ANALISA PENDETEKSIAN SERANGAN BLACKHOLE PADA JARINGAN MANET (MOBILE AD-HOC NETWORK) MENGGUNAKAN METODE GENETIC ALGORITMA

[1]Kafi Ramadhani Borut, [2]Supeno Djanali, [3]Radityo Anggoro
[1]Program Studi Teknik Informatika, Fakultas Ilmu Komputer
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Jalan Raya Rungkut Madya Gunung Anyar Surabaya
[2,3]Program Studi Magister Teknik Informatika, Fakultas Teknologi Informasi,
Institut Teknologi Sepuluh Nopember, Surabaya
Email: [1]kafiramadhani@gmail.com, [2]supeno@its.ac.id, [3]onggo@if.its.ac.id

Abstrak. *MANET merupakan sebuah topologi baru dalam jaringan wireless yang sering digunakan dan dikembangkan untuk sebuah penelitian saat ini. MANET (Mobile Ad-hoc network) merupakan sebuah jaringan yang terdisentralisasi namun tidak tergantung oleh infrastruktur seperti router. Jaringan MANET ini juga tidak dapat dikatakan 100 % aman dari sisi keamanan jaringannya. Banyak serangan-serangan yang sering digunakan untuk membuat jaringan MANET ini down. Namun serangan yang sering digunakan dalam beberapa penelitian yang ada dalam jaringan MANET khususnya pada protokol routing AODV adalah serangan blackhole.Serangan blackhole ini mengadopsi kelemahan dalam jaringan MANET yaitu dari sisi Route Discovery atau pencarian rute. Pada proses Route Discovery dalam jaringan MANET dimana setiap node dalam jaringan mengirimkan RREQ (Route Request) dengan sistem broadcast untuk mencari sebuah rute jaringan dan mengenali node tetangganya. Masing-masing node akan menerima dan mengirim kembali broadcast dengan header Route Replay (RREP).Dalam penelitian ini, penulis ingin mengemukakan rancangan untuk mendeteksi dan mengklasifikasikan serangan blackhole dalam jaringan AODV menggunakan metode GA (Genetic Algorithm) Serta menganalisa dan mendeteksi pola serangan blackhole berdasarkan nilai throughput dan delay dari aktifitas jaringan masing-masing node ketika serangan blackhole tersebut terjadi.*

Kata Kunci: Serangan Blackhole, Genetic Algoritma, SVM, Throughput, Delay

Research dalam jaringan wireless sudah berkembang saati ini. Muncul beberapa topologi baru seperti WSN (Wireless Sensor Network) dan MANET (Mobile Ad-Hoc Network). Masing-masing topologi baru ini di-kembangkan untuk membuat jaringan wireless yang tidak membutuhkan sumber daya infrastruktur yang besar namun dapat dinikmati oleh segala pengguna jaringan wireless. MANET merupakan sebuah topologi baru dalam jaringan wireless yang sering digunakan dan dikembangkan untuk sebuah penelitian saat ini. MANET (Mobile Ad-hoc network) merupa-kan sebuah jaringan terdisentralisasi namun tidak tergantung oleh infrastruktur seperti router. Node dapat berkomunikasi dengan semua node lain dalam rentang radio yang mereka miliki, sementara node yang tidak di kisaran range jangkauan wireless dapat lang-sung menggunakan node lain (s) yang terdekat jangkauannya untuk berkomunikasi dengan satu sama lain [1].

Jaringan MANET ini juga tidak dapat dikatakan 100 % aman dari sisi keamanan jaringannya. Banyak serangan-serangan yang sering diguna-kan untuk membuat jaringan MANET ini down dan antara node tidak dapat berkomunikasi [2]. Adapun beberapa serangan yang sering diguna-kan dalam jaringan MANET antara lain Wormhole Attack, Suspicious Attack, Flooding Attack dan Blackhole Attack. Namun serangan yang sering digunakan dalam beberapa penelitian yang ada dalam jaringan MANET khususnya pada protokol routing AODV adalah serangan blackhole. Serangan blackhole ini mengadopsi kelemahan dalam jaringan MANET yaitu dari sisi Route Discovery atau pencarian rute. Pada proses Route Discovery dalam jaringan MANET dimana setiap node dalam jaringan mengirim-kan RREQ (Route Request) dengan sistem broadcast [3] untuk mencari sebuah rute jaringan dan mengenali node tetangganya. Masing-masing node akan menerima dan mengirim kembali broadcast dengan header

Route Replay (RREP) yang telah dikirim dari destination node. Malicious node sebagai penyerang mencoba untuk mencegah pencarian rute yang di lakukan oleh source node. Dengan mengirim paket RREP (Route Reply) palsu pada source node sehingga mampu membanjiri jaringan dan menggagalkan terjadinya rute dalam jaringan AODV antara source node dengan destination node. Untuk mengatasi permasalahan diatas, beberapa penelitian telah dilakukan.

Pada penelitian selanjutnya [4], penulis mem-buat sebuah permodelan IDS (Intrusion Detection System) pada sistem seleksi fitur menggunakan Genetic algoritma dan metode SVM (Support Vetcor Machine) pada proses klasifikasinya. Dimana genetic algoritma ini digunakan untuk menemukan fitur-fitur yang cocok pada dataset

Oleh karena itu, Dalam penelitian ini, penulis ingin mengemukakan rancangan untuk mendeteksi serangan blackhole dalam jaringan AODV menggunakan metode GA (Genetic Algorithm) sebagai proses pemilihan fitur dataset dan mengklasifikasikan serangan tersebut menggunakan metode SVM (Support Vector Machine). Serta menganalisa dan mendeteksi pola serangan blackhole berdasar-kan nilai throughput dan delay dari aktfitas jaringan masing masing node ketika serangan blackhole tersebut terjadi.

I. Metodologi

Pada bab ini, akan dibahas 2 simulasi untuk mendukung penelitian ini. Simulasi AODV dan simulasi serangan blackhole digunakan untuk menghasilkan sebuah data awal yang digunakan untuk proses pre-processing pada IDS. Proses pre-processing ini digunakan untuk memfilter data apa yang akan digunakan untuk mendetek-si sebuah malicious node dan normal node khususnya pada serangan blackhole. Proses ini dapat disebut juga dengan proses pemilihan fitur dataset. Pada proses pemilihan fitur dataset, genetic algoritma digunakan untuk menyeleksi fitur data yang terbaik. Hasil data dari pemilihan / seleksi fitur GA (Genetic Algorithm) digunakan dan dikelola oleh system Intrusi (SVM) untuk menentukan apakah ini serangan blackhole atau hanya sebuah normal node yang bekerja. Harapan dari penilitian ini, dengan metode GA menaikkan nilai deteksi serangan blackhole dan mengurangi nilai kesalahan deteksi.

Studi Literatur

Pada penelitian sebelumnya [5], penulis mene-mukan sebuah konsep baru dengan menggu-nakan ANT Colony Optimization untuk men-deteksi dan mencegah serangan blackhole. Penulis mengembangkan dan menambahan source code pada script AODV dengan menambahkan sebuah fitur FORWARD_ANT dan BACKWARD _ANT. FORWARD ANT digunakan untuk menganalisa jumlah malicious node yang akan melakukan serangan. Setelah serangan tersebut terjadi dimana malicious node mengirimkan sebuah paket data yang memiliki sequence number yang cukup besar, maka BACKWARD_ANT akan menampung jumlah paket yang dikirimkan oleh malicious node tersebut untuk mengantisipasi dampak dari serangan tersebut.

Pada penelitian selanjutnya[4], penulis mem-buat sebuah permodelan IDS (Intrusion Detection System) pada sistem seleksi fitur menggunakan Genetic algoritma dan metode SVM (Support Vetor Machine) pada proses klasifikasinya. Dimana genetic algoritma ini digunakan untuk menemukan fitur-fitur yang cocok pada dataset untuk mendeteksi serangan yang terjadi dalam jaringan MANET. Penulis merubah fitness function untuk menyeleksi serangan tersebut dengan rumus detection rate dikurangi oleh false positive rate untuk menggenerate sebuah dataset yang baru yang akan diklarifikasi oleh SVM untuk menentukan apakah ini sebuah serangan atau bukan, dan hasilnya penulis mendapatkan peningkatan detection rate dengan rata-rata peningkatan 0.5 % pada masing-masing simulasinya.

Simulasi AODV

Pada sub-bab ini, penulis merancang sebuah percobaaan atau simulasi jaringan AODV untuk mendapatkan data awal untuk proses seleksi fitur pada penelitian ini. Adapun scenario percobaan AODV yang digunakan pada penelitian ini dan akan dijelaskan secara detail pada Tabel 1.

Tabel 1 Simulasi AODV

PARAMETER	VALUE
Simulator	NS (Network Simulator)-3.21
Waktu simulasi	80 Second
Jumlah Node	25
Routing Protokol	AODV
Traffic Model	CBR
Wifi	Wifi PHY standart 802-11 b
Mobility	Random Way Point
Terrain Area	500 m x 500 m
Transmision Range	250 m
Source Node	Node 0 – nodes 13
Destination Node	Node 14 – 24

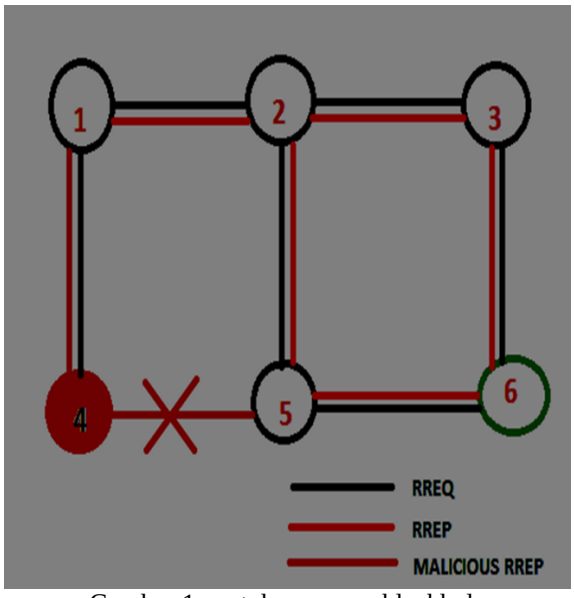
Serangan Blackhole

Serangan blackhole adalah sebuah serangan yang sering dilakukan dalam jaringan MANET. Serangan blackhole ini mengadopsi kelemahan dalam jaringan MANET yaitu dari sisi Route Discovery atau pencarian rute. Pada proses Route Discovery dalam jaringan MANET dimana setiap node dalam jaringan mengirimkan RREQ (Route Request) dengan sistem broadcast [3] untuk mencari sebuah rute jaringan dan mengenali node tetangganya. Masing-masing node akan menerima dan mengirim kembali broadcast dengan header Route Replay (RREP) yang telah dikirim dari destination node. Malicious node sebagai penyerang mencoba untuk mencegah pencarian rute yang di lakukan oleh source node.

Pengirmian RREP palsu yang dikirim oleh malicious node atau attacker's itu merupakan tipuan untuk source node. Sehingga ketika source node mencari sebuah rute baru untuk menuju ke destination terkelabui dengan RREP palsu tersebut. RREP palsu yang dikirim memiliki ciri-ciri sebagai berikut:

1. No dari sequence number yang dikirimkan dalam paket RREP palsu oleh malicious node lebih besar dari pada sequence number pada umumnya.
2. No hop count yang ada dalam paket RREP palsu lebih kecil dari Hop count pada umumnya yang terjadi dalam penentuan rute dalam jaringan MANET. Sehingga source node menentukan arah tujuan ke destination node harus melalui malicious node.
3. Ketika malicious node mendapatkan kirim-an packet data dari source node menuju destination node, secara langsung malicious node akan menolak packet data tersebut dengan mengirimkan route reques error untuk sampai ketujuan.

Adapun contoh gambar serangan blackhole yang dijelaskan oleh gambar 1 dibawah ini:



Gambar 1 contoh serangan blackhole

Simulasi Serangan Blackhole

Pada penelitian ini simulasi serangan blackhole yang akan dilakukan dijelaskan dalam tabel 2 dibawah ini

Tabel 2 Simulasi Serangan Blackhole

Uji Coba	**protocol**	**Malicous**	**Node Attack**	**Normal Node**
1	AODV	1	N0	24
2	AODV	2	N0, N11	23
3	AODV	3	N0,N7,N11	22
4	AODV	4	N0,N5.N11,N18	21
5	AODV	5	N0,N5,N7,N11, N18	20

Adapun penjelasan skenario pengujian serangan blackhole pada penelitian ini adalah sebagai berikut

1. Pengujian serangan ke 1 akan dilakukan oleh 1 malicious node yang akan melancarkan serangan blackhole. Node yang akan melakukan serangan blackhole adalah node 0.

2. Pengujian serangan ke 2 akan dilakukan oleh 2 malicious node yang akan melancarkan serangan blackhole. Node yang akan melakukan serangan blackhole adalah node 0 dan node 11.
3. Pengujian serangan ke 3 akan dilakukan oleh 3 malicious node yang akan melancarkan serangan blackhole. Node yang akan melakukan serangan blackhole adalah node 0, node 7, dan node 11.
4. Pengujian serangan ke 4 akan dilakukan oleh 4 malicious node yang akan melancarkan serangan blackhole. Node yang akan melakukan serangan blackhole adalah node 0, node 5, node 11 dan node 18.
5. Pengujian serangan ke 5 akan dilakukan oleh 5 malicious node yang akan melancarkan serangan blackhole. Node yang akan melakukan serangan blackhole adalah node 0, node 5, node 7, node 11, dan node 18

Klasifikasi

Klasifikasi dan prediksi adalah dua bentuk analisis data yang bisa digunakan untuk mengekstrak model dari data yang berisi kelas-kelas atau untuk memprediksi trend data yang akan datang. Klasifikasi memprediksi data dalam bentuk kategori, sedangkan prediksi memodelkan fungsi-fungsi dari nilai yang kontinyu. Misalnya model klasifikasi bisa dibuat untuk mengelompokkan aplikasi peminjaman pada bank apakah beresiko atau aman, sedangkan model prediksi bisa dibuat untuk memprediksi pengeluaran untuk membeli peralatan komputer dari pelanggan potensial berdasarkan pendapatan dan lokasi tinggalnya. Prediksi bisa dipandang sebagai pembentukan dan penggunaan model untuk menguji kelas dari sampel yang tidak berlabel, atau menguji nilai atau rentang nilai dari suatu atribut[6].

Data input untuk klasifikasi adalah koleksi dari record. Setiap record dikenal sebagai instance atau contoh, yang ditentukan oleh sebuah tuple (x,y), dimana x adalah himpunan atribut dan y adalah atribut tertentu, yang dinyatakan sebagai label kelas. Pemodelan klasifikasi dibagi menjadi 2 yaitu pemodelan deskriptif dan pemodelan prediktif. Pemodelan deskriptif merupakan model klasifikasi dapat bertindak sebagai alat penjelas untuk membedakan objek-objek dari kelas-kelas yang berbeda. Sedangkan pada pemodelan prediktif, model klasifikasi yang juga dapat digunakan untuk memprediksi label kelas dari record yang tidak diketahui. Beberapa teknik klasifikasi yang digunakan untuk jenis model ini adalah support vector machine, rule-based classifier, decision tree classifier, neural network dan naive bayes classifier

Pendekatan umum yang digunakan dalam masalah klasifikasi adalah pertama training set berisi record yang mempunyai label kelas yang diketahui haruslah tersedia. Training set digunakan untuk membangun model klasifikasi, yang kemudian diaplikasikan ke test set, yang berisi record-record dengan label kelas yang tidak diketahui.

SVM (Support Vector Machines)

Support Vector Machine dikembangkan oleh Boser, Guyon, Vapnik, dan pertama kali dipresentasikan pada tahun 1992 di Annual Workshop on Computational Learning Theory. Konsep SVM dapat dijelaskan secara sederhana sebagai usaha mencari hyperplane terbaik yang berfungsi sebagai pemisah dua buah kelas pada input space. pattern yang merupakan anggota dari dua buah kelas : +1 dan -1 dan berbagi alternative garis pemisah (discrimination boundaries). Margin adalah jarak antara hyperplane tersebut dengan pattern terdekat dari masing-masing kelas. Pattern yang paling dekat ini disebut sebagai support vector. Usaha untuk mencari lokasi hyperplane ini merupakan inti dari proses pembelajaran pada SVM [7].

Pembahasan teori SVM dimulai dengan kasus klasifikasi yang secara linier bisa dipisahkan. Dalam hal ini fungsi pemisah yang dicari adalah fungsi linier. Fungsi ini bisa didefinisikan sebagai

g(x) := sgn(f(x))

dengan$(x) = w\mathrm{T}\ x+b$

$$atau\ g(x) = \begin{cases} +1, jika\ (Wx+b) \geq +1 \\ -1, jika\ (Wx+b) \leq -1 \end{cases}$$

dimanax, w $\in\Re$n and b $\in\Re$.

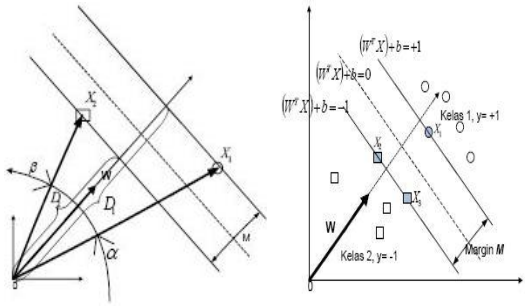
Masalah klasIfikasi ini bisa dirumuskan sebagai berikut: kita ingin menemukan set parameter (w, b) sehingga f(xi) =< w, x >+b =yi untuk semua i. Dalam teknik ini kita berusaha menemukan fungsi pemisah

(klasifier/hyperplane) terbaik diantara fungsi yang tidak terbatas jumlahnya untuk memisahkan dua macam obyek.

Hyperplane terbaik adalah hyperplane yang terletak di tengah-tengah antara dua set obyek dari dua kelas. Mencari hyperplane terbaik ekuivalen dengan memaksimalkan margin atau jarak antara dua set obyek dari kelas yang berbeda. Jika $wx1+b=+1$ adalah pendukung hyperplane dari kelas +1 ($wx2+b=+1$) dan $wx2+b=-1$ pendukung hyperplane dari kelas -1($wx2+b=-1$) , margin antara dua kelas dapat dihitung dengan mencari jarak antara kedua pendukung hyperplane dari kedua kelas. Secara spesifik, margin dihitung dengan cara berikut:

$$w(x_1 - x_2)) = 2 \rightarrow (\frac{w}{||w||}(x_1 - x_2)) = \frac{2}{||w||}$$

Dan secara detailnya bagaimana nilai margin optimal diperoleh seperti dijelaskan pada gambar 3 berikut ini :



(a) (b)

Gambar 2.(a). Nilai jarak optimal (b) hyperplane

Confusion Matrix

Confusion matrix merupakan metode yang menggunakan tabel matriks seperti pada Tabel 1, jika data set hanya terdiri dari dua kelas, kelas yang satu dianggap sebagai positif dan yang lainnya negatif [8].

Tabel 3. Model Confusion Matrix

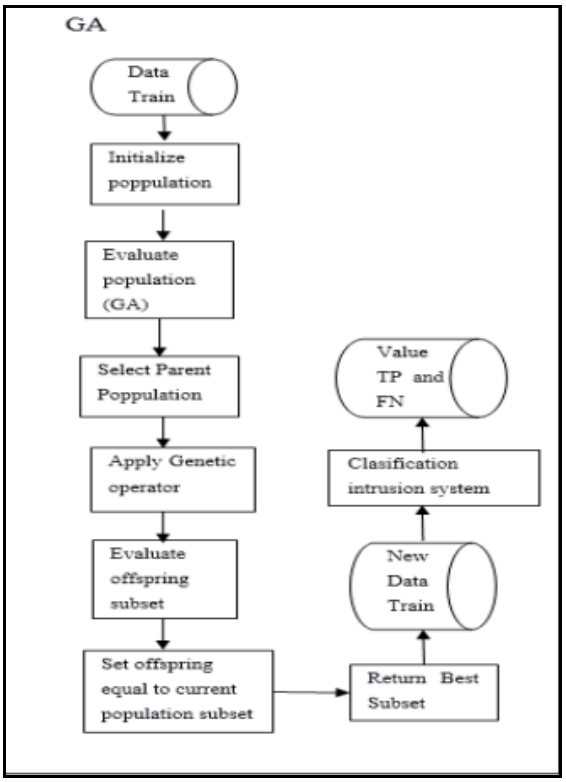
		True Class	
		Positive	*Negative*
Predicted Class	*Positive*	*True positives count (TP)*	*False negatives count (FP)*
	Negative	*False positives count (FN)*	*True negatives count (TN)*

True positives adalah jumlah record positif yang diklasifikasikan sebagai positif, false positives adalah jumlah record negatif yang diklasifikasikan sebagai positif, false negatives adalah jumlah record positif yang diklasifikasikan sebagai negatif, true negatives adalah jumlah record negatif yang diklasifikasikan sebagai negative, kemudian masukkan data uji. Setelah data-data telah masuk ke dalam confusion matrix maka dapat dihitung nilai-nilai sensitivity (recall), specificity, precision dan accuracy. Untuk menghitung digunakan persamaan di bawah ini [8]:

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP}$$

Diagram Alur seleksi fitur dan klasifikasi serangan blackhole menggunakan Metode GA (Genetic Algoritma)

Pada tahapan ini, merupakan tahapan penting untuk keberhasilan penelitian ini. Dimana sebuah analisis pengujian algoritma GA (Genetic Algoritma) yang dipakai untuk penelitian ini. Penjelasan lebih detailnya dijelaskan oleh gambar 3 yang ada dibawah. Penelitian ini fokus kepada mendeteksi serangan blackhole menggunakan metode Genetic algoritma sebagai proses pemilihan fitur dataset terbaik guna meningkatkan nilai detection rate dan mengurangi nilai false detection rate pada metode SVM untuk mengklasifikasi serangan blackhole. Setelah percobaan serangan blackhole dilakukan, didapatkan 20 DataSet dan DataTrain dari 5 percobaan scenario serangan blackhole ber-dasar-kan masing-masing kondisi jaringan yang sudah ditentukan dan dijelaskan pada sub-bab berikutnya. Pembeda antara masing-masing percobaan adalah jumlah malicious node / node penyerang. Proses pengumpulan data dilakukan setelah proses seleksi fitur data yang berguna untuk menemukan titik terdekat solusi per-masalahan fitur data dalam mendeteksi serang-an blackhole.



Gambar 3. Alur Genetik Algoritma

Setelah process pemilihan fitur dilakukan maka akan menghasilkan sebuah dataset untuk mendeteksi serangan blackhole yang sudah optimal untuk diklasifikasikan oleh metode SVM (Support Vector Machine) sebagai malicious node atau normal node. Sehingga menghasilkan nilai detection rate dan nilai false detection rate

Parameter Uji

Adapun parameter yang akan diujikan dalam penelitian ini adalah sebagai berikut:

1. Variasi Nilai presentase deteksi rate serangan blackhole menggunakan metode Genetic Algoritma (GA)-SVM dan Ant Colony Optimization (ACO)-SVM. Berdasarkan kondisi jaringan yang dibedakan menjadi 4 yaitu
   a. Low Mobility (5 m/s) - Medium Traffic (512 Kbps) (LMMT)
   b. Low Mobility (5 m/s) - High Traffic (1 Mbps) (LMHT)
   c. High Mobility (20 m/s) - Medium Traffic (512 Kbps) (HMMT)
   d. High Mobility (20 m/s) - (High Traffic) (1 Mbps) (HMHT)
2. Variasi Nilai throughput jaringan AODV ketika terjadinya serangan Blackhole sesuai dengan scenario dan berdasarkan 4 kondisi jaringan.
3. Variasi Nilai delay jaringan AODV ketika terjadinya serangan Blackhole sesuai dengan scenario dan dan berdasarkan 4 kondisi jaringan

II. Hasil dan Pembahasan

Pada sub bab ini akan dibahas tentang hasil uji coba dari penelitian ini. Adapun hasilnya akan dijelaskan pada beberapa sub bab dibawah ini:

Hasil Uji Coba Deteksi Serangan dengan GA-SVM

Adapun hasil seleksi fitur dan klasifikasi GA-SVM yang sudah dilakukan ini berdasarkan 4 kondisi jaringan yang sudah dilakukan dapat dilihat pada tabel 4, tabel 5, tabel 6, tabel 7 di bawah ini:

Tabel 4. Hasil fitur seleksi dan Klasifikasi GA-SVM pada kondisi jaringan LMMT

Sk	Data		GA-SVM			
	DS	DT	FS	BC	DR	FN
1	100	400	2,3,4,5	0.51	400 Data	0 Data
					100 %	0 %
2	100	400	4,5,6	1.34	400 Data	0 Data
					100 %	0 %
3	100	400	1,2,4,5,6	0.86	400 Data	0 Data
					100 %	0 %
4	100	400	2,5,6	1.76	400 Data	0 Data
					100 %	0 %
5	100	400	1,3,4,6	1,6	398 Data	2 Data
					99.5 %	0.5 %

Tabel 5. Hasil fitur seleksi dan Klasifikasi GA-SVM pada kondisi jaringan LMHT

Sk	Data		GA-SVM			
	DS	DT	FS	BC	DR	FN
1	100	400	1,3,4,5,6	1.64	398 Data	2 Data
					99.5 %	0.5 %
2	100	400	2,5,6	1.42	400 Data	0 Data
					100 %	0 %
3	100	400	1,3,4,6	0.5	398 Data	2 Data
					99.5 %	0.5 %
4	100	400	1,2,4,6	1.03	398 Data	2 Data
					99.5 %	0.5 %
5	100	400	1,3,6	0.3	399 Data	1 Data
					99.75 %	0.25 %

Tabel 6. Hasil fitur seleksi dan Klasifikasi GA-SVM pada kondisi jaringan HMMT

Sk	Data		GA-SVM			
	DS	DT	FS	BC	DR	FN
1	100	400	1,2,4,6	1.83	399 Data	1 Data
					99.75 %	0.25 %
2	100	400	1,2,4,5,6	1.05	390 Data	10 Data
					97.5 %	2.5 %
3	100	400	1,3,5,6	1.85	388 Data	12 data
					97 %	3 %
4	100	400	1,2,4,5,6	1.61	380 Data	20 data
					95 %	5 %
5	100	400	1,3,5,6	2.2	399 Data	1 Data
					99.75 %	0.25 %

Tabel 7. Hasil fitur seleksi dan Klasifikasi GA-SVM pada kondisi jaringan HMHT

Sk	Data		GA-SVM			
	DS	DT	FS	BC	DR	FN
1	100	400	3,6	1.37	399 Data	1 Data
					99.75 %	0.25 %
2	100	400	2,3,4,5,6	1.87	377 Data	23 Data
					94.25 %	5.75 %
3	100	400	1,3,4,5,6	1.38	365 Data	35 Data
					91.25 %	8.75 %
4	100	400	1,2,4,6	1.07	382 Data	18 Data
					95.5 %	4.5 %
5	100	400	1,3,5,6	1.77	390 Data	10 Data
					97.5 %	2.5 %

Dari 5 scenario yang ada terdapat 20 hasil Detection rate fitur seleksi dan klasifikasi serangan blackhole menggunakan GA (Genetic Algorithm)-SVM. Adapun rata-rata detection rate serangan blackhole menggunakan metode GA-SVM diatas berdasarkan kondisi jaringan LMMT sebesar 99.9 %, LMHT sebesar 99.65 %, HMMT sebesar 97.8 %, HMHT sebesar 95.65 %. Dari 4 kondisi tabel diatas dapat disimpulkan oleh tabel 8 dibawah ini:

Tabel 8. Hasil Rata-Rata Detection Rate mengunakan GA-SVM berdasarkan 4 kondisi jaringan

Simulation	GA-SVM
Low Mobility Medium Traffic (LMMT)	99.9
Low Mobility High Traffic (LMHT)	99.65
High Mobility Medium Traffic (HMMT)	97.8
High Mobility High Trrafic (HMHT)	95.65

Dari keterangan table diatas dapat disimpulkan bahwa mengklasifikasikan serangan blackhole menggunakan metode Genetik Agoritma (GA) sangat akurat. Adapun hasil Rata-rata True Positif dan False Negative berdasarkan kondisi jaringan LMMT mendapatkan nilai TP 99.9 % dan FN 0.1, LMHT dengan nilai TP 99.65% dan FN 0.35 , HMMT dengan nilai TP 97.8 % dan FN 2.2, HMHT dengan nilai TP 95.65 % dan FN 4.35.

Analisa Perbandingan nilai thdoughput dan delay jaringan

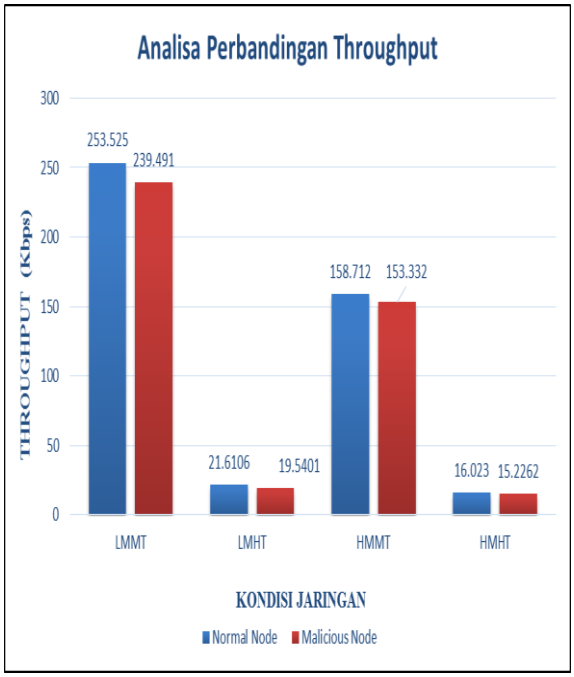
Adapun hasil dari analisa perbandingan nilai normal throughput, delay dengan malicious throughput, delay dapat dijelaskan oleh tabel 9 dibawah ini

Tabel 9 Analisa perbandingan average through-put dan delay normal node dan malicious node berdasarkan 4 kondisi jaringan

Simulasi	Normal T	Normal D	MaliciousT	Malicious D
LMMT	253.525	5430.7	239.491	5238.778
LMHT	21.6106	3638.41	19.5401	3742.682
HMMT	158.712	4195.42	153.332	4045.61
HMHT	16.023	3777.25	15.2262	3267.544

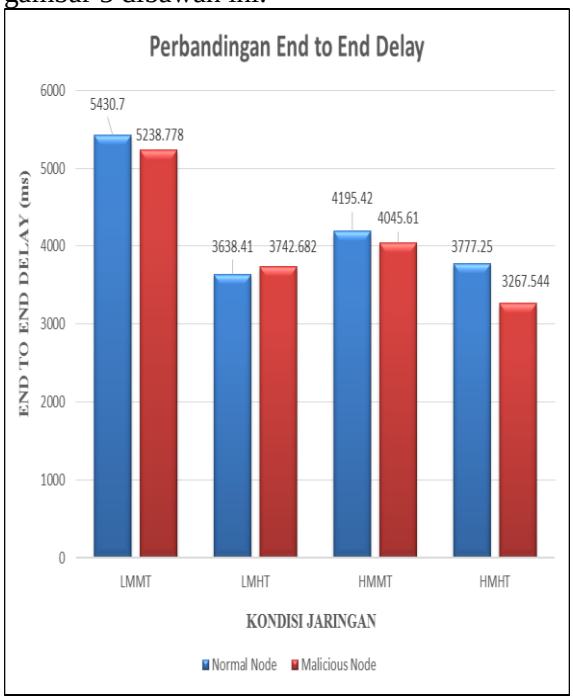
Dapat disimpulkan bahwa terdapat perbedaan antara hasil throughput dan delay dari jaringan AODV untuk normal node dan jaringan AODV yang memiliki malicious node. Dimana hasil average throughput dari malicious node lebih kecil dari pada jumlah average

throughput jaringan AODV node normal tanpa malicious node seperti yang dijelaskan pada gambar 4 dibawah.



Gambar 4. Analisa Perbandingan Throughput normal node dengan malicious node.

Dan hasil end to end delay malicious node lebih kecil daripada hasil dari end to end delay normal node seperti yang dijelaskan pada gambar 5 dibawah ini.



Gambar 5. Analisa perbandingan end to end delay normal node dengan malicious node.

III. Simpulan

Berdasarkan hasil analisa uji coba fitur seleksi dan klasifikasi serangan blackhole mengguna-kan metode Genetik algoritma (GA) – Support Vector Machine (SVM) memiliki tingkat akurasi yang tinggi. Adapun hasil rata-rata deteksi dan akurasi menggunakan metode GA–SVM sebesar 98.25 % dengan nilai FN (False Negative) 1.75. Mekanisme untuk mendeteksi serangan blackhole menggunakan nilai through-put dan delay jaringan berdasarkan terjadinya serangan dapat dilakukan. Berdasarkan hasil ujicoba membuktikan bahwa hasil average throughput dari jaringan AODV dengan malicious node lebih kecil dari pada jumlah average throughput jaringan AODV node normal tanpa malicious. Dan hasil end to end delaydari jaringan AODV dengan malicious node lebih kecil daripada hasil daripada end to end delay dari jaringan AODV dengan normal node.

IV. Daftar Pustaka

[1] Alokparna Bandyopadhyay, Satyanarayana Vuppala and Prasenjit Choudhury “A Simulation Analysis of Flooding Attack in MANET using NS-3”, Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Syst,, Feb. 28 2011-March 3 2011.

[2] Mohamed M Ibrahim, Nayera Sadek and Mohamed El-Banna, “Prevention of dropping routing traffic attack in wireless Ad-Hoc AODV-based network using Real-time Host Intrusion Detection” Radio Science Conference, IEEE, 2009

[3] Yoav Sasson, David Cavin, and Andre Schiper,”Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks” CiteSeer Conference 2002.

[4] Sevil Sen and Zeynep Dogmus, “Feature Selection for Detection of Ad Hoc Flooding Attacks” NeCom 2012

[5] Sowmya K.S, Rakesh T, Deepthi P Hudedagaddi.”Detection and Prevention of Blackhole Attack in MANET Using ACO”IJCSNS Vol 12, No.5, May 2012

[6] Anonim, 2013, DOS Attack id.wikipedia.com.

[7] Like Zhang, Gregory B.White, 2007, Analysis of Payload Based Application Level Network Anomaly Detection, The 40th Hawaii International Conference on System Sciences.

[8] Qinglei Zhang, Wenying Feng, 2009. Network Intrusion Detection by Support Vectors and Ant Colony. Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009), pp 639-642.

Halaman ini sengaja dikosongkan.