Penerapan Metode *Anomaly Based Detection* untuk Mendeteksi Serangan *Black hole* pada Topologi Mesh di LoRa

Anjar Apriyanti[1], Vera Suryani[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]anjarap@students.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstrak

LoRa adalah sistem telekomunikasi nirkabel jarak jauh, dan berdaya rendah. LoRa masih rentan terhadap bentuk serangan yang dapat merusak rute pengiriman data, serta dapat menghapus data beserta informasi pada LoRa. Salah satu serangan yang terdapat pada LoRa adalah Black Hole. Penilitian ini fokus pada pendeteksian dan pencegahan node yang berperan sebagai node black hole yang mendrop paket dengan menggunakan metode Anomaly Based Detection dan menggunakan parameter packet loss pada topologi mesh di LoRa. Pengujian ini dilakukan dengan jumlah node sebanyak 6 node, 1 node berperan sebagai gateway, node 6 berperan sebagai node black hole, dengan kondisi pada node normal dan node yang terdapat black hole node. Dari penilitian ini dapat disimpulkan bahwa node black hole dapat terdeteksi dengan menggunakan anomaly based detection. Serta dapat melakukan pencegahan terhadap node black hole dengan menggunakan metode Baited Based.

Kata kunci : LoRa, Black Hole, Node, Mesh.

Abstract

LoRa is a low-power wireless telecommunications system. LoRa is still vulnerable to forms of attack that can damage data delivery routes, and can delete data and information on LoRa. One of the attacks found on LoRa is the Black Hole attack. This research focuses on detecting and prevention nodes that act as black hole nodes dropping packets using the Anomaly Based Detection method and using packet loss parameters on the mesh topology in LoRa. This test is carried out with 6 nodes, 1 node acts as a gateway, node 6 acts as a black hole node, with conditions on normal nodes and nodes that have black hole nodes. From this research it can be concluded that black hole nodes can be detected using anomaly based detection. And can prevent black hole nodes using by Baited Based method.

Keywords: LoRa, Black Hole, Node, Mesh.

1. Pendahuluan

Latar Belakang

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 [1].

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 *black hole*, *black hole* hampir selalu bisa melakukan serangan pada saat proses komunikasi atau pengiriman data antar node terjadi [2].

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 mengguankan 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.

Topik dan Batasannya

Dalam penelitian, masalah yang dibahas adalah bagaimana mendeteksi serangan *black hole* yang dapat menganggu proses pengiriman data yang terjadi pada LoRa. Serta bagaimana melakukan pencegahan *black hole* yang terjadi pada proses pengiriman paket. Batasan pada penilitian yang dilakukan pada jenis serangan single blackhole. *single black hole attack* merupakan *blackhole attack* hanya memiliki satu node black hole pada jaringan. Selain itu, jumlah node yang digunakan, pada proses pengiriman paket antar node menggunakan node LoRa sebanyak 6 node, 1 node yang berfungsi sebagai gateway, 1 node yang berfungsi sebagai node blackhole, 1 node yang berfungsi sebagai sender. Selain itu, pada penilitian ini menggunakan routing protocol AODV untuk menentukan rute pengiriman paket, dan pada penilitian ini proses pengiriman paket jaringan LoRa tidak menggunakan node LoRa yang bergerak serta menggunakan topologi mesh sebagai topologi dasar dari jaringan LoRa. Gateway mendeteksi node yang terindikasi sebagai node *black hole* dengan menerapkan metode *anomaly based detection* pada gateway, gateway akan memberikan node berapa yang terindikasi sebagai node *black hole* atau node penyerangan dalam jaringan LoRa.

Tujuan

Penilitian yang dilakukan bertujuan untuk mendeteksi serangan *black hole* pada jaringan LoRa dengan menggunakan metode *anomaly based detection*. Serta melakukan pencegahan saat terjadi serangan black hole pada pengiriman paket.

Organisasi Tulisan

Urutan penyajian pada paper ini dimulai dengan studi terkait, kemudian dilanjutkan dengan perancangan sistem yang dibangun, evaluasi dan pada bagian terakhir berisi kesimpulan dan saran terkait hasil penelitian yang dilakukan penulis.

2. Studi Terkait

Pada penelitian [3][4] menjelaskan bahwa LoRa memiliki kelebihan komunikasi dengan jarak jauh seperti seluler, namun berdaya rendah seperti *Bluetooth*, sehingga penggunaannya sangat cocok untuk perangkat sensor dengan sumber daya baterai, tetapi LoRa memiliki keterbatasan dalam hal komputasi dan penyimpanan karena hanya menggunakan komponen penyimpanan dan komputasi yang terbatas, meskipun LoRa memiliki banyak kelebihan namun tidak dapat melakukan penyimpanan data. Maka dari itu LoRa menggunakan komputasi berbasis *cloud*, tetapi LoRa tidak dapat langsung mengirimkan data ke *cloud* karena komunikasi LoRa menggunakan radio frekuensi.

Menurut referensi [2] dibahas mengenai *attack* yang terdapat pada jaringan LoRa, pada referensi tersebut dipaparkan beberapa serangan yang terdapat pada LoRa. Namun pada referensi tersebut tidak diberikan solusi untuk mendeteksi serangan tersebut. Sementara itu, pada penelitian [5] terjadi serangan *black hole* pada jaringan lain yaitu jaringan *wireless mesh network*, dan menggunakan dua perbandingan *routing protocol* yaitu AODV dan OLSR, dengan menggunakan *routing protocol* tersebut, *black hole* pada *wireless mesh network* teratasi dengan baik. Routing protocol dpaat menemukan rute pengiriman paket. AODV memastikan rute ke tujuan tidak mengandung loop dan merupakan jalur terpendek. Routing protocol menggunakan tabel routing untuk melakukan pengecekan tetangga node. Sebelum mengirimkan RREQ, node sender akan mengecek pada tabel routing milik node sender apakah node sender bertetangga atau terhubung langsung dengan node tujuan. Jika

terhubung, node sender dapat lagsung mengirimkan paket tersebut, jik tidak node sender mengirimkan Route Request (RREQ) kepada node tetangga yang dimiliki oleh node sender. Node tetangga akan mengecek tabel routing milik node tersebut, apakah node tersebut bertetangga atau terhubung dengan node tujuan dari node sender, jika tidak bertetangga node tersebut tidak mengirimkan pesan belasan, jika iya node tersebut mengirimkan pesan balasan Route Reply (RREP) kepada node sebelumnya, dan RREP berisikan node tujuan, node asal, dan hop count. Maka node tersebutlah yang terpilih untuk mengirimkan paket kepada node tujuan yang berasal dari node sender [6][7] .

Pada penelitian [8][9] menjelaskan tentang pendeteksian serangan *black hole* serta pencegahan *black hole* pada jaringan MANET, pada penelitian tersebut membuktikan bahwa, *black hole* dapat menyerangan MANET dan menggunakan metode *routing protocol* AODV. Selain itu pada penelitian [10] menjelaskan pendeteksian *black hole* dengan menggunakan jaringan yang sama tetapi menggunakan *routing protocol* yang berbeda.

Pada referensi [1] yang membahas mengenai topologi mesh pada jaringan LoRa, pada referensi tersebut dijelaskan bahwa topologi mesh dapat diterapkan di jaringan LoRa dan dapat membuat jangkauan jaringan semakin luas, maka dari itu pengujian penulis menggunakn topologi mesh sebagai topologi dasar dalam pengujian penulis.

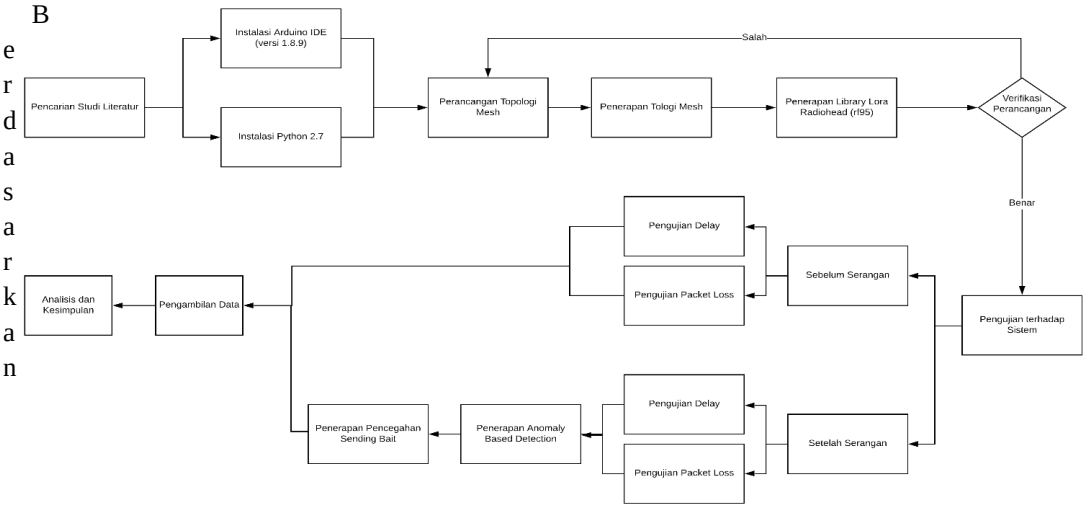
Pada penilitian [11] menjelaskan tentang metode *anomaly* yang dapat mendeteksi serangan *black hole* pada jaringan *wireless sensor network* atau WSN, pada penilitian tersebut dibuktikan bahwa metode *anomaly* dapat mendeteksi serangan *black hole*, serta referensi trersebut memberikan saran bahwa metode *anomaly based detection* dapat digunakan jaringan *wireless* lainnya termasuk LoRa. Dapat disimpulkan bahwa serangan *black hole* dapat menganggu proses pengiriman data yang terjadi pada beberapa jaringan, selain itu *black hole* dapat diatasi dengan beberapa metode termasuk dengan metode *routing protocol*, tetapi tidak semua *routing protocol* dapat diterapkan pada jaringan WSN termasuk LoRa. Serangan *black hole* dapat menganggu proses pengiriman data pada jaringan termasuk jaringan LoRa, serangan *black hole* dapat membuat node palsu yang serupa dengan node asli, lalu node *black hole* tidak meneruskan pengiriman data tersebut ke node tujuan, node *black hole* akan mendrop paket tersebut. Karena masalah tersebut, penulis menggunakan metode *anomaly based detection* untuk mengatasi serangan *black hole* karena *anomaly* dapat mendeteksi serangan *black hole* pada LoRa yang dideteksi melalui gateway, *metode anomaly based detection* memiliki karateristik yang dapat mendeteksi pergerakan yang mecurigakan pada jaringan termasuk jaringan LoRa. Selain itu, penulis menggunakan Teknik pencegahan *Baited Based*, berdasarkan paper acuan "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique" [12] pencegahan ini membuktikan node yang teridentifikasi node penyerang merupakan node *black hole* sungguhan dan melakukan isolasi node penyerang dalam pengujian ini.

3. Sistem yang Dibangun

3.1. Perancangan Sistem

Perancangan sistem menjelaskan tentang rancangan sistem yang akan dibangun pada penelitian tugas akhir ini. Adapun Perancangan sistem dibagi menjadi 4 bagian yaitu alur kerja sistem, alur kerja *black hole attack*, alur kerja pencegahan *black hole attack* dan rancangan topologi yang digunakan.

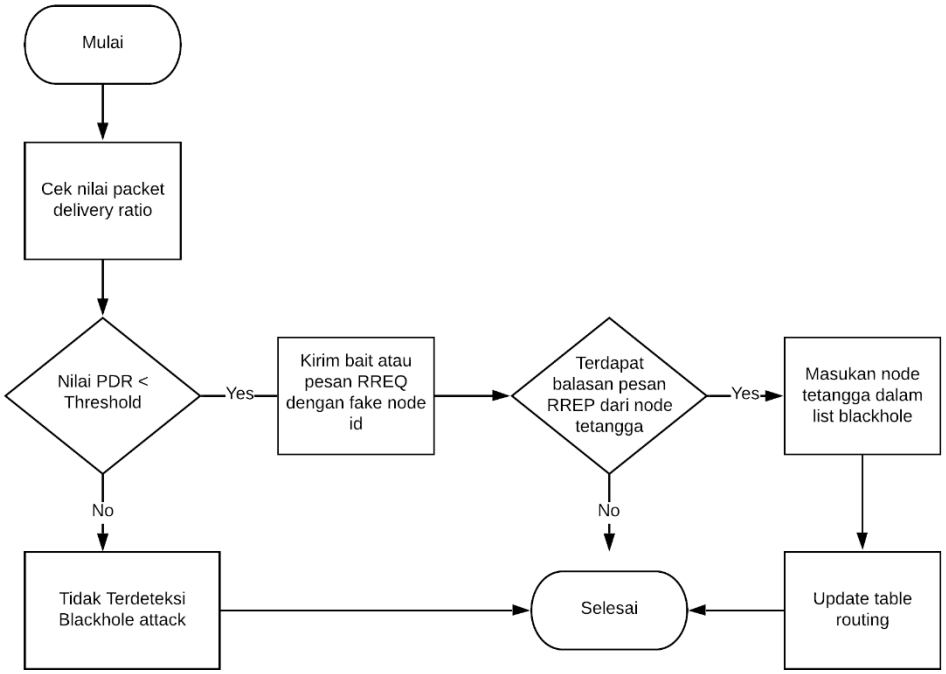
3.1.1. Alur Kerja Sistem



Gambar 3.1 Alur Kerja Sistem

gambar 3.1 dijelaskan bahwa untuk memulai pengerjaan terhadap sistem, terlebih dahulu dilakukan instalasi Arduino Ide versi 1.8.9. dan juga dilakukan instalasi Python. Setelah melakukan tahap instalasi, dilakukan perancangan dan penerapan topologi mesh untuk sistem yang dibangun, selain itu pada sistem dilakukan penerapan *Library Lora Radiohead* yang berfungsi sebagai tempat menyimpan rute pengiriman paket dalam sistem. Setelah dilakukan perancangan dan penerapan terhadap sistem yang dibangun, slenajutnya dilakukan verifikasi apakah sistem yang dibuat sudah berjalan dengan benar atau tidak. Hal ini dilakukan dengan cara melakukan cek terhadap hasil yang diperoleh apakah sistem sudah dapat saling berkomunikasi dengan baik sesuai topologi yang digunakan. Jika masing-masing node telah terhubung sesuai topologi yang diterapkan, selanjutnya dilakukan pengujian sistem, pengujian dilakukan berdasarkan dua skenario yakni sebelum terjadinya serangan dan sesudah terjadinya serangan. Selanjutnya melakukan pengujian terhadap dua parameter yakni Delay dan Packet Loss. Pada proses pengujian setelah serangan, dilakukan penerapan metode anomaly based detection untuk mendetksi node id berapa yang merupakan node blackhole. Selanjutnya, dilakukan penerapan pencegahan *Baited Based*. *Baited Based* merupakan metode pencegahan dalam proses pengiriman paket jika terjadi serangan dan bekerja dengan cara mengirimkan RREP pada node tetangga dengan node id palsu. Setelah pengujian dilakukan, data yang didapatkan diambil dan dilakukan analisis serta pengambilan kesimpulan akhir. Selain melakukan perancangan dan penerapan terhadap sistem yang dibangun, dilakukan juga perancangan topologi yang digunakan. Dalam hal ini, topologi yang digunakan adalah Mesh.

3.1.2. Alur Kerja *Black hole Attack*

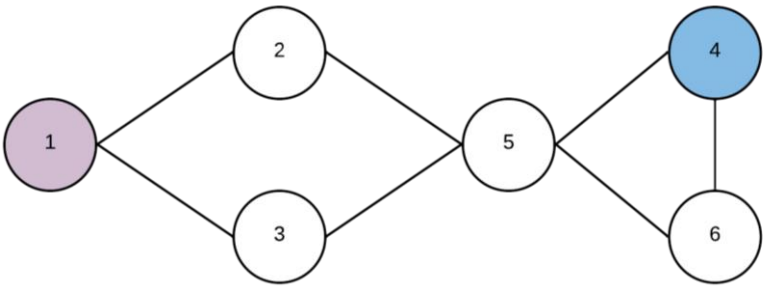


Gambar 3.2 Alur Kerja Blackhole Attack

Berdasarkan gambar 3.2 dijelaskan bahwa serangan *black hole* dapat terdeteksi ketika *anomaly* memeriksa berapa nilai paket delivery ratio yang terdapat dalam sistem, lalu nilai packet delivery ratio dibandingkang dengan jumlah tresholdnya, jika nilai PDR lebih kecil jumlah treshold, maka node tersebut terdeteksi sebagai node *black hole*, jika tidak maka dalam pengiriman paket tersebut tidak terdapat serangan blackhole. Setelah node blackhole terdeteksi, maka metode

pencegahan sending baited bekerja dengan cara mengirimkan bait atau RREQ dengan *fake* node id yang tidak terdapat dalam pengiriman paket tersebut, jika tidak terdapat RREP atau pesan balasan dari node yang teridentifikasi sebagai node blackhole, maka tidak terdapat node *black hole*, jika terdapat balasan, membuktikan bahwa node tersebut adalah node *black hole* dan node tersebut akan dimasukan kedalam list node *black hole* yang akan diblokir dan system akan mengupdate tabel *routing* agar tidak memasukkan node tersebut sebagai node yang terpilih untuk mengirimkan paket ke gateway.

3.1.3. Rancangan Topologi Sistem



Gambar 3.3 Rancangan Topologi yang Digunakan

Rancangan topologi mesh yang akan digunakan digambarkan pada gambar 3.3 Tolopologi terdiri dari 6 buah node dengan masing - masing memiliki node id sesuai dengan gambar topologi. Dalam pengujian sebelum terjadi serangan blackhole, Node 4 akan bertindak sebagai sender dan melakukan proses pengiriman paket menuju node 1 sebagai gateway. Sedangkan dalam pengujian penyerangan, selain proses pengiriman paket dari node 4 menuju node 1, node 6 akan bertindak sebagai node yang melakukan serangan blackhole.

3.2. Spesifikasi Kebutuhan Penilitian

Untuk pengujian sistem yang dibangun, kebutuhan penelitian terbagi menjadi dua yaitu kebutuhan perangkat lunak dan kebutuhan perangkat keras. Detail dari kebutuhan penelitian dideskripsikan pada Tabel 3.1 Kebutuhan Perangkat Lunak dan Tabel 3.2 Kebutuhan Perangkat Keras. Secara garis besar sistem diimplementasikan menggunakan 6 buah perangkat LoRa dragino frekuensi 915mhz dan terhubung dengan perangkat arduino uno. Setiap perangkat lora memiliki node id yang unik dimulai dari angka 1 hingga 6. Selain itu untuk proses deteksi anomali, diimplementasikan menggunakan bahasa *python*. Dimana data yang diolah pada program dengan bahasa *python* merupakan data yang dikirim dari gateway.

Tabel 3..1 Spesifikasi Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Detail	Keterangan
1	Sistem Operasi	Ubuntu 18.04	
2	Tools	Python 2.7	Untuk implementasi deteksi dan pencegahan *blackhole attack*,
		Arduino IDE (Versi 1.8.9)	Untuk memprogram board arduino uno dan lora

			dragino
		Library Lora Radiohead (rf95)	Untuk implementasi routing antar node menggunakan library radiohead

Tabel 3.2 Spesifikasi Kebutuhan Perangkat Keras

No	Perangkat Keras	Keterangan
1	Arduino Uno R3	Sebagai board mikrokontroller berjumlah 6 buah
2	Lora Dragino Frekuensi 915mhz	Sebagai perangkat untuk mengirimkan paket antar node

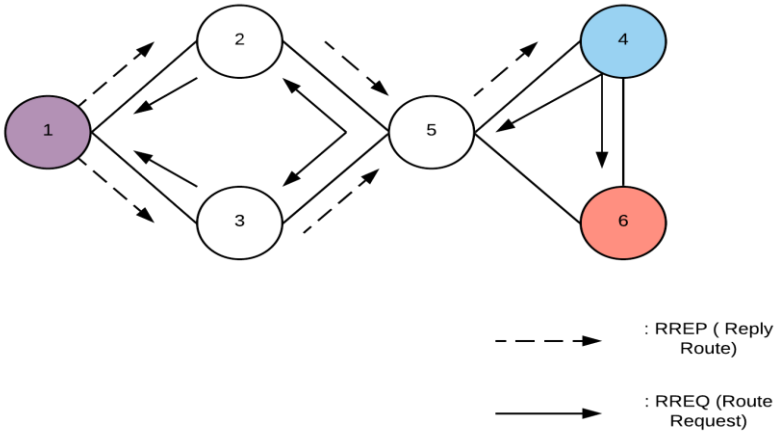
3.3. Skenario Pengujian

Untuk mendapatkan hasil pengujian dari sistem yang dibangun, maka dilakukan 6 skenario pengujian sebagai berikut :

3.3.1. Pengujian Paket

Pengujian pengiriman paket bertujuan untuk mengetahui bahwa sistem yang diimplementasikan dapat melakukan pengiriman paket dari node sender ke gateway. Selain itu, pengujian ini untuk melihat proses route discover dan route maintenance pada node sender ketika akan melakukan proses pengiriman paket menju gateway.

3.3.2. Pengujian Penentuan Rute Pengiriman



Gambar 3.4 Proses Routing Protocol AODV

Proses pencarian rute dari node 4 ke node node 1, ketika node 4 ingin mengirimkan paket kepada node 1, node 4 terlebih dahulu mengecek table routing milik node 4. Tujuan dari pengecekan ini adalah mengetahui apakah node 4 bertetangga atau terhubung dengan node 1.
Setelah melakukan pengecekan table routing node 4, node 4 tidak terhubung atau bertetangga dengan node 1. Maka dari itu node 4 mengirimkan RREQ atau Route Request kepada node tetangganya yaitu node 5 dan node 6.

Node 5 dan node 6 akan mengecek tabel routing milik node 5 dan node 6, apakah node 5 dan node 6 memiliki tetangga dan terhubung dengan node 1. Node 6 tidak memiliki tetangga dan tidak terhubung dengan node 1. Maka dari itu node 6 tidak mengirimkan pesan balasan atau RREP kepada node 4, karena node 6 tidak memiliki jalur menuju node 1.

Sedangkan node 5 memiliki node tetangga yaitu node 2 dan 3. Node 5 mengirimkan RREQ kepada node 2 dan node 3, bahwa node 5 ingin mengirimkan paket kepada node 1. Node 2 dan node 3 menerima RREQ dari node 5 dan mengecek tabel routing milik node 2 dan node 3, apakah node 2 dan node 3 terhubung dengan node 1 atau tidak. Node 2 dan node 3 terhubung dengan node 1, node 2 dan node 3 mengirimkan RREQ kepada node 1 bahwa node 4 ingin mengirimkan paket kepada node 1.

Node 1 menerima RREQ tersebut dan membalas RREQ tersebut bahwa node 1 akan menerima paket. Node 2 dan node 3 mengirimkan RREP kepada node 5 bahwa jika ingin mengirimkan paket menuju node 1 dapat melalui node 2 atau node 3. Node yang akan terpilih untuk rute pengiriman paket adalah node yang mengirimkan RREP terlebih dahulu kepada node 5, karena node 5 menganggap bahwa node yang terlebih dahulu mengirimkan RREP memiliki jalur terpendek. Seljutnya node 5 akan mengirimkan pesan balasan RREP kepada node sender atau node 4, RREP tersebut berisikan node destinationnya adalah node 1, via node 5 dan hopcount nya adalah 2, yang artinya pengiriman paket dari node 4 menuju node 1 dapat melalui node 5 dengan hopcount 2.

3.3.3. Pengujian Blackhole Attack

Pengujian *black hole attack* bertujuan untuk mengetahui bahwa node penyerang dapat melakukan penyerangan terhadap node sender sesuai dengan cara kerja yang dijelaskan pada alur kerja *black hole attack*. Adapun node yang akan menjadi penyerang adalah node 6. Proses penyerangan diawali dengan node penyerang yaitu node 6 bertindak sebagai node normal yang akan mengirimkan informasi *routing* berdasarkan tabel routing yang dimilikinya ketika ada pesan RREQ dari node lain. Ketika *black hole attack* dilakukan, maka node 6 akan mengklaim bahwa setiap paket RREQ yang didapatkan akan secara cepat dibalas dengan pesan RREP tanpa melihat data tabel *routing* node 6 dengan informasi *hop count* bernilai 0. Dengan demikian node sender akan memilih jalur melalui node 6 dikarenakan node 6 mengklaim bahwa tujuan dari node sender terhubung langsung dengan node 6.

3.3.4. Pengujian Deteksi dan Pencegahan *Black hole Attack*

Pengujian ini bertujuan untuk mengetahui keberhasilan program dalam mendeteksi terjadinya serangan *black hole* berdasarkan anomali. Pengujian ini dilakukan ketika proses pengiriman paket dari node sender menuju gateway. Ketika *anomaly* terdeteksi, program akan mengirimkan sinyal atau pesan broadcast ke setiap node. Kemudian setiap node akan melakukan pengiriman paket RREQ ke setiap node tetangga yang terhubung dengan node tersebut. Pesan RREQ yang dikirim, merupakan pesan berisi *fake* node id yang sebenarnya tidak ada pada jaringan tersebut. Hal ini dikarenakan, karakteristik dari node *black hole* yaitu melakukan pengiriman paket RREP tanpa memperhatikan informasi tabel *routing* dan mengklaim bahwa jalur terbaik melalui node *black hole*. Sehingga ketika node lain mendapatkan pesan RREP dari node *black hole* terhadap pesan RREQ dengan node id palsu, akan dianggap sebagai node *black hole* dan memasukan id node *black hole* ke dalam list *black hole* untuk selanjutnya melakukan update tabel *routing* tanpa memasukan node *black hole*. Proses deteksi dan pencegahan ini berdasarkan paper [12] dikenal dengan metode *Baited Blackhole* DSR yang cara kerjanya telah dijelaskan sebelumnya.

3.3.5. Pengujian Parameter Delay

Pengujian parameter delay dilakukan dengan dua kondisi yaitu ketika sebelum terjadi serangan dan setelah terjadi serangan *black hole attack*. Pengujian ini bertujuan untuk mengetahui dampak end to end delay pada saat melakukan pengiriman paket dari node sender ke gateway. Nilai delay yang didapat merupakan nilai rata - rata delay, dengan cara menjumlahkan selisih waktu pengiriman dan penerimaan dari setiap paket yang dikirim. Kemudian membagi total penjumlahan waktu selisih pengiriman paket dengan jumlah paket yang diterima pada node gateway. Waktu pengiriman paket dari sender ke gateway selama 1 menit. Berdasarkan paper [12] rumus perhitungan delay sebagai berikut:

$$Delay = \sum \frac{waktu\ menerima\ paket - waktu\ pengiriman\ paket}{jumlah\ paket\ yang\ dikirim}$$

3.3.6. Pengujian Parameter Packet Loss

Pengujian parameter packet loss mencari nilai selisih antara paket yang dikirim dan paket yang diterima, sehingga akan mendapatkan perbandingan nilai antara paket yang dikirim oleh node sender dengan paket yang diterima oleh node gateway. Dari perbandingan paket tersebut akan mendapatkan total packet loss pada saat melakukan pengiriman paket. Adapun rumus perhitungan Packet Loss sebagai berikut:

$$Packet\ Loss = \frac{total\ paket\ yang\ dikirim\ sender - total\ paket\ yang\ diterima\ gateway}{total\ paket\ yang\ dikirim\ sender}\ x\ 100\%$$

3.3.7. Pengujian Durasi Waktu Pencegahan *Black hole Attack*

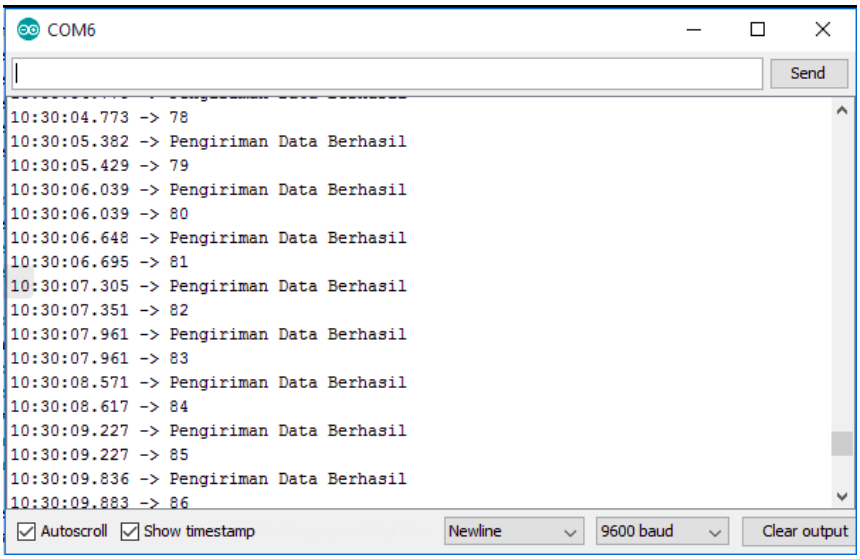
Pengujian durasi waktu pencegahan *black hole attack* bertujuan untuk mengetahui durasi waktu yang dibutuhkan untuk melakukan deteksi dan pencegahan ketika terjadi serangan *black hole.* Pengujian dilakukan dengan cara menghitung waktu mulai ketika terdeteksi *anomaly* serangan *black hole* pada gateway, proses pencegehan dengan metode *Baited Based* hingga proses *blocking* node *blackhole* oleh node sender.

4. Hasil dan Pembahasan

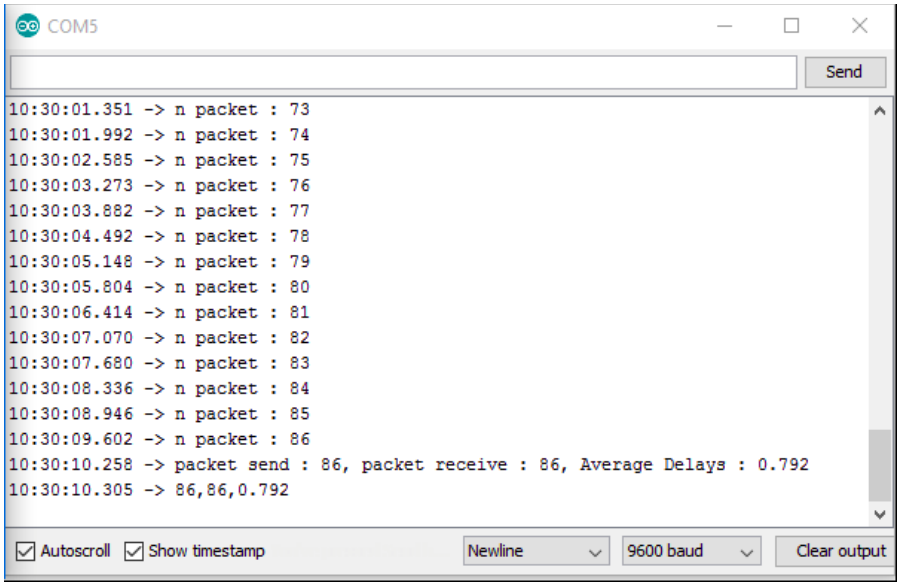
Pada bab ini menjelaskan terkait hasil pengujian dan analisis terhadap sistem yang dibangun. Berdasarkan skenario pengujian yang dijelaskan pada bab 3, pengujian dibagi menjadi 6 bagian yaitu Pengujian Pengiriman Paket, Pengujian *Black hole Attack*, Pengujian Deteksi dan Pencegahan *Black hole Attack*, Pengujian Parameter Delay, Pengujian Parameter Packet Loss, Pengujian Durasi Waktu Pencegahan *Black hole Attack.*

4.1. Pengujian Pengiriman Paket

Pengujian dilakukan dengan melakukan pengiriman paket dari node sender menuju node gateway. Pengiriman paket dilakukan selama 1 menit. Pengujian bertujuan untuk mengetahui bahwa node sender dapat melakukan pengiriman paket menuju node gateway.



Gambar 4.1 Tampilan proses pengiriman paket dari sender



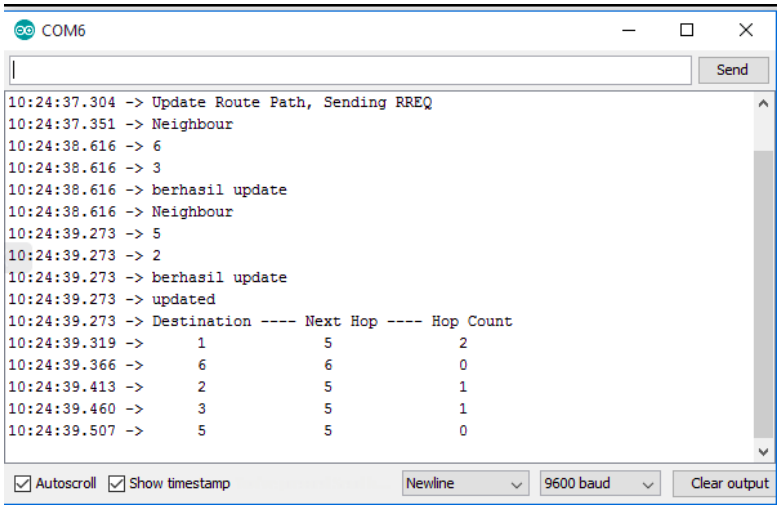
Gambar 4.2 Tampilan proses penerimaan paket dari gateway

Berdasarkan proses pengiriman paket pada Gambar 4.1 dan Gambar 4.2, proses pengiriman paket dari sender menuju gateway dapat diimplementasikan. Pada Gambar 4.1 sender mengirimkan paket dengan informasi nomor paket ditampilkan pada serial monitor. Pada Gambar 4.2 node gateway menerima setiap paket yang dikirim oleh node sender dan ditampilkan informasi nomor paket yang dikirim setiap detik n packet. Ketika pengiriman telah dilakukan selama 1 menit, node gateway akan menampilkan informasi jumlah paket yang dikirim sender, paket yang diterima node gateway, dan rata - rata delay pengiriman paket.

4.2. Pengujian *Black hole Attack*

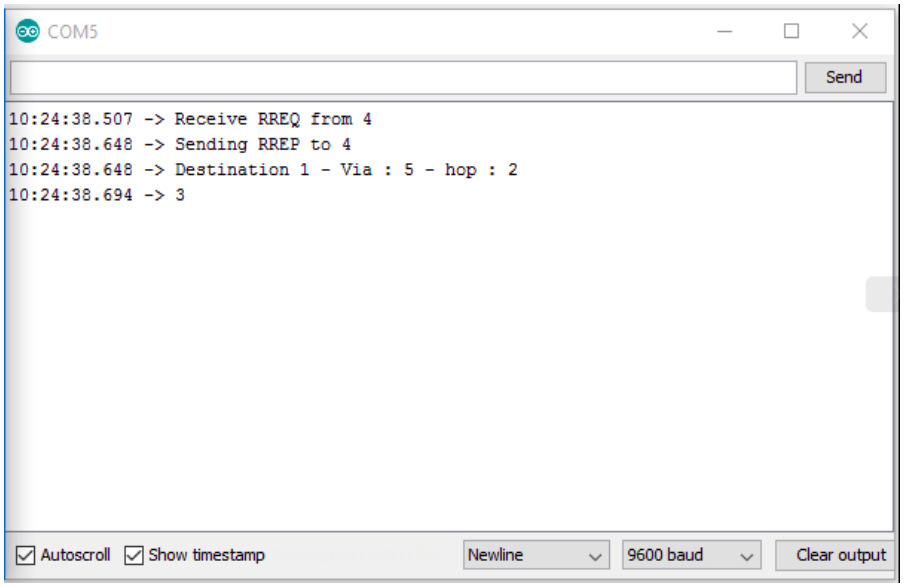
Hasil pengujian ini menjelaskan node yang teridentifikasi sebagai node *black hole* didapatkan melalui metode *anomaly based detection* yang bertugas mendeteksi node *black hole*. Sebelum terjadi serangan, node sender memilih node perantara untuk mengiirmkan paket dengan cara mengirimkan RREQ, node 6 akan mengklaim bahwa node 6 merupakan node yang langsung terhubung dengan gtateway. Sehingga node 6 terpilih sebgai node pengirim paket kepada gateway. Berikut hasil pengujian setelah serangan dan penerapan metode *anomaly based detection* dalam pengujin ini.

4.2.1. Sebelum Terjadi Serangan *Black hole*



Gambar 4.3 Tampilan proses *Route Discover* pada node sender

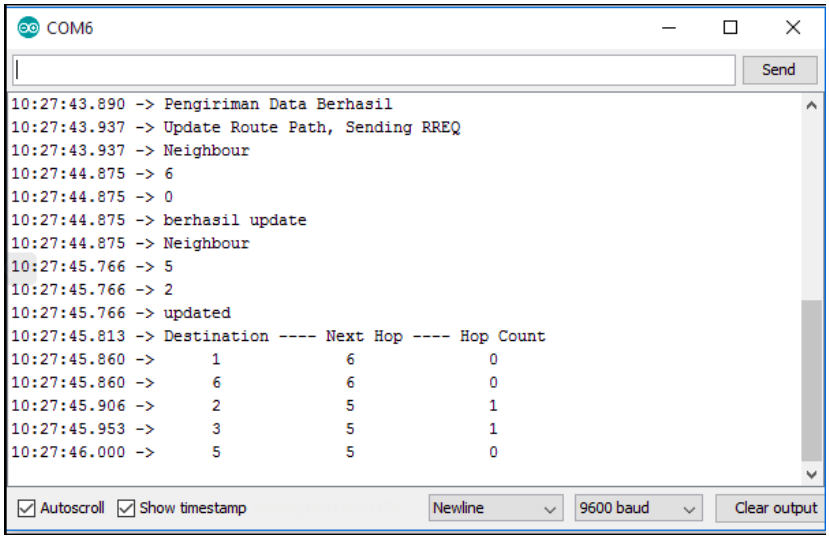
Proses *router discover* diawali ketika node sender melakukan pengiriman pesan paket RREQ dengan isi pesan mencari rute menuju node gateway yaitu node 1, ke setiap node tetangga dari node sender. Pada pengujian ini, node tetangga dari node sender adalah node 5 dan node 6. Kemudian node sender akan menerima balasan pesan paket RREP dengan isi pesan node jalur menuju gateway dan jumlah *hop count* yang dilewati. Berdasarkan proses *router discover* pada gambar 4.3, node sender menerima dua balasan pesan paket RREP dari node 5 dan node 6, dimana *hop count* dari node 5 adalah 2 dan hop count dari node 6 adalah 3. Sehingga node sender akan melakukan update tabel *routing* menuju node gateway yaitu node 1 dengan memasukan next hop node 5 dan *hop count* adalah 2 dikarenakan *hop count* dari node 5 lebih kecil dibandingkan node 6.



Gambar 4.4 Tampilan proses RREQ dan RREP pada node attacker

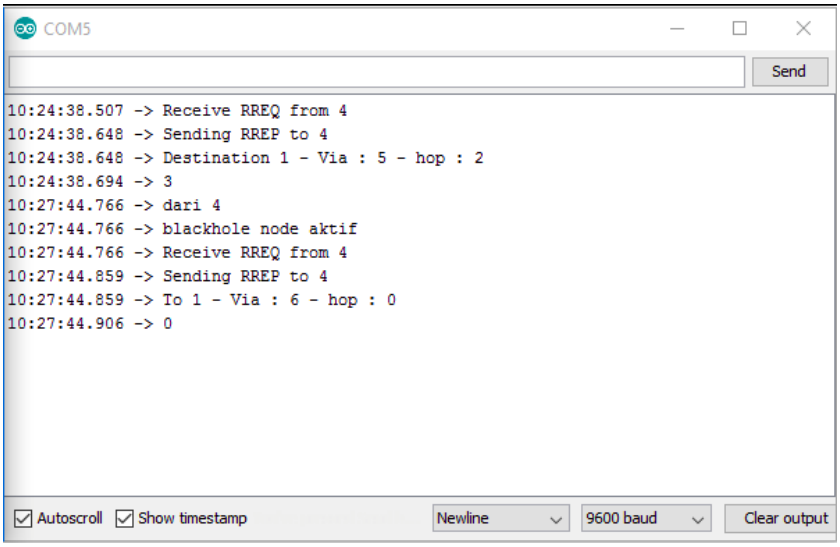
Berdasarkan proses pertukaran pesan paket *RREQ* dan *RREP* gambar 4.4, Pada saat node 4 sebagai sender mengirim pesan RREQ kepada node 6. Sebelum terjadi serangan, node 6 sebagai *attacker* akan melihat tabel *routing* untuk mencari jalur menuju node gateaway atau node 1. Kemudian node 6 akan membalas pesan paket RREQ node 4 dengan mengirim pesan paket RREP berisi informasi *hop count* dan node yang dilalui oleh node 6. Pada gambar 4.4 node 6 mengirim pesan RREP berisi *hop count* dengan jumlah 3, nilai *hop count* 3 didapatkan dengan menjumlahkan *hop count* node 5 ditambah 1. Hal ini berdasarkan tabel routing node 6 dimana untuk menuju node 1 atau gateway, harus melalui node 5 dengan jumlah hop count 2.

4.2.2. Saat Terjadi Serangan



Gambar 4.0.5 Tampilan proses Route Discover pada node sender

Berdasarkan proses *router discover* gambar 4.5, saat terjadi serangan *black hole*, pesan paket RREP yang didapatkan oleh node sender yaitu node 4 mengalami perbedaan disaat sebelum serangan. Dimana pada saat sebelum serangan, node yang harusnya dilalui adalah node 5 dengan jumlah *hop count* adalah 2, sedangkan ketika terjadi serangan, node 6 mengklaim bahwa untuk menuju node gateway yaitu node 1 dapat melalui node 6 dengan jumlah *hop count* yang lebih kecil atau 0, hal ini menandakan bahwa node 6 terhubung langsung pada node gateway yaitu node 1. Sehingga node sender atau node 4 memilih route melalui node 6 dikarenakan jumlah *hop count* lebih kecil dibanding node 5.

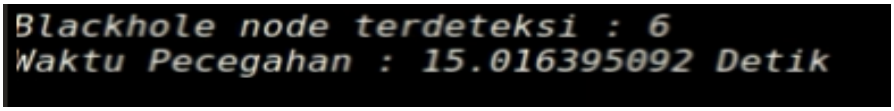


Gambar 4.6 Tampilan proses RREQ dan RREP pada node attacker

Berdasarkan proses pertukaran pesan paket RREQ dan RREP pada gambar 4.6, node 6 sebagai node attacker ketika terjadi serangan, akan membalas setiap packet pesan RREQ yang diterima tanpa melihat data tabel *routing* terlebih dahulu, tetapi secepat mungkin membalas peasn RREQ dengan RREP dan mengklaim bahwa pengiriman pesan menuju gateway adalah melalui node 6. Hal ini ditandai dengan *hop count* pada pesan RREP yang dikirim berisi nilai 0, sebagai tanda bahwa node 6 terhubung langsung dengan node gateway atau node 1.

4.3. Pengujian Deteksi dan Pencegahan Blackhole Attack

Pengujian ini dilakukan dengan cara anomaly mendeteksi adanya serangan dalam proses pengiriman paket dari gateway yang tidak menerima paket apapun selama proses pengiriman paket. Gateway akan mengirimkan RREQ ke node sender, memberitahu bahwa terdapat node black hole yaitu dengan id node 6. Gateway akan mengiirmkan RREQ secara terus menerus sampai node sender menerima RREQ dari gateway, sending baited akan bekerja dengan mengirimkan fake id node kepada node 6, node 6 membalas kepada node 6 dan sending baited akan memblokir node 6 dan memasukkan node 6 kedalam list node black hole yang disimpan kedalam library.

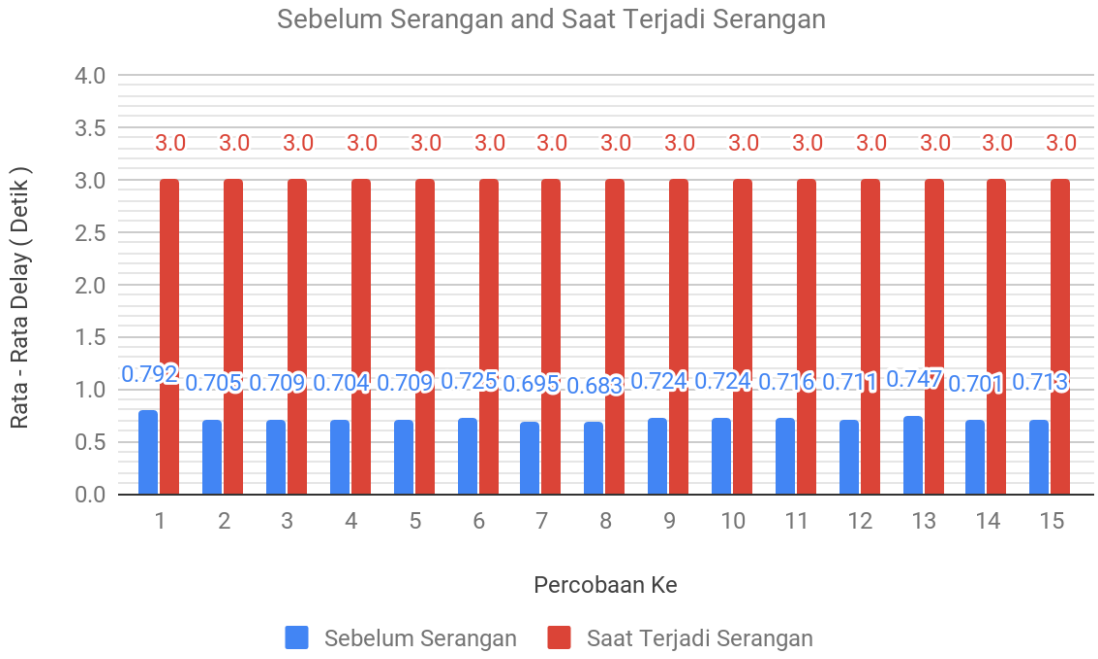


Gambar 4.7 Tampilan pendeteksian blackhole dan waktu pencegahan

Berdasarkan Gambar 4.7 node 6 terdeteksi sebagai node blackhole dan proses sending baited telah melakukan pemblokiran kepada node 6, sehingga node 6 tidak menerima paket dari sender dna tidak termasuk kedalam rute pengiriman. Selain itu waktu pencegahan menghabiskan waktu selama 15,06 detik, waktu tersebut terhitung dari node sender menerima pesan RREQ dari gateway bahwa terdapat node black hole dalam proses pengiriman paket tersebut hingga dilakukan tindakan pemblokiran node blackhole selesai.

4.4. Pengujian Parameter Delay

Pengujian dilakukan dengan cara mengirim paket dari sender yaitu node 4 menuju gateway node 1 selama 1 menit. Pengiriman paket dari sender ke gateway dilakukan sebanyak 15 kali.



Gambar 4.8 Hasil Pengujian Rata - Rata Delay Sebelum dan Setelah Serangan

Berdasarkan Gambar 4.8, nilai rata - rata delay terkecil sebelum terjadi serangan didapat pada percobaan ke 8 sebesar 0.683 detik, sedangkan nila rata - rata delay terbesaer didapat pada percobaan ke 0.792. Berdasarkan hasil pengujian, faktor yang mempengaruhi nilai delay adalah faktor rute pengiriman paket dari node sender menuju node gateway, pada percobaan ini rute yang dilalui adalah node 4 - 5 - 2 - 1. Semakin banyak node yang dilalui maka nilai delay akan semakin besar begitu juga sebaliknya semakin sedikit node yang dilalui maka nilai delay semakin kecil. Sedangkan ketika terjadi serangan *blackhole*, paket yang dikirim dari node 4 tidak ditersukan oleh node 6 sebagai attacker menuju gateway melainkan di drop. Sehingga nilai rata - rata delay yang didapat merupakan nilai *acktimout* yang diterima oleh gateway, dikarenakan tidak ada balasan pengiriman paket dari node 4.

4.5. Pengujian Parameter Packet Loss

Pengujian dilakukan dengan dengan cara sender mengirim paket selama 1 menit, kemudian menghitung jumlah paket yang diterima oleh gateway yaitu node 1. Packet loss didapat dengan membandingkan antara paket yang diterima di gateway dengan paket yang dikirim oleh sender.

Gambar 4.9 Hasil pengujian nilai Packet Loss sebelum dan saat terjadi serangan blackhole

Berdasarkan hasil pengujian packet loss pada gambar 4.9, pengujian dilakukan sebanyak 15 kali percobaan. Sebelum terjadi serangan *black hole*, nilai packet loss berkisar antara 0 - 1%. Nilai *packet loss* ini diakibatkan adanya gangguan dalam pengiriman. Sedangkan ketika terjadi serangan *black hole*, nilai *packet loss* setiap percobaan menjadi 100%. Hal ini diakibatkan dampak dari serangan *black hole*, dimana node 4 sebagai sender mengirim paket melalui jalur node attacker yaitu node 6. Paket yang diterima node 6 tidak diteruskan ke node gateway melainkan di drop. Sehingga tidak ada paket yang diterima di gateway yang berasal dari node sender dan menyebabkan nilai packet loss 100%.

5. Kesimpulan

Balckhole mempengaruhi pengiriman paket yang terjadi pada jaringan LoRa. Untuk melakukan pendeteksian node yang merupakan node blackhole, penilitian ini menggunakan metode anomaly based detection dan menggunakan parameter pengukuran packet loss, metode tersebut dapat mendeteksi node blackhole yang tidak mengirimkan paket kepada gateway. metode anomaly dapat diterapakan pada jaringan LoRa serta penulis menggunakan topologi mesh sebagai topologi pada pengujian ini, dan topologi mesh dapat diterapkan pada jaringan LoRa. Pada pengujian delay, nilai delay sebelum serangan lebih kecil dibandingkan nilai delay setelah serangan, dikarenakan setelah serangan nilai delay didapatkan dari rata-rata *acktimeout* dari gateway yang tidak menerima paket apapun. Pada saat pengujian packet loss, tidak terdapat packet loss sebelum terjadinya serangan, packet loss terjadi setelah terjadinya serangan. Sebelum terjadi serangan, gateway menerima jumlah paket yang sama dari masing-masing node, tetapi setelah serangan, gateway menerima paket jumlahnya tidak sama dari masing-masing node, yang menandaskan bahwa node yang paling sedikit mengirim paket kepada gateway maka node tersebut adalah node blackhole. Baited based teknik dapat diterapkan pada jaringan LoRa untuk mendeteksi serangan blackhole dan memblokir node yang teridentifikasi sebagai node blackhole.

Daftar Pustaka

[1] J. Y. Kim, "LoRa-based Mesh Network for IoT Applications," *2019 IEEE 5th World Forum Internet Things*, pp. 524–527, 2019.

[2] I. Butun and N. Pereira, "Security Risk Analysis of LoRaWAN and Future Directions," pp. 1–22, 2019.

[3] P. Devi, D. Istianti, S. Y. Prawiro, N. Bogi, A. Karna, and I. A. Nursafa, "Analisis Performansi Teknologi Akses LPWAN LoRa Antares Untuk Komunikasi Data End Node," *Citee 2019*, pp. 24–25, 2019.

[4] A. Botta, W. De Donato, and V. Persico, "Integration of Cloud computing and Internet of Things : A survey," no. October, 2015.

[5] W. Virgi, A. Bhawiyuga, and R. Primananda, "Analisis Perbandingan Dampak Serangan Black Hole pada Peformansi Protokol Routing OLSR dan AODV di Jaringan Wireless Mesh Network," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 3, pp. 1017–1026, 2018.

[6] M. June, "Effect of Black Hole Attack on AODV , OLSR and ZRP Protocol in MANETs," vol. 2, no. 2278, pp. 43–46, 2013.

[7] L. Klein-berndt, "A Quick Guide to AODV Routing," pp. 1–7.

[8] I. Pratomo and H. Hizburrahman, "Pendeteksian Dan Pencegahan Serangan Black Hole," *JAVA J. Electr. Electron. Eng.*, vol. 13, pp. 47–53, 2015.

[9] B. Singh, D. Srikanth, and C. R. S. Kumar, "Mitigating effects of black hole attack in mobile Ad-Hoc NETworks: Military perspective," *Proc. 2nd IEEE Int. Conf. Eng. Technol. ICETECH 2016*, no. March, pp. 810–814, 2016.

[10] I. Nurhidayat, P. H. Trisnawan, and R. A. Siregar, "Analisis Pengaruh Blackhole Attack Terhadap Kinerja Protokol Routing BATMAN (Better Approach To Mobile Ad Hoc Network) Pada Mobile Ad Hoc Network," vol. 3, no. 3, pp. 2853–2861, 2019.

[11] V. Bansal, "Anomaly based detection of Black Hole attack on leach protocol in WSN," 2016.

[12] A. Yasin and M. Abu Zant, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.