BAB I. PENDAHULUAN

1.1. Latar belakang

Dalam perkembangan teknologi di masa ini, *Wireless Sensor Network* (WSN) telah memberikan kemudahan dalam berkomunikasi, memahami, dan mengontrol lingkungan sekitar. Oleh karena itu, WSN digunakan di berbagai lingkungan karena fitur-fiturnya. Karakteristik ini, dipadukan dengan kemampuan menghubungkan node ke Internet, menjadi dasar paradigma *Internet of Things* (IoT). WSN mengintegrasikan banyak sensor, node, router, dan gateway untuk mengkomunikasikan data melalui jaringan. Selain itu, semua node dalam jaringan memiliki akses Internet dan dapat dikelola dari jarak jauh [1]. WSN menghadapi banyak tantangan untuk memastikan keandalan jaringan, efisiensi energi, dan keakuratan data dalam jaringan. Karena sifat WSN yang *broadcast*, penyerang dapat mengeksploitasinya untuk melemahkan dan membahayakan kinerja jaringan.

Keamanan adalah aspek penting untuk melindungi jaringan dari serangan. Pentingnya keamanan di WSN dapat diukur dengan mempertimbangkan kerentanan WSN terhadap berbagai jenis serangan. Salah satu serangan umum terhadap WSN adalah serangan *virtual jamming. Virtual jamming* adalah serangan berbahaya karena memblokir saluran komunikasi nirkabel dengan menyediakan paket palsu dan membatasi frekuensi komunikasi radio dalam jaringan. Oleh karena itu, serangan ini menimbulkan ancaman serius terhadap jaringan sensor yang terdiri dari node dengan kebutuhan energi dan sumber daya yang rendah [2]. Penyerang *virtual jamming* dapat memblokir transmisi pada saluran nirkabel dengan memancarkan sinyal interferensi yang kuat [3].

Berdasarkan penelitian yang telah dilakukan oleh Anton dkk [4] sebelumnya menggunakan metode NB, hasil pengujian menunjukkan bahwa akurasi *Neural Network* sebesar 95.2381%, sedangkan NB mencapai 99.9%. Berdasarkan analisis, metode NB terbukti lebih baik dibandingkan dengan *Neural Network* dalam konteks ini. Metode NB mempunyai beberapa kelebihan, yaitu perhitungan yang cepat, algoritma yang sederhana, dan akurasi tinggi [4]. Metode NB hanya memerlukan sedikit data pelatihan untuk mengestimasi jumlah parameter yang dibutuhkan dalam *proses pengklasifikasian*. Algoritma NB juga mudah digunakan karena memiliki prosedur perhitungan yang sederhana [5].

Melalui penelitian ini, metode NB diusulkan sebagai solusi untuk mendeteksi serangan *virtual jamming*. Penelitian ini dilakukan menggunakan NS-2 yang adalah aplikasi untuk simulasi jaringan untuk dianalisa aktivitasnya. Selain itu, dalam

percobaan penelitian ini akan melibatkan penggunaan *confusion matrix*, sebuah alat evaluasi yang membantu mengukur performa deteksi serangan *virtual jamming*. *Confusion matrix* digunakan untuk mengidentifikasi dan memahami sejauh mana metode NB dapat secara akurasi membedakan antara serangan dan aktivitas normal dalam lingkungan jaringan.

1.2. Rumusan masalah

Berdasarkan latar belakang, rumusan masalah penelitian ini adalah:

A. Bagaimana mengimplementasikan NB untuk mendeteksi serangan virtual jamming?
B. Bagaimana performansi NB dalam mendeteksi serangan virtual jamming?

1.3. Tujuan

Tujuan dari penelitian ini, diantaranya:

A. Melakukan implementasi NB untuk mendeteksi serangan virtual jamming di NS-2.
B. Melakukan analisis akurasi performansi NB dalam mendeteksi serangan virtual jamming di NS-2.

1.4. Batasan Masalah

Penelitian ini dilakukan dengan menggunakan simulasi simulator NS-2.

1.5. Rencana Kegiatan

A. Studi Literatur

Kegiatan ini melibatkan pencarian, identifikasi, dan studi pustaka yang relevan terkait dengan topik penelitian, seperti metode NB, deteksi serangan *virtual jamming*, dan simulasi jaringan menggunakan NS-2. Tujuan utama studi literatur adalah memahami dasar teoritis dan penelitian terdahulu untuk merancang percobaan dengan informasi yang kuat.

B. Perancangan Percobaan

Kegiatan ini merupakan langkah perencanaan eksperimen dengan merinci parameter yang akan diuji, pemilihan skenario simulasi, dan tahapan implementasi metode NB. Perancangan percobaan juga mencakup pemilihan dataset, pemilihan ukuran sampel, dan pengaturan variabel yang diperlukan untuk mendukung pengujian yang akurasi.

C. Implementasi

Tahap implementasi melibatkan penerapan metode NB dalam lingkungan simulasi NS-2. Ini mencakup penulisan kode atau konfigurasi yang diperlukan untuk

menerapkan algoritma deteksi serangan *virtual jamming* dengan menggunakan metode NB.

D. Pengujian

Setelah implementasi, dilakukan serangkaian pengujian untuk mengevaluasi kinerja metode NB dalam mendeteksi serangan *virtual jamming*. Pengujian mencakup pengumpulan data, simulasi skenario, dan penerapan matrik evaluasi seperti confusion matrix untuk mengukur keberhasilan deteksi.

E. Analisis Data

Data yang diperoleh dari pengujian dievaluasi secara rinci. Proses analisis melibatkan interpretasi hasil pengujian, pengidentifikasian kelemahan, dan penentuan efektivitas metode NB dalam konteks deteksi serangan *virtual jamming*.

F. Penulisan Laporan

Tahap terakhir melibatkan penyusunan laporan penelitian. Laporan ini mencakup semua aspek dari studi literatur, perancangan percobaan, implementasi, pengujian, dan analisis data. Laporan memberikan konteks, metodologi, hasil, dan kesimpulan penelitian secara komprehensif.

1.6. Jadwal kegiatan

Jadwal kegiatan yang akan dilaksanakan selama periode 6 bulan dapat dilihat pada tabel 1.6.1.

Tabel 1.6.1 Rencana Kegiatan

	Bulan 1	Bulan 2	Bulan 3	Bulan 4	Bulan 5	Bulan 6
Studi Literatur						
Perancangan Percobaan						
Implementasi						
Pengujian						
Analisis Data						
Penulisan Laporan						