BAB I
PENDAHULUAN

1.1. Latar Belakang

Karakteristik Industri 4.0 dapat ditemukan dalam aplikasinya yang universal di berbagai sektor industri. Ini melibatkan aspek seperti *Internet of Things* (IoT), *Internet of Services, Internet of Media, big data*, komunikasi antar-mesin, dan sistem *cyber-physical* [1]. Revolusi industri 4.0 melibatkan kemajuan *Internet of Thing*s (IoT). Indonesia telah memasuki era revolusi industri 4.0 yang ditandai oleh adopsi teknologi informasi. Selain itu, kemajuan internet dan teknologi yang sangat cepat telah menjadi unsur kunci dalam konvergensi dan integrasi antara manusia dan mesin [2]. *Wireless Sensor Network* (WSN) telah muncul sebagai salah satu teknologi yang paling menjanjikan [3]. Pada tahun 2021, jumlah pengguna *Internet of Things* (IoT) mencapai 10 miliar di sektor industri. Diperkirakan angka ini akan meningkat pada tahun 2030, mencapai rentang antara 10 miliar hingga 25,4 miliar. Situasi ini dapat terjadi karena fokus utama pada teknologi *Internet of Things* (IoT) saat ini adalah pada *Wireless Sensor Network* (WSN) [4]. Penggunaan *Wireless Sensor Network* (WSN) menjadi elemen penting yang mendukung perkembangan IoT. Kehadiran *Wireless Sensor Network* (WSN) memberikan berbagai keuntungan dalam menangani tantangan, termasuk efisiensi energi dan mengatasi berbagai hambatan yang muncul. Penerapan *Wireless Sensor Network* (WSN) digunakan untuk penginderaan dan pemantauan, dengan mengintegrasikan sensor-sensor pada mesin kontrol melalui kabel dan nirkabel [5].

Sifat transmisi melalui saluran nirkabel membuatnya sangat rentan terhadap serangan *Denial of Service* (DoS). *Denial of Service* (DoS) menjadi suatu jenis serangan yang tujuannya mengganggu dari hak akses pengguna jaringan yang dilakukan secara kuat [13]. Dalam serangan *virtual jamming*, node jahat secara berkala mengirimkan paket RTS-CTS palsu dengan maksud menipu node lain dan memaksa mereka memperbarui *Network Allocation Vectors*, yang menyatakan bahwa saluran dalam keadaan sibuk untuk periode yang lama. Dampak dari *virtual jamming* ini secara substansial menurunkan *throughput* dari node yang sedang berkomunikasi, terutama jika sumber daya energi terbatas. Pengirim dan penerima

saling bertukar paket *Ready-To-Send* (RTS) dan *Clear-To-Send* (CTS) sebelum mengirimkan paket untuk melakukan request saluran selama periode transmisi yang sesungguhnya. Karena ketidakvalidan saluran, serangan (DoS) mudah dimanfaatkan dengan mengirimkan paket RTS/CTS palsu. Oleh karena itu, musuh dapat merancang serangan (DoS) hingga menyebabkan partisi dalam jaringan dengan tingkat energi yang sangat rendah, menghemat energi, dan meningkatkan masa pakai *virtual jammer*, yang tetap menjadi ancaman dalam jangka waktu yang lebih lama. Dampaknya termasuk penurunan signifikan dalam *throughput* dan kapasitas dari lalu lintas jaringan. Dalam upaya pendekatan yang dilakukan dengan menggabungkan pembelajaran mesin dan jaringan nirkabel. Menerapkan metode klasifikasi untuk mengenali node yang bersifat merugikan dan memulai *virtual jamming*, serta mengisolasi mereka dari node yang menunjukkan perilaku positif, bertujuan untuk mencegah serangan *Denial of Service* (DoS) [6].

Dalam riset ini, *Support Vector Machine* (SVM) dipilih karena menunjukkan tingkat akurasi yang jauh lebih tinggi jika dibandingkan dengan pengklasifikasi lain seperti regresi logistik [7]. Metode SVM ini menjadi salah satu klasifikasi yang paling sering digunakan dan dikenal dalam penelitian di berbagai bidang [16]. SVM membangun hyperplane di dalam ruang multidimensi untuk memisahkan kelas yang berbeda. Pendekatan SVM menghasilkan *hyperplane* optimal secara iteratif, yang dimanfaatkan untuk mengurangi kesalahan [7]. Menggunakan SVM Kernel memudahkan dalam memetakan data ke dimensi yang lebih tinggi, memungkinkan pemisahan data. Kernel berperan dalam mengubah ruang data dari dimensi yang rendah menjadi dimensi yang lebih tinggi [8].

1.2. Perumusan Masalah

Berdasarkan latar belakang di atas, penulis dapat mengenali permasalahan sebagai berikut:

1. Bagaimana cara mengimplementasikan algoritma SVM dalam mendeteksi serangan terhadap *virtual jamming*?
2. Bagaimana performansi algoritma SVM dalam mendeteksi dan mengklasifikasikan serangan terhadap *virtual jamming*?

1.3. Tujuan

Adapun tujuan penelitian yang dilakukan mengenai ”Perlindungan Terhadap *Virtual Jamming* Menggunakan *Support Vector Machine* (SVM)” adalah sebagai berikut:

1. Melakukan implementasi SVM dalam mendeteksi serangan terhadap *virtual jamming* dengan dataset yang di *generated* di NS-2.
2. Mengetahui kinerja atau performansi algoritma SVM dalam mendeteksi dan mengklasifikasikan serangan terhadap *virtual jamming*.

1.4. Hipotesis

Dalam sebuah penelitian yang bertujuan untuk menyelidiki adanya serangan berupa paket palsu terhadap *virtual jamming* yang menghambat lalu *lintas Wireless Sensor Networ*k (WSN) dengan metode *Support Vector Machine* (SVM) pengklasifikasian terbaik. Diduga dalam penelitian ini mungkin menyatakan bahwa metode *Support Vector Machine* (SVM) bukan menjadi pengklasifikasian terbaik untuk mengatasi serangan paket palsu terhadap *virtual jamming* dengan *Wireless Sensor Network* (WSN) yang menghambat lalu lintas jaringan.

1.5. Batasan Masalah

Penelitian ini dibuat memiliki batasan masalah, dengan penggunaan algoritma *Support Vector Machine* (SVM) menggunakan simulator jaringan NS-2.

1.6. Rencana Kegiatan

Jadwal kegiatan dalam penulisan ini dibuat agar setiap tahapan proses penulisan dapat direncanakan dengan mudah secara sistematis dan terorganisir.

Table 1 Rencana Kegiatan

Kegiatan	**Bulan**					
	1	2	3	4	5	6
Studi Literatur						
Analisis Permasalahan						
Perancangan Percobaan						
Implementasi						
Penulisan Laporan						