BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan Sensor Nirkabel (JSN) merupakan jaringan nirkabel yang terbentuk atas kumpulan sensor, yang disebut simpul-simpul, yang saling berkomunikasi untuk mengindra dan mengontrol lingkungan sekitar (Kocakulak dan Butun, 2017). Kontrol ini dapat dilakukan karena tiap simpul pada JSN mampu untuk memproses sifat fisik hal-hal yang dapat diindera serta mengirimkan informasi tersebut kepada sistem kontrol pusat agar dapat diproses lebih lanjut dan kemudian menghasilkan respon (Modieginyane dkk., 2017).

Aplikasi penggunaan JSN pada kehidupan sehari-hari saat ini dapat dianggap sebagai sistem kritis karena menangani data yang sensitif dan informasi yang penting (Radhappa dkk., 2017). Radhappa dkk. (2017) juga mengungkapkan bahwa perkembangan JSN pada dekade ini sedang mencapai puncaknya. Aplikasinya pun luas meliputi keamanan lingkungan hidup, pengawasan kekokohan struktur, pengawasan hewan, pertanian presisi, dan implementasi pada bangunan pintar (Jino Ramson dan Moni, 2017; Radhappa dkk., 2017). Setiap simpul pada JSN dilengkapi dengan alat komputasi, penginderaan, manajemen tenaga, serta alat untuk mengirim dan menerima sinyal radio, sehingga sensor-sensor tersebut dapat saling berkomunikasi dengan sinyal radio secara nirkabel (Kocakulak dan Butun, 2017). Pada saat ini, alat-alat yang memanfaatkan sinyal radio bisa didapatkan dengan mudah dan harga rendah karena ketersediaannya yang besar di pasaran, dan oleh karena itu pengguna yang tidak bertanggung jawab dapat dengan mudah

menggunakan alat-alat tersebut untuk melancarkan serangan terhadap jaringan nirkabel (Pinto dkk., 2018).

Salah satu serangan yang dapat terjadi terhadap jaringan nirkabel adalah serangan *denial-of-service* (DoS), yang memiliki karakteristik membanjiri target dengan serangkaian permintaan palsu dalam jumlah besar dengan tujuan untuk membuat target kelebihan beban, sehingga tidak sanggup menangani permintaan asli yang datang (Gu dkk., 2019; Osanaiye dkk., 2018). Gu dkk. (2019) juga menambahkan bahwa pada saat ini, jumlah serangan DoS meningkat secara signifikan dan dalam jumlah besar.

Serangan DoS pada JSN dapat terjadi pada kelima lapisan protokol TCP/IP dan memiliki jenis yang bermacam-macam, tetapi penelitian oleh Gunduz dkk. (2015) mengungkapkan bahwa serangan DoS pada lapisan *network* (jaringan) merupakan serangan yang memiliki ragam paling banyak. Lebih dari itu, aplikasi JSN mengharuskan penempatan alat-alat sensor tersebut berada pada tempat yang ekstrem dan sulit dijangkau oleh manusia (Almomani dan Mamdouh, 2018; Revathi dan Anjana, 2019). Pada penelitian yang dilakukan oleh Kim dkk. (2011), diketahui bahwa ketidakefektifan penanganan serangan DoS disebabkan oleh kesalahan konfigurasi serta tidak tersedianya sumber daya untuk turut mengikuti perubahan dinamis jaringan, tanpa interferensi manusia. Hal ini menyebabkan solusi otomasi, yang dapat mengoperasikan penanganan terhadap serangan berdasarkan pada sifat dan karakteristik lalu lintas jaringan, perlu digunakan (Filho dkk., 2019). Solusi otomasi ini dapat direalisasikan dengan menggunakan *machine learning* (pembelajaran mesin).

Banyak metode atau algoritma yang dapat digunakan untuk menganalisis serangan DoS. Tan dkk. (2019), Wankhede dan Kshirsagar (2018), dan Mourabit dkk. (2015) melakukan perbandingan berbagai teknik *machine learning* untuk mengklasifikasi serangan pada JSN. Berdasarkan ketiga penelitian tersebut, metode Random Forest (RF) menghasilkan performa terbaik dibandingkan beberapa metode klasifikasi lain, seperti *Naïve Bayes*, *Multi-Layer Perceptron*, dan *Support Vector Machine*. Metode RF adalah metode *ensemble* yang menggunakan *decision tree* sebagai basis klasifikasi yang dilakukan (Tan dkk., 2019). Algoritma RF tidak memerlukan pemangkasan *tree* serta kebal terhadap masalah *overfitting* (Wankhede dan Kshirsagar, 2018). RF juga tidak rentan terhadap data *noise* dan data yang tidak valid, serta memiliki skalabilitas yang baik untuk menangani masalah klasifikasi yang memiliki dimensi tinggi (Tan dkk., 2019).

Implementasi algoritma RF ditingkatkan menggunakan *Synthetic Minority Oversampling Technique* (SMOTE). SMOTE merupakan teknik *oversampling* yang diusulkan oleh Chawla dkk. (2002) untuk mengatasi masalah data yang *imbalance* atau tidak seimbang (Tan dkk., 2019). Tan dkk. (2019) memaparkan bahwa SMOTE merupakan teknik yang optimal karena mampu mengurangi batasan metode *sampling* sebelumnya dengan menggunakan teori dasar matematika interpolasi linear. Penelitian tersebut dan beberapa penelitian lain oleh Abdoh dkk. (2018) dan Tao dkk. (2021) juga memberikan kesimpulan bahwa penggunaan teknik SMOTE memberikan hasil klasifikasi yang lebih akurat pada algoritma RF.

Penelitian lain telah dilakukan oleh Almomani dkk. (2016) dengan menggunakan *dataset* yang digunakan juga pada penelitian ini. Penelitian tersebut mengimplementasikan *Multilayer Perceptron* (MLP) untuk melakukan klasifikasi

serangan *DoS* terhadap lapisan jaringan pada JSN. Hasil akurasi yang didapatkan adalah 92.8%, 99.4%, 92.2%, 75.6%, dan 99.8% untuk lima buah kelas klasifikasi yang terdapat pada *dataset* tersebut.

Berdasarkan latar belakang di atas, penelitian ini berfokus pada implementasi metode SMOTE dan algoritma RF untuk mendeteksi serangan *DoS* terhadap lapisan jaringan pada JSN.

1.2 Rumusan Masalah

Berdasarkan latar belakang, rumusan masalah yang diangkat pada penelitian ini adalah sebagai berikut.

1. Bagaimanakah mengimplementasikan metode SMOTE dan algoritma *Random Forest* untuk mendeteksi serangan *denial-of-service* pada jaringan sensor nirkabel?
2. Berapakah tingkat *True Positive Rate* (TPR), *True Negative Rate* (TNR), *False Positive Rate* (FPR), *False Negative Rate* (FNR), *accuracy*, dan *precision* dari implementasi metode SMOTE dan *Random Forest* untuk mendeteksi serangan *denial-of-service* pada jaringan sensor nirkabel?

1.3 Batasan Masalah

Beberapa batasan masalah dalam penelitian ini adalah sebagai berikut.

1. Dataset yang digunakan pada penelitian ini adalah WSN-DS yang dikembangkan oleh Almomani, I., Al-Kasasbeh, B., dan Al-Akhras, M. (2016).

2. Kategori serangan yang diteliti adalah serangan *denial-of-service* yang dapat terjadi pada lapisan jaringan dalam jaringan sensor nirkabel yang mengimplementasikan protokol *Low-Energy Aware Cluster Hierarchy* (LEACH), yaitu *Blackhole Attack, Grayhole Attack, Flooding Attack,* dan *Scheduling* atau TDMA *Attack.*
3. Penelitian ini tidak menghasilkan sebuah *Intrusion Detection System* (IDS).

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut.

1. Mengimplementasikan metode SMOTE dan algoritma *Random Forest* untuk mendeteksi serangan *denial-of-service* pada jaringan sensor nirkabel.
2. Mengukur tingkat *True Positive Rate* (TPR), *True Negative Rate* (TNR), *False Positive Rate* (FPR), *False Negative Rate* (FNR), *accuracy*, dan *precision* dari implementasi metode SMOTE dan *Random Forest* untuk mendeteksi serangan *denial-of-service* pada jaringan sensor nirkabel.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini dapat dijabarkan sebagai berikut.

1. Membantu pengembangan sistem deteksi intrusi yang optimal, khususnya untuk serangan *denial-of-service* pada lapisan jaringan dalam jaringan sensor nirkabel.

2. Memberikan pengetahuan secara umum terkait jaringan sensor nirkabel, serangan *denial-of-service* pada lapisan jaringan dalam jaringan sensor nirkabel, dan memberikan simulasi klasifikasi serangan *denial-of-service* tersebut berdasarkan sampel data yang ada.

1.6 Sistematika Penulisan

Sistematika penulisan laporan adalah sebagai berikut.

BAB 1 Pendahuluan

Pendahuluan terdiri dari latar belakang masalah, rumusan masalah, batasan permasalahan, tujuan penelitian, dan manfaat penelitian. Secara garis besar, isi pendahuluan memberikan gambaran terhadap ide pokok dan alasan penyusunan penelitian ini.

BAB 2 Landasan Teori

Landasan Teori membahas topik-topik terkait penggunaan SMOTE dan Random Forest untuk mendeteksi serangan *denial-of-service* pada jaringan sensor nirkabel, yaitu protokol pada jaringan sensor nirkabel, jenis-jenis serangan *denial-of-service* pada lapisan jaringan dalam jaringan sensor nirkabel, metode SMOTE, algoritma *decision tree*, algoritma Random Forest, dan parameter evaluasi performa.

BAB 3 Metodologi Penelitian

Metodologi Penelitian menjelaskan metodologi atau langkah-langkah yang dilakukan dalam melakukan penelitian ini. Selain itu, Metodologi Penelitian juga

berisi *flowchart* aplikasi dan algoritma, serta rancangan antarmuka aplikasi yang digunakan pada penelitian ini.

BAB 4 Hasil dan Diskusi

Hasil dan Diskusi menjelaskan inti penelitian yang terdiri dari hasil penelitian dan analisis yang telah dilakukan. Hasil penelitian dan analisis disajikan dalam bentuk gambar, tabel, dan tulisan yang menjelaskan secara rinci hasil yang telah didapatkan.

BAB 5 Simpulan dan Saran

Bagian ini merupakan bagian penutup yang berisi simpulan dan saran dari penelitian yang telah dilakukan