



**PENANGANAN SERANGAN BLACKHOLE PADA JARINGAN
SENSOR NIRKABEL DENGAN METODE ENHANCED
CHECK AGENT**



RIKO SAPUTRA

55416120026

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
PROGRAM PASCASARJANA
UNIVERSITAS MERCU BUANA
2020**



**PENANGANAN SERANGAN BLACKHOLE PADA JARINGAN
SENSOR NIRKABEL DENGAN METODE ENHANCED
CHECK AGENT**

TESIS

Diajukan sebagai salah satu syarat untuk menyelesaikan

Program Studi Magister Teknik Elektro

**UNIVERSITAS
MERCU BUANA**

Oleh:

RIKO SAPUTRA

55416120026

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
PROGRAM PASCASARJANA
UNIVERSITAS MERCU BUANA
2020**

PERNYATAAN SIMILARITY CHECK

Saya yang bertanda tangan di bawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh

Nama : Riko Saputra
NIM : 55416120026
Program Studi : Magister Teknik Elektro

Dengan judul

“Penanganan Serangan Blackhole Pada Jaringan Sensor Nirkabel Dengan Metode Enhanced Check Agent”, telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal 25 Juli 2020, didapatkan nilai persentase sebesar 27% (dua puluh tujuh persen).

Jakarta, 25 Juli 2020

Administrator Turnitin



Arie Pangudi, A.Md

PENGESAHAN TESIS

Judul : **Penanganan Serangan Blackhole pada Jaringan Sensor Nirkabel dengan Metode Enhanced Check Agent**

Nama : Riko Saputra

N I M : 55416120026

Program : Pascasarjana Program Magister Teknik Elektro

Konsentrasi : Keamanan Jaringan ICT

Tanggal : 15 Agustus 2020

Mengesahkan

Pembimbing I



(Prof. Dr.-ing, Mudrik Alaydrus)

Pembimbing II



(Julpri Andika, ST.,M.Sc.)

Direktur Pascasarjana



(Prof. Dr.-ing, Mudrik Alaydrus)

Ketua Program Studi

Magister Teknik Elektro



(Prof. Dr. Ir. Andi Adriansyah, M.Eng)

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam tesis ini :

Judul : Penanganan Serangan Blackhole pada Jaringan Sensor Nirkabel dengan Metode Enhanced Check Agent
Nama : Riko Saputra
NIM : 55416120026
Program : Pascasarjana Program Magister Teknik Elektro
Konsentrasi : Keamanan Jaringan ICT

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Komisi Dosen Pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Karya ilmiah ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, 15 Agustus 2020
Yang membuat pernyataan,



(Riko Saputra)
55416120026

SURAT PERNYATAAN BEBAS PLAGIAT

Nama : Riko Saputra

NIM : 55416120026

Konsentrasi : Keamanan Jaringan ICT

Program Pascasarjana Program Studi Magister Teknik Elektro

Universitas Mercu Buana Jakarta

Dengan ini menyatakan bahwa:

1. Karya tulis ini adalah asli dan belum pernah diajukan untuk mendapat gelar akademik Magister Teknik Elektro baik di Universitas Mercu Buana maupun di perguruan tinggi lainnya.
2. Karya tulis ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Tim Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya dengan norma yang berlaku di perguruan tinggi.

Jakarta, 15 Agustus 2020
Yang membuat pernyataan,



(Riko Saputra)
55416120026

DAFTAR ISI

PENGESAHAN TESIS	iv
PERNYATAAN	vi
SURAT PERNYATAAN BEBAS PLAGIAT	vii
DAFTAR ISI	ixiii
DAFTAR GAMBAR	xi
DAFTAR TABEL	ixiii
ABSTRAK	xv
BAB I PENDAHULUAN	1
1.1. LATAR BELAKANG	1
1.2. PERUMUSAN MASALAH	3
1.3. TUJUAN DAN MANFAAT PENELITIAN	4
1.4. BATASAN PENELITIAN	4
BAB II TINJAUAN PUSTAKA	6
2.1. WIRELESS SENSOR NETWORK	6
2.2. SISTEM KOMUNIKASI WSN	6
2.3. TOPOLOGI JARINGAN PADA WIRELESS SENSOR NETWORK	6
2.3.1. TOPOLOGI JARINGAN STAR	7
2.3.2. TOPOLOGI CLUSTER	7
2.3.3. TOPOLOGI MESH	7
2.4. KENDALA PADA WIRELESS SENSOR NETWORK	8

2.4.1.	KETERBATASAN SUMBER DAYA-----	8
2.4.2.	KOMUNIKASI YANG TIDAK DAPAT DIANDALKAN -----	8
2.4.3.	KETERBATASAN PUSAT KENDALI PADA WSN-----	8
2.4.4.	LOKASI SENSOR YANG TERISOLASI-----	9
2.5.	JENIS-JENIS SERANGAN PADA WIRELESS SENSOR NETWORK-----	9
2.5.1.	JAMMING ATTACK-----	9
2.5.2.	TAMPERING -----	9
2.5.3.	SYBIL ATTACK-----	10
2.5.4.	WORMHOLE ATTACK -----	10
2.5.5.	HELLO FLOOD ATTACK-----	10
2.5.6.	BLACK HOLE ATTACK-----	10
2.6.	TEKNOLOGI ZIGBEE-----	11
2.7.	PENELITIAN TERKAIT-----	12
2.7.1.	DETEKSI BLACKHOLE DENGAN METODE CHECK AGENT-----	12
2.7.2.	DETEKSI BLACKHOLE DENGAN METODE HEEIDS-----	16
2.7.3.	DETEKSI BLACKHOLE DENGAN METODE SECURE MD5 -----	17
2.7.4.	DETEKSI BLACKHOLE DENGAN METODE SECURE HYBRID-----	22
2.7.5.	RANGKUMAN PENELITIAN TERKAIT-----	25
BAB III	METODE PENELITIAN -----	27
3.1.	METODOLOGI PELAKSANAAN PENELITIAN-----	27
3.1.1.	TAHAP STUDI LITERATUR -----	27
3.1.2.	PERANCANGAN METODE -----	28
3.1.3.	PERANCANGAN SISTEM PENDETEKSIAN -----	28

3.1.4. PERANCANGAN ENHANCED CHECK AGENT -----	30
3.1.5. PENGUMPULAN DATA-----	32
BAB IV HASIL DAN PEMBAHASAN-----	33
4.1. PENGUJIAN SISTEM DAN PENGUKURAN -----	33
4.1.1. PENGUKURAN SISTEM TANPA SERANGAN BLACKHOLE -----	34
4.1.2. PENGUKURAN SISTEM DENGAN SERANGAN BLACKHOLE -----	40
4.1.3. PENGUKURAN SISTEM DENGAN SERANGAN BLACKHOLE DAN DETEKSI ENHANCED CHECK AGENT-----	47
4.2. PEMBAHASAN HASIL PENGUJIAN -----	54
4.3. PEMBANDINGAN HASIL PENGUJIAN -----	57
BAB V KESIMPULAN DAN SARAN-----	58
5.1. KESIMPULAN -----	58
5.2. SARAN -----	58
DAFTAR PUSTAKA-----	59

DAFTAR GAMBAR

Gambar 2.1 Topologi Jaringan WSN.....	7
Gambar 2.2 Serangan Blackhole Pada WSN	11
Gambar 2.3 Diagram Alur Proses Deteksi Metode Check Agent.....	13
Gambar 2.4 Jumlah Rata-rata Energi yang Disimpan berbanding dengan Waktu	14
Gambar 2.5 Jumlah Node berbanding dengan Radius Black Hole.....	14
Gambar 2.6 Kompleksitas Pesan Dalam Paket berbanding Jumlah Node.....	15
Gambar 2.7 Probabilitas Deteksi Blackhole Berbanding Jumlah Node Pada Metode Check Agent.....	15
Gambar 2.8 Skema Sistem Deteksi Intrusi	16
Gambar 2.9 Skema Sistem Deteksi Blackhole Metode MD5 Secure	19
Gambar 2.10 Grafik Rasio Pengiriman Data Paket Pada Metode Secure MD5 ...	20
Gambar 2.11 Grafik Throughput Pada Jaringan Metode Secure MD5.....	21
Gambar 2.12 Grafik Nilai Waktu Tunda Pada Jaringan Metode Secure MD5.....	21
Gambar 2.13 Diagram Alur Metode Secure Hybrid	22
Gambar 2.14 Grafik Nilai Packet Loss pada Jaringan Dengan dan Tanpa Blackhole.....	23
Gambar 2.15 Grafik Nilai Throughput pada Jaringan	24
Gambar 2.16 Grafik Tingkat Efisiensi	25
Gambar 3.1 Flowchart Metode Enhanced Check Agent.....	28
Gambar 3.2 Arsitektur Perancangan Sistem Untuk Mendeteksi Blackhole	29
Gambar 3.3 Diagram Alur Paket Referensi Agent.....	31

Gambar 3.4 Diagram Alur Mekanisme Penerimaan Data oleh Node	32
Gambar 4.1 Skema Sistem Tanpa Serangan Blackhole	34
Gambar 4.2 RSSI Pengukuran Packet Loss Tanpa Gangguan Blackhole	34
Gambar 4.3 Pengukuran Throughput dan Packet Loss pada Jaringan Tanpa Gangguan Blackhole	35
Gambar 4.4 Grafik Transfer Ratio pada Jaringan Tanpa Gangguan Blackhole ...	36
Gambar 4.5 Skema Sistem Dengan Serangan Blackhole.....	40
Gambar 4.6 RSSI Pengukuran Packet Loss pada Jaringan Dengan Blackhole	41
Gambar 4.7 Pengukuran Throughput dan Packet Loss pada Jaringan Dengan Blackhole.....	42
Gambar 4.8 Grafik Transfer Ratio pada Jaringan Dengan Blackhole	43
Gambar 4.9 Skema Sistem Dengan Serangan Blackhole dan Deteksi Enhanced Check Agent.....	47
Gambar 4.10 RSSI Pengukuran Packet Loss pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent.....	48
Gambar 4.11 Pengukuran Throughput dan Packet Loss pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent.....	49
Gambar 4.12 Grafik Transfer Ratio pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent.....	50
Gambar 4.13 Grafik Perbandingan Nilai Rata-Rata Delay pada Setiap Skenario Jaringan	56
Gambar 4.14 Grafik Persentase Paket Sampai Tujuan	57

DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian Terkait	26
Tabel 4.1 Delay Paket pada Jaringan Tanpa Gangguan Blackhole Dengan Panjang Paket 64 Byte	36
Tabel 4.2 Delay Paket pada Jaringan Tanpa Gangguan Blackhole Dengan Panjang Paket 98 Byte	37
Tabel 4.3 Delay Paket pada Jaringan Tanpa Gangguan Blackhole Dengan Panjang Paket 128 Byte	38
Tabel 4.4 Delay Paket pada Jaringan Tanpa Gangguan Blackhole Dengan Panjang Paket 183 Byte	38
Tabel 4.5 Delay Paket pada Jaringan Tanpa Gangguan Blackhole Dengan Panjang Paket 256 Byte	39
Tabel 4.6 Delay Paket pada Jaringan Tanpa Gangguan Blackhole Dengan Panjang Paket 267 Byte	40
Tabel 4.7 Delay Paket pada Jaringan Dengan Blackhole Dengan Panjang Paket 64 Byte	43
Tabel 4.8 Delay Paket pada Jaringan Dengan Blackhole Dengan Panjang Paket 98 Byte	44
Tabel 4.9 Delay Paket pada Jaringan Dengan Blackhole Dengan Panjang Paket 128 Byte	45
Tabel 4.10 Delay Paket pada Jaringan Dengan Blackhole Dengan Panjang Paket 183 Byte	45

Tabel 4.11 Delay Paket pada Jaringan Dengan Blackhole Dengan Panjang Paket 256 Byte	46
Tabel 4.12 Delay Paket pada Jaringan Dengan Blackhole Dengan Panjang Paket 267 Byte	47
Tabel 4.13 Delay Paket pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent Dengan Panjang Paket 64 Byte	51
Tabel 4.14 Delay Paket pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent Dengan Panjang Paket 98 Byte	51
Tabel 4.15 Delay Paket pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent Dengan Panjang Paket 128 Byte	52
Tabel 4.16 Delay Paket pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent Dengan Panjang Paket 183 Byte	53
Tabel 4.17 Delay Paket pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent Dengan Panjang Paket 256 Byte	53
Tabel 4.18 Delay Paket pada Jaringan Dengan Blackhole dan Deteksi Enhanced Check Agent Dengan Panjang Paket 267 Byte	54
Tabel 4.19 Hasil Nilai Rata-Rata Delay Untuk Setiap Panjang Paket pada Jaringan Tanpa Serangan Blackhole.....	55
Tabel 4.20 Hasil Nilai Rata-Rata Delay Untuk Setiap Panjang Paket pada Jaringan Dengan Metode Deteksi Check Agent yang Ditingkatkan	55

ABSTRAK

Wireless Sensor Network (WSN) merupakan suatu jenis jaringan heterogen yang terdiri dari simpul-simpul sensor yang tersebar dan bekerja bersama untuk fungsi pengumpulan data, proses dan transmisi [1][2]. Oleh karena WSN banyak dipergunakan dalam hal-hal vital, maka aspek dari keamanannya pun harus diperhatikan. Ada banyak jenis serangan yang mungkin dapat dilakukan untuk mengacaukan jaringan WSN. Adapun metode-metode serangan yang ada pada WSN diantaranya yaitu, jamming attack, tampering, Sybil attack, wormhole attack, hello flood attack dan black hole attack[3]. Serangan black hole merupakan salah satu yang serangan paling berbahaya pada jaringan WSN.

Metode Enhanced Check Agent dirancang untuk mendeteksi serangan black hole dengan cara mengirimkan check agent untuk mendata node-node yang dianggap black oke. Metode ini adalah penggabungan antara dua metode deteksi yaitu metode Check Agent dengan metode Hybrid dengan beberapa penyesuaian untuk mendapatkan hasil yang optimal.

Implementasi akan di uji coba kan pada jaringan sensor nirkabel dengan menggunakan teknologi zigbee. Toplogi jaringan menggunakan mesh dimana setiap node dapat mempunyai lebih dari satu tabel ruting[4]. Metode Enhanced Check Agent dapat meningkatkan throughput dibandingkan metode yang ada sebelumnya.

Keywords: Jaringan Sensor Nirkabel, Black Hole Attack, Zigbee 802.15.4, Keamanan Jaringan, Internet of Things.