1. Pendahuluan

1.1. Latar Belakang

Low Power Wide Area Non Seluler (LPWAN) merupakan teknologi berbasis IoT yang memiliki karakteristik sebagai teknologi komunikasi jarak jauh dan memiliki daya rendah khususnya untuk pengiriman data kecil. Teknologi modulasi yang digunakan oleh LPWAN dirancang untuk mencapai link budget 150 dB. LPWAN dibagi menjadi dua kategori tekknologi, yaitu teknologi berbasis 3GPP (LTE-M, EC-GSM dan NB-IoT) dan teknologi proprietary atau non-3GPP (SigFox dan LoRa). LoRa memiliki perbedaan dengan jaringan LPWAN lainnya seperti SigFox dan NB-IoT, perbedaan tersebut terletak pada segi bandwith yang dimiliki masing-masing jaringan, pada LoRa memiliki bandwith yang paling besar diantara SigFox dan NB-IoT yaitu sebesar 250 kHz, sedangkan ZigFox memiliki bandwith sebesar 100 kHz dan NB-IoT memiliki bandwith sebesar 200 kHz. Selain itu SigFox dan NB-IoT tidak mendukung adaptive data rate, sedangkan LoRa mendukung adaptive data rate [1].

Long Range (LoRa) merupakan salah satu media komunikasi berbasis *wireless* yang menyediakan komunikasi jarak jauh dan berdaya rendah. LoRa memiliki ketahanan terhadap gangguan sinyal-sinyal yang tidak diinginkan yang selalu ada dalam proses pengiriman data pada LoRa yang nantinya dapat menganggu dalam proses penerimaan data atau pengiriman data [2].

Pada LoRa terdapat beberapa serangan yang dapat menghambat proses transmisi data, salah satunya adalah *Black hole Attack, Black Hole Attack* yang dapat menyerang proses pengiriman data yang terjadi pada jaringan LoRa dengan cara memaksakan dirinya menjadi node penegah pada rute yang ada. *Black hole Attack* dapat merusak seluruh proses pengiriman data karena black hole attack akan terlihat seperti node yang berada pada LoRa. LoRa berfungsi untuk mengirmkan informasi, dengan adanya serangan *black hole* maka fungsi LoRa tidak berjalan dengan baik, karena paket akan dihilangkan oleh node *blackhole, black hole* hampir selalu bisa melakukan serangan pada saat proses komunikasi atau pengiriman data antar node terjadi [3].

Pada beberapa jaringan wireless, terdapat beberapa metode yang dapat menentukan rute pengiriman paket yaitu dengan menggunakan *routing protocol AODV*. Routing protocol AODV dapat menentukan rute pengiriman dari node sender menuju node tujuan dengan mengirimkan RREQ kepada node tetangga. Routing protocol AODV akan bekerja jika node sender tidak bertetangga dengan node tujuan.

Pada penelitian sebelumnya yang membahas mengenai cara mendeteksi serangan *black hole* dengan menggunakan metode *anomaly based detection*. Pada penelitian tersebut membahas tentang serangan *black hole*, dan bagaimana cara mendeteksi serangan black hole dengan menggunakan metode *anomaly based detection* WSN. *Anomaly based detection* terbukti dapat mendeteksi *black hole attack* yang terjadi pada *Wireless Sensor*

Network. Anomaly based detection dapat mendeteksi serangan *black hole*. *Anomaly based detection* memiliki karakteristik utama yaitu mendeteksi pergerakan yang mencurigakan pada jaringan.

Pada penelitian sebelumnya yang membahas mengenai pencegahan serangan *black hole* dengan menggunakan baited based metode. Pada penelitian, tersebut membahas bahwa metode baited based dapat mendeteksi serangan blackhole pada jaringan WSN dengan cara mengirimkan *fake* id node kepada node yang teridentifikasi node *black hole.* Jika node tersebut membalas fake id tersebut maka node tersebut merupakan node black hole dan akan diblokir oleh sistem.

Untuk memudahkan pendeteksian *black hole* pada jaringan LoRa, penulis menggunakan 6 jaringan LoRa dengan kondisi node yang tidak bergerak, masing-masing node LoRa mengirimkan info paket ke node yang berfungsi sebagai gateway. LoRa gateway dapat menerima data yang berasal dari node-node yang telah terkoneksi dengan topologi mesh, gateway dapat mendeteksi satu node yang dicurigai sebagai node *black hole* dengan menggunakan metode *anomaly based detection,Anomaly based detection* akan memberikan info node berapa yang terdeteksi sebagai node black hole serta dapat menghitung berapa nilai packet loss dan delay dalam pengiriman paket pada jaringan LoRa. Pada penelitian ini menggunakan routing protocol AODV untuk menentukan rute pengiriman paket. Serta memblokir node yang teridentifikasi sebagai node *black hole* dengan menggunakan metode pencegahan Baited Based yang membuktikan bahwa node tersebut merupakan node blackhole dan jika node tersebut node blackhole maka node tersebut akan diblokir dan tidak termasuk dalam node rute pengiriman paket dalam LoRa.

1.2.Rumusan Masalah

Rumusan masalah pada Tugas Akhir ini sebagai berikut :

1. Bagaimana mendeteksi serangan *black hole* pada topologi Mesh yang dapat menganggu proses pengiriman paket yang terjadi pada LoRa ?
2. Bagaimana mencegah terjadinya *black hole* pada proses pengiriman paket pada LoRa ?
3. Bagaimana hasil pengujian performansi dengan menggunakan parameter delay dan packet loss ?

1.3.Tujuan

Tujuan pada Tugas Akhir ini sebagai berikut :

1. Dapat mendeteksi jaringan LoRa dari serangan *black hole* dengan menggunakan *anomaly based detection* pada topologi Mesh.
2. Melakukan penerapan pencegahan Baited Based pada jaringan LoRa dalam mendeteksi serangan *black hole*.
3. Melakukan analisis performansi dengan menggunakan parameter pengujian delay dan packet loss.

1.4.Batasan Masalah

Batasan Masalah pada Tugas Akhir ini adalah sebagai berikut :

1. Menggunakan LoRa sebagai alat pengiriman paket pada sistem yang digunakan.
2. Menggunakan topologi Mesh sebagai topologi dasar dalam pengujian.
3. Tipe serangan yang digunakan adalah *Single Blackhole Attack*.
4. Tipe node yang digunakan adalah tipe node yang tidak bergerak.
5. Menggunakan routing protocol AODV untuk menentukan rute pengiriman paket.
6. Parameter yang digunakan untuk melakukan analisis adalah delay dan packet loss.

1.5.Metodologi

Metode-metode yang digunakan pada tugas akhir ini adalah :

- Studi literatur
  Pada tahapan ini, akan dilakukan pencari literatur terkait dengan materi blackhole attack pada beberapa jaringan, serta serangan yang dapat menyerang Lora. Selain itu mencari studi literatur cara mendeteksi serangan blackhole pada LoRa, metode yang cocok diterapkan untuk mendeteksi serangan pada LoRa. Serta mteri mengenai parameter yang cocok untuk pengujian ini. Dan mencari penelitian terkait pencegahan untuk mengatasi serangan pada LoRa pada penilitian sebelumnya untuk dijadikan kerangka acuan.

- Pengumpulan Data
  Pada tahapan ini akan dilakukan pencarian data-data yang dibutuhkan untuk melakukan pengujian ini. Seperti informasi terkait karakteristik LoRa, karakteristik topologi yang dapat diterapkan pada jaringan LoRa serta mengumpulkan *library* LoRa yang tersedia yang dapat digunakan pada pengujian ini.

- Analisis dan Perancangan Sistem
  Pada tahap ini dilakukan analsisi terhadap perancangan sistem yang akan digunakan baik pembuatan topologi pada LoRa dan perancanagan dan node-node yang akan digunakan pada pengujian ini. Selain itu, melakukan perancangan terhadap pengujian serangan yang akan dilakukan, seperti menetapkan node yang berfungsi sebagai node serangan, menentukan jalur dan memalsukan jalur asli, penerapan parameter serta penerapan pendetksian serangan dan pencegahan serangan yang terjadi pada LoRa.

- Implementasi dan Pengujian
  Tahapan ini merupakan penerapan terhadap sistem yang telah dirancang pada tahapan sebelumnya, yakni melakukan penerapan topologi yang akan digunakan, penerapan dan inisialisasi node-node yang akan digunakan. Serta melakukan pengujian terhadap sistem yang telah

dibangun dengan menerapkan node penyerang pada proses pengiriman paket dan melakukan pengujian metode yang akan digunakan untuk mendeteksi serangan serta menerapkan metode pencegahan untuk mnegatasi serangan yang terjadi. Dan melakukan pengujian parameter dalam keadaan normal sebelum terjadi serangan dan setelah terjadi serangan dengan parameter yang telah disebutkan sebelumnya.

- Analisis hasil
  Pada tahap ini dilakukan analisis terhadap hasil yang didapatkan setelah melakukan simulasi. Setelah didapatkan hadil dari simulasi yang sesuai dengan skenario pengujian yang ada, akan dilakukan kebenarannya terhadap teori yang ada. Kemudian menarik kesimpulan terkait dengan hipotesis awal yang telah dideskripsikan sebelumnya dengan hasil yang didapatkan.

- Dokumentasi
  Tahapan ini merupakan tahapan terakhir, dimana seluruh kegiatan yang dilakukan dilakukan dokumentasi berupa dibuatkannya sebuah laporan yang berisikan langkah-langkah yang dilakukan pada simulasi ini, serta hasil yang didapatkan, dan studi literatur terkait.