BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi yang berkembang saat ini tentu sangat mempermudah manusia dalam melakukan berbagai aktivitas sehari-hari, diantaranya mengakses data ataupun informasi. Dengan memanfaatkan perkembangan jaringan internet pada saat ini, pengguna dapat mengakses informasi dengan cepat, mudah, serta akurat. Cara memperoleh data atau informasi tersebut adalah dengan mengakses internet. Saat ini ada beberapa macam tipe koneksi ke internet, salah satunya adalah koneksi tanpa menggunakan kabel (*wireless*). Teknologi ini adalah perkembangan dari teknologi jaringan komputer lokal (*Local Area Network*) yang memungkinkan efisiensi dan implementasi dari perkembangan jaringan komputer yang dapat meningkatkan mobilitas *user* dan dapat menggantikan keterbatasan dari media kabel. Pada awalnya, teknologi *wireless* ini ditemukan oleh IBM pada tahun 1970 (ISP Telematika, 2017). Pada saat itu IBM bekerja sama dengan perusahaan *Hewlett-Packard* (HP) untuk menguji WLAN RF (frekuensi radio). Namun, hasilnya belum sesuai standar IEEE (*Institute of Electrical and Electronics Engineer*) untuk membangun suatu LAN yaitu 1Mbps (Santoso, 2012).

Dengan teknologi yang canggih pada saat ini, internet sudah menjadi bagian dari hidup manusia. Salah satu pemanfaatan kecanggihan internet saat ini adalah munculnya konsep *Internet of Things* (IoT). IoT ini adalah konsep tentang menghubungkan perangkat agar terintegrasi satu sama lain. Seperti contohnya *smartphone*, lampu, mesin cuci bahkan mobil sekalipun. Bahkan *IoT* juga diterapkan pada komponen mesin seperti pesawat terbang, robot militer dan lain-lain (Yana, 2016).

Salah satu penerapan teknologi *wireless* dan sekaligus menerapkan tentang *Internet of Things* adalah teknologi jaringan sensor nirkabel atau WSN (*Wireless Sensor Network*). WSN adalah teknologi yang terdiri dari perangkat kecil dengan daya rendah yang mengintegrasikan kemampuan algoritma, sensor dan komunikasi yang terbatas (Abdullah, Rahman, & Roy, 2015).

Tujuan utama penggunaan WSN adalah untuk pemantauan dan pengumpulan informasi jarak jauh (Abdullah dkk., 2015). WSN biasanya digunakan pada lingkungan terbuka dan tidak terkendali atau di dalam wilayah yang kurang bersahabat, saat ini WSN dikembangkan untuk diterapkan pada pemantauan lingkungan, pemantauan jembatan, pemantauan aktivitas gunung api, komponen pendukung smart city, atau juga bisa pada pemantauan dan kontrol aktivitas di bidang pertanian (Abdullah dkk., 2015).

Pada WSN sulit untuk mengimplementasikan pertahanan, dikarenakan tingkat pemrosesan dan sumber daya yang terbatas. Oleh karena itu WSN rentan terhadap serangan. Serangan pada WSN dapat dibagi menjadi dua, yaitu serangan aktif dan serangan pasif. Serangan aktif adalah serangan yang dapat menyebabkan gangguan fungsi normal jaringan, dengan menghapus atau modifikasi informasi, contoh dari serangan aktif adalah *jamming*, *impersonating*, modifikasi, dan *denial of service (DoS)* (Lupu & Parvan, 2009). Sedangkan serangan pasif adalah serangan dengan mendapatkan data tanpa mengganggu aktifitas pertukaran data yang ada pada jaringan tersebut, contoh dari serangan pasif adalah *eavesdropping*, *traffic analysis*, dan *traffic monitoring* (Lupu & Parvan, 2009). Protokol *routing* yang digunakan untuk WSN sangat sederhana dan sangat rentan terhadap serangan (ErVICES, Cesana, & Milano, 2003). Sebagian besar serangan *routing* adalah *hello flood attack*, *sybil attack*, *wormhole attack*, *blackhole attack* dan *selective forwarding attack* (ErVICES dkk., 2003). Beberapa serangan memanipulasi data pengguna secara langsung dan beberapa serangan mempengaruhi protokol *routing* (ErVICES dkk., 2003).

Salah satu serangan yang menyerang pada *network layer* adalah *hello flood attack*. *Hello Flood Attack* membanjiri *node-node* tetangga dengan *hello messages*, sehingga energi yang dimiliki *node* tetangganya berkurang hingga habis. *Node* tersebut menyebarkan *hello messages* yang digunakan untuk meyakinkan bahwa *node* tersebut adalah tetangganya (Dubey, Meena, & Gaur, 2014).

Solusi yang dapat dilakukan jika terjadi *hello flood attack* salah satunya adalah dengan cara menerapkan *Intrusion Detection System (IDS)* berbasis

signature approach. IDS akan mendeteksi jika terdapat serangan pada WSN. Usulan yang ditambahkan pada tugas akhir ini adalah dengan menggunakan *system shutdown* yang ditambahkan pada WSN. Ketika *hello flood attack* menyerang WSN, IDS *signature approach* akan mendeteksi serangan tersebut, kemudian WSN melakukan *shutdown sink node*.

I.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah yang dikaji pada penelitian ini adalah sebagai berikut :

1. Bagaimana performa IDS dengan *signature based approach* yang diterapkan pada WSN dalam memitigasi serangan *hello flood* ?
2. Bagaimana performa WSN setelah mengimplementasikan *signature based IDS* dan *system shutdown*?
3. Bagaimana mengantisipasi serangan *hello flood* menggunakan IDS *signature based* dengan *System Shutdown* pada WSN?

I.3 Tujuan Penelitian

Tujuan adanya penelitian ini adalah sebagai berikut :

1. Mengetahui performa sistem IDS *signature based* dalam mendeteksi serangan *hello flood* pada WSN.
2. Mengetahui performa WSN setelah mengimplementasikan *signature based IDS* dan *system shutdown*.
3. Mengimplementasikan sistem IDS *Signature Based* dan *system shutdown* pada WSN.

I.4 Batasan Penelitian

Adapun batasan masalah pada penelitian ini sebagai berikut :

1. Penelitian ini menggunakan 49 *nodes* dan luas area 1600m x 1600m, dan hanya terdapat 1 *sink node*.
2. Mitigasi *hello flood* menjadi fokus utama dalam penelitian ini.
3. Penelitian ini hanya mensimulasikan pengiriman data dari satu *source node* ke *sink node*.

4. Spesifikasi dan konfigurasi *sink node* sama dengan *node* lain.
5. Metode *routing* yang digunakan penulis pada penelitian ini adalah AODV.
6. Pada penelitian ini penulis menggunakan simulator NS2.
7. Pada penelitian ini serangan *hello flood* tertanam pada beberapa *node* di WSN.
8. Pada penelitian ini hanya dilakukan pengukuran konsumsi energi dan performa jaringan meliputi *throughput*, *delay*, dan *packet loss*.
9. Sistem keamanan usulan WSN pada penelitian ini adalah *system shutdown* pada *sink node*.
10. *Node* pengirim adalah *node* 0, dan *node* penerima adalah *node* 42.
11. *System Shutdown* pada penelitian ini hanya sebagai langkah pengamanan sementara dalam menangani serangan *hello flood*.

I.5 Manfaat Penelitian

Manfaat yang didapatkan dari penelitian ini adalah sebagai berikut :

1. Mampu menunjukkan performa signature based IDS dalam mendeteksi serangan *hello flood*.
2. Mampu menunjukkan performa WSN yang lebih baik.
3. Mampu mengimplementasikan *Signature Based IDS* dan *system shutdown* pada WSN.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi tentang uraian latar belakang, rumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini berisi tentang literatur yang relevan dengan permasalahan yang dihadapi, penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sedang dilakukan.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi tentang penjelasan mengenai langkah-langkah penelitian yang dilakukan secara rinci yang dimulai dari tahap awal, tahap simulasi, tahap analisis dan tahap akhir dari penelitian.

BAB IV PERANCANGAN SISTEM

Bab ini menjelaskan tentang rancangan sistem meliputi spesifikasi software dan hardware, parameter sistem, perancangan topologi dan skenario pengujian.

BAB V PENGUJIAN DAN ANALISIS SISTEM

Bab ini menjelaskan hasil dari pengujian, meliputi hasil pengujian skenario I, skenario II, dan skenario III, serta analisis hasil pengujian setiap skenario.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang dapat diambil dari pengujian yang dilakukan, serta saran untuk penelitian selanjutnya.