BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Evolusi pada teknologi jaringan telekomunikasi telah melahirkan *Internet of Things* (*IoT*) atau disebut juga dengan komunikasi *Machine-to-Machine* (*M2M*) [1]. Entitas *IoT* memiliki karakteristik dengan *resource* (*memory*, *storage*, dan daya) yang terbatas [2]. Salah satu protokol yang mendukung keterbatasan *IoT* ialah *Message Queuing Telemetry Transport* (*MQTT*). *MQTT* menggunakan pola komunikasi *publish/subscribe* sehingga membutuhkan *broker* sebagai penghubung antara *subscriber* dengan *publisher* [3]. Keterbatasan pada *MQTT* menyebabkan jaringan rentan terhadap serangan [4] sehingga sistem keamanan standar yang digunakan *MQTT* ialah *SSL/TLS*. Namun, *SSL/TLS* tidak mampu menangani beberapa serangan, salah satunya adalah serangan *Denial of Service* (*DoS*) [5]. *DoS* merupakan salah satu serangan yang populer digunakan [1]. Pada tahun 2017 dan 2018, *DoS* berada pada urutan tiga teratas yang menyebabkan kerugian terbesar pada sektor industri [6]. Salah satu metode untuk menghadapi serangan *DoS* ialah dengan menggunakan *Intrusion Detection System* (*IDS*) [7].

Implementasi *IDS* dapat dilakukan menggunakan beberapa algoritma berikut, yaitu *fuzzy logic* [1], *machine learning* [8], *deep learning* [9], atau *blockchain* [10]. Penerapan *fuzzy logic* pada protokol *MQTT* merupakan pilihan yang sesuai karena memiliki beberapa keunggulan. Pertama, memiliki pendekatan yang baik untuk *decision making problem*. Kedua, implementasi yang mudah dan sederhana [11].

Tugas akhir ini membuat *IDS* menggunakan algoritma *fuzzy logic* untuk mendeteksi *DoS* pada jaringan *IoT* berbasis protokol *MQTT*. *Fuzzy* akan ditanam pada salah satu *node* jaringan dan akan melakukan *subscribe* topik mengenai *broker status* sehingga *broker* akan mengirim informasi alir trafik *MQTT* secara berkala dengan bantuan *nodes feature selection*. Kemudian *fuzzy* akan memilah trafik *MQTT* yaitu *SUBSCRIBE* dan *SUBACK* sebagai variabel *input* sehingga *fuzzy* mampu memantau kondisi jaringan terhadap serangan *DoS*. Penggunaan *node fuzzy*

pada jaringan *IoT* berbasis protokol *MQTT* diharapkan mampu mendeteksi serangan *DoS* dengan akurat.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, dapat dirumuskan beberapa permasalahan pada tugas akhir ini, yaitu:

1. Bagaimana cara mendapatkan informasi tentang alir trafik jaringan IoT berbasis protokol *MQTT* dari *broker*?
2. Bagaimana mendeteksi serangan *DoS* menggunakan algoritma *fuzzy logic* berdasarkan trafik *SUBSCRIBE* dan *SUBACK* sebagai variabel *input*?
3. Parameter apa saja yang diperlukan untuk mengukur kinerja algoritma *fuzzy logic* saat mendeteksi serangan *DoS*?
4. Bagaimana kinerja algoritma *fuzzy logic* mendeteksi serangan *DoS*?

1.3 Tujuan dan Manfaat

Tujuan dari tugas akhir ini antara lain:

1. Membuat algoritma *fuzzy logic* yang dapat memantau alir trafik jaringan *IoT* berbasis protokol *MQTT*.
2. Mendeteksi serangan *DoS* pada jaringan *IoT* berbasis protokol *MQTT* menggunakan algoritma *fuzzy logic* berdasarkan trafik *SUBSCRIBE* dan *SUBACK* sebagai variabel *input*.
3. Parameter yang digunakan untuk mengevaluasi kinerja algoritma *fuzzy logic* yaitu *False Positive Ratio* (*FPR*), *accuracy*, *precision*, *recall*, dan *f-score*.
4. Mengetahui kinerja algoritma *fuzzy logic* saat mendeteksi serangan *DoS* pada jaringan *IoT* berbasis *MQTT*.

Manfaat dari tugas akhir ini yaitu dapat mengetahui kinerja algoritma *fuzzy logic* saat mendeteksi serangan *DoS* pada jaringan *IoT* berbasis protokol *MQTT*.

1.4 Batasan Masalah

Batasan masalah pada tugas akhir ini antara lain:

1. Protokol yang digunakan pada jaringan *IoT* adalah protokol *MQTT*.

2. *Quality of service* yang digunakan pada protokol *MQTT* adalah 0.
3. Lebar *bandwidth* yang digunakan merupakan *bandwidth* ideal.
4. Tugas akhir ini hanya mendeteksi serangan *DoS*.
5. Tugas akhir ini menggunakan trafik *SUBSCRIBE* dan *SUBACK* sebagai variabel *input*.
6. Parameter yang digunakan untuk mengukur kinerja algoritma *fuzzy logic* antara lain *False Positive Ratio* (*FPR*), *accuracy*, *precision*, *recall*, dan *f-score*.
7. Tugas akhir ini menggunakan simulator jaringan *COOJA* pada operasi sistem *Contiki-NG*.
8. *Broker* yang digunakan pada tugas akhir ini ialah *Mosquitto v3.1*.
9. Menggunakan empat macam skenario, yaitu 15, 20, 25, dan 30 *nodes*.
10. Setiap skenario menggunakan 20% *nodes* peyerang dari *nodes* keseluruhan dengan interval serangan 3, 5, 7, dan 9 detik.
11. Algoritma *fuzzy logic* ditanam pada salah satu *node* jaringan *IoT*.
12. Menggunakan lima *nodes* tambahan untuk membantu *node fuzzy* mengamati alir trafik *MQTT* pada jaringan *IoT* secara berkala.

1.5 Metode Penelitian

Metodologi yang dilakukan pada tugas akhir ini antara lain:

1. Studi Literatur

   Mengumpulkan, mempelajari, dan merangkum teori dari buku ataupun jurnal yang berkaitan dengan algoritma *fuzzy logic*, serangan *DoS*, jaringan *IoT*, dan protokol *MQTT*.

2. Simulasi

   Simulator jaringan *COOJA* akan digunakan untuk mensimulasikan algoritma *fuzzy logic* pada jaringan *IoT* berbasis protokol *MQTT*.

3. Eksperimental

   Melakukan uji coba dengan mengubah jumlah *node* pada simulator jaringan *COOJA* sehingga dapat mengetahui pengaruh jumlah *node* terhadap tingkat akurasi algoritma *fuzzy logic* saat mendeteksi serangan *DoS* pada jaringan *IoT* berbasis protokol *MQTT*.

4. Kuantitatif

   Hasil pengukuran tingkat akurasi algoritma *fuzzy logic* saat mendeteksi serangan *DoS* berbasis protokol *MQTT* akan dimuat dalam suatu grafik sehingga mempermudah saat pengumpulan data.

5. Pengumpulan Data

   Data tingkat akurasi yang diperoleh dari hasil simulasi deteksi serangan *DoS* akan dikumpulkan dalam bentuk grafik dengan parameter acuan antara lain *False Positive Ratio* (*FPR*), *accuracy*, *precision*, *recall*, dan *f-score* dengan variabel *input* yaitu trafik *SUBSCRIBE* dan *SUBACK*.

6. Penarikan Kesimpulan

   Pada tahap ini dilakukan penarikan kesimpulan terhadap tingkat akurasi algoritma *fuzzy logic* saat mendeteksi serangan *DoS* berdasarkan grafik yang telah didapat.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan pada pengerjaan tugas akhir ini ialah sebagai berikut:

1. BAB I PENDAHULUAN

   Bab yang menguraikan latar belakang masalah, rumusan masalah, tujuan dan manfaat, batasan masalah, metode penelitian, serta sistematika penulisan.

2. BAB II TINJAUAN PUSTAKA

   Bab yang membahas teori-teori dasar yang berhubungan dengan Jaringan *IoT*, Protokol *MQTT*, algoritma *fuzzy logic*, serangan *DoS*, serta Simulator *COOJA*.

3. BAB III MODEL SISTEM DAN PERANCANGAN

   Bab yang menguraikan rancangan sistem, parameter, dan hal-hal harus dipersiapkan sebelum melakukan pengujian.

4. BAB IV PENGUJIAN DAN ANALISIS SITEM

   Bab yang menguraikan, menganalisis, dan mencatat hasil uji coba dari skenario yang digunakan.

5. BAB V KESIMPULAN DAN SARAN

Bab yang menguraikan kesimpulan yang telah didapat berdasarkan hasil uji coba tugas akhir ini serta saran-saran yang diperlukan untuk pengembangan lebih lanjut.