Yazılım-Tanımlı Ağların Güvenliğinde Yapay Zekâ Tabanlı Çözümler: Ön İnceleme

Muhammet Fatih Akbaş
Bilgi İşlem Daire Başkanlığı
İzmir Kâtip Çelebi Üniversitesi
İzmir, Türkiye
mfatih.akbas@ikc.edu.tr

Enis Karaarslan
Bilgisayar Mühendisliği Bölümü
Muğla Sıtkı Koçman Üniversitesi
Muğla, Türkiye
enis.karaarslan@mu.edu.tr

Cengiz Güngör
Uluslararası Bilgisayar Enstitüsü
Ege Üniversitesi
İzmir, Türkiye
cengiz.gungor@ege.edu.tr

***Özet*—Büyük ve karmaşık ağların etkin bir şekilde yönetilmesini sağlayan Yazılım-Tanımlı Ağ (Software-Defined Networks, SDN) mimarisi, kontrol düzlemini veri düzleminden ayırarak merkezi bir denetleyici üzerinden ağın doğrudan programlanabilmesini sağlamaktadır. SDN, dinamik ve esnek bir ağ mimarisi sunmaktadır. Bu yeni nesil ağ yaklaşımının geleneksel bilgisayar ağlarının yerini alması beklenmektedir. SDN mimarisinin sahip olduğu ağ yönetimi avantajlarına karşın bazı yeni saldırı vektörleri ortaya çıkmakta ve ağ güvenliği konseptinin yeniden gözden geçirilmesi gerekmektedir. SDN mimarisindeki güvenlik problemlerinin yapay zekâ (Artificial Intelligence, AI) tabanlı çözümlere ihtiyaç duyduğunu düşünmekteyiz. Bu çalışma kapsamında, AI-tabanlı ağ yaklaşımına değinilmekte, literatürdeki AI-tabanlı SDN güvenliği çözümlerine yer verilmekte ve SDN güvenliğinde AI-tabanlı ağ yaklaşımının önemi vurgulanmaktadır.**

***Anahtar Kelimeler*—Yazılım-Tanımlı Ağlar, SDN, SDN Güvenliği, Yapay Zekâ, Zeki Sistemler, AI-Tabanlı Ağlar, AI-Tabanlı SDN Güvenliği, Bilişsel Ağlar**

***Abstract*—Software-Defined Networks (SDN) architecture provides effective management of large and complex networks by separating the control plane from the data plane. SDN enables directly programming the network by the central controller. SDN provides dynamic and flexible network architecture. SDN is a new generation networking approach which is expected to take place of the traditional computer networks. SDN has benefits from the network management perspective, but also brings new attack vectors. We believe that the network security problems in SDN architecture need artificial intelligence (AI) based solutions. In this work, AI-based networking approach is mentioned, specific AI-based SDN security solutions in the literature are given and the importance of AI-based networking approach in SDN security is emphasized.**

***Index Terms*—Software-Defined Networks, SDN, SDN Security, Artificial Intelligence, Intelligent Systems, AI-Based Networking, AI-Based SDN Security, Cognitive Networks**

I. GİRİŞ

Bilgisayar ağlarında birçok ağ cihazı bulunmaktadır. Bu cihazlar üzerinde karmaşık ve birbirinden farklı protokoller çalışmaktadır. Özellikle, nesnelerin interneti (Internet of Things, IoT) kavramı ile birlikte internete bağlı cihaz sayısı her geçen gün artmaktadır. IoT, günlük yaşamda kullandığımız nesnelerin diğer nesnelerle etkileşim içinde olabildiği bir ortam sunmaktadır. Ağ teknolojisi desteğini barındıran bilgisayarlar, tabletler, akıllı telefonlar, buzdolapları, arabalar vb. tüm cihazlar sürekli olarak veri üretmekte ve bu veriler her geçen gün büyümektedir. Bunun sonucunda, geleneksel yöntemlerle saklanamayan, yönetilemeyen ve işlenemeyen yüksek hacimli, karmaşık ve düzensiz verileri ifade eden büyük veri kavramı karşımıza çıkmaktadır. Giderek daha değerli bir hale gelen büyük verinin işlenmesi ve buradan anlamlı sonuçların çıkartılması gerekmektedir. Büyük verinin işlenebilmesi için daha fazla bant genişliğine gereksinim duyulmaktadır.

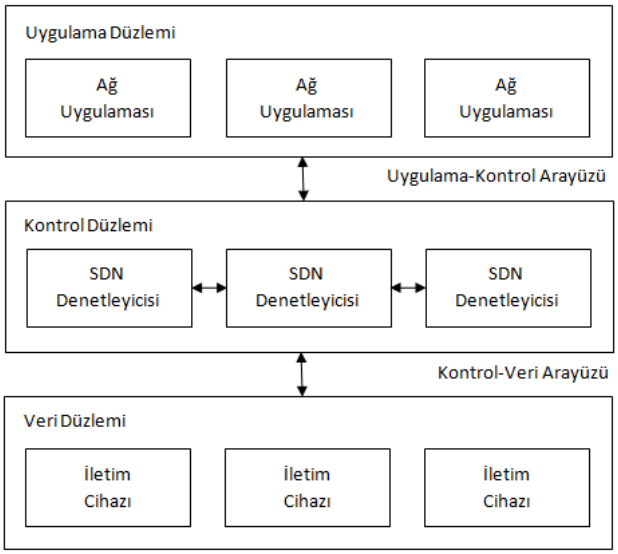
Bu gelişmeler, ağları daha karmaşık ve heterojen bir hale getirmekte ve ağın yönetimini zorlaştırmaktadır. Geleneksel ağ yönetimi yaklaşımı büyük ölçekli bilgisayar ağlarının yönetiminde yetersiz kalmaktadır. Daha iyi bir ağ yönetimi yaklaşımına ve yeni yöntemlerin geliştirilmesine gereksinim duyulmaktadır. Bu yüzden, yönetimsel açıdan kolaylık sunan, dinamik ve esnek bir mimariye sahip yazılım-tanımlı ağlar (Software-Defined Networks, SDN) kavramı ortaya çıkmıştır.

Yeni ağ yönetimlerinin de başarımı için yapay zekâ (Artificial Intelligence, AI) kavramının kullanımı tartışılmaya başlanmıştır. İnsana özgü yeteneklerin ağ yönetimine kazandırılması amaçlanmaktadır. AI tekniklerinin kullanılması ile geliştirilen uygulamalar geçmiş verilerden öğrenerek gelecek olaylarla ilgili karar verebilme ve eksik veri ile problem çözebilme yeteneklerine sahip olmaktadır. Böylece, sistemlerin daha akıllı ve faydalı hale getirilmesi hedeflenmektedir.

II. TEMEL KAVRAMLAR

A. Yazılım-Tanımlı Ağlar (SDN)

SDN, merkezi bir ağ yönetimi ve ağ üzerinde global bir bakış açısı sunarak büyük ve karmaşık ağların etkin bir şekilde yönetilebilmesini sağlamaktadır. Geleneksel bilgisayar ağlarının yerini alması beklenen SDN yeni nesil bir ağ yönetimi yaklaşımı getirmektedir.



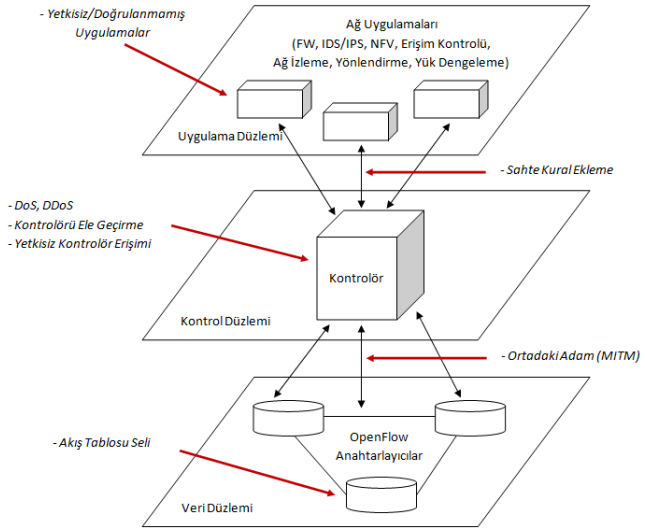
Şekil 1. Yazılım-Tanımlı Ağ (SDN) Mimarisi [1]

SDN mimarisi, Şekil 1'de [1] gösterilmektedir. SDN mimarisinde, uygulama, kontrol ve veri olmak üzere üç düzlem bulunmaktadır. Kontrol düzlemi, ağ paketlerinin nereye yönlendirileceğine dair kararın verildiği yerdir. Veri düzlemi ise ağ trafiğinin hedefe iletiminin yapıldığı yerdir. Günümüzde kullanılan yönlendirici ve anahtarlayıcı cihazlarda kontrol düzlemi ve veri düzlemi aynı donanım üzerinde bütünleşik olarak bulunmaktadır. SDN, kavram olarak bu düzlemlerin birbirinden ayrılması düşüncesine dayanmaktadır. Kontrol düzlemi diğer bir deyişle ağın zekâsı, yüksek performanslı bir sunucuya taşınmakta ve ağın yönetimi merkezi bir denetleyici yazılımı üzerinden gerçekleştirilmektedir. Veri düzlemi ise OpenFlow [2] protokolü destekli yönlendirici veya anahtarlayıcı üzerinde bırakılmakta ve sadece paketlerin iletiminden sorumlu olmaktadır.

SDN mimarisi, ağın doğrudan programlanabilmesini ve ağ servislerinin ve uygulamalarının altyapı katmanından yani veri düzleminden soyutlanabilmesini sağlamaktadır. Böylece, geleneksel ağ altyapılarına göre daha dinamik, esnek, ölçeklenebilir bir platform sunmakta ve yönetimsel açıdan kolaylık sağlamaktadır.

B. SDN Güvenliği

SDN mimarisi, ağın programlanabilirliği ve merkezi kontrol avantajlarına sahiptir fakat bu avantajlar beraberinde yeni tehdit vektörlerinin ortaya çıkmasına ve saldırı yüzeyinin artmasına neden olmaktadır. Bu düzlemleri ve arayüzleri hedef alan çeşitli güvenlik tehditleri bulunmaktadır. SDN'deki güvenlik tehditleri ve saldırı yüzeyleri, Şekil 2'de [1] gösterilmektedir.



Şekil 2. SDN Güvenlik Tehditleri & Saldırı Yüzeyleri [1]

SDN'deki güvenlik tehditlerini ve saldırılarını, bir önceki çalışmamızda [1] incelemiş ve SDN güvenliği üzerine de bir literatür çalışması sunmuştuk. Geleneksel ağ mimarilerinde, servis reddi (Denial of Service, DoS), yetkisiz erişim, veri sızıntısı, veri modifikasyonu ve zararlı uygulamalar gibi güvenlik tehditleri bulunmaktadır. Bu tehdit vektörlerine ek olarak, denetleyici yazılımını, kontrol düzlemi ile veri düzlemi arasındaki iletişimi ve kontrol düzlemi ile uygulama düzlemi arasındaki iletişimi hedef alan saldırılar olmak üzere SDN'e özgü olan üç tehdit vektörü ortaya çıkmaktadır [3].

C. Akıllı Şehirler ve Yapay Zekâ (AI)

AI kavramı, teoriden çıkıp kendine her geçen gün daha fazla uygulama alanı bulmakta ve günlük yaşamın bir parçası haline gelmektedir. Günümüzde, akıllı cihazlar, akıllı şehirler ve akıllı yönetimler gibi akıllı konseptler daha fazla ön plana çıkmaya başlamıştır. Gündelik yaşamda yapılan işlerin kolaylaştırılarak daha fazla konfor, güvenlik ve enerji tasarrufu sağlanması amaçlanmaktadır. Bulunulan çevredeki trafik yoğunluğunun, otoparkların doluluk oranlarının öğrenilebilmesi birer akıllı şehir uygulamasıdır. Yine aynı şekilde bir evde bulunan sıcaklık, aydınlatma, perde kontrolü ve güvenlik sistemleri bir evin akıllı olmasını sağlayan unsurlardır. Bir sistemin zeki olarak adlandırılabilmesi için öğrenme, algılama, tanıma, karar verme, problem çözme gibi yeteneklere sahip olması gerekmektedir.

AI, insan zekâsının taklit edilmesini hedefleyen disiplinlerarası bir çalışma alanıdır. Algılama, öğrenme, çıkarsama, akıl yürütme, karar verme ve problem çözme gibi insana özgü yeteneklerin bilgisayar sistemlerine kazandırılması amaçlanmaktadır. Geliştirilen sistemlerin veya uygulamaların daha etkin olması için zekâ unsurunu barındırması gerekmektedir.

Öğrenme yolu ile geleceğe dair öngörülerde bulunmayı geleneksel programlama ile gerçekleştirmek oldukça zordur. Bu amaçla kullanılabilecek olan AI-tabanlı programlamanın geleneksel programlamadan ayrılan yönleri bulunmaktadır. AI-tabanlı programlama, sezgisel ve esnek bir yapıya sahiptir. Geleneksel programlama ise nümerik ve algoritmik olup esnek değildir. AI-tabanlı programlamanın, geçmiş verilerden öğrenme ve eksik veri ile problem çözebilme gibi artıları vardır.

Zeki sistemlerin geliştirilebilmesi için birden fazla AI tekniğinin bir arada kullanılması gerekmektedir. Makine öğrenmesi, matematiksel ve istatistiksel yöntemlerle birlikte eldeki verileri kullanarak bilinmeyene dair çıkarımlarda bulunan bilgisayar algoritmalarıdır. Sınıflandırma ve kümeleme problemlerinin çözümünde kullanılan etkili bir yöntemdir. Öğrenme süreci için veri kümeleri kullanılmakta olup doğru özelliklerin seçilmesi en önemli adımlardan biridir. Özellikle, büyük verinin işlenmesi için makine öğrenmesi tekniklerinin kullanımı ön plana çıkmakta olup bu tekniklerin tekrar gözden geçirilmesi gerekmektedir [4]. Yapay sinir ağları, genetik algoritmalar ve bulanık mantık gibi çeşitli makine öğrenmesi teknikleri bulunmaktadır. Her bir teknik de kendi içinde birçok alt tekniğe sahiptir.

III. AI-TABANLI AĞLAR

Karmaşık ve heterojen ağların daha etkin bir şekilde yönetiminde AI tekniklerinin kullanımı giderek daha fazla ilgi uyandırmaktadır. Ağın yönetimi ve optimizasyonu için makine öğrenmesi, optimizasyon teorisi, oyun teorisi, kontrol teorisi teknikleri ve üst-sezgisel algoritmalar kullanılmaktadır. Bu yöntemler, bulut bilişim, ağ işlevleri sanallaştırma (Network Functions Virtualization, NFV) ve SDN gibi ağ yönetimini basitleştirmeyi vaat eden yeni nesil ağ yaklaşımlarının ve zeki servislerin verilebilmesini sağlayacak geleceğin 5G mobil ağlarının da ilgisini çekmektedir [5]. AI tekniklerinin bu yeni nesil ağ yaklaşımlarına başarılı bir şekilde entegre edilmesi; güvenlik, yönlendirme, bant genişliği yönetimi gibi birçok konuda akıllı davranışlar sergileyen bilişsel ağların (Cognitive Networks, CN) geliştirilebilmesinde önemli rol oynayacaktır. AI-tabanlı ağlar üzerine şu ana kadar yapılan çalışmalar ağırlıklı olarak IoT, CN, 4G ve 5G ağlar, heterojen ağlar (HetNets), araç ad-hoc ağlar (VANETs) üzerine yoğunlaşmaktadır.

Mobil ağların giderek büyümesi, ağın yönetimi ve optimizasyonu gibi konularda problemleri de beraberinde getirmektedir. HetNets'i daha etkin ve akıllı bir hale getirmek için makine öğrenmesi, genetik algoritmalar, yapay sinir ağları, bulanık mantık, karınca kolonisi optimizasyonu, bayes teoremi ve markov modeli tekniklerinin entegrasyon yöntemleri güncel bir çalışmada [6] ele alınmıştır. Bu çalışmada AI teknikleri detaylı olarak sınıflandırılmış ve bu tekniklerin HetNets'de öz-düzenleyici ağların (Self-Organizing Networks, SON) [7] oluşturulabilmesinde önemli fırsatlar sunduğu belirtilmiştir. Öz-yapılandırma (self-configuration), öz-iyileştirme (self-healing) ve öz-optimizasyon (self-optimization) gibi SON'a ait özellikler de bu kapsamda açıklanmakta olup HetNets'de geliştirilen SON'un geleceğin akıllı mobil ağlarının ortaya çıkmasında önemli rol oynayacağı vurgulanmaktadır.

5G HetNets'in dinamik ve etkin bir şekilde yönetilebilmesi için SDN tabanlı akıllı bir sistem tasarımı bir başka çalışmada [8] önerilmektedir. Sistemde, kaynakların optimizasyonu görevini denetleyici üstlenmektedir. Trafik davranışı tahmini, kullanıcı yoğunluğu tahmini, yük dengeleme ve radyo kaynak tahsisi gibi 5G HetNets'deki önemli problemler saptanmış ve bu problemlerin çözümü için akıllı tasarımlar geliştirilmiştir.

Telekomünikasyon ağlarının yönetimi ve optimizasyonu için öğrenmeye dayalı ağlara gereksinim duyulmaktadır. İleri makine öğrenmesi tekniklerinin kullanıldığı bir çalışmada [9], öğrenmeye ve dağıtık zekâya dayalı bir yaklaşım önerilmektedir. Bilişsel-tabanlı ağlar (COgnition-BAsed NETworkS, COBANETS) adını verdikleri bu yaklaşımda öğrenme, modelleme, optimizasyon ve verinin temsili için danışmansız derin öğrenme (Deep Learning, DL) tekniği ve olasılıksal modeller kullanılmaktadır. Bu öğrenme tekniklerinin, NFV ile birlikte kullanılmasının sistem seviyesinde otomatik optimizasyona ve yeniden yapılandırmaya olanak sağlayacağı belirtilmektedir. Ayrıca, önerilen yaklaşım güvenlik perspektifinden de gözden geçirilmektedir. Buna göre, istatistiksel yöntemlerin ve veri madenciliği gibi ileri makine öğrenmesi tekniklerinin kullanıldığı sistemlerde çok fazla veri sürekli olarak öğrenme sürecinden geçirilmektedir. Bu yüzden, kişisel verilerin gizliliği geleneksel ağ altyapılarına göre daha fazla önem arz etmektedir. Gizliliği hedef alan saldırılara karşı anonimleştirme tekniklerinin kullanımının, verinin kime ait olduğunun anlaşılabilmesinin önüne geçilmesini sağlayacağı ifade edilmektedir.

IV. AI-TABANLI SDN GÜVENLİĞİ ÇÖZÜMLERİ

Bilgisayar ve ağ sistemlerindeki zararlı yazılımların tespiti her geçen gün zorlaşmakta ve gelişmiş kalıcı tehditlere (Advanced Persistent Threat, APT) [10] karşı imza tabanlı anti-virüs, saldırı tespit/önleme sistemlerindeki (IDS/IPS) güvenlik yaklaşımları yetersiz kalmaktadır. Güvenlik sistemlerinde AI tabanlı çözümlerin etkinleştirilmesine dair çeşitli çalışmalar bulunmaktadır.

SDN güvenliği ile ilgili literatürdeki çalışmalar daha çok saldırı ve anomali tespitine yöneliktir. Günümüzde ağ güvenliğini en fazla tehdit eden unsurların başında dağıtık servis reddi (Distributed Denial of Service, DDoS) saldırıları gelmektedir. Normal trafik ile sahte trafiği birbirinden ayırt etmek kolay değildir. Çok fazla sayıda paketin analiz edilmesi gerekmektedir. Ayrıca, sahte trafiğin başarılı bir şekilde tespit edilebilme oranı ve tepki süresi önem arz etmektedir. Ağın yönetiminin merkezi bir denetleyici üzerinden yapılması SDN'in artılarından biridir. Fakat denetleyicinin hedef alındığı DDoS saldırıları tek bir nokta üzerinden tüm ağın çökmesi (Single Point of Failure, SPOF) durumuna sebep olabilir.

Güncel bir çalışmada [11], SDN altyapısında sızma girişimlerine ve DDoS saldırılarına karşı koruma sağlamak amacıyla makine öğrenmesi teknikleri analiz edilmektedir. Bir başka çalışmada [12], NOX [13] denetleyicisinden ve OpenFlow destekli anahtarlayıcılarından oluşan bir ağda, DDoS saldırılarının tespiti için bir yöntem önerilmektedir. Bu yöntemde, genellikle sınıflandırma problemlerinin çözümünde tercih edilen ve danışmansız öğrenme türünde bir yapay sinir ağı olan öz düzenleyici haritalar (Self-Organizing Maps, SOM) [14] kullanılmaktadır. OpenFlow destekli anahtarlayıcılarda tüm aktif akışlara ait istatistiklerle birlikte akış tabloları tutulmaktadır. Ağdaki anahtarlayıcılar NOX denetleyicisi üzerinden belli aralıklarla izlenmektedir. Bu süre zarfında tüm anahtarlayıcılardan trafik akışları toplanmakta ve akışlara ait özellikler çıkarsanmaktadır. Akış başına ortalama paket sayısı, byte değeri, süre vb. trafik akışına ait özellikler kullanılarak eğitilen SOM ile ilgili trafik normal ve anormal şeklinde sınıflandırılmaktadır. Akış toplayıcı (flow collector), özellik çıkarsayıcı (feature extractor) ve sınıflandırıcı (classifier) olmak üzere üç modülden oluşan bu yöntem NOX denetleyicisi ile yan yana çalışmaktadır. Bu yaklaşım, geleneksel yaklaşımlara kıyasla bazı katkılar sunmaktadır. Trafik akışına ait özelliklerin çıkarsanması, KDD-99 veri kümesinin kullanıldığı yöntemlere göre çok daha düşük oranda bir yük (overhead) getirmektedir. Tespit mekanizması yeni saldırılara karşı güncellenebilmekte ve kullanılan sınıflandırma tekniği gerektiğinde değiştirilebilmektedir. Tespit döngüsüne OpenFlow destekli yeni anahtarlayıcıların eklenebilmesine veya çıkarılabilmesine olanak sağlamaktadır. Ağ topolojisi değiştiğinde tespit döngüsü de buna göre uyarlanabilmektedir. Ayrıca, DDoS saldırılarının tespitinde yüksek oranda bir başarı sağladığı ve düşük oranda yanlış pozitif (false positive, FP) değerlerine sahip olduğu belirtilmektedir.

SDN'de anomali tespitine yönelik bir başka çalışmada [15] ise denetleyici üzerine konumlandırılmış veri toplayıcı (data collector), özellik seçimi (feature selection) ve sınıflandırma (classification) modüllerinden oluşan bir sistem önerilmektedir. Öncelikle, ağdaki veriler toplanmakta, sonrasında önemli özellikler seçilmekte ve son olarak trafik normal veya anomali şeklinde sınıflandırılmaktadır. Özellik seçimi, anomalinin doğru bir şekilde tespit edilebilmesinde önemli bir rol oynamaktadır. En uygun özelliklerin seçilebilmesi sınıflandırma algoritmasının performansını arttırmaktadır. Bunun için de bazı optimizasyon teknikleri bulunmaktadır. Bu çalışmada, özellik seçimi için optimizasyon amaçlı üst-sezgisel bir algoritma türü olan ikili yarasa algoritması (Binary Bat Algorithm, BBA) [16] ve sınıflandırma için entropi yöntemi kullanılmaktadır. NSL-KDD [17] veri kümesinde normal trafiğe ve dört farklı saldırı çeşidine ait paketler bulunmaktadır. Özellik seçimi için NSL-KDD veri kümesi BBA algoritmasına girdi olarak verilmiştir. Çıktı olarak istenmeyen özellikler elimine edilmiş ve geriye kalan özellikler sınıflandırma modülüne girdi olarak verilmiştir. DoS, tarama (probe), uzaktan yerel alan ağına oturum açma (Remote to Local, R2L) ve kullanıcı hesabını tam yetkili yönetici hesabına yükseltme (User to Root, U2R) saldırılarının her biri için farklı özellikler seçilmiştir. Sınıflandırma işlemi için J48 [18] karar ağacı (decision tree) algoritması kullanılmıştır. Çalışmada, saldırıların tespit oranı ve FP oranı ölçülerek sınıflandırmanın başarısı değerlendirilmektedir. Saldırı tespit oranında en iyi sonucu U2R, FP oranında ise DoS vermiştir.

Dotcenko ve arkadaşlarının çalışmasında [19], SDN'de esnek hesaplamaya (soft computing) dayalı bilgi güvenliği yönetim sistemi algoritması ve bulanık mantık-tabanlı IDS sunulmaktadır. IDS, istatistik toplama, işleme ve karar verme modüllerinden oluşmaktadır. Karar verme sürecinde kullanılan bulanık kuralların daha iyi sonuçlar verdiği, kod satır sayısını %20-30 arasında azalttığı ve hesaplama gereksinimlerini düşürdüğü belirtilmektedir.

V. SONUÇ VE GELECEK ÇALIŞMA

Akıllı cihazlar, akıllı şehirler ve akıllı yönetimler gibi konseptlerin daha fazla ön plana çıktığı günümüzde birçok alanda olduğu gibi SDN yönetimi, güvenliği ve optimizasyonu gibi konularda da daha dinamik, etkin ve akıllı çözümler sunacak AI-tabanlı yaklaşımlara gereksinim duyulmaktadır. SDN'deki büyük verinin de makine öğrenmesi gibi AI teknikleri kullanılarak işlenmesi, bilgiye ve öğrenmeye dayalı, akıllı davranışlar sergileyen CN'lerin geliştirilebilmesine olanak sağlayacaktır. CN ile geçmiş verilerden öğrenerek gelecekte karşılaşılan olaylarla ilgili kendi kendine karar verebilen ağların geliştirilmesi mümkün hale gelebilecektir. Böylece daha akıllı bir ağ mimarisi ortaya çıkacak ve bu sayede kullanıcılara özel servisler verilebilecektir. AI teknikleri ile SDN, 4G/5G ağların, HetNets'in ve mobil ağların entegrasyonunun sağlanmasına yönelik çalışmalar CN'lerin oluşturulmasında önemli bir rol oynayacaktır.

SDN güvenliğinde AI-tabanlı çalışmalar daha çok saldırı ve anomali tespitine yöneliktir. İleri makine öğrenmesi teknikleri ile SDN'in entegrasyonu sağlanarak daha etkin bir ağ koruması gerçekleştirilebilir. SDN'deki trafik akışları, ileri makine öğrenmesi teknikleri ile sınıflandırılabilir ve anomaliler tespit edilebilir. Bu alanda şu ana kadar yapılan çalışmalar çok az sayıda olup henüz yeterli seviyede değildir. Bu yüzden, SDN güvenliğinde AI tekniklerinin kullanımı üzerine çok daha fazla çaba harcanarak çalışma yapılması gerektiğini düşünmekteyiz.

REFERANSLAR

[1] M. F. Akbaş, E. Karaarslan and C. Güngör. "A Preliminary Survey on the Security of Software-Defined Networks". 3rd International Conference on Advanced Technology & Sciences (ICAT'16), 2016.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner. "OpenFlow: Enabling Innovation in Campus Networks". ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, 2008.

[3] D. Kreutz, F. M. V. Ramos and P. Verissimo. “Towards Secure and Dependable Software-Defined Networks”. Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, pp. 55-60, 2013.

[4] J. Qiu, Q. Wu, G. Ding, Y. Xu, S. Feng. “A Survey of Machine Learning for Big Data Processing”. EURASIP Journal on Advances in Signal Processing, 2016.

[5] J. Kadir, K. A. Yau, M. A. Imran, Q. Ni and A. V. Vasilakos. “Artificial Intelligence Enabled Networking”. IEEE Access Special Section Editorial, vol. 3, pp. 3079-3082, 2015.

[6] X. Wang, X. Li and V. C. M. Leung. “Artificial Intelligence Based Techniques for Emerging Heterogeneous Networks: State of the Arts, Opportunities and Challenges”. IEEE Access Special Section on Artificial Intelligence Enabled Networking, vol. 3, pp. 1379-1391, 2015.

[7] Z. Zhang, W. Huangfu, K. Long, X. Zhang, X. Liu and B. Zhong. “On the Designing Principles and Optimization Approaches of Bio-Inspired Self-Organized Network: A Survey”. Science China Information Science, vol. 56, no. 7, pp. 1-28, 2013.

[8] S. Sun, L. Gong, B. Rong and K. Lu. “An Intelligent SDN Framework for 5G Heterogeneous Networks”. IEEE Communications Magazine, vol. 53, no. 11, pp. 142-147, 2015.

[9] M. Zorzi, A. Zanella, A. Testolin, M. De Filippo De Grazia and M. Zorzi. “Cognition-Based Networks: A New Perspective on Network Optimization Using Learning and Distributed Intelligence”. IEEE Access Special Section on Artificial Intelligence Enabled Networking, vol. 3, pp. 1512-1530, 2015.

[10] C. Tankard, Q. Wu, G. Ding, Y. Xu and S. Feng. “Advanced Persistent Threats and How to Monitor and Deter Them”. Network Security, vol. 2011, no. 8, pp. 16-19, 2011.

[11] J. Ashraf and S. Latif. “Handling Intrusion and DDoS Attacks in Software Defined Networks Using Machine Learning Techniques”. IEEE National Software Engineering Conference (NSEC 2014), pp. 55-60, 2014.

[12] R. Braga, E. Mota and A. Passito. “Lightweight DDoS Flooding Attack Detection using NOX/OpenFlow”. 35th IEEE Conference on Local Computer Networks (LCN 2010), pp. 408-415, 2010.

[13] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown and S. Shenker. “NOX: Towards an Operating System for Networks”. ACM SIGCOMM Computer Communication Review, vol. 38, no. 3, pp. 105-110, 2008.

[14] T. Kohonen. “The Self-Organizing Map”. IEEE, vol. 78, no. 9, pp. 1464-1480, 1990.

[15] R. Sathya and R. Thangarajan. “Efficient Anomaly Detection and Mitigation in Software Defined Networking Enviroment”. IEEE Second International Conference on Electronics and Communication Systems (ICECS 2015), pp. 479-484, 2015.

[16] S. Mirjalili, S. M. Mirjalili and X. S. Yang. “Binary Bat Algorithm”. Neural Computing and Applications, vol. 25, no. 3, pp. 663-681, 2014.

[17] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani. “A Detailed Analysis of the KDD CUP 99 Data Set”. IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA 2009), pp. 1-6, 2009.

[18] N. Bhargava, G. Sharma, R. Bhargava and M. Mathuria. “Decision Tree Analysis on J48 Algorithm for Data Mining”. International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 6, pp. 1114-1119, 2013.

[19] S. Dotcenko, A. Vladyko and I. Letenko. “A Fuzzy Logic-Based Information Security Management for Software-Defined Networks”. 16th International Conference on Advanced Communication Technology (ICACT 2014), pp. 167-171, 2014.