# ABSTRAK

Dalam era perkembangan teknologi Wireless Sensor Network (WSN) dan Internet of Things (IoT), keamanan menjadi aspek krusial untuk melindungi jaringan dari berbagai serangan, salah satunya serangan virtual jamming. Serangan ini membahayakan kinerja jaringan sensor yang memiliki keterbatasan energi dan sumber daya. Penelitian ini mengusulkan penggunaan metode Naive Bayes (NB) sebagai solusi untuk mengatasi serangan virtual jamming di WSN. Berdasarkan penelitian sebelumnya, NB terbukti memiliki akurasi tinggi dalam konteks keamanan jaringan. Metode NB akan diimplementasikan melalui simulasi menggunakan NS-2, sebuah aplikasi untuk analisis aktivitas jaringan. Rencana percobaan mencakup penggunaan confusion matrix sebagai alat evaluasi, memungkinkan pengukuran performa deteksi serangan virtual jamming. Percobaan ini bertujuan untuk mengidentifikasi sejauh mana NB dapat membedakan antara serangan dan aktivitas normal dalam lingkungan jaringan. Dalam penelitian ini, diharapkan dapat memberikan kontribusi pada pengembangan keamanan, dalam menerapkan kecepatan perhitungan, algoritma sederhana, dan akurasi yang tinggi, terhadap keunggulan metode NB.

Kata Kunci: *Naive Bayes, virtual jamming, Wireless Sensor Network,* NS-2