Düzce University
Journal of Science & Technology

Research Article

Anomaly Detection in Software-Defined Networking Using Machine Learning

Soumaine BOUBA MAHAMAT [a,*], Celal ÇEKEN [b]

[a] *Department of Computer and Information Engineering, Sakarya University, Sakarya, TURKEY*
[b] *Department of Computer and Information Engineering, Sakarya University, Sakarya, TURKEY*
** Corresponding author's e-mail address: soumaine.mahamat@ogr.sakarya.edu.tr*

ABSTRACT

In recent years, the Software-Defined Networking (SDN) approach has emerged that aims to make computer networks more flexible. Although the SDN application on Google's internal network demonstrates the usefulness of the Software-Defined Network approach and the promise of future technology, security is a vital concern that cannot be ignored. In the SDN architecture, the attacker can now attack the network from any of the three planes because the Data Plane is separated from the Control Plane. Machine learning algorithms are methods used to detect attacks and intrusions on computer networks and can also be used for SDN. In this study, a new testbed has been implemented for anomaly detection using machine learning algorithms in SDN. The developed system analyzes flows passing through the OpenFlow supported switch and tries to detect abnormal situations using the decision tree machine learning algorithm. The results show that the system constructed using the decision tree algorithm works successfully against Distributed Denial of Service (DDoS) attacks.

Keywords: *Software Defined Networking, Anomaly Detection, Machine Learning, POX Controller*

Yazılım Tanımlı Ağlarda Makine Öğrenimi ile Anomali Tespiti

ÖZET

Son yıllarda, bilgisayar ağlarını daha esnek bir hale getirmeyi amaçlayan Yazılım Tanımlı Ağ yaklaşımı ortaya çıkmıştır. Google'ın iç ağındaki Yazılım tanımlı ağ uygulaması, Yazılım Tanımlı Ağ yaklaşımının kullanışlılığını ve gelecek vadeden bir teknoloji olacağını kanıtlamasına rağmen güvenlik konusu göz ardı edilemeyecek hayati bir sorundur. SDN mimarisinde, Veri Düzlemini Kontrol Düzleminden ayrıldığı için saldırganlar artık üç düzlemden herhangi birinden ağa saldırabilirler. Makine öğrenimi algoritmaları, bilgisayar ağlarına yapılan saldırıları ve izinsiz girişleri tespit etmede kullanılan yöntemlerdir ve Yazılım Tanımlı Ağlar için de kullanılabilir. Bu çalışmada, Yazılım Tanımlı Ağlarda makine öğrenme algoritmaları kullanılarak anomali tespiti için yeni bir test düzeneği geliştirilmiştir. Oluşturulan sistem OpenFlow destekli anahtar cihazından geçen akışları inceler ve karar ağacı makine öğrenmesi algoritmasını kullanarak anormal durumları tespit etmeye çalışır. Elde edilen sonuçlar karar ağacı algoritması kullanılarak oluşturulan sistemin DDoS saldırılarına karşı başarılı bir şekilde çalıştığını göstermiştir.

Anahtar Kelimeler: *Yazılım Tanımlı Ağ, Anomali Tespiti, Makine Öğrenimi, POX*

Geliş: 13/06/2018, Düzeltme: 14/08/2018, Kabul: 18/09/2018