEEE Symposium on Security and Privacy, IEEE Computer Society.

Bhosale, D. A., & Mane, V. M. (2015, October). Comparative study and analysis of network intrusion detection tools. In 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 312-315). IEEE.

Boite, J., Nardin, P. A., Rebecchi, F., Bouet, M., & Conan, V. (2017, July). Statesec: Stateful monitoring for DDoS protection in software defined networks. In 2017 IEEE Conference on Network Softwarization (NetSoft) (pp. 1-9). IEEE.

Boob, S., & Jadhav, P. (2010). Wireless intrusion detection system. International Journal of Computer Applications, 5(8), 9-13.

Byrnes, J., Hoang, T., Mehta, N. N., & Cheng, Y. (2020, October). A Modern Implementation of System Call Sequence Based Host-based Intrusion Detection Systems. In 2020 Second IEEE International Conference on Trust, Privacy and

Security in Intelligent Systems and Applications (TPS-ISA) (pp. 218-225). IEEE.

Catherine, F. L., Pathak, R., & Vaidehi, V. (2014, April). Efficient host based intrusion detection system using Partial Decision Tree and Correlation feature selection algorithm. In 2014 International Conference on Recent Trends in Information Technology (pp. 1-6). IEEE.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

Chawla, A., Lee, B., Fallon, S., & Jacob, P. (2018, September). Host based intrusion detection system with combined CNN/RNN model. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 149-158). Springer, Cham.

Choudhary, S., & Kesswani, N. (2021). A Hybrid Classification Approach for Intrusion Detection in IoT Network. Journal of Scientific and Industrial Research (JSIR), 80(09), 809-816.

Cordero, C. G., Vasilomanolakis, E., Wainakh, A., Mühlhäuser, M., & Nadjm-Tehrani, S. (2021). On generating network traffic datasets with synthetic attacks for intrusion detection. ACM Transactions on Privacy and Security (TOPS), 24(2), 1-39.

Creech, G., & Hu, J. (2013). A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. IEEE Transactions on Computers, 63(4), 807-819.

Creech, G. (2014). Developing a high-accuracy cross platform Host-Based Intrusion Detection System capable of reliably detecting zero-day attacks. Doctoral dissertation, University of New South Wales, Canberra, Australia.

Deniz, E., & Samet, R. (2018, December). A new model for secure joining to ZigBee 3.0 networks in the internet of things. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 102-106). IEEE.

Deshpande, P., Sharma, S. C., Peddoju, S. K., & Junaid, S. (2018). HIDS: A host based intrusion detection system for cloud computing environment. International Journal of System Assurance Engineering and Management, 9(3), 567-576.

Devan, P., & Khare, N. (2020). An efficient XGBoost–DNN-based classification model for network intrusion detection system. Neural Computing and Applications, 1-16.

Dwivedi, S., Vardhan, M., Tripathi, S., & Shukla, A. K. (2020). Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection. Evolutionary Intelligence, 13(1), 103-117.

Ethala K., Seshadri R., Renganathan N.G. and Saravanan M.S., 2013. A Role of Intrusion Detection System for Wireless Lan Using Various Schemes and Related Issues. American Journal of Applied Sciences 10(9), pp. 979-985.

Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897.

Fladby, T., Haugerud, H., Nichele, S., Begnum, K., & Yazidi, A. (2020, October). Evading a Machine Learning-based Intrusion Detection System through Adversarial Perturbations. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems (pp. 161-166).

Farshchi, J. (2003). Statistical-based intrusion detection. Retrieved October, 10, 2009.

Ferreri, F., Bernaschi, M., & Valcamonici, L. (2004, March). Access points vulnerabilities to DoS attacks in 802.11 networks. In 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733) (Vol. 1, pp. 634-638). IEEE.

Fluhrer, S., Mantin, I. and Shamir, A. 2001. "Weaknesses in the key scheduling algorithm of RC4". In: Selected areas in cryptography. Springer, pp. 1–24.

Ford, M., Mallery, C., Palmasani, F., Rabb, M., Turner, R., Soles, L., & Snider, D. (2016, March). A process to transfer Fail2ban data to an adaptive enterprise intrusion detection and prevention system. In SoutheastCon 2016 (pp. 1-4). IEEE.

Ganesh R.K., Purushothama R.V. , Bhimavaram S. and Pradesh A., 2017. An Effective Analysis on Intrusion Detection Systems in Wireless Mesh Networks. International Conference on Advances in Computing, Communications and Informatics (ICACCI).

Gassais, R., Ezzati-Jivan, N., Fernandez, J. M., Aloise, D., & Dagenais, M. R. (2020). Multi-level host-based intrusion detection system for Internet of things. Journal of Cloud Computing, 9(1), 1-16.

Geramiraz, F., Memaripour, A. S., & Abbaspour, M. (2012). Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy Controller. Int. J. Netw. Secur., 14(6), 352-361.

Ghanem, K., Aparicio-Navarro, F. J., Kyriakopoulos, K. G., Lambotharan, S., & Chambers, J. A. (2017, December). Support vector machine for network

intrusion and cyber-attack detection. In 2017 sensor signal processing for defence conference (SSPD) (pp. 1-5). IEEE.

Ghanshala, K. K., Mishra, P., Joshi, R. C., & Sharma, S. (2018, December). BNID: a behavior-based network intrusion detection at network-layer in cloud environment. In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) (pp. 100-105). IEEE.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

Gupta, S., & Mamtora, R. (2012). Intrusion detection system using wireshark. International Journal of Advanced Research in Computer Science and Software Engineering, 2(11), 358-363.

Gupta, D., Bhatt, S., Gupta, M., Kayode, O., & Tosun, A. S. (2020, May). Access control model for google cloud iot. In 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 198-208). IEEE.

Han, S. J., & Cho, S. B. (2003). Detecting intrusion with rule-based integration of multiple models. Computers & Security, 22(7), 613-623.

Harish, B. S., & Kumar, S. A. (2017). Anomaly based Intrusion Detection using Modified Fuzzy Clustering. Int. J. Interact. Multim. Artif. Intell., 4(6), 54-59.

Hasan, M. A. M., Nasser, M., Ahmad, S., & Molla, K. I. (2016). Feature selection for intrusion detection using random forest. Journal of information security, 7(3), 129-140.

Hassine, K., Erbad, A., & Hamila, R. (2019, June). Important complexity reduction of random forest in multi-classification problem. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 226-231). IEEE.

Hubballi, N., & Suryanarayanan, V. (2014). False alarm minimization techniques in signature-based intrusion detection systems: A survey. Computer Communications, 49, 1-17.

Hick, P., Aben, E., Claffy, K., & Polterock, J. “the CAIDA DDoS attack 2007 dataset,” ed, 2007.

Idhammad, M., Afdel, K., & Belouch, M. (2017). Dos detection method based on artificial neural networks. International Journal of Advanced Computer Science and Applications, 8(4), 465-471.

IEEE Computer Society LAN/MAN Standards Committee. (2007). IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11.

Iwendi, C., Khan, S., Anajemba, J. H., Mittal, M., Alenezi, M., & Alazab, M. (2020). The use of ensemble models for multiple class and binary class classification for improving intrusion detection systems. Sensors, 20(9), 2559.

Kang, B., McLaughlin, K., & Sezer, S. (2016, August). Towards a stateful analysis framework for smart grid network intrusion detection. In 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4 (pp. 124-131).

Karimi, Z., Kashani, M. M. R., & Harounabadi, A. (2013). Feature ranking in intrusion detection dataset using combination of filtering methods. International Journal of Computer Applications, 78(4).

Karatas, G., & Sahingoz, O. K. (2018, March). Neural network based intrusion detection systems with different training functions. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-6). IEEE.

Kasongo, S. M., & Sun, Y. (2019). A deep learning method with filter based feature engineering for wireless intrusion detection system. IEEE Access, 7, 38597-38607.

Kasongo, S. M., & Sun, Y. (2020). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. Computers & Security, 92, 101752.

Kaur, S.,& Singh, M. (2019). Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks. Neural Computing and Applications, 1-19.

Kayacik, H. G., Zincir-Heywood, A. N., & Heywood, M. I. (2007). A hierarchical SOM-based intrusion detection system. Engineering applications of artificial intelligence, 20(4), 439-451.

Khan, M. A. (2021). HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System. Processes, 9(5), 834.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1), 1-22.

Klein, A. (2008). Attacks on the RC4 stream cipher. Designs, codes and cryptography, 48(3), 269-286.

Kolias, C., Kambourakis, G., Stavrou, A. and Gritzalis, S. 2015. “Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset”. IEEE Communications Surveys & Tutorials 18 (1), pp. 184-208.

Kore, K. (2004). chopchop (experimental WEP attacks). http://www. netstumbler. org/showthread. php? t= 12489.

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Generation Computer Systems, 100, 779-796.

Kousar, H., Mulla, M. M., Shettar, P., & Narayan, D. G. (2021, June). Detection of DDoS Attacks in Software Defined Network using Decision Tree. In 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT) (pp. 783-788). IEEE.

KR, K., & Indra, A. (2010). Intrusion Detection Tools and techniques–a Survey'. International Journal of Computer Theory and Engineering, 2(6), 901.

Kumar, S., Viinikainen, A., & Hamalainen, T. (2016, December). Machine learning classification model for network based intrusion detection system. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 242-249). IEEE.

Kumar, V., & Sangwan, O. P. (2012). Signature based intrusion detection system using SNORT. International Journal of Computer Applications & Information Technology, 1(3), 35-41.

Kumar, P., Gupta, G. P., & Tripathi, R. (2021). Design of Anomaly-Based Intrusion Detection System Using Fog Computing for IoT Network. Automatic Control and Computer Sciences, 55(2), 137-147.

Lai, C., Chavez, A. R., Jones, C. B., Jacobs, N., Hossain-McKenzie, S., Johnson, J. B., & Summers, A. (2021). Review of Intrusion Detection Methods and Tools for Distributed Energy Resources (No. SAND2021-1737). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Larijani, H., Ahmad, J. and Mtetwa N. (2018, September). A novel random neural network based approach for intrusion detection systems. In 2018 10th Computer Science and Electronic Engineering (CEEC) (pp. 50-55). IEEE.

Lewis, B., Broadbent, M., & Race, N. (2019, November). P4ID: P4 enhanced intrusion detection. In 2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 1-4). IEEE.

Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert systems with applications, 39(1), 424-430.

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.

Lim, Y. X., Yer, T. S., Levine, J., & Owen, H. L. (2003, June). Wireless intrusion detection and response. In IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003. (pp. 68-75). IEEE.

Liu, M., Xue, Z., He, X., & Chen, J. (2021). SCADS: A Scalable Approach Using Spark in Cloud for Host-based Intrusion Detection System with System Calls. arXiv preprint arXiv:2109.11821.

Liu, C., Yu, J., & Brewster, G. (2010, June). Empirical studies and queuing modeling of denial of service attacks against 802.11 WLANs. In 2010 IEEE International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 1-9). IEEE.

Liu, Y., Jin, Z., & Wang, Y. (2010, September). Survey on security scheme and attacking methods of WPA/WPA2. In 2010 6th international conference on wireless communications networking and mobile computing (wicom) (pp. 1-4). IEEE.

Lupari, P. (2021). Detecting Anomalies in TLS Traffic Using Encrypted Traffic Analysis.

Malek, Z. S., Trivedi, B., & Shah, A. (2020, July). User behavior Pattern-Signature based Intrusion Detection. In 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) (pp. 549-552). IEEE.

Malekzadeh, M., Ghani, A. A., Desa, J., & Subramaniam, S. (2009). Empirical analysis of virtual carrier sense flooding attacks over wireless local area network. Journal of Computer science, 5(3), 214.

Manzoor, I., & Kumar, N. 2017. A feature reduced intrusion detection system using ANN classifier. Expert Systems with Applications, 88, 249-257.

Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University-Computer and Information Sciences, 31(4), 541-553.

Meftah, S., Rachidi, T., & Assem, N. (2019). Network based intrusion detection using the UNSW-NB15 dataset. International Journal of Computing and Digital Systems, 8(5), 478-487.

Meng, Y., & Li, W. (2013, June). Evaluation of detecting malicious nodes using Bayesian model in wireless intrusion detection. In International Conference on Network and System Security (pp. 40-53). Springer, Berlin, Heidelberg.

Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: an ensemble of autoencoders for online network intrusion detection. arXiv preprint arXiv:1802.09089.

Mudzingwa, D., & Agrawal, R. (2012, March). A study of methodologies used in intrusion detection and prevention systems (IDPS). In 2012 Proceedings of IEEE Southeastcon (pp. 1-6). IEEE.

Martínez, A., Zurutuza, U., Uribeetxeberria, R., Fernández, M., Lizarraga, J., Serna, A., & Vélez, I. (2008, March). Beacon frame spoofing attack detection in IEEE 802.11 networks. In 2008 Third International Conference on Availability, Reliability and Security (pp. 520-525). IEEE.

Meiners, L. F. (2009). But... my station is awake! Power Save Denial of Service in 802.11 Networks.

Mitchell, R., & Chen, R. 2014. A survey of intrusion detection in wireless network applications. Computer Communications, 42, 1-23.

Moon, D., Im, H., Kim, I., & Park, J. H. (2017). DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks. The Journal of supercomputing, 73(7), 2881-2895.

More, S., Mathews, M.L., Joshi, A. and Finin, T. 2012. A semantic approach to situational awareness for intrusion detection. Proceedings of the National Symposium on Moving Target Research, (MTR' 12), UMBC.

Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In 2015 military communications and information systems conference (MilCIS) (pp. 1-6). IEEE.

Moustafa, N., & Slay, J. 2016. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective, 25(1-3), 18-31.

Moustafa, N., Turnbull, B., & Choo, K. K. R. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 6(3), 4815-4830.

Musa, U. S., Chhabra, M., Ali, A., & Kaur, M. (2020, September). Intrusion detection system using machine learning techniques: A review. In 2020 international

conference on smart electronics and communication (ICOSEC) (pp. 149-155). IEEE.

Moskowitz, R. (2003). Weakness in passphrase choice in WPA interface. http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface. html.

Nguyen, T. D., Nguyen, D. H., Tran, B. N., Vu, H., & Mittal, N. (2008, August). A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks. In 2008 Proceedings of 17th International Conference on Computer Communications and Networks (pp. 1-6). IEEE.

Nguyen, K. K., Hoang, D. T., Niyato, D., Wang, P., Nguyen, D., & Dutkiewicz, E. (2018, April). Cyberattack detection in mobile cloud computing: A deep learning approach. In 2018 IEEE wireless communications and networking conference (WCNC) (pp. 1-6). IEEE.

Narsingyani, D., & Kale, O. (2015, October). Optimizing false positive in anomaly based intrusion detection using Genetic algorithm. In 2015 IEEE 3rd International Conference on MOOCs, Innovation and Technology in Education (MITE) (pp. 72-77). IEEE.

Nitin, T., Singh, S. R., & Singh, P. G. (2012). Intrusion detection and prevention system (idps) technology-network behavior analysis system (nbas). ISCA J. Engineering Sci, 1(1), 51-56.

Olusola, A. A., Oladele, A. S., & Abosede, D. O. (2010, October). Analysis of KDD'99 intrusion detection dataset for selection of relevance features. In Proceedings of the world congress on engineering and computer science (Vol. 1, pp. 20-22). WCECS.

Otoum, Y., & Nayak, A. (2021). AS-IDS: Anomaly and Signature Based IDS for the Internet of Things. Journal of Network and Systems Management, 29(3), 1-26.

Ou, Y. J., Lin, Y., & Zhang, Y. (2010, April). The design and implementation of host-based intrusion detection system. In 2010 third international symposium on intelligent information technology and security informatics (pp. 595-598). IEEE.

Ozkan-Okay, M., & Samet, R. 2020. Hybrid Intrusion Detection Approach for Wireless Local Area Network. In 2020 7th International Conference on Control and Optimization with Industrial Applications (COIA) (pp. 311-313).

Ozkan-Okay, M., Samet, R., & Aslan, Ö. (2021, September). A New Feature Selection Approach and Classification Technique for Current Intrusion Detection System. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 227-232). IEEE.

Ozkan-Okay, M., Samet, R., Aslan, Ö., & Gupta, D. (2021). A Comprehensive Systematic Literature Review on Intrusion Detection Systems. IEEE Access.

Ozkan-Okay, M., Aslan, Ö., Eryigit, R., & Samet, R. (2021). SABADT: Hybrid Intrusion Detection Approach for Cyber Attacks Identification in WLAN. IEEE Access, 9, 157639-157653.

Pacheco, J., Benitez, V., & Félix, L. (2019, July). Anomaly behavior analysis for IoT network nodes. In Proceedings of the 3rd International Conference on Future Networks and Distributed Systems (pp. 1-6).

Park, D., Kim, S., Kwon, H., Shin, D., & Shin, D. (2021). Host-Based Intrusion Detection Model Using Siamese Network. IEEE Access, 9, 76614-76623.

Patel, A. M., Patel, A. R., & Patel, H. R. (2014). Rap problems and solutions in 802.11 wireless LAN. Int. J., 2(1), 669-674.

Rajagopal, S., Hareesha, K. S., & Kundapur, P. P. (2020). Feature Relevance Analysis and Feature Reduction of UNSW NB-15 Using Neural Networks on MAMLS. Journal: Advances in Intelligent Systems and Computing Advanced Computing and Intelligent Engineering, 321-332.

Rashid, A., Siddique, M. J., & Ahmed, S. M. (2020, February). Machine and deep learning based comparative analysis using hybrid approaches for intrusion detection system. In 2020 3rd International Conference on Advancements in Computational Sciences (ICACS) (pp. 1-9). IEEE.

Rai, K., Devi, M. S., & Guleria, A. (2016). Decision tree based algorithm for intrusion detection. International Journal of Advanced Networking and Applications, 7(4), 2828.

Resmi, A. M., & Manicka, R. (2017). Intrusion detection system techniques and tools: A survey. Scholars Journal of Engineering and Technology (SJET).

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

Riyaz, B., & Ganapathy, S. (2020). A deep learning approach for effective intrusion detection in wireless networks using CNN. Soft Computing, 24, 17265-17278.

Samrin, R., & Vasumathi, D. (2017, December). Review on anomaly based network intrusion detection system. In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 141-147). IEEE.

Satam, P., & Hariri, S. (2020). WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol. IEEE Transactions on Network and Service Management, 18(1), 1077-1091.

Sawwashere, S. S., & Nimbhorkar, S. U. (2014, April). Survey of RTS-CTS attacks in wireless network. In 2014 Fourth International Conference on Communication Systems and Network Technologies (pp. 752-755). IEEE.

Saxena, H.,& Richariya, V. (2014). Intrusion detection in KDD99 dataset using SVM-PSO and feature reduction with information gain. International Journal of Computer Applications, 98(6).

Sbai, O., & El boukhari, M. (2020, September). Data Flooding Intrusion Detection System for MANETs Using Deep Learning Approach. In Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications (pp. 1-5).

Scarfone, K.A. and Mell, P.M. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology.

Seo, D., Lee, H., & Nuwere, E. (2013). SIPAD: SIP–VoIP anomaly detection using a stateful rule tree. Computer Communications, 36(5), 562-574.

Shabtai, A., Moskovitch, R., Elovici, Y., & Glezer, C. (2009). Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. information security technical report, 14(1), 16-29.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108-116.

Sharma, V., You, I., Yim, K., Chen, R., & Cho, J. H. (2019). BRIoT: Behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems. IEEE Access, 7, 118556-118580.

Siddique, K., Akhtar, Z., Khan, F. A., & Kim, Y. (2019). KDD cup 99 data sets: A perspective on the role of data sets in network intrusion detection research. Computer, 52(2), 41-51.

Singhrova, A. (2011, September). A host based intrusion detection system for DDoS attack in WLAN. In 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011) (pp. 433-438). IEEE.

Singh, N. B., Singh, M. M., Sarkar, A., & Mandal, J. K. (2021). A novel wide & deep transfer learning stacked GRU framework for network intrusion detection. Journal of Information Security and Applications, 61, 102899.

Srivastav, A., Kumar, P., & Goel, R. (2013). Evaluation of Network Intrusion Detection System using PCA and NBA. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(11).

Subba, B., Biswas, S., & Karmakar, S. (2017, November). Host based intrusion detection system using frequency analysis of n-gram terms. In TENCON 2017-2017 IEEE Region 10 Conference (pp. 2006-2011). IEEE.

Song, Y., Yang, C., & Gu, G. (2010, June). Who is peeping at your passwords at Starbucks?—To catch an evil twin access point. In 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN) (pp. 323-332). IEEE.

Tama, B. A., Comuzzi, M., & Rhee, K. H. (2019). TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. IEEE Access, 7, 94497-94507.

Tavallaee, M., Bagheri, E., Lu W. and Ghorbani, A. A. (July 2009). "A detailed analysis of the KDD CUP 99 data set," In 2009 IEEE symposium on computational intelligence for security and defense applications (pp. 1-6).

Tews, E., Weinmann, R. P., & Pyshkin, A. (2007, August). Breaking 104 bit WEP in less than 60 seconds. In International Workshop on Information Security Applications (pp. 188-202). Springer, Berlin, Heidelberg.

Thakkar, A., & Lohiya, R. (2020). A review of the advancement in intrusion detection datasets. Procedia Computer Science, 167, 636-645.

Thanthrige, U. S. K. P. M., Samarabandu, J., & Wang, X. 2016. Machine learning techniques for intrusion detection on public dataset. In 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) (pp. 1-4). IEEE.

Timofte, J. (2008). Intrusion detection using open source tools. Informatica Economica Journal Issn, 14531305, 75-79.

Tinnirello, I., & Choi, S. (2005, May). Efficiency analysis of burst transmissions with block ACK in contention-based 802.11 e WLANs. In IEEE International Conference on Communications, 2005. ICC 2005. 2005 (Vol. 5, pp. 3455-3460). IEEE.

Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. expert systems with applications, 36(10), 11994-12000.

Uddin, M., Rahman, A. A., Uddin, N., Memon, J., Alsaqour, R. A., & Kazi, S. (2013). Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents. Int. J. Netw. Secur., 15(2), 97-105.

Verma, J., Bhandari, A., & Singh, G. (2020). Review of existing data sets for network intrusion detection system. Advances in Mathematics: Scientific Journal, 9(6), 3849-3854.

Vijayakumar, D. S., & Ganapathy, S. (2018). Machine Learning Approach to Combat False Alarms in Wireless Intrusion Detection System. Comput. Inf. Sci., 11(3), 67-81.

Vinchurkar, D. P., & Reshamwala, A. (2012). A review of intrusion detection system using neural network and machine learning. J. Eng. Sci. Innov. Technol, 1, 54-63.

Potteti, S., & Parati, N. (2017, May). Intrusion detection system using hybrid Fuzzy Genetic algorithm.

Primartha, R., & Tama, B. A., 2017. Anomaly detection using random forest: A performance revisited. In 2017 International conference on data and software engineering (ICoDSE) (pp. 1-6). IEEE.

Shapoorifard, H., & Shamsinejad, P. (2017). Intrusion detection using a novel hybrid method incorporating an improved KNN. Int. J. Comput. Appl, 173(1), 5-9.

Ullah, I., & Mahmoud, Q. H. (2017, December). A filter-based feature selection model for anomaly-based intrusion detection systems. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 2151-2159). IEEE.

Usha, M., & Kavitha, P. 2017. Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier. Wireless Networks, 23(8), 2431-2446.

Viegas, E., Santin, A., Bessani, A., & Neves, N. (2019). BigFlow: Real-time and reliable anomaly-based intrusion detection for high-speed networks. Future Generation Computer Systems, 93, 473-485.

Qassim, Q., Zin, A. M., & Ab Aziz, M. J. (2016). Anomalies Classification Approach for Network-based Intrusion Detection System. Int. J. Netw. Secur., 18(6), 1159-1172.

Qureshi, A. U. H., Larijani, H., Ahmad, J., & Mtetwa, N. (2019, July). A heuristic intrusion detection system for Internet-of-Things (IoT). In Intelligent computing-proceedings of the computing conference (pp. 86-98). Springer, Cham.

Wang, X., Kordas, A., Hu, L., Gaedke, M., & Smith, D. (2013, October). Administrative evaluation of intrusion detection system. In Proceedings of the 2nd annual conference on Research in information technology (pp. 47-52).

Wattanapongsakorn, N., Srakaew, S., Wonghirunsombat, E., Sribavonmongkol, C., Junhom, T., Jongsubsook, P., & Charnsripinyo, C. (2012, June). A practical network-based intrusion detection and prevention system. In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 209-214). IEEE.

Xiao, L.,& Liu, Y. (2009, April). A two-step feature selection algorithm adapting to intrusion detection. In 2009 International Joint Conference on Artificial Intelligence (pp. 618-622). IEEE.

Yang, Y., McLaughlin, K., Sezer, S., Yuan, Y. B., & Huang, W. (2014, July). Stateful intrusion detection for IEC 60870-5-104 SCADA security. In 2014 IEEE PES General Meeting| Conference & Exposition (pp. 1-5). IEEE.

Yang, S. U. (2021, March). Research on Network Malicious Behavior Analysis Based on Deep Learning. In 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (Vol. 5, pp. 2609-2612). IEEE.

Yassin, W., Udzir, N. I., Muda, Z., Abdullah, A., & Abdullah, M. T. (2012, June). A cloud-based intrusion detection service framework. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 213-218). IEEE.

Yassin, W., Udzir, N. I., Muda, Z., & Sulaiman, M. N. (2013). Anomaly-based intrusion detection through k-means clustering and naives bayes classification.

Ye, N., Emran, S. M., Chen, Q., & Vilbert, S. (2002). Multivariate statistical analysis of audit trails for host-based intrusion detection. IEEE Transactions on computers, 51(7), 810-820.

Youssef, A., & Emam, A. (2011). Network intrusion detection using data mining and network behaviour analysis. International journal of computer science & information technology, 3(6), 87.

Yu, S. J., Koh, P., Kwon, H., Kim, D. S., & Kim, H. K. (2016, December). Hurst parameter based anomaly detection for intrusion detection system. In 2016 IEEE International Conference on Computer and Information Technology (CIT) (pp. 234-240). IEEE.