

## ABSTRAK

Nama : Muchamad Oktarin Jatmika  
NIM : 41518210001  
Pembimbing TA : Rahmat Budiarto, Dr. Prof  
Judul : Implementasi *Naive Bayes* Dan KNN Pada Deteksi Serangan DDOS Pada Jaringan Metro

*Peningkatan konsumsi data yang luas di masyarakat dan industri memicu operator jaringan yang ingin meningkatkan jaringan metro mereka dengan persyaratan bandwidth yang lebih tinggi. Penyedia layanan dan operator ditantang untuk menemukan cara yang sederhana, paling efisien dan hemat biaya untuk memenuhi permintaan dengan kecepatan dan standar baru yang akan datang. Serangan Distributed Denial of Service (DDoS) adalah serangan cyber yang menggunakan metode untuk membanjiri lalu lintas jaringan internet di server, sistem, atau jaringan yang menjadi sasaran serangan. Terjadinya serangan DDoS pada jaringan metro dapat membuat sistem operasi tidak dapat beroperasi dengan baik bahkan crash. DDoS dapat dicegah dengan memantau lalu lintas secara teratur, meningkatkan kapasitas sumber daya server, dan menerapkan beberapa strategi perlindungan. Makalah ini mengimplementasikan sistem deteksi serangan DDoS dengan menggabungkan Seleksi fitur Information Gain dan pengklasifikasi Naïve Bayes. Sebagai perbandingan, pengklasifikasi K-Nearest Neighbor (KNN) juga dipertimbangkan. Tujuan utamanya adalah untuk meningkatkan akurasi deteksi sehingga dapat membantu jaringan metro secara optimal menyediakan bandwidth yang diperlukan. Hasil eksperimen menggunakan dataset CICIDS-2018 menunjukkan bahwa KNN mengungguli classifier Naïve Bayes dengan tingkat akurasi 99%.*

Kata Kunci: Jaringan Metro, KNN, Naïve Bayes, Serangan DDoS

## ABSTRACT

Nama : Muchamad Oktarin Jatmika  
NIM : 41518210001  
Pembimbing TA : Rahmat Budiarto, Dr. Prof  
Judul : Implementasi *Naive Bayes* Dan KNN Pada Deteksi Serangan DDOS Pada Jaringan Metro

*Broad increase in data consumption in society and industry trigger network operators looking to upgrade their metro networks with higher bandwidth requirements. Service providers and operators are challenged to find a simple, the most efficient and cost-effective way of meeting the demand with new speeds and standards on the horizon. Distributed Denial of Service (DDoS) attack is a cyber attack that uses a method to flood internet network traffic on the server, system, or network of the targeted attack. The occurrence of DDoS attacks on the metro networks can make the operating system unable to operate properly and even crash. DDoS can be prevented by monitoring traffic regularly, increasing server resource capacity and implementing multiple protection strategies. This paper implements DDoS attacks detection system by combining Information Gain feature Selection and Naïve Bayes classifier. As comparison, K-Nearest Neighbor (KNN) classifier is also considered. The main aim is to improve the detection accuracy as such may help the metro network optimally provides the necessary bandwidth. Experimental results using CICIDS-2018 dataset show that the KNN outperforms Naïve Bayes classifier with the accuracy level 99%*

Keyword: Metro Network, DDoS attack, Naïve Bayes, KNN