BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi informasi dan komunikasi saat ini telah menjadi kebutuhan primer bagi masyarakat. Maka dari itu dikembangkan teknologi *wireless* yang memungkinkan kita untuk mendapatkan informasi dimana saja dan kapan saja. *Wireless* adalah suatu teknologi dimana manusia dapat berkomunikasi baik secara langsung maupun tidak langsung menggunakan media udara (gelombang elektromagnetik). Pada awalnya teknologi *wireless* ditemukan yaitu pada tahun 1970an oleh IBM dalam pembuatan rancangan WLAN (Atma, 2012). Seiring berjalannya waktu penggunaan *wireless* pun semakin beragam, mulai dari telepon seluler, GPRS navigasi, *mouse* dan *keyboard* nirkabel, televisi, *wireless* LAN atau Wi-Fi.

Dengan perkembangan teknologi *wireless* yang semakin pesat mengakibatkan penerapan teknologi *wireless* juga merambah ke berbagai bidang, salah satunya adalah pemanfaatan teknologi *wireless* pada konsep *Internet of Things* (IoT). Secara umum IoT adalah konsep untuk menghubungkan perangkat-perangkat pintar (*smart object*), sehingga dapat berinteraksi dengan perangkat lain dan lingkungan melalui jaringan internet (Meutia, 2015). Pemanfaatannya sudah banyak ditemui dimanapun mulai dari *smart house*, *smart city*, *smart car*.

Salah satu teknologi yang digunakan pada IoT merupakan pemanfaatan dari *wireless* yaitu *Wireless Sensor Network* (WSN). WSN merupakan sekumpulan sensor otomatis yang tersebar di berbagai tempat, dimana pada setiap titik sensor dilengkapi dengan alat komunikasi *wireless*. Sensor-sensor ini bekerja bersama-sama untuk melakukan pemantauan kondisi lingkungan sekitar seperti suhu, suara, getaran, tekanan, dan lain-lain. Dengan adanya WSN ini maka dalam melakukan pemantauan tidak perlu untuk mendatangi tempat yang dimaksud, karena *node* sensor yang telah disebar akan mengirimkan data ke *base station* sehingga dapat melakukan aktivitas pemantauan dari jarak jauh serta dapat melakukan tindakan dengan lebih cepat dan tepat (Ioannou, Vassilioi, & Sergiou, 2017).

Namun dikarena *node* sensor yang tersebar di ruang terbuka, hal ini menjadi salah satu kerentanan bagi WSN yang dapat di serang oleh pihak-pihak yang tidak bertanggung jawab. Keamanan dalam WSN menjadi sangat penting karena berkaitan dengan data. *Node* sensor yang mengalami gangguan dapat menyebabkan informasi yang dikirim tidak akurat atau menyesatkan, sehingga tujuan dari jaringan itu sendiri tidak tercapai. Berbagai teknik keamanan pada jaringan kabel (*wired*) telah dikembangkan untuk digunakan pada WSN. Namun hal itu tidak mudah dilakukan karena *node* sensor *wireless* memiliki daya, memori dan CPU yang kecil sehingga memerlukan sistem keamanan yang sesuai untuk mendeteksi dan memitigasi serangan yang ada (Ioannou, Vassilioi, & Sergiou, 2017).

Serangan pada WSN dapat dibedakan menjadi dua yaitu serangan pasif dan serangan aktif. Serangan pasif adalah serangan dengan memantau dan mendengarkan saluran komunikasi oleh penyerang yang tidak memiliki hak akses. Serangan jenis ini bertujuan untuk mengumpulkan informasi penting yang bisa penyerang gunakan. Beberapa contoh dari serangan pasif adalah *Eavesdropping* dan *Traffic Analysis*. Sedangkan serangan aktif adalah serangan yang tidak hanya memantau dan mendengarkan saja, namun juga memodifikasi aliran data yang ada didalam jaringan. Serangan jenis ini bisa mengakibatkan informasi dapat berubah atau bahkan tidak sampai pada tujuan. Beberapa contoh dari serangan aktif adalah *Routing Attack, Denial of Service* (DoS), *Node Malfunction, Physical Attack,* dan lain-lain (Ioannou, Vassilioi, & Sergiou, 2017).

Setiap *layer* pada WSN berpotensi untuk diserang, hal ini terjadi karena tidak adanya arsitektur standar berlapis pada protokol komunikasinya. Mulai dari *layer physical*, *layer MAC, layer Network*, sampai *layer application* memiliki potensi terjadinya serangan. Namun pada *layer network* menjadi fokus utama karena merupakan jalur integrasi data, *routing* dan serangan pada *layer* ini memiliki jenis serangan yang banyak. Beberapa contoh serangan yang dapat terjadi pada *layer network* di antaranya *sinkhole attack, blackhole attack, selective forwarding* dan *sybil attack*.

Blackhole Attack merupakan salah satu serangan yang terjadi ketika penyerang menangkap dan memprogram ulang satu set *node* dalam jaringan untuk memblokir paket data yang mereka terima tanpa meneruskannya ke *base station*. Akibatnya setiap informasi yang masuk ke wilayah *blackhole* akan terperangkap dan tidak akan sampai ke tujuan (Alrajeh, Khan, & Shams, 2013).

Salah satu solusi untuk mengantisipasi terjadinya serangan *blackhole* ini adalah dengan menerapkan *Intrusion Detection System* (IDS) pada WSN menggunakan *signature approach* pada WSN. Sehingga ketika salah satu node menunjukan ciri-ciri dari serangan *blackhole*, maka IDS memberikan peringatan bahwa telah terdeteksi serangan *blackhole*(Shrivastava, Agrawal, & Jain, 2015). Namun IDS hanya dapat memberikan peringatan saja, maka dari itu peneliti mengusulkan sebuah sistem untuk memitigasi serangan *blackhole* ini. Usulan yang diajukan pada tugas akhir ini adalah menambahkan fitur *system shutdown*. *System shutdown* berfungsi untuk mematikan *sink node* yang merupakan penghubung *node* sensor dan *application layer* diatasnya. Sehingga ketika terjadi serangan *blackhole* pada WSN dan terdeksi oleh IDS menggunakan *signature approach*, *system shutdown* langsung mematikan *sink node* untuk menghindari kesalahan pengambilan keputusan pada *application layer*.

I.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan, didapatkan rumusan masalah sebagai berikut:

1. Bagaimana kinerja sistem IDS yang telah diterapkan pada WSN untuk mendeteksi serangan *blackhole*?
2. Bagaimana kinerja WSN setelah mengimplementasikan IDS *based on signature approach* dengan *system shutdown*?
3. Bagaimana mengantisipasi serangan *blackhole* menggunakan IDS *based on signature approach* dengan *system shutdown* pada WSN?

I.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengetahui kinerja IDS untuk mendeteksi serangan *blackhole* pada WSN.
2. Mengetahui kinerja WSN setelah mengimplementasikan IDS *based on signature approach* dengan *system shutdown*.
3. Mengimplementasikan IDS *based on signature approach* dan *system shutdown* pada WSN.

I.4 Batasan Penelitian

Adapun batasan masalah pada penelitian ini sebagai berikut:

1. Mitigassi serangan *blackhole* merupakan fokus utama dalam penelitian ini.
2. Serangan *blackhole* telah ditanamkan sejak awal simulasi berjalan.
3. Serangan hanya dilakukan oleh satu *node* yaitu *node* 24.
4. *Sink node* pada penelitian ini terletak di *node* 33.
5. Menggunakan *Intrusion Detection System* (IDS) berbasis *signature approach.*
6. Menambahkan fitur *system shutdown* pada IDS.
7. *Routing* yang digunakan pada penelitian ini adalah AODV.
8. Dalam tahap simulasi menggunakan *Network Simulator* (NS2).
9. Spesifikasi *sink node* pada penelitian ini memiliki konfigurasi yang sama dengan *node* lainnya dikarenakan keterbatasan pada simulator NS2.
10. *System shutdown* hanya digunakan sebagai langkah pengamanan sementara dalam menangani serangan.

I.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Dapat mengaplikasikan IDS *based on signature approach* dan *system shutdown* pada WSN.
2. Dapat mengetahui kinerja WSN yang lebih baik.
3. Sebagai informasi tambahan untuk penelitian selanjutnya mengenai pengamanan WSN.

I.6 Sistematika Penulisan

Penelitian ini akan dijabarkan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini memberikan uraian latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan literatur yang relevan dengan permasalahan yang dihadapi, penelitian sebelumnya yang memiliki keterkaitan dengan penelitian yang sedang dilakukan dan menjelaskan tentang *improvement* yang diajukan.

BAB III METODEPENELITIAN

Bab ini menjelaskan tentang langkah-langkah penelitian secara rinci, mulai dari tahap awal, tahap analisis, tahap pengumpulan data dan tahap akhir dari penelitian.

BAB IV PERANCANGAN SISTEM

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

BAB V PENGUJIAN DAN ANALISIS SISTEM

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

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang dapat diambil dari pengujian yang dilakukan selama penelitian dan saran untuk penelitian selanjutnya.