Büyük Veri Kullanarak Anomali Tabanlı Ağ Saldırı Tespit Sistemi (ANODE)

Beste Aydemir, Berfin Kavşut, Şevki Gavrem Kulkuloğlu,
Ege Ozan Özyedek, Meltem Toprak

Prof. Serdar Kozat
Elektrik ve Elektronik Mühendisliği Bölümü, Bilkent Üniversitesi

Oğuzhan Karaahmetoğlu
DataBoss Security & Analytics A. Ş., Türkiye

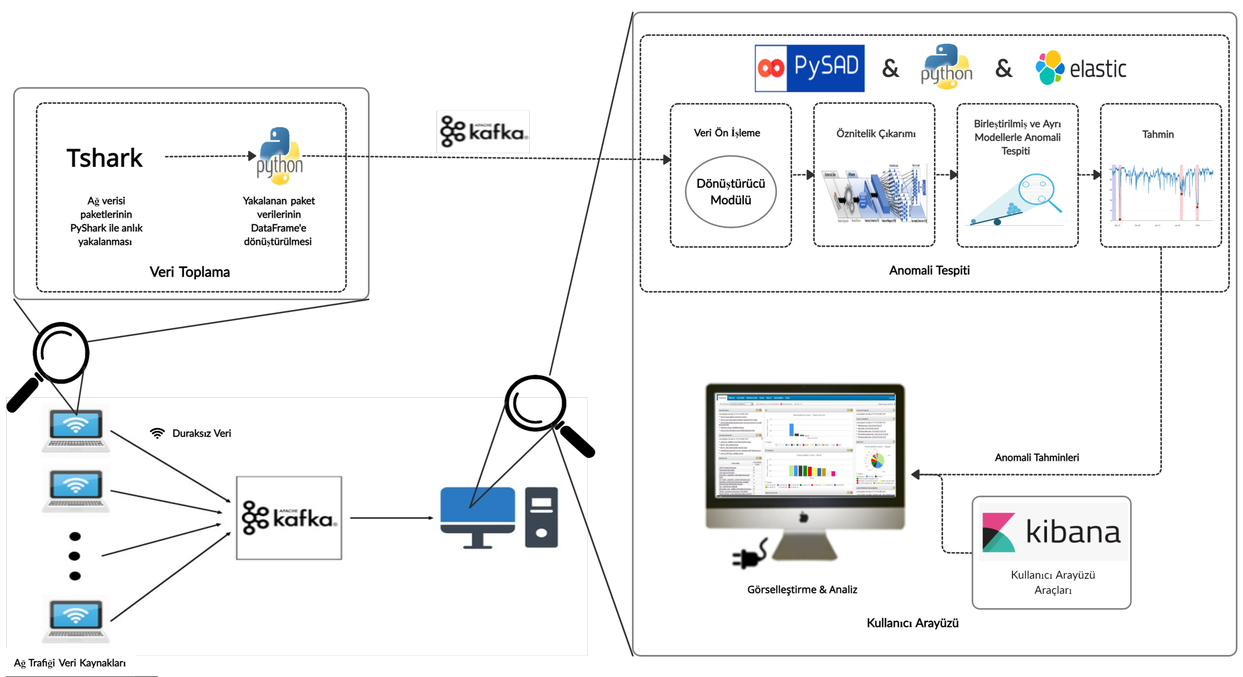
Proje Tanımı ve Amacı

Bilgisayarların ağ trafiği, ağ davranışındaki anormal eylemleri yakalamak için veri analiz yöntemleri ile incelenebilir. Bu analiz, bireyler, şirketler ve devletler tarafından kullanılacak ağ güvenliği sistemlerinin geliştirilmesi için önemlidir [1].

ANODE, tek ve çok kaynaklı duraksız akan ağ trafiği üzerinde gerçek zamanlı çalışan bir anomali tabanlı saldırı tespit sistemidir. Anomali tabanlı saldırı tespit sistemlerinin avantajı, imza tabanlı saldırı tespit sistemlerinden farklı olarak daha önce karşılaşılmamış ağ saldırılarını tespit edebilmesidir [2].

Sistemin Özellikleri ve Gereksinimleri

Genel Görünüm



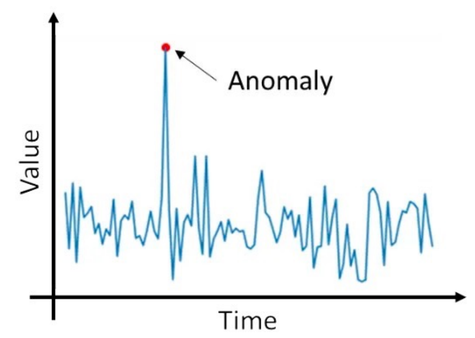
Kullanılan Bileşenler

PyShark + kafka + PySAD + elastic + kibana

Sistem Özellikleri

Bilesenler	Açıklama	Kullanım Alanı
Pyshark	Tshark icin Python fonksiyon çeviricisidir	Ağ veri paketleri yakalanması
Kafka	Dağıtık bir veri akış platformudur	Yakalanan paketlerin anomali modülüne taşınması
PySAD	Akan veri üzerine anomali tespiti kütüphanesidir	Akan paketler üzerine anomali tespiti yapılması
Elastic	Toplanan verilerin analizi ve içerik arama gibi işlemlerin yapılmasını sağlayan bir arama motorudur	Verinin Kibanaya göderilmesi için kaydedilmesi
Kibana	Elasticteki verinin görselleştirme işlemini yapar	Verilerin grafikler ve tablolar ile görselleştirilmesi, kullanıcı ara yüzünün oluşması

Kullanılan Yöntemler

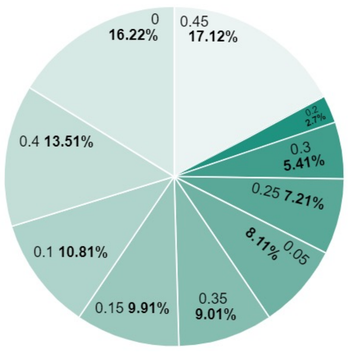


İlk olarak ağ hakkında zaman, ağ katmanı ve paket büyüklüğü gibi bilgileri içeren ağ verisi, ağ paketlerini toplamaya yönelik PyShark ile toplanır. Ardından belirli öznitelikler seçilerek Kafka kullanılarak anomali tespit modülüne gönderilir.

Anomali içeren paketleri bulmak için gözetimsiz uzaklık tabanlı, karar ağaçları, derin sinir ağı tabanlı ya da otomatik kodlayıcı ile çalışan algoritmalar kullanılır. Hepsi aynı anda mevcut olmayan ve akış halinde olan paketlerde bu algoritmaların kullanılarak incelenir. Akış halindeki veride, önceki paketlerle etkileşimi anlamak için pencereleme gibi istatiksel yöntemler de kullanılabilir. Böylece her ağdaki her paketin anormal olma olasılığı hesaplanır.

Kullanıcı arayüzü Kibana ile sağlanır. Paketlerin anormal olma olasılığı ve paket bilgileri canlı grafiklerle gösterilir. Bunlara ek olarak anormal olay üzerine kullanıcıya alarm verme ve kullanıcıya algoritmaları hiper-parametreleri belirleyerek değiştirme olanağı verilir.

Sonuçlar



Anomali sonuçlarının olasılıklarına göre dağılımı

Anomali olasılıklarının canlı grafik üzerinde zamana bağlı olarak gösterilmesi

Kafka'dan Veri Alma	Veri Önişlem	Öznitelik Çıkarımı	Eğitim Hızı	Tespit Hızı
0.05s	0.02s	0.07s	0.4s	0.1s

- Gerçek zamanlı akan bir sistemde anomali tespiti başarıyla gerçekleştirilmiştir.
- Anomali skorları, zamana bağlı canlı grafiklerle ve pasta grafiğinde gösterilmektedir.
- Bir paketin değerlendirilmesi için gereken süre tabloda gösterilmiştir.
- AUROC değeri 0.6'dan büyüktür.
- F1-Skoru 0.4'ten büyüktür.
- PR eğrisi, sabit çizginin üstündedir.

Kaynaklar

[1] Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, and A. Abuzneid, " Features Dimensionality Reduction Approaches for Machine Learning Based Network Intrusion Detection", Electronics, vol. 8, p. 322, Mar. 2019. doi:10.3390/electronics8030322.
[2] Veeramreddy, V. Prasad, and K. Prasad, "A Review of Anomaly Based Intrusion Detection Systems", International Journal of Computer Applications, vol. 28, pp. 26–35, Aug. 2011.doi:10.5120/3399-4730.

Teşekkürler

Ders koordinatörlerimiz Dr. M. Alper Kutay, Yeşim Gülseren, Dilan Öztürk ve Elif Aygün'e,
Asistanımız Arda Atalık'a,
Akademik danışmanımız Prof. Serdar Kozat'a,
Şirket danışmanımız Oğuzhan Karaahmetoğlu'na teşekkür ederiz.
Bu çalışma 2209-B programı kapsamında TÜBİTAK tarafından desteklenmiştir.