Abdurrahman KÜÇÜKKOÇ

Abdurrahman.kucukkoc@agu.edu.tr
0009-0008-5773-1978

Thesis Advisor

Associate Prof. Zafer Aydın

zafer.aydin@agu.edu.tr

06.05.2024

Analysing Network Traffic and Detecting Network Threats By Using The Algorithms of Machine Learning

As information technologies progress, the possibilities of access to information increase and therefore it becomes difficult to ensure the security of information. Today, with the use of information systems in all areas of life, network threats have also increased. The increase in individual access to and use of the internet has also brought network threats. In addition, the latest developments in information technologies, developing global communication networks, the internet of things aiming to connect all objects with networks, cloud technologies, the spread of mobile internet and the renewal of devices have brought network threats and uncertainties. Network threats increase the security vulnerabilities in the information and communication systems of individuals and organisations day by day. This situation causes systems to malfunction, economic damage and cyber security to be jeopardised. In order to contribute to individuals, institutions and organisations, our thesis aims to protect information systems against network threats, to ensure data confidentiality, integrity and accessibility, to detect network threats in advance and to take measures against these threats. We believe that by analysing heterogeneous network traffic, which includes most network attacks on the Internet, and using machine learning algorithms, we will reach a result close to reality in the detection of network threats. In line with this result, we will be able to take precautions against network threats in information systems and structures

Keywords: Network threats, Machine Learning, Security vulnerabilities

Bilgi teknolojileri ilerledikçe bilgiye erişim imkânları artmakta ve dolayısıyla da bilginin güvenliğinin sağlanması zorlaşmaktadır. Günümüzde bilişim sistemlerinin hayatın her alanında kullanılmaya başlanması ile birlikte ağ tehditleri de artmıştır. Bireysel olarak internete erişimin ve internet kullanımının artması ağ tehditlerini de beraberinde getirmiştir. Ayrıca bilişim teknolojilerindeki son gelişmeler, gelişen global iletişim ağları, tüm nesnelerin ağlarla birbirine bağlanmasını hedefleyen nesnelerin interneti, bulut teknolojileri, mobil internetin yaygınlaşması ve cihazların yenilenmesi ile birlikte ağ tehditleri ve belirsizlikleri de beraberinde getirmiştir. Ağ tehditleri bireyleri, kurumların bilgi ve iletişim sistemlerinde güvenlik zafiyetlerini her geçen gün arttırmaktadır. Bu durum sistemlerin çalışmamasına, ekonomik zarara ve siber güvenliğin tehlikeye girmesine neden olmaktadır. Birey, kurum ve kuruluşlara katkı sağlaması adına tez çalışmamız ağ tehditlerine karşı bilgi sistemlerini korumayı, veri gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına almayı, ağ tehditlerini önceden tespit etmeyi ve bu tehditlere karşı önlem almayı hedeflemektedir. İnternet üzerindeki çoğu ağ saldırılarını içeren heterojen ağ trafiğini analiz ederek ve makine öğrenmesi algoritmalarını kullanarak ağ tehditlerinin tespitinde gerçeğe yakın bir sonuca ulaşacağımıza inanıyoruz. Bu sonuç doğrultusunda bilişim sistem ve yapılarında ağ tehditlerine karşı önlemler almayı sağlayacağını düşünmekteyiz.

Anahtar kelimeler: Ağ saldırıları, Makine öğrenme, Güvenlik açıklıkları