SDN Ağlarda Atakların Tespiti

Ümit AYAZ

13 Aralık 2022

İçindekiler

Şekil Listesi

Tablo Listesi

Özet

Geleneksel ağ mimarisinin operasyonel güçlükler ve değişikliklere anında cevap verememesinden dolayı ortaya çıkan SDN(yazılım tanımlı ağlar) atak yüzeyini bu teknolojiye taşımakta ve bir ağ altyapsını tamamen riske edebilme olasılığını artırmıştır. Bu çalışmada SDN'de gerçekleşebilecek ataklar incelenecektir. Analiz edilen ataklar için tespit mekanizmaları geliştirmek ve bunu derin öğrenme ve makine öğrenmesi teknolojileri ile gerçekleştirmek hedeflenmiştir. Geliştirilen model ile atakların daha önceki çalışmalara göre daha uygulanabilir ve çeviklikte olduğu gösterilecektir. Çalışma sonucunda SDN atak tespitlerinde incelenecek öznitelikler belirlenmiş yeni öznitelikler ortaya atılmış ve atak tespit oranın en yüksek %9999 seviyesine ulaştığı gözlemlenmiştir ve bunu yaparken gerçek zamanlı bir tepi süresi elde edilmiştir.

Not: Bilimsel Araştırma Teknikleri ve Etik Dersi, Makale Denemesi Ödevidir, İçerisinde gerçek bilgilerin yanı sıra doğaçlama yapılmış bilgiler vardır. Referans alınamaz.

Keywords – SDN, IDS, IPS, Cyber Security, Machine Learning, Deep Leraning

1 Giriş

Günümüzde geleneksel ağların bekelenenlere karşılık vermekteki hızı profesyonelleri tatmin etmediği için ortaya atılan yazılım temmelli ağlarda hatanın teknoktada birleşmesi sonucu kurum ve kuruluşları büyük riske atmaktadır. A teknoloji kurumunda SDN [12] üzerinde yapılan çalışmalarda operasyonel süreçlerin kritik açıklıklara sebep olabileceği görüşü doğmuştur. Bu nedenle SDN mimarisinde geleneksel güvenlik anlayışının yanı sıra akıllı sistemlerin devreye alınması gerektiği ihtiyacı ortaya çıktığı belirtilmiştir.

Test ve diğerleri [12] yaptıkları arastırmada akıllı sistemlere geçme ihtiyacını doğrulamışlardır. Önerilen metod yazılım temmelli ağlardaki atakların tespit edildiğini gösteren nihai bir çalışmadır. Makalenin bundan sonraki kısımlarından 2. bölümde geçmiş çalışmalar, 3. bölümde veriseti, yapılan işlemler ve kullanılan teknikler, 4. bölümde önerilen model, 5. bölümde deneyimler ve bunların değerlendirilmesi için karşılaştırmalar 6. bölümde sonuç ve geleceğe dair öneriler bulunmaktadır.

2 İlişkili Çalışmalar

inSDN datasetinin oluşmasına dek araştırmacılar SDN ile ilgili atak tespit sistemlerinde doğrudan olarak oluşturdukları SDN topolojileri üzerinde ya da SDN yapısındaki trafiği tam olarak karşılamayan daha eski datasetlerden faydalanmışlardır[6].

Amaral ve diğerleri(2016)[4] bir uygulama geliştirerek 2 farklı noktadan trafikten veri toplamışlardır. Birincisinde SND networkünden flow bilgileri(12 öznitelik) alınırken 2.sinde klasik network switch üzerinden mirror trafiği almışlardır. Elde edilen veriler Radom Forest, Stochastatic Gradient Boosting ve Extreme Gradiant Boosting sınıflardırma algoritmalarına tabi tutarak Bittorent,Dorpbox,HTTP vb toplam 8 adet uygulama türünü tespit etmeye çalışmışlardır. %96 accuracy ile Random Forest ile HTTP sınıflandırmasını, %71.20 SGB ile en düşük video uygulamasını sınıflandırabilmişlerdir.

Cheng Ye ve diğerleri(2018)[13] DDOS ataklarını tespit etmeye yönelik 1 controller ve 5 host bulunan ağ kurmuşlardır. Bunlardan 2'si atağı gerçekleştiren bot makineler 2'si normal trafik üreten makineler 1'i ise kurban makinedir. Hping3 aracı ile TCP,UDP ve ICMP flood atakları gerçekleştirerek DDOS atağını simule ederek normal ve atack trafiğini ayrıt etmek için SVM sınıflandırma algoritmasını kullanmışlardır. Cheng ve diğerleri %95.24 kesinlik değerine ulaşmışlardır.

Elsayed ve diğerleri(2020)[6] tarafından 2020 yılında inSDN veriseti oluşturularak bilime sunulmuştur. Çalışmada veri setini sanallaştırma ortamında küçük bir topoloji ile oluşturmuş ve atak çeşitliliğini yüksek tutmaya çalışmışlardır. Bu çalışmada veri setini birden fazla algoritmaya tabi tutararak %80 öğrenme oranı ile algoritmaların karşılaştırmalarını yapmışlardır. Paylaştıkları sonuçlardan görüldüğüne göre Adaboost algoritması ile yüksek kesinlik değerlerine ulaşılmış ancak öğrenme süreleri büyüklüğü ile dikkat çekmiştir. Yüksek kesinlik ve düşük öğrenme süreli sonuçlar tek bir algoritmada tüm atak kategorileri için gözlemlenmemiştir.

Abdallah diğerleri(2021)[2] CNN ve LSTM'i birleştirerek atak tespit sistemi geliştirmişlerdir. Bu çalışmada 2 farklı algoritamayı bir arada kullanarak algoritmaların tekil performanslarından daha başarılı sonuçlar alınmıştır. Çalışma sonuçları atak kategorilerini verecek şekilde değil de genel olan Atak ve Normal olarak istatistikler paylaşılmıştır.

Abbas ve diğerleri(2021)[1] inSDN data setini uyarlayarak 6 farklı atak çeşiti ile çalışma yapmışlardır. Daha sonra veriyi ön işleyerek alakasız özellikleri ortadan kaldırmışlar ve atağı tespit etmede en yüksek etkiye sahip özelliği tanımlak için tek değişkenli özellik seçme kullanma çalışmasını gerçekleştirerek çalışmalarını tamamlamışlardır.

ElSayed ve diğerleri(2021)[5] 2021yılında hybrid DL-based mimari model ile farklı öğrenme algoritmalarını deneyerek katmanlı bir mimari ile inSDN data setinde iki farklı öznitelik sayısı ile uygulama çalışması yapmıştır. Böylelikle fazla sayıda öz nitelik indirgenerek aynı kesinlik sonucunu elde etmeye çalışarak daha makul fiyat performans dengesine ulaşmaya çabalamışlardır.

Friha ve diğerleri(2022)[7] 2022 yılında Tarım ve IOT'nin harmanlandığı tedarik zincirinin güvenliğinin sağlanması ile ilgili yaptığı çalışmada FELIDS olarak adlandırdıkları merkezi olmayan ve dağınık Federated Deep Learning'e sahip IDS'i sunmuşlardır. SDN altyapısına ait testleri inSDN datasetini kullanarak başarım oranlarını ölçmüşlerdir.

Janabi ve diğerleri(2022)[8] akış temelli DL-EWPS adlı IDS sistemini öne sürmüşlerdir, bu IDS 3 modülden oluşmaktadır. Bunlardan biricisi akışların istatistiklerini toplar ve 2. modüle iletir, 2 modul gelen istatiskten 11 özelliği seçerek gerekli ayarlamaları yapar ve 3. modüle iletir. 3. modül sayısal özellikleri RGB image'ine çevirerek CNN algoritmasına tabi tutar ve atak olup olmadığına dair karar mekanizması tamamlanmış olur.

Myint ve diğerleri(2019)[9] DDOS ataklarını tespit edebilmek için UDP flood ve TCP SYN flood atakları ile birlikte normal atak trafiği pyhton scapy ile üretmişlerdir ve üretilen datayı flow olarak kaydetmişlerdir. Öz nitelikleri flow daki ortalama paket sayısı, flow büyüklüğü(byte), paket sayısındaki sapmalar vb. değerlerler ortaya koyarak SDNTrafficDS datasetini ortaya koymuşlardır. AVSM (Advanced Support Vector Machine) modeli ile %97'lik bir accuracy değerine ulaşmışlardır.

Ajaeiya ve diğerleri(2017)[3], TCP DOS, HTTP brute force, Network SynScan, Port Scan, ICMP flood, SSH bruteforce ve normal trafiği içerecek şekilde bir test ortamı hazırlamışlardır. Sınıflandırma olarak Bagged Trees'i seçerek bunun diğer sınıflandırma makine algoritmaları olan SVM, Decision Trees, Random Forest ve KNN ile kıyaslamışlardır. Python ile yazdıkları bir uygulama ile 8 adet özniteliği aggregate ederek 9 adet aggregated özniteliği öğrenme ve test'e tabi tutmuşlardır. 6 atak bir normal sınıf üretmelerine rağmen testlerinde TCP DOS, ICMP flood ve PortScan'i DOS altında birleştirerek 4 atak 1 normal sınıflandırma üzerinde multiclass tespitinde RF algoritması 0.964 TPR ile en iyi performansı göstermiştir. Normal ve Attack olarak iki sınıflı testte ise RF 0.983 başarıya ulaştığı bilgilendirilmiştir.

Santos ve diğerleri(2020)[11] SDN networkündeki DDOS atakarlının tespiti için MLP, SVM, Decision Tree ve RandomForest algoritmalarını karşışlatıran çalışma gerçekleştirmişlerdir. Mininet Virtual Network aracı ile 6 host 1 switch ve 1 controller bulunan ortamda, Scapy ile 20000 farklı ip sppof edilerek HTTP,SYN, ICMP ve UDP flood ataklarının yanında normal trafikde üretilmiştir. Hyper paramatre hesaplamaları için Scikit-Learn tarafından uygulanan Gridsearch ve algoritmalar için K-fold tekniği ile %70 roanında eğitilerek RF ve DT algoritamalarında %100 accuracy değerine ulaştığı bildirilmiştir.

Hüseyin ve diğerleri(2020)[10] DDOS atağını tespit edebilmek için SDN neworkünden belli öz nitelikler ile birlikte normal ve atak olarak 2 sınıfta dataset elde etmişlerdir. Dataset hping3 aracı ile oluşturulmuş ve 12 öznitelik 129000 örnek içermektedir. Normal Traffic, ICMP Flood, TCP flood ve UDP flood olarak sınıflandırılmıştır. Oluşturdukları datasetten özellik seçme metodu ile yeni bir dataset oluşturarak iki datasetide SVM, NB, ANN ve KNN classification modellerine tabi tuttuklarında %98.3 accuracy değeri ile KNN ipi göğüslemiştir. Feature Selection olmadan KNN %95.67 accuracy değerine ulaşmıştır, Filter-Based Feature Selection ile %97.15, Filter-Based Feature Selection ile KNN %98.30, Filter-Based Feature Selection ile KNN %98.30 accuracy değerine ulaşmıştır.

inSDN datasetinde geçekleştirilmiş çalışmalar								
Year	Author	Model	Dataset	Features	Accuracy Multic-lass[%]	Accuracy Bi-nary[%]	ROC	Precision Bi-nary[%]
2020	Elsayed, Mahmoud Said	RF	inSDN	48	na	na	na	99,4259
2020	Elsayed, Mahmoud Said	RF	inSDN	All	na	na	na	99,4259
2021	Abdallah, Mahmoud Said	CNN-LTSM	inSDN	48	na	96,32	0.956	na
2021	Abbas, Nadine	SelectKBest method from Scikit-learn	inSDN	14	na	na	na	na
2021	ElSayed, Mahmoud Said	CNN-RF(with DL-based)	inSDN	48	98,92	99,28	0.990	na
2021	ElSayed, Mahmoud Said	CNN-RF(with DL-based)	inSDN	9	97,37	97,42	0.968	na
2022	Friha, Othmane	DNN	inSDN	na	98,54	na	na	na
2022	Janabi, Ahmed H.	CNN	inSDN	6	na	96,43	na	na
2022	Janabi, Ahmed H.	CNN	inSDN	11	na	100	na	na
2022	Janabi, Ahmed H.	CNN	inSDN	All	na	98.94	na	na

Tablodada görüleceği üzere çalışmaların odak noktaları atakarın tespiti olmakla beraber ölçütler farklı noktalarda verilmişdir.

3 Yöntem ve Gereçler

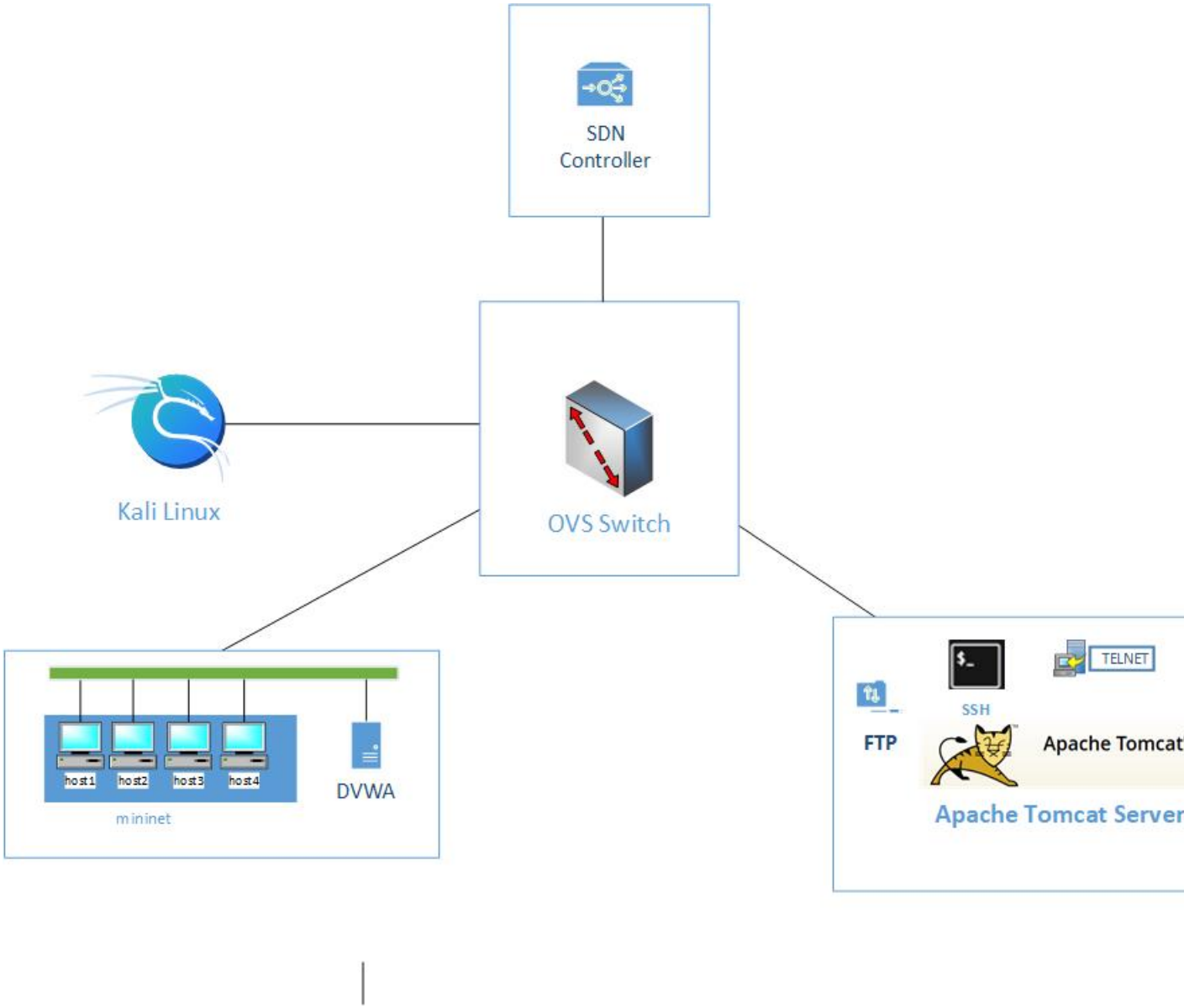
3.1 InSDN dataset

SDN ortamlarında gerçekleşen atakların veya uygulamaların tespit edilebilmesi adına bugüne kadar farklı datasetler farklı bilim adamları tarafından çalışmalarına özel oluşturulmuştur ancak bunların geneli DDOS tespiti veya çok az bir atak veya uygulama çeşiti ile sınırlı kalmıştır[6]. Bunu gidermek adına public olmak üzere birden fazla atak çeşidini barındıran SDN ortamları için IDS hesaplamalarında kullanılması için Elsayed et al. tarafından inSDN veri seti 2020 yılında oluşturulmuştur.

Verisetini oluşturmak için windows 10 üzerinde VMware Workstation ile topoloji oluşturmuşlardır. Bu ortamda 1 adet Kali Linux, 2 adet Ubuntu 16.4 ayağa kaldırılarak Kali Linux attacker'ı Ubuntu serverlardan biri Open Network Operationg Systemi(ONOS=SDN controller) ve diğer Ubuntu Server ise Mininet ve OV switch olarak hizmet etmektedir ve içerisinde docker containers ile DVWA kuruludur. Sonuncu olarak ise yaygın zaafiyetleri içinde barındıran Metasploitable2 server konumlandırılmıştır.

Daha önceki veri setlerinin sınama ortamlarındaki temel fark atak çeşitliliği ve oluşturulan trafiğin gerçekliğidir. Gerçekleştirilen ataklar DOS, DDOS, Web Attacks, Password -Guessing, Botnet, Exploitation, Probe ayrıca atak trafiğininin yanında HTTPS,HTTP,SSH,mail, DNS,FTP,Telnet vb. normal trafikte mevcuttur.

Veri seti 3 temel gruptan oluşmaktadır birincisi normal trafiğin , ikincisi Metasploitable 2 server'a gelen atakların ve 3.cüsü OVS üzerinde gerçekleşen atakların olduğu gruptur. Dataset toplamda 343939 normal ve atak trafiğinden oluşmaktadır. Bunların 68424'ü normal, 275515 atak trafiğidir[6].



Şekil 1: inSDN dataseti için hazırlanmış ağ topolojisi.

inSDN datasetine ait temel veriler					
Data Group Name	Application/Attack Name	Count	Total Count	Rate[%]	PCAP Size[GB]
Normal	Skype, Facebook, File Transfer, Youtube, Email, DNS, Chat, Browsing	68424	68424	19.9	3.58
Metasploitable-2	Ddos Probe DoS Brute Force Attack Exploitation (R2L)	73529 61757 1145 295 17	136743	39.76	0.669
OVS	DoS DdoS Probe Brute Force Attack Web_Attack Botnet	52471 48413 36372 1110 192 164	138722	40.34	1.21
TOTAL	ALL	343889	343889	100	5.459

Kanada Enstitütüsü Cybersecurtiy tarafından geliştirilen CICFlowMeter aracı kullanılarak oluşturulan 80+ özniteliğe sahip inSDN data setinin özellikleri aşağıdaki tabloda gösterilmiştir.

Attributes explanation of of inSDN dataset			
Feature	**Feature Name**	**Description**	**Type**
F1	Flow-id	ID of the flow	C
F2	Src-IP	Source Ipa address	C
F3	Src-Port	Source port number	C
F4	Dst-IP	Destination IP address	C
F5	Dst-Port	Destination port number	C
F6	Protocol-Type	Type of protocol, e.g., tcp, udp, etc.	D
F7	Timestamp	Timestamp	C
		Byte-based attributes	
F8	Fwd-Header-Len	Total bytes used for headers in forward direction	C
F9	Bwd-Header-Len	Total bytes used for headers in backward direction	C
		Packet-based attributes	
F10	Tot-Fwd-Pkts	Total packets in the forward direction	C
F11	Tot-Bwwd-Pkts	Total packets in the backward direction	C
F12	TotLen-Fwd-Pkts	Total size of packets in forward direction	C
F13	TotLen-Bwd-Pkts	Total size of packets in backward direction	C
F14	Fwd-Pkt-Len (Min, Mean, Max, Std)	Min, Mean, Max, and standard deviation of the size of packets in forward direction	C
F15	Bwd-Pkt-Len (Min, Mean, Max, Std)	Min, Mean, Max, and standard deviation of the of packets in backward direction	C
F16	Pkt-Len (Min, Mean, Max, Var, Std)	Min, Mean, Max, Var and standard deviation of the length of a packet	C
F17	Pkt-Size-Avg	Average size of packet	C
		Interarrival Times attributes	
F18	Duration	Duration of the flow in Microsecond	C
F19	Flow-IAT (Min, Mean, Max, Std)	Min, Mean, Max, and standard deviation of the time between two packets sent in the flow	C
F20	Fwd-IAT (Tot, Min, Mean, Max, Std)	Tot, Min, Mean, Max, and standard deviation of the time between two packets sent in the forward direction	C
F21	Bwd-IAT (Tot, Min, Mean, Max, Std)	Tot, Min, Mean, Max, and standard deviation of the time between two packets sent in the backward direction	C
		Flow& Timers attributes	
F22	Active-Time (Min, Mean, Max, Std)	Min, Mean, Max, and standard deviation of the time flow was active before becoming idle	C
F23	Idle (Min, Mean, Max, Std)	Min, Mean, Max, and standard deviation of the time flow was idle before becoming active	C
		Flag-based atributes	
F24	Fwd-PSH-Flags	Number of the times the PSH flag was set in packets travelling in the forward direction	D
F25	Bwd-PSH-Flags	Number of the times the PSH flag was set in packets travelling in the forward direction (0 for UDP)	D
F26	Fwd-URG-Flags	Number of the times the URG flag was set in packets travelling in the forward direction	D
F27	Bwd-URG-Flags	Number of the times the URG flag was set in packets travelling in the forward direction (0 for UDP)	D
F28	FIN-Flag-Cnt	Number of the packets with FIN	D
F29	SYN-Flag-Cnt	Number of the packets with SYN	D
F30	RST-Flag-Cnt	Number of the packets with RST	D
F31	PSH-Flag-Cnt	Number of the packets with PSH	D

F32	ACK-Flag-Cnt	Number of the packets with ACK	D
F33	URG-Flag-Cnt	Number of the packets with URG	D
F34	CWE-Flag-Cnt	Number of the packets with CWE	D
F35	ECE-Flag-Cnt	Number of the packets with ECE	D
Attributes explanation of of inSDN dataset			
Feature	**Feature Name**	**Description**	**Type**
Flow-based attributes			
F36	Down/Up-Ratio	Download and upload ratio	D
F37	Fwd-Seg-Size-Avg	Average size observed in the forward direction	C
F38	Bwd-Seg-Size-Avg	Average number of bytes bulk rate in the forward direction	C
F39	Fwd-Byts/b-Avg	Average number of bytes bulk rate in the forward direction	D
F40	Fwd-Pkts/b-Avg	Average number of packets bulk rate in the forward direction	D
F41	Fwd-Blk-Rate-Avg	Average number of bulk rate in the forward direction	D
F42	Bwd-Byts/b-Avg	Average number of bytes bulk rate in the backward direction	D
F43	Bwd-Pkts/b-Avg	Average number of packets bulk rate in the backward direction	D
F44	Bwd-Blk-Rate-Avg	Average number of bulk rate in the backward direction	D
F45	Init-Fwd-Win-Byts	The total number of bytes sent in initial window in the forward direction	C
F46	Init-Bwd-Win-Byts	The total number of bytes sent in initial window in the backward direction	C
F47	Fwd-Act-Data-Pkts	Count of packets with at least 1 byte of TCP data payload in the forward direction	C
F48	Fwd-Seg-Size-Min	Minimum segment size observed in the forward direction	C
F49	Flow-Byts/s	Number of flow bytes per second	C
F50	Flow-Pkts/s	Number of flow packets per second	C
F51	Fwd-Pkts/s	Number of forward packets per second	C
F52	Bwd-Pkts/s	Number of backward packets per second	C
Subflow-based attributes			
F53	Subflow-Fwd-Pkts	The average number of packets in a sub flow in the forward direction	C
F54	Subflow-Fwd-Byts	The average number of bytes in a sub flow in the forward direction	C
F55	Subflow-Bwd-Pkts	The average number of packets in a sub flow in the backrward direction	C
F56	Subflow-Bwd-Byts	The average number of bytes in a sub flow in the backward direction	C
C-Continuous, **D**-Discrete			

3.2 Ön İşleme

Veri seti toplamda 83 öz nitelik taşımaktadır Bunlardan Subflow-Fwd-Pkts, Subflow-Fwd-Byts, Subflow-Bwd-Pkts öznitelikleri her zaman değişken olacağı ve atak tespitine bir faydası olmayacağı için cıkarılmıştır. Fwd-Seg-Size-Min ve Fwd-Seg-Size-Avg çarpımı alınarak yeni bir öznitelik yeni$_o$znitelikolarakverisetineeklenmi$_s$tir, bunu

3.3 Kullanılan Teknikler

GErçekleştirilen çalışmada inSDN veri setini Machine Learning ve DeepLearning teknolojileri ile işledik. Daha sonra bunların Apache Spark ile entegre ettik. Bu teknolojileri kullanmamızın sebebi[12] yapılan çalışmalarda en iyi sonuçların bu teknolojilerle alınmasıdır.

4 Önerilen Model

Önerdiğimiz sistem inSDN veri setini işleyerek makine öğrenmesi, özelliklerin kaldırılması ve yeni özellikerin eklenmesi bundan sonra derin ogrenmeye tabi tutularak atakların tespitini sağlayan daha önceki modellerde bulunmayan yeni$_o$zellikvemakineogrenmesivederinogrenmekombinedilmi$_s$farkolaraksunulmu$_s$tur.

5 Deney ve Değerlendirmeler

Gerçekleştirilen deneyde Down/Up-Ratio özniteliğinin sonuçlara olumsuz etkisi olduğu gozlemlenmiştir. Deney ortamımızın işlemci ve ram özellikleri düşük kaldığı için sonuçların alınmasında gecikmeler yaşanmıştır. %999 precision değerine ulaşılarak diğer çalışmalardan daha iyi bir sonuca ulaşılmıştır.

5.1 Model Parametreleri

Önerilen modelin sınıftlandırma aşamasında attacklar RF ve CNN kullanılarak derin ogrenme ile gerçekleştirilmiştir. Bu model özellikle SDN ağlarında dengesiz ataklar için yüksek kesinlik değerine ulaşmaktadır.

5.2 Sonuçlar ve Karşılatırmaları

Önerilen modelde tüm özellikler devreye alınarak ve yeni özellikler ortaya atılarak en iyi sonuca ulaşılmıştır.

inSDN datasetinde geçekleştirilmiş çalışmalar								
Year	Author	Model	Dataset	Features	Accuracy Multic-lass[%]	Accuracy Bi-nary[%]	ROC	Precision Bi-nary[%]
2020	Elsayed, Mahmoud Said	RF	inSDN	48	na	na	na	99,4259
2020	Elsayed, Mahmoud Said	RF	inSDN	All	na	na	na	99,4259
2021	Abdallah, Mahmoud Said	CNN-LTSM	inSDN	48	na	96,32	0.956	na
2021	Abbas, Nadine	SelectKBest met-hod from Scikit-learn	inSDN	14	na	na	na	na
2021	ElSayed, Mahmoud Said	CNN-RF(with DL-based)	inSDN	48	98,92	99,28	0.990	na
2021	ElSayed, Mahmoud Said	CNN-RF(with DL-based)	inSDN	9	97,37	97,42	0.968	na
2022	Friha, Oth-mane	DNN	inSDN	na	98,54	na	na	na
2022	Janabi, Ah-med H.	CNN	inSDN	6	na	96,43	na	na
2022	Janabi, Ah-med H.	CNN	inSDN	11	na	100	na	na
2022	Janabi, Ah-med H.	CNN	inSDN	All	na	98.94	na	na
2022	ayaz	RF-CNN-extracted feature	inSDN	All+1	99.9	99.99	99.9	99.9

6 Sonuç ve Müstakbel Çalışmalar

Bu çalışmada SDN alt yapısında gerçekleşen atakları tespit etmek için özellik çıkartma işlemi ile birlikte RF-CNN makine ogrenmeleri ve derin ogrenme metotları kullanan yöntem kullanıldı. Gerçekleştirilen çalışmada %99.99 kesinlik değerine ulaşılarak en başarılı sonuç elde edildi.
Geliştirilen model exploit veritabanları ile entegre edilerek canlı veri üzerinde yeni çözümler elde edilebilir.

Kaynaklar

[1] Nadine Abbas, Youssef Nasser, Maryam Shehab, and Sanaa Sharafeddine. Attack-specific feature selection for anomaly detection in software-defined networks. pages 142–146. Institute of Electrical and Electronics Engineers Inc., 2021.

[2] Mahmoud Abdallah, Nhien An Le Khac, Hamed Jahromi, and Anca Delia Jurcut. A hybrid cnn-lstm based approach for anomaly detection systems in sdns. Association for Computing Machinery, 8 2021.

[3] Georgi A. Ajaeiya, Nareg Adalian, Imad H. Elhajj, Ayman Kayssi, and Ali Chehab. *Flow-Based Intrusion Detection System for SDN*. Institute of Electrical and Electronics Engineers Inc., 7 2017.

[4] Pedro Amaral, Joao Dinis, Paulo Pinto, Luis Bernardo, Joao Tavares, and Henrique S. Mamede. Machine learning in software defined networks: Data collection and traffic classification. volume 2016-December, pages 91–95. IEEE Computer Society, 12 2016.

[5] Mahmoud Said ElSayed, Nhien An Le-Khac, Marwan Ali Albahar, and Anca Jurcut. A novel hybrid model for intrusion detection systems in sdns based on cnn and a new regularization technique. *Journal of Network and Computer Applications*, 191, 10 2021.

[6] Mahmoud Said Elsayed, Nhien An Le-Khac, and Anca D. Jurcut. Insdn: A novel sdn intrusion dataset. *IEEE Access*, 8:165263–165284, 2020.

[7] Othmane Friha, Mohamed Amine Ferrag, Lei Shu, Leandros Maglaras, Kim Kwang Raymond Choo, and Mehdi Nafaa. Felids: Federated learning-based intrusion detection system for agricultural internet of things. *Journal of Parallel and Distributed Computing*, 165:17–31, 7 2022.

[8] Ahmed H. Janabi, Triantafyllos Kanakis, and Mark Johnson. Convolutional neural network based algorithm for early warning proactive system security in software defined networks. *IEEE Access*, 10:14301–14310, 2022.

[9] Myo Myint Oo, Sinchai Kamolphiwong, Thossaporn Kamolphiwong, and Sangsuree Vasupongayya. Advanced support vector machine-(asvm-) based detection for distributed denial of service (ddos) attack on software defined networking (sdn). *Journal of Computer Networks and Communications*, 2019, 2019.

[10] Huseyin Polat, Onur Polat, and Aydin Cetin. Detecting ddos attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability (Switzerland)*, 12, 2 2020.

[11] Reneilson Santos, Danilo Souza, Walter Santo, Admilson Ribeiro, and Edward Moreno. Machine learning algorithms to detect ddos attacks in sdn. volume 32. John Wiley and Sons Ltd, 8 2020.

[12] test. test. *http://test*, 1, 1 2017.

[13] Jin Ye, Xiangyang Cheng, Jian Zhu, Luting Feng, and Ling Song. A ddos attack detection method based on svm in software defined network. *Security and Communication Networks*, 2018, 4 2018.