先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	サイバーレジリエンス構成学 （門林　雄基　（教授））		
学籍番号	2211009	提出日	令和 6年 1月 19日
学生氏名	荒木　亮介		
論文題目	Detecting DDoS Attacks on the Network Edge: Combination approach of Information-Theoretic and Correlation Analysis		

要旨

DDoS (Distributed Denial of Service) attacks have become a significant threat to cloud services. Attackers intentionally aim to reduce the availability of the target service by sending a vast number of malicious requests. A robust mitigation system is essential to combat these attacks. Our focus is on the network edge, which faces security challenges due to the increased usage of IoT devices. This includes DDoS attacks targeting the network edge. We propose an anomaly-based DDoS detection approach that combines information-theoretic metrics with multivariate correlation analysis. The information-theoretic metric assesses the randomness and complexity of traffic behavior, while multivariate correlation analysis examines the relationships among traffic features. By integrating these metrics, we create profiles for normal and attack traffic to train the system to estimate traffic density. These profiles are based on metrics that include Triangle Area Mapping (TAM) combined with correlation analysis, Rényi's divergence, covariance, mean, and standard deviation, which improve the detection capabilities. We evaluated the effectiveness of our method using testbed and benchmark datasets. The results indicate that our approach achieves higher accuracy by 0.17%, 2.32%, and 0.50% compared to the baseline methods on the testbed, UNSW, and CIC-DDoS datasets, respectively.