ИНФОРМАТИКА

ӘОЖ004.8
МҒТАР 28.23
https://doi.org/10.47526/2024-1/2524-0080.07

A.N. AMANOV[1], D.Ş. İSAKOV[2]
[1]*PhD, Hoca Ahmet Yesevi Türk-Kazak Üniversitesi, (Kazakistan, Türkistan), e-mail: anuarbek.amanov@ayu.edu.kz*
[2]*Yüksek Lisans Öğrencisi, Hoca Ahmet Yesevi Türk-Kazak Üniversitesi (Kazakistan, Türkistan), e-mail: davron.issakov02@gmail.com*

SDN TABANLI ARAÇSAL TASARSIZ AĞLARDA DDOS SALDIRI TESPİTİ

Özet. Günümüz şehir içi kavşak yapılarının fiziksel özellikleri ve plansız yol kesişmelerinden dolayı oluşan trafik akımları, zaman/nakit kaybı, stres, daha fazla yakıt tüketimi gibi birçok olumsuz etkiye sebep olmaktadır. Bu nedenle hem akademik hem de ticari çevrelerde bir akıllı şehir uygulaması olan trafik yönetim sistemleri üzerine birçok çalışmalar yapılmaktadır. Son yıllarda yapılan bu çalışmalarda araçların birbirleri arasında veya saha kenarındaki cihazlar ile haberleşmelerini kolayca sağlayarak ilgili trafik verilerinin merkeze taşınmasını sağlayan VANET (Araçsal Tasarsız Ağlar – Vehicular Ad Hoc Networks) mimarisinin çok sık kullanıldığı görülmektedir. Yazılım Tanımlı Ağ yeni bir teknoloji olarak ortaya çıktığında, yüksek kullanılabilirlik, ölçeklenebilirlik ve performans gibi pek çok avantaj getirirken, aynı zamanda da saldırganların hedef aldığı yeni güvenlik açıklıklarını da beraberinde getiriyor. Bu araştırmada ağırlıklı olarak Dağıtık Hizmet Dışı Bırakma Saldırılarına karşı Yazılım Tanımlı Ağ ve s-Flow-RT teknolojisinin güçlerini birleştirerek kaynak temelli tespit yaklaşımına odaklanılmıştır. Bu çalışma kapsamında gerçekleştirilen benzetim çalışmasında SDN (Yazılım Tanımlı Ağlar – Software Defined Networking) tabanlı DDoS (Distributed Denial of Service – Dağıtılmış Hizmet Reddi) saldırısı gerçekleştirilip, saldırı öncesi ve sonrası verilerdeki değişiklikler incelenmiştir. Hping3 uygulaması ile DDoS saldırısı için trafik oluşturulmuştur. Yazılım tanımlı ağları oluşturmak için yazılım tanımlı ağ kontrolcüsü olarak RYU (bileşen tabanlı yazılım tanımlı bir ağ çerçevesi) kontrolcüsü seçilmiş ve Mininet emülatörü kullanılmıştır. Çalışma kapsamındaki saldırıyı gerçekleştirmek için geleneksel bilgisayar ağlarında Ubuntu sanal makinesi kullanılmıştır.

Anahtar kelimeler: *Yazılım Tanımlı Ağlar, sFlow-RT, VANET, SUMO, InfluxDB, Grafana, WEKA*

А.Н. Аманов[1], Д.Ш. Исаков[2]
[1] *PhD, аға оқытушы, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, (Қазақстан, Түркістан қ.), e-mail: anuarbek.amanov@ayu.edu.kz*
[2] *Магистрант, Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, (Қазақстан, Түркістан қ). e-mail: davron.issakov02@gmail.com*

SDN негізіндегі VANET желілерде DDOS шабуылдарын анықтау

Андатпа. Бүгінгі күнімізде қалада көше қиылысы құрылымдарының физикалық сипаттамалары және жоспарланбаған жол қиылыстарының нәтижесінде пайда болатын көлік ағындары уақытты (ақшаны) жоғалту, стресс және жағармай шығынын арттыру сияқты көптеген жағымсыз әсерлерді тудырады. Сондықтан, академиялық және коммерциялық орталарда ақылды қалалардың бір қосымшасы болып табылатын көлік басқару жүйелері бойынша көптеген зерттеулер жүргізілуде. Соңғы жылдары жасалған бұл зерттеулерде

көліктердің бір-бірімен немесе жол жиегіндегі құрылғылармен оңай хабарласып, тиісті көлік деректерін орталыққа жеткізуге мүмкіндік беретін VANET (Құралдандырылған Арнайы Желілер – Vehicular Ad Hoc Networks) архитектурасының жиі қолданылғаны байқалуда. Бағдарламалық Жасақтамамен Анықталған Желілер (SDN- Software Defined Networking) жаңа технология ретінде пайда болғанда, жоғары қолжетімділік, масштабтаушылық және өнімділік сияқты көптеген артықшылықтар әкелгенімен, сонымен қатар цифрлық шабуылдаушылардың нысанасы болған жаңа қауіпсіздік осалдықтары ортаға шығуда. Бұл зерттеуде негізінен Таралған Қызметтен Бас Тарту SDN және s-Flow-RT технологиясының күштерін біріктіре отырып, ресурстық анықтау тәсіліне баса назар аударылған. Осы зерттеу аясында жүргізілген симуляциялық зерттеуде SDN негізіндегі DDoS (таратылған қызмет көрсетуден бас тарту) шабуылы жасалды және шабуылға дейінгі және кейінгі деректердегі өзгерістер зерттелді. Hping3 қолданбасымен DDoS шабуылы үшін трафик жасалды. Бағдарламалық құралмен анықталған желілерді жасау үшін бағдарламалық құралмен анықталған желі контроллері ретінде RYU (компонент негізіндегі бағдарламалық құралмен анықталған желілік құрылым) контроллері таңдалды және Mininet эмуляторы пайдаланылды. Зерттеу аясында шабуыл жасау үшін дәстүрлі компьютерлік желілерде Ubuntu виртуалды машинасы пайдаланылды.

Түйін сөздер: *Бағдарламалық Жасақтамамен Анықталған Желілер, sFlow-RT, VANET, SUMO, InfluxDB, Grafana, WEKA*

А.Н. Аманов[1], Д.Ш. Исаков[2]

[1]*PhD, старший преподаватель, Международного казахско-турецкого университета имени Ходжи Ахмеда Ясави,Казахстан, г. Туркестан, e-mail: anuarbek.amanov@ayu.edu.kz*

[2]*Магистрант, Международного казахско-турецкого университета имени Ходжи Ахмеда Ясави, Казахстан, г. Туркестан, e-mail: davron.issakov02@gmail.com*

Обнаружение DDoS-атак в SDN-ориентированных автомобильных самоорганизующихся сетях

Аннотация. Физические характеристики современных городских перекрестков и потоки движения, вызванные непланируемыми дорожными пересечениями, приводят к множеству негативных последствий, таких как потери времени/денег, стресс, увеличение расхода топлива и другие. Поэтому в академических и коммерческих кругах проводится множество исследований систем управления дорожным движением, являющихся приложением умных городов. В последние годы было замечено, что архитектура VANET (Адаптивные сети для транспортных средств), которая легко позволяет осуществлять коммуникацию между транспортными средствами или с устройствами на обочине, тем самым перенося соответствующие данные о движении в центр, часто используется в этих исследованиях. Появление новой технологии, как сетевая архитектура, Программно-определяемые сети (SDN), принесла много преимуществ, таких как высокая доступность, масштабируемость и производительность, но также ввела новые уязвимости безопасности, нацеленные на атакующих. В этом исследовании в основном сосредоточено внимание на подходе к обнаружению на основе ресурсов путем объединения возможностей сетевой архитектуры, определенной программной сети, и технологии s-Flow-RT против распределенных атак типа "отказ в обслуживании". В рамках этой работы было проведено симуляционное исследование, в ходе которого была осуществлена атака DDoS (Распределенный отказ в обслуживании) на базе SDN (Программно-определяемые сети), и были изучены изменения в данных до и после атаки. Для создания трафика для DDoS-атаки использовалось приложение Hping3. В качестве контроллера для создания программно-определенных сетей был выбран контроллер RYU (фреймворк для программно-определенной сетевой архитектуры на базе компонентов), и использовался эмулятор Mininet.

Для осуществления атаки в рамках работы использовалась виртуальная машина Ubuntu в традиционных компьютерных сетях.

Ключевые слова: *Программно-определяемые сети, sFlow-RT, VANET, SUMO, InfluxDB, Grafana, WEKA*

A.N. Amanov[1], D.S. Isakov[2]

[1]*PhD, Senior Lecturer of Khoja Akhmet Yassawi International Kazakh-Turkish University, (Kazakhstan, Turkistan), e-mail: anuarbek.amanov@ayu.edu.kz*

[2]*Master's Student of Khoja Akhmet Yassawi International Kazakh-Turkish University (Kazakhstan, Turkistan), e-mail: davron.issakov02@gmail.com*

DDoS Attack Detection in SDN-Based Instrumented Ad Hoc Networks

Abstract. The physical characteristics of today's urban intersection structures and the traffic flows caused by unplanned road intersections lead to many negative effects such as time/cash loss, stress, increased fuel consumption, and more. For this reason, many studies are being conducted on traffic management systems, an application of smart cities, in both academic and commercial circles. In recent years, it has been observed that the VANET (Vehicular Ad Hoc Networks) architecture, which easily enables communication between vehicles or with devices on the side of the field, thus transporting relevant traffic data to the center, is frequently used in these studies. When Software Defined Networking emerged as a new technology, it brought many advantages such as high availability, scalability, and performance, but also introduced new security vulnerabilities targeted by attackers. This research primarily focuses on a resource-based detection approach by combining the powers of Software Defined Networking and s-Flow-RT technology against Distributed Denial of Service Attacks. In the simulation study conducted within the scope of this work, an SDN (Software Defined Networking)-based DDoS (Distributed Denial of Service) attack was carried out, and changes in data before and after the attack were examined. Traffic for the DDoS attack was generated with the Hping3 application. The RYU controller (a component-based software-defined networking framework) was selected as the software-defined network controller to create software-defined networks, and the Mininet emulator was used. A traditional computer network's Ubuntu virtual machine was used to carry out the attack in the scope of the work.

Keywords: *Software Defined Networks, sFlow-RT, VANET, SUMO, InfluxDB, Grafana, WEKA*

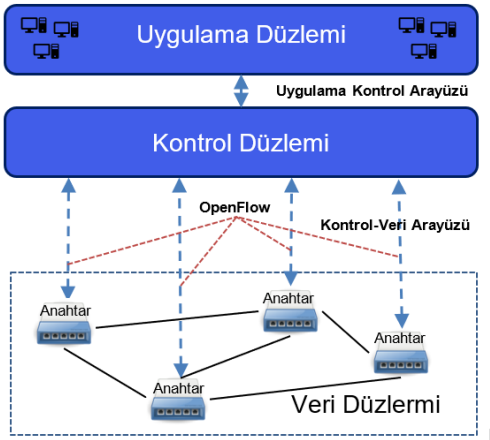
Giriş

İnternet kullanılabilirliği oranı muazzam bir şekilde artırıldı; bu nedenle, güvenlik önlemleri eskiye göre daha fazla gereklidir. En önemli konulardan biri, DDOS kötü amaçlı akışlarını daha doğru bir şekilde tespit ederek, kötü amaçlı akışları atarak kaynakların arızalanmasını önlemektir.

A. Yazılımlı Tanımlı Ağlar

Mevcut İnternet durumu, devam eden ağ yapılandırmasını ve ağ kontrolünü imkânsız kılan geleneksel ağ mimarisinin karmaşıklığından kaynaklanmaktadır. Bu nedenle, ağ uzmanları ve bilim adamları, gelecekteki İnternet mimarisi olarak Yazılım Tanımlı Ağ (SDN) adı verilen yeni bir bağımsız mimari önerdiler [1]. Bu mimarinin ana fikri, veri ve kontrol akışlarının ayrılmasıdır. Bu mimari uygulama, kontrol ve veri olmak üzere üç katmandan oluşmaktadır, şekil 1.1'de detaylı gösterilmiştir. Bu mimari, ağı çok daha programlanabilir, esnek ve yönetilebilir hale getirir [2][3]. Üç katmana ek olarak, uygulama, denetleyici ve veri katmanlarını birbirine bağlamak için kullanılan kuzey ve güney olmak üzere üç API bulunurken doğu-batı API, Denetleyici Yerleştirme Problemi (CPP-Controller Placement Problem) olarak denetleyici sayısını genişletmek için kullanılır. [4][5]. Bu mimari, araştırmacıların ağ güvenliği, kötü nietli DDOS saldırılar, performans

ve Hizmet Kalitesi (QoS) iyileştirmesi için yeni bir model önerebilmesine neden oldu çünkü geleneksel ağ mimarisi, yeniliği ağ donanımı satıcılarıyla sınırladı.



Şekil 1.1. SDN Mimarisi

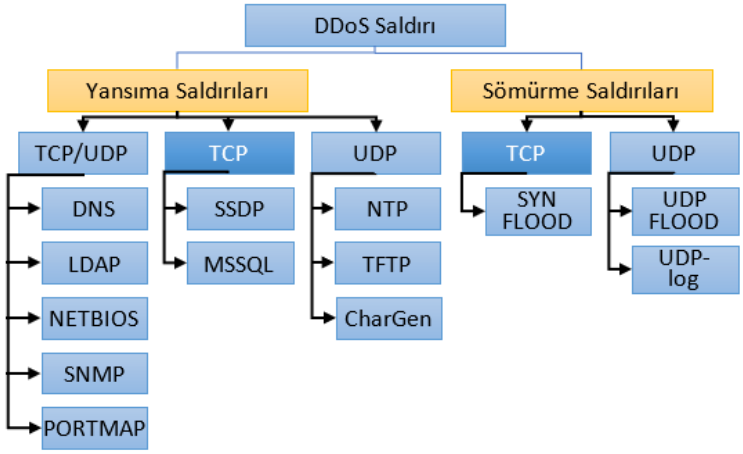
B. Problem Durumu

Küresel olarak, araba kazaları, Dünya Sağlık Örgütü'nün 2018'de yol güvenliği ile ilgili bir raporunda gösterildiği gibi, dünya çapında 100.000 nüfus başına 18.2 ve bazı bölgelerde 100.000 nüfus başına yaklaşık 26.6 oranında yüksek bir trafik ölüm oranını temsil etmektedir. Bu nedenle trafik güvenliğini arttırmak ve iyileştirmek, insanların hayatlarını güvence altına almak için teknolojiden yararlanmak, zorunlu bir ihtiyaçtan kaynaklanmaktadır [6]. Bu bağlamda, bu tür trafik kazası oranlarının azaltılmasında yeni teknolojilerin kullanılması için çeşitli çalışmalar önerilmiştir. Bu teknolojiler arasında, insanların ve toplulukların güvenliği ile bağlantısı ve etkisi nedeniyle çok popüler ve önemli bir teknoloji olan Araçsal Tasarsız Ağlar (Vehicular Ad hoc NETworks-VANETs) bulunmaktadır. Bu sistem, akıllı ulaşım sistemi (…- ITS), mobil tasarsız ağ (Mobile Ad Hoc Network- MANET) ve nesnelerin interneti(Internet of Things-IoT) uygulaması da dahil olmak üzere çeşitli kablosuz ve sensör teknolojilerinin bir kombinasyonudur. VANET, kablosuz ağ teknolojilerini bir iletişim aracı olarak kullanan düğümlerden oluşur. Araç düğümleri, her bir araçtaki yerleşik ünite (On Board Unit-OBU) adı verilen bir iletişim ünitesi aracılığıyla birbirleriyle ve yol kenarı üniteleriyle (Road Side Units-RSU) iletişim kurar ve bu da bir uygulama ara yüzü sağlamak için uygulama ünitesine (Application Unit-AU)bağlanır [7].

VANET hem güvenlik hem de güvenlik dışı uygulamaları destekler. Güvenlik uygulamalarının temel amacı, sürücüleri çarpışmadan kaçınma, yol işareti bildirimleri ve olay yönetimi için alarmlar konusunda uyararak kazaları en aza indirmek ve sürüş güvenliğini arttırmaktır. Buna karşılık, güvenlik dışı uygulamalar iki alt bölüme ayrılmıştır: trafik koordinasyonu ve bilgi-eğlence uygulamaları. Trafik koordinasyonu, yoldaki araçlar arasındaki trafik bilgilerini yayınlamak için araç iletişiminden yararlanır; bu, trafik akışını optimize eder ve sürücü deneyimini geliştirir. Bilgi-eğlence uygulamaları, sürücülere yolculukları sırasında eğlencenin yanı sıra ilgili reklamlar ve Park yardımı gibi bağlamsal bilgiler sağlamayı amaçlamaktadır [8]. VANET'te yönlendirme, ağın benzersiz özellikleri ve topolojide hızlı değişimlere neden olan düğümlerin hızlı hareketliliği nedeniyle zorlu bir faktördür. Ek olarak, yoldaki araçların yoğunluğunun ve hızının farklılaşması, seyrek dağıtım nedeniyle ek yüke veya zayıf bağlantıya neden olabilir. Mevcut VANET yönlendirme protokolleri topoloji, konum, küme, yayın ve coğrafi yayın tabanlı protokollere göre kategorize edilir. VANET'in benzersiz özellikleri, onu tüm VANET sistemini tehlikeye atabilecek ve bozabilecek birçok tehdide maruz bırakmaktadır. Tehditler, iletişim protokolleri, enerji akışı ve kimlik doğrulama, bilgi gizliliği ve bütünlüğü gibi güvenlik açıklarından kaynaklanabilir. Bu saldırılar arasında, aracı, altyapıyı veya her ikisini de sahte mesajlarla doldurarak ağ kullanılabilirliğini reddetmeyi amaçlayan dağıtılmış hizmet reddi (DDoS) saldırısı yer almaktadır.

İlgili çalişmalar

VANET ağlarında SDN teknolojilerinin uygulanması, yeni hizmet türlerinin ortaya çıkmasına veya halihazırda var olanların geliştirilmesine yol açabilir. [9]'de yazarlar, yazılım tanımlı VANET uygulamalarını özetlemektedir. Geliştirmeleri, SDN Destekli VANET Güvenlik Hizmeti, SDN tabanlı İsteğe Bağlı VANET Gözetim Hizmeti ve Kablosuz Ağ Sanallaştırma Hizmeti olmak üzere üç yöne ayırırlar (SDN Destekli VANET Güvenlik Hizmeti, SDN tabanlı İsteğe Bağlı VANET Gözetim Hizmeti, Kablosuz Ağ Sanallaştırma Hizmeti). Kategorize edilmiş ağdaki DDOS saldırılarını azaltmak için birçok yaklaşım önerilmiştir [10]. Önerilen bu yöntemler genel olarak Makine Öğrenimi (ML) tabanlı ve istatistiksel yöntemler olarak sınıflandırılabilir.



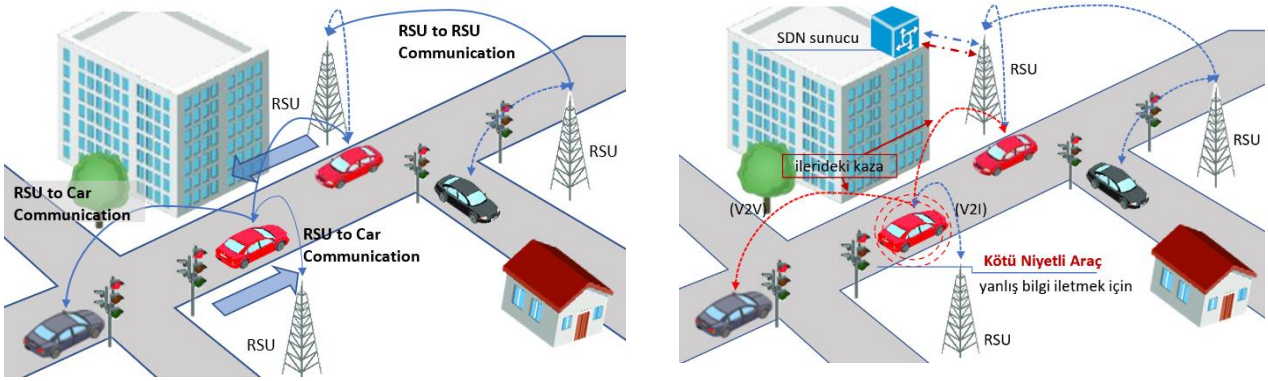
Şekil 2.1. DDOS saldırısı taksonomisi [10]

DDoS saldırısı, kötü amaçlı ağ trafikleri kullanılarak gerçekleştirilir ve kaynakları (sunucu ve bant genişliği) bu kötü niyetli ağ akışları tarafından boğulmuş hale getirerek ağa erişilemez hale getirir. Şekil 2.1'de DDOS saldırısı ağdaki hangi protokollerden geçtiği ayrıntılı taksonomisi gösterilmektedir.

Cisco'nun 2020 yılında yayınladığı yıllık internet raporuna göre, dünya genelinde DDoS saldırılarının sayısı 2023 yılına kadar ikiye katlanarak 15,4 milyona ulaşacak [11]. Bu rapor, gelecekte DDoS saldırılarının artacağını ve geçmişte olduğundan daha fazla dikkat edilmesi gerektiğini gösteriyor. Örneğin 2006 yılında CNN, Netflix, Twitter gibi tanınmış şirket ve kuruluşlarda meydana gelen DDoS saldırıları hizmet reddine neden olmuştur [12]. Saldırganlar hedef ağını aşmak için botnet'ten yararlanırsa, DDoS saldırılarının etkisi büyük ölçüde artabilir. Artan bant genişliği ve işlem gücü nedeniyle saldırganların DDoS saldırıları başlatması için mükemmel bir platformdur [11]. Security Operation Center'ın (SOC) en önemli bileşeni, DDoS kötü amaçlı akışlarını ilk adımda doğru bir şekilde tespit etmektir. Bir sonraki adımda, hizmetlerini sunabilmeleri için kaynağı güvenli hale getirmek için bu kötü niyetli akışlar atılmalıdır. DDoS akış tespiti, bu yazıda doğruluğunu iyileştirmek için ele alınacak bir konudur. DDoS kötü amaçlı akışlarını tespit etmek için bu modül, (fiziksel veya kavramsal) olan denetleyicide uygulanacaktır.
SDN'nin kontrolü veri düzleminden ayırması nedeniyle birçok fayda sağlayabileceği iyi bilinen bir gerçektir. Ancak yine de SDN ve DDoS saldırıları arasında hassas bir ilişki vardır. SDN'nin kendisi DDoS saldırılarının hedefi olabilir. Ağın küresel görünümü, iletme kurallarının dinamik olarak güncellenmesi vb. gibi ağ yetenekleri, DDoS saldırılarının tespit edilmesini kolaylaştırabilir, ancak kontrol düzleminin veri düzleminden ayrılması yeni saldırı türlerinin ortaya çıkmasına neden olur. [11] Örneğin, bir saldırgan SDN'nin özelliklerini kullanarak SDN'nin kontrol, altyapı ve uygulama katmanlarına DDoS saldırıları yapabilir.

Vanet'e genel bakiş

VANETs, araçtan araca (V2V), araçtan altyapıya (V2I) ve altyapılar arası (I2I) iletişim olmak üzere 3 tür iletişim modu sunar. Saldırılar genellikle bu üç iletişim modu üzerinden yapılır. İletişim modları Şekil 3.1(a)'da gösterilmektedir [12].



a) *b)*

Şekil 3.1. a) Araçsal Tasarsız Ağlarda İletişim b) SDN tabanlı VANET'lerde Dağıtılmış Hizmet Reddi (DDoS) saldırısı.

Araç-araç iletişimi(V2V): V2V'de, iletişim aralığındaki araçlar kablosuz ağ üzerinden veri alışverişi yapar. Değiştirilen veriler arasında hız, konum, yön, trafik bilgileri, sürücü davranışı, yol durumu ve gezginler için gerekli diğer yararlı bilgilerbulunur.

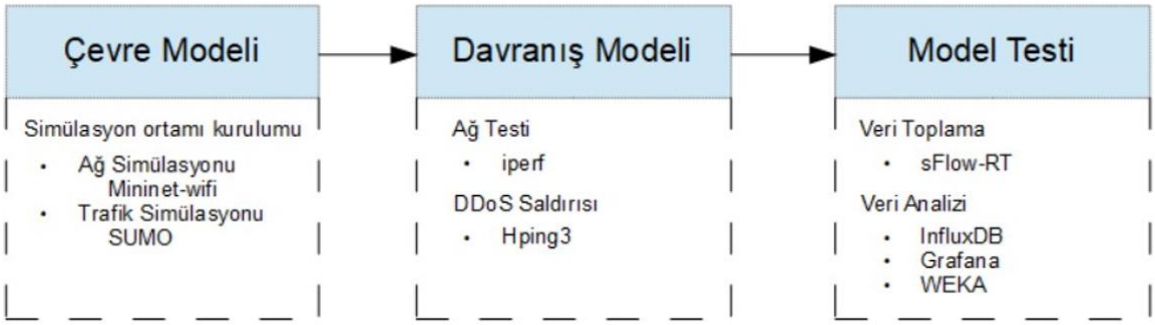
Araç-altyapı iletişimi (V2I): V2I'de, araçlar ve trafik kavşakları ve yol kenarı erişim noktaları gibi yol kenarı altyapısı arasında iletişim gerçekleşir. Öncelikle motor kazalarından kaçınmak, ambulans yardımı ve daha geniş bir hareketlilik yelpazesine ulaşmak gibi güvenlik uygulamaları için tasarlanmıştır.

Altyapılar arası iletişim (I2I): Altyapılar arası iletişim modunda, yol kenarı altyapı birimleri daha geniş bir aralık elde etmek için birbirleriyle iletişim kurar. İçerik paylaşımında daha fazla esneklik sunar ve çoklu atlama iletişimi sunarak iletişim aralığını artırır. Bu tür bir iletişim, araçların RSU'larla tek bir hop veya birden fazla hop ile iletişim kurabildiği ve kesintisiz bağlantı sağlayan hibrit bir VANET mimarisine yol açar [13].

Bu araştırmada araç-araç iletişimi arasında yapılan DDoS saldırısı ele alınmıştır. Amaç, araçlar arası iletişim ağını kapatmaktır. Bu saldırı sonucu kurban araç bir süre sonra ağdaki diğer araçlarla iletişim kuramaz.

Yöntem

Proje, yöntem olarak 3 aşamada gerçekleştirilmiştir. 1. aşamada Mininet-wifi ile ağ simülasyonu, SUMO ile trafik simülasyonu oluşturularak simülasyon ortamı kurulmuştur. 2. aşamada iperf ile ağ test edildikten sonra hping3 ile DDoS saldırısı yapılmıştır. 3. aşamada ise toplanan verilerin model testi gerçekleştirilmiştir. Süreçmodeli Şekil 4.1.'de sunulmuştur.



Şekil 4.1. *Süreç Modeli*

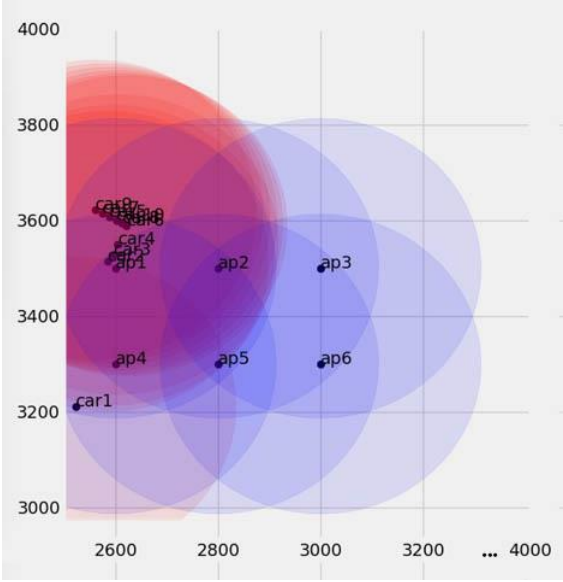
Mininet, yazılım tanımlı ağlar (Software Defined Networks-SDN) oluşturmaya, test etmeye ve gerçeklemeye olanak sağlayan açık kaynak kodlu bir projedir [14]. SDN, ağın tutarlı olarak yönetimini sağlamaktadır. Bu araştırmada, Mininet ile araçların yol alacağı ve RSU'lar ile birbirleriyle haberleşebilecekleri trafik topolojisi Python API'si üzerinden oluşturulup Mininet-wifi ile çalıştırılmıştır.

```
cd mininet wifi/
```

SDN mimarisindeki uygulama düzlemindeki uygulamalar tarafından alınan talimatları, araçlar tarafından yürütülen kurallara dönüşmesi için RSU denetleyici kullanılmıştır [15].
VANET'te oluşturulan topolojiyi bir simülasyon üzerinde incelemek için bir mobilite simülatörüne ihtiyaç vardır. Araçların bir güzergâh dâhilinde hareket etmesi SUMO yazılımı tarafından sağlanılmıştır.

```
sudo python examples/vanet-sumo.py
```

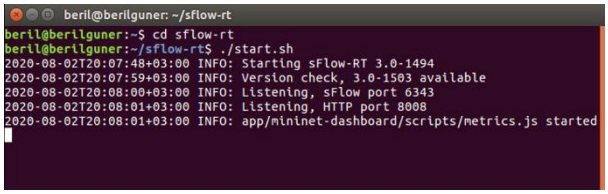
OpenFlow, sFlow-RT vb. gibi ağ cihazlarını yönetmek için çeşitli protokolleri desteklediği için kontrolcü olarak RYU kontrolcüsü kullanılmıştır. RYU kontrolcüsü, bileşen tabanlı bir frameworktür. Çevik ve esnek bir kontrolcüdür. Daha sonra mininet-wifi terminali üzerinden hping3 trafik oluşturma aracı kullanılarak DDOS saldırıları için trafik oluşturulmuştur. Saldırı öncesi ve sonrası bandwith ve throughput değerlerinin kontrolü için iperf uygulamasından yararlanılmıştır. Saldırı için gerekli ortam hazırlandıktan sonra DDoS saldırısı gerçekleştirilmiştir. Saldırının gerçekleştirilmesiyle yüksek hızda veri transferi yapan ağda paket düzeyinde inceleme yapabilmek amacıyla verilerin kontrolü sFlow-RT protokolü ile sağlanmıştır. Toplanan analiz verilerini saklamak amacıyla InfluxDB veritabanı kullanılmıştır. sFlow-RT ile toplanan ve InfluxDB veritabanı üzerine aktarılan veriler Grafana uygulaması ile oluşturulan dashboardlar üzerinde daha iyi bir sorgulama yapabilmek amacıyla görüntülenmiştir. Toplanan saldırı öncesi ve sonrası verileri, veri madenciliği ve makine öğrenmesi alanlarında kullanılan veri işleme programı olan WEKA (Waikato Environment for KnowledgeAnalysis) ile kıyaslanmak amacıyla işlenmiştir.
Tüm yazılımlar Ubuntu 16.04 Linux işletim sisteminde çalıştırılmıştır. Test topolojisi Şekil 4.2.'de verilmiştir.



Şekil 4.2. *Test Topolojisi*

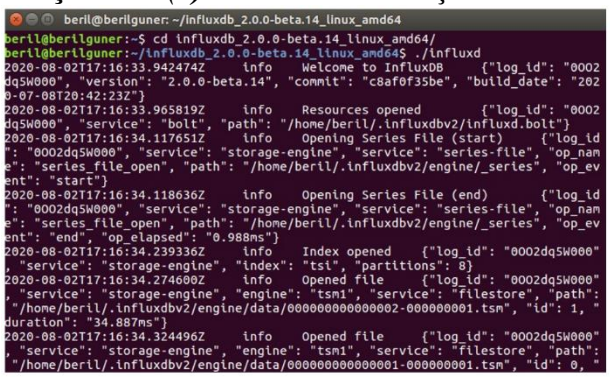
DENEY ve SİMÜLASYON

Simülasyonda ilk olarak trafiği gerçek zamanlı olarak kontrol etmek için sFlow-RT trafik analizörü başlatılmıştır (Şekil 5.1(a)). sFlow-RT ağ yönetimini sağlamak amacıyla RYU kontrolcüsü başlatılmıştır (Şekil 5.1(b)). Daha sonra anlık olarak çekilen verilerin kaydı için InfluxDB veri tabanı başlatılmıştır (Şekil 5.1(c)).

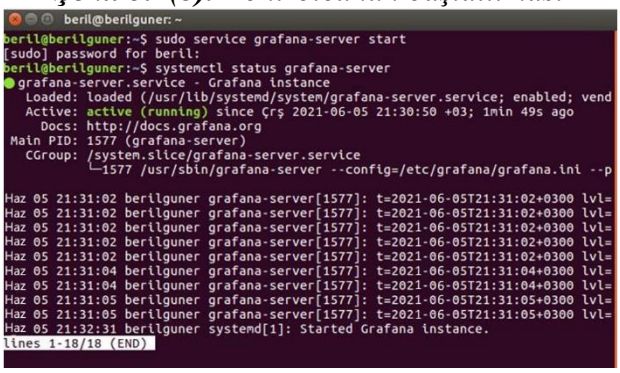


Şekil 5.1(a). *sFlow-RT'nin başlatılması*

Şekil 5.1(b). *Kontrolcünün başlatılması*

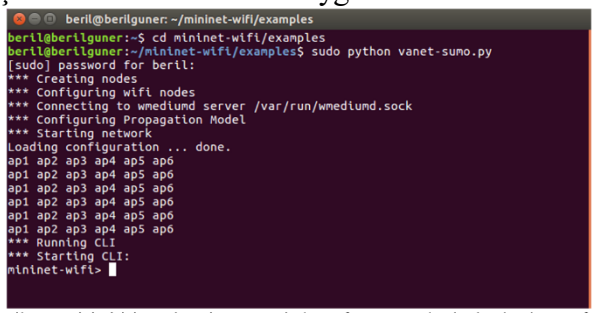


Şekil 5.1(c). InfluxDB veri tabanının başlatılması



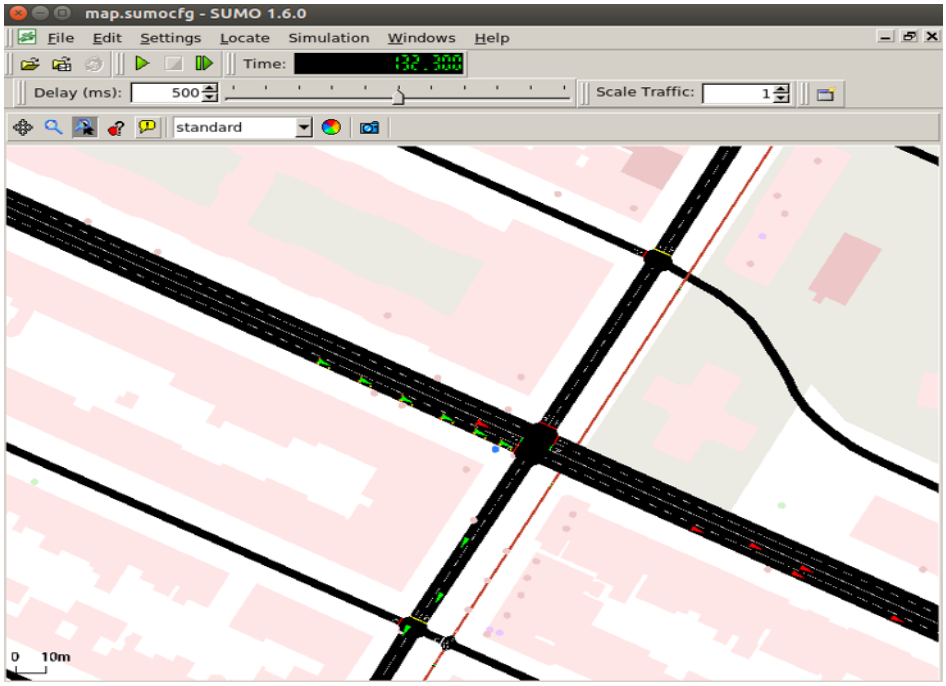
Şekil 5.1(d). Grafana'nın başlatılması

Veri tabanına kaydedilen verileri görselleştirmek amacıyla Grafana uygulaması başlatılmıştır (Şekil 5.1(d)). sFlow-RT başlatıldığı an versiyon kontrolü yapılmakta ve portlar dinlenmeye başlamaktadır. Ryu kontrolcüsü ile Mininet-wifi içerisinde ağ uygulaması simüle edilebilmektedir. Grafana'nın başlatılması için sudo komutu ile yönetici girişi yapılıp, sistem üzerinde grafana-server başlatılmaktadır. Grafana uygulaması aktif edilmektedir.



Şekil 5.2. *Topolojinin çalıştırılması*

Python kodu ile oluşturulan vanet topolojisi, sudo python komutu ile çalıştırılmaktadır. Daha sonra sunucuya bağlanılmakta ve network başlatılmaktadır. Topolojideki 10 adet araç, çalıştırılan vanet-sumo.py dosyasındakipython kodlarından eklenmiştir. Aynı şekilde 6 adet erişim noktası'da (AccessPoint-AP) simülasyon sistemine eklenmiştir. Topoloji çalıştırıldığında açılan SUMO yazılımı penceresinden simülasyon başlatılmıştır.

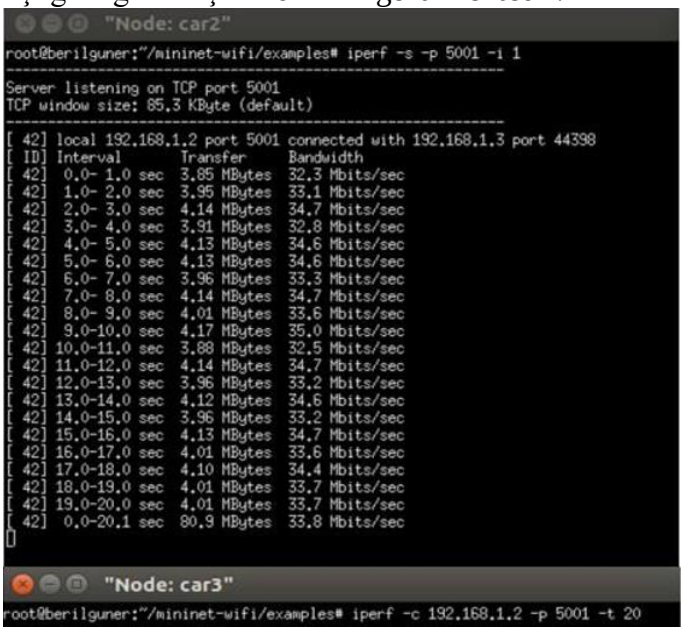


Şekil 5.3. *SUMO*

Araçlar haritaya girerek ağda aktif hale gelmektedir. Simülasyonun başlatılmasını ardından araçlar harita üzerinde sıra ile konumlandırılır. Bu esnada mininet üzerinden düğümler hakkında bilgiler edinilir.

Her araç iki adet kablosuz ağ ara yüzüne sahiptir. Wlan0 olarak aktif edilen arayüzvarsayılan olarak aktif gelir ve normal AP-CAR arası iletişim için kullanılmaktadır. Wlan1 üzerinde sanallaştırılan mp1 arayüzü ise mesh point olarak görev yapar. Araçların birbirleri ile mesh ağına dahil edilen AP'ler ile haberleşme mp1 arayüzü aracılığı ile sağlanır. Araçlarda yer alan ara yüzlerin ip adresleri tespit edilir. Dahasonra iletişimin testi için ping atma işlemi gerçekleştirilir.

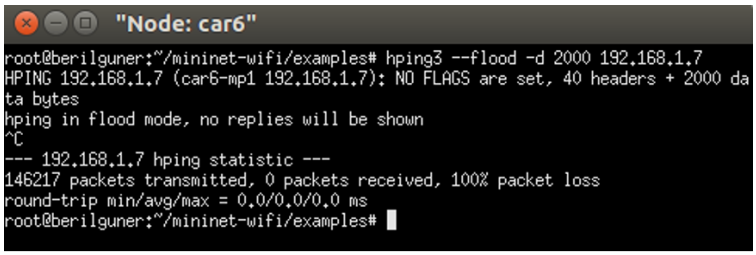
DDOS saldırısı öncesi ağın bant genişliğini tespit etmek üzere iperf uygulaması çalıştırılmıştır. Car2 server olarak ayarlanır ve 3 numaralı araçtan test için jperf uygulaması çalıştırılmıştır. Bant genişliği değerleri Şekil 5.4.'da görülmektedir.



Şekil 5.4. *Bant genişliği değerleri*

Hping3 programı ile araçlar arasında DDOS saldırısı yapılmıştır. Saldırıda ICMP paketleri kullanılmış ve pakete 2000 bytelık veri eklenmiştir. Saldırı Car6 ve Car7 araçları arasında

yapılmıştır.

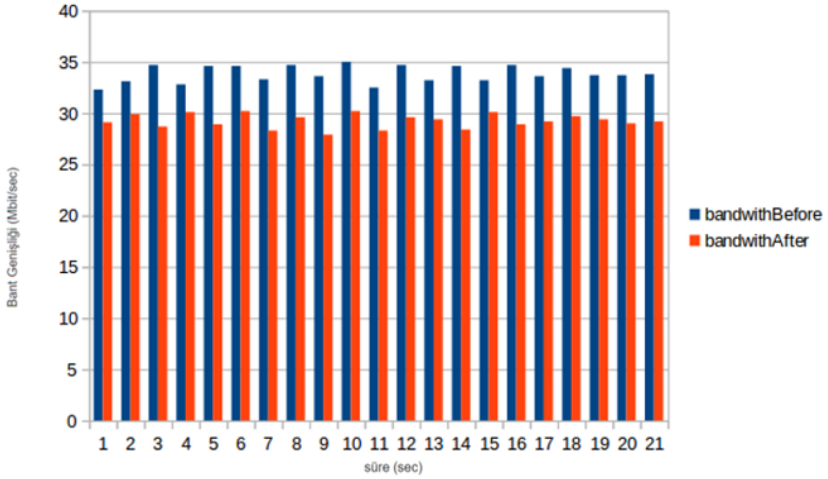


Şekil 5.5. *Saldırının gerçekleştirilmesi*

Bulgular ve değerlendirme

DDOS saldırıları araç ortamında çok tehlikelidir, çünkü saldırı süreci, etkinin ağda yayıldığı dağıtılmış bir şekilde gerçekleşir. Bu saldırıda, saldırgan ağdaki diğer düğümlerin kontrolünü ele geçirir ve farklı konumlardan saldırı başlatır. Uygulamadan elde edilen sonuçlar ile, DDOS saldırılarının düğümler ile altyapı arasında bilgi gönderilmesini engellediği görülmüştür.

Saldırı sonrasında bant genişliği testi tekrarlanmış ve sonuçları aşağıda sunulmuştur. Hedefin yoğun bir şekilde isteğe maruz kalması sonucunda bant genişliği %85 oranında azalmıştır. Bant genişliği (Bandwidth) kapasite demektir. Bandwidth terimi, bir veri iletişim ortamının ya da haberleşme kanalının kapasitesini ifade etmek için kullanılır. Veri iletişim kaynaklarındaki veri miktarının bit/saniye veya byte/saniye cinsinden ölçülmesidir. Şekil 6.1.'de Mbit/saniye olarak saldırı öncesi ve saldırı sonrası bant genişliklerinin değişimi görülmektedir.

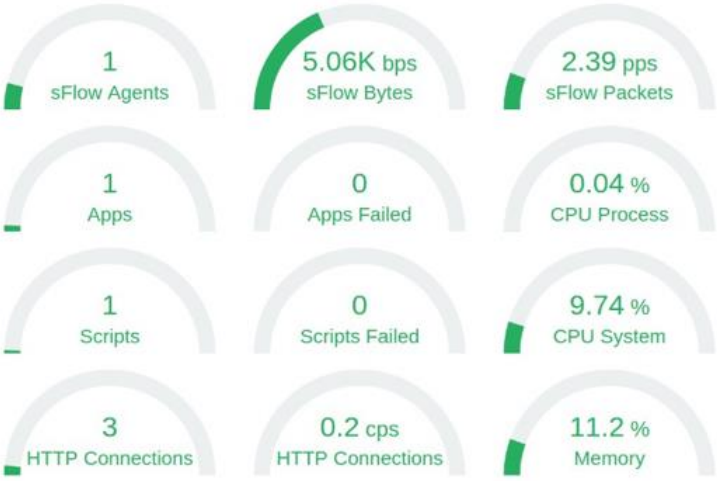


Şekil 6.1. *Saldırı öncesi & Saldırı sonrası bant genişliklerinin karşılaştırılması*

Bant genişliği ne kadar büyükse, belli bir süre içinde aktarılabilecek verinin hacmi de o kadar büyük olur. Grafikteki her saniyede saldırı sonrası paket iletim hacmi saldırı öncesi paket iletim hacminden az olduğu görülmektedir.

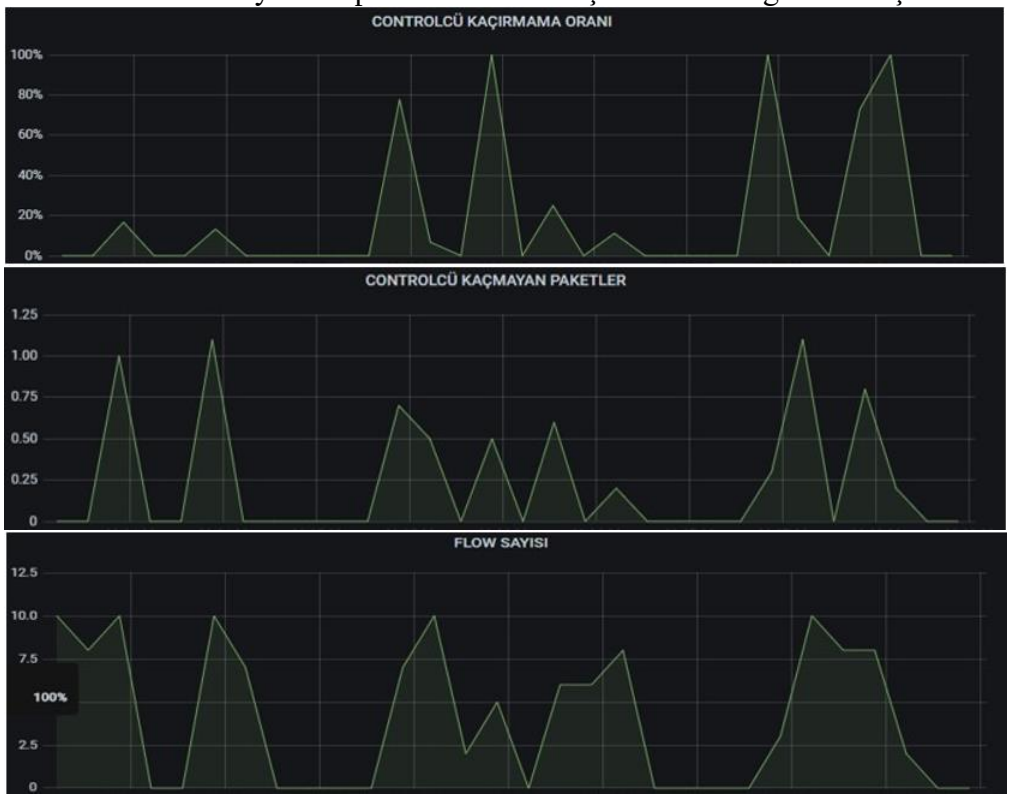
Grafana ile Veri Görselleştirme

Grafana ne işe yarıyo anlat. Sflow-RT ile toplanan veriler grafana ile görselleştirilmiş ve sonuçlar aşağıda sunulmuştur.



Şekil 6.2. sFlow-RT ile verilerin alınması

Kontrolcüye gönderilen kural sorma paketlerinin toplam paketlere oranı Şekil 6.3.a'de, kontrolcü tarafından kural yazılan paket oranları ise Şekil 6.3.b'degösterilmiştir.



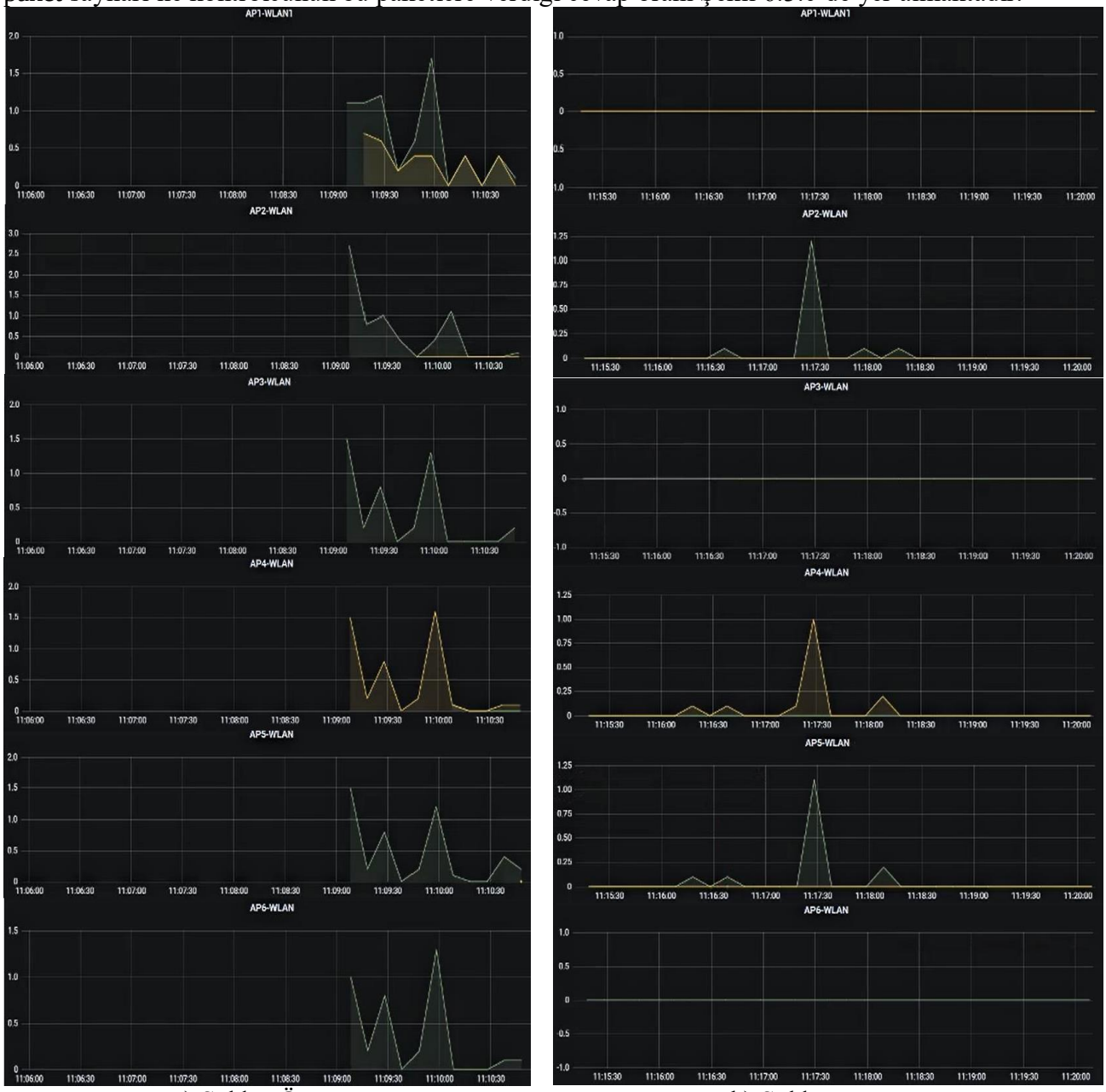
a)

b)

c)

***Şekil 6.3**. a) Kural sorma paketlerinin toplam paketlere oranı b) Kural yazılan paket oranları c) Akiş sayısı*

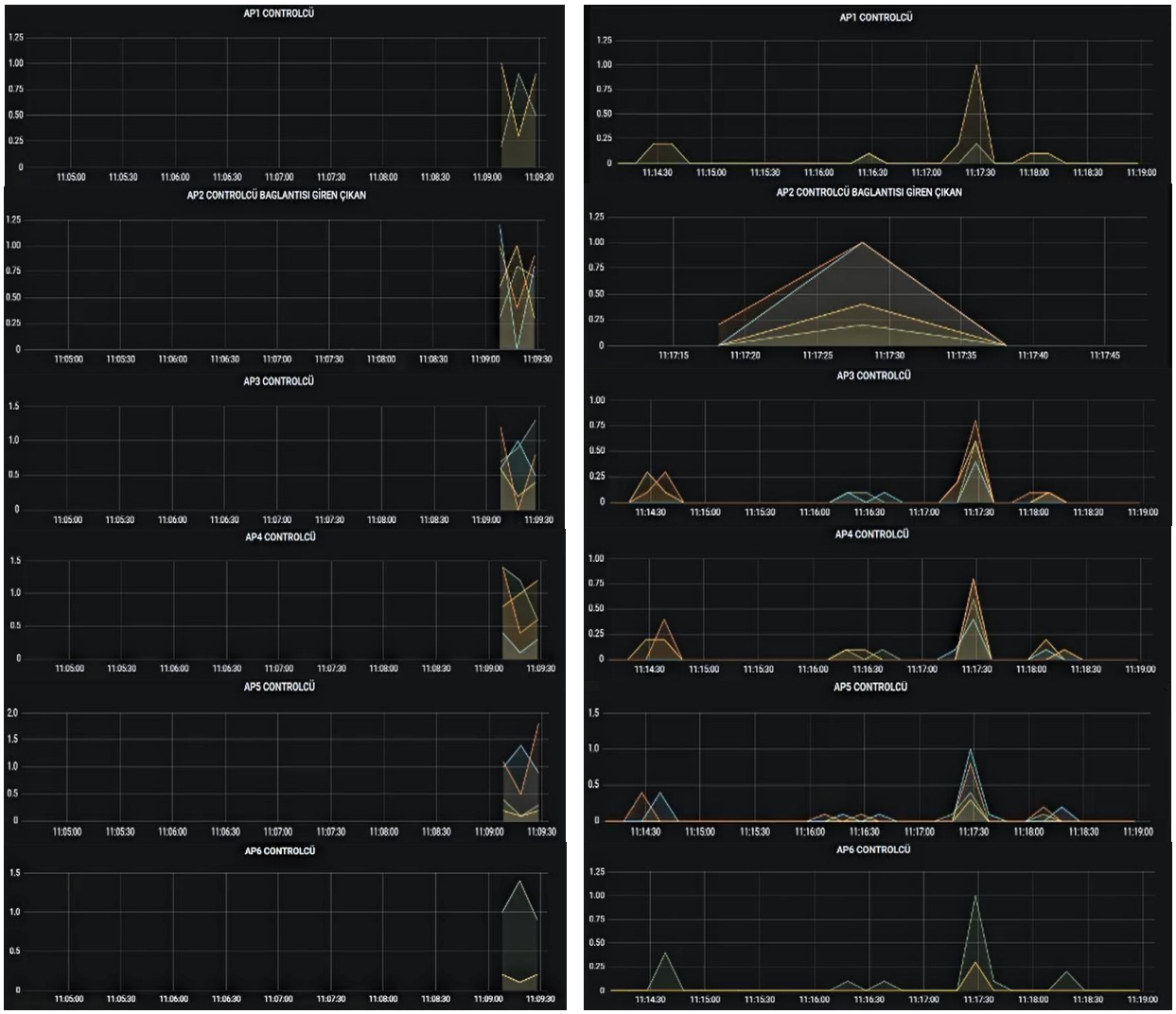
Grafik şekilleri hemen hemen birbiri ile aynıdır. Zira kontrolcüye ulaşan paketlerintamamına kontrolcü cevap vermiştir. Ancak AP'de oluşan bufferover flow (bellek taşması) nedeniyle kural paketleri direk drop edildiğinden kontrolcüye ulaşamamıştır. Kontrolcüye gönderilen openflow paket sayıları ile kontrolcünün bu paketlere verdiği cevap oranı Şekil 6.3.c'de yer almaktadır.



a) Saldırı Öncesi b) Saldırı sonrası

Şekil 6.5. *WLAN Durumları*

AccessPoint'lerde oluşan paket trafik grafikleri Şekil 6.5(a) ve Şekil 6.5(b)'de gösterilmiştir. AP1, AP3 ve AP6'da hiç hareketlilik gözlenmemiştir. Araçların AP wlanının kapsama alanı dışında olmasından dolayı AP1-Wlan, AP3-Wlan ve AP6-WLan ile paket etkileşimleri yoktur.



a) Saldırı öncesi b) Saldırı sonrası

Şekil 3.6. *Kontrolcü Durumları*

AP'ler arasında iletişim ethernet hattı üzerinde gerçekleştirilmektedir. Bu kapsamda ethernet hattında yer alan trafik verileri aşağıda gösterilmiştir. Linear topoloji gereği AP1'e ve AP1'den diğer AP'lere trafik AP2 üzerinden akmaktadır. AP2'nin ethernet arayüzünde yoğun paket trafiği gözlemlenmiştir. Saldırının durdulması sonucu, kontrolcü belleğinde flow paketleri drop edildiğinde iletişim normale dönmüştür. "Visualize" ile veri setindeki örneklerin özniteliklere göre nasıl dağıldığı Şekil 3.10. ve Şekil 3.11.'de gösterilmiştir. Şekil 3.10. ve Şekil 3.11.'deki çarpılar veri dosyasındaki örneklere karşılık gelmektedir.

Sonuç

DDOS saldırıları araç ortamında çok tehlikelidir, çünkü saldırı süreci, etkinin ağda yayıldığı dağıtılmış bir şekilde gerçekleşir. Bu saldırıda, saldırgan ağdaki diğer düğümlerin kontrolünü ele geçirir ve farklı konumlardan saldırı başlatır. Güvenlik, birçok yol kullanıcısı için birincil hedeftir. Bu nedenle, güvenlik gereksinimleri, kaza bildirimi vb. gibi birçok güvenlik uygulaması tarafından iyi desteklenmelidir. Ayrıca, hayati öneme sahip mesajlar VANET ağındaki düğümden düğüme güvenilir ve zamanında iletilmelidir. Bu uygulamada VANET için bir simulator sunulmuştur ve VANET için geçerli olabilecek DDOS saldırı türü incelenmiştir. DDOS saldırısı durumunda ağ kullanılabilirliğinin doğrudan etkilendiği ve saldırıların ağın bozulmasına neden olarak ciddi bir etkiye yol açtığı görülmüştür.

KAYNAKLAR

1. A. Shirmarz and A. Ghaffari, “An Autonomic Software Defined Network (SDN) Architecture WithPerformance Improvement Considering,” J. Inf. Syst. Telecommun., vol. 8, no. 2, (2020) 1–9.
2. A. Shirmarz and A. Ghaffari, “Performance issues and solutions in SDN-based data center: a survey,” J. Supercomput., vol. 76 (2020) 7545–7593.
3. A. Shirmarz and A. Ghaffari, “An adaptive greedy flow routing algorithm for performance improvement in a software-defined network,” Int. Numer. Model. Electron. networks, Devices, Fields-Wiley online Libr., vol. 33, no. 1, (2019) 1–21.
4. A. Shirmarz and A. Ghaffari, “Taxonomy of controller placement problem (CPP) optimization in Software Defined Network (SDN): a survey,” J. Ambient Intell. Humaniz. Comput., (2021) 1–26.
5. G. Ramya and R. Manoharan, “Enhanced Multi-Controller Placements in SDN,” J. Ambient Intell. Humaniz. Comput., (2020) 1–5.
6. World Health Organization (WHO). Global status report on road safety 2018. WHO (2018) https://www.who.int/violence_injury_prevention/road_safety_status/2018/English-Summary-GSRRS2018.pdf (accessed 20 August 2019).
7. Jain, M, Saxena, R. VANET: security attacks, solution and simulation. In: Bhateja, V, Tavares, JMR, Rani, BP, et al. (eds) Proceedings of the second international conference on computational intelligence and informatics. Singapore: Springer, (2018) 457–466.
8. Ghebleh, R. A comparative classification of information dissemination approaches in vehicular ad hoc networks from distinctive viewpoints: a survey. Comput Netw (2018) 131:15–37.
9. I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy,” Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2019-Octob (2019).
10. Quagga Routing Software Suite. [Online]. Available: http://www.nongnu.org/quagga/
11. Q. Yan; F. R. Yu, “Distributed denial of service attacks in software-defined networking with cloud computing,” IEEE Communications Magazine, Volume: 53, Issue: 4, (2015) 52 - 59,
12. M Raya, P Papadimitratos, JP Hubaux, “Securing Vehicular Communications”, IEEE Wireless Communications, Vol 13, October (2006).
13. S. Zeadally, R, Hunt, Y. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, (2010) 217-241.
14. Feamster, Nick, Jennifer Rexford, and Ellen Zegura. "The road to SDN: an intellectual history of programmable networks." ACM SIGCOMM Computer Communication Review 44, No. 2 (2014), 87–98.
15. Xiao, X.; Kui, X. The characterizes of communication contacts between vehicles and intersections for software-defined vehicular networks. Mob. Netw. Appl. (2015) 20, 98–104.