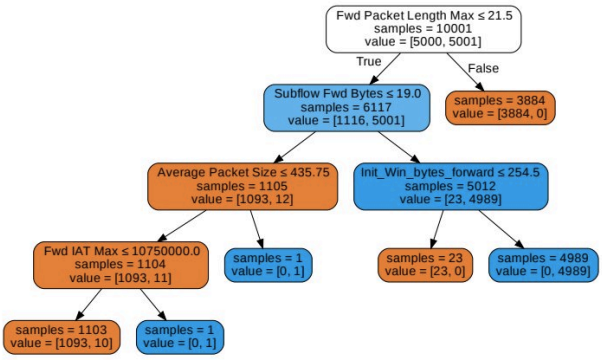
A new feature selection technique for intrusion detection systems

12 July 2021, by Ingrid Fadelli



Decision Tree based on the MICorr-selected features. Blue and orange nodes indicate DDoS and benign instances respectively. Credit: Kamalov et al.

Network-based technologies have become increasingly widespread, and they are now being used by countless individuals, professionals, and businesses worldwide. Despite their advantages, most network-based systems are highly vulnerable to malicious attacks.

The consequences of a malicious attack on network-based systems can be extremely severe and devastating. For instance, an attack on a power utility network could leave millions of individuals and offices without electricity, while attacks on social media networks can lead to breeches of confidential user information.

To overcome the vulnerabilities of network-based systems, computer scientists worldwide have been trying to develop advanced intrusion detection systems (IDSs) that could help to identify and counteract malicious attacks, increasing a network's safety. In recent years, machine learning (ML) algorithms have been found to be particularly promising for automatically detecting attacks and intrusions on a network's functioning.

A key step in the development and training of ML-based IDSs is the selection of data features that a model can rely or focus on when making predictions. Ideally, by analyzing large datasets, researchers should be able to identify the most suitable features for solving a given task using ML tools, and this is also applicable to intrusion detection.

Researchers at Canadian University Dubai in the UAE have recently developed a new feature selection method that could enable the development of more effective ML-based IDSs. This method, presented in a paper pre-published on arXiv, was found to perform remarkably well when compared with other commonly employed feature selection techniques.

"Our goal is to study feature selection in network traffic data with the aim of detecting potential attacks," Firuz Kamalov, Sherif Moussa, Rita Zgheib and Omar Mashaal, the researchers who carried out the study, wrote in their paper. "We consider various existing feature selection methods as well as propose a new feature selection algorithm to identify the most potent features in network traffic data."

Firstly, Kamalov and his colleagues analyzed a series of feature selection methods that could be used to detect features or characteristics of network traffic data that are relevant to intrusion detection. They specifically focused on three standard selection methods, known as correlation-based univariate, MI-based univariate, and correlation-based forward search algorithms.

Subsequently, the researchers developed a new feature selection method, dubbed MICorr, which addresses some of the limitations of existing feature selection techniques. They evaluated this method on the CSE-CIC-IDS2018 dataset, which contains 10,000 benign and malicious network intrusion instances.

"We propose a new feature selection method that addresses the challenge of considering continuous input features and discrete target values," the researchers explained in their paper. "We show that the proposed method performs well against the benchmark selection methods."

Using the features they identified as salient for intrusion detection, Kamalov and his colleagues created a highly efficient ML-based detection system. This system was found to be capable of discerning between DDoS (Distributed Denial of Service) attacks and harmless network signals with 99% accuracy.

In the future, the feature selection method developed by this team of researchers and the findings presented in their paper could inform the development of new, highly effective IDSs. In addition, the system they created using the features they identified could be implemented in real-world settings to detect malicious attacks on real networks.

More information: Feature selection for intrusion detection systems. arXiv:2106.14941 [cs.CR]. arxiv.org/abs/2106.14941

APA citation: A new feature selection technique for intrusion detection systems (2021, July 12) retrieved 28 January 2022 from https://techxplore.com/news/2021-07-feature-technique-intrusion.html