Analisis Penerapan Teknik Pertahanan Jaring Laba – Laba Untuk Meningkatkan Akurasi Deteksi Serangan *Wireless Sensor Network* (WSN)

Analysis Implementation of Web Spider Defense Technique for Increase The Accuracy of Attack Detection in Wireless Sensor Network (WSN)

Maulina Ngalimatul Ghoniya[1], Fazmah Arif Yulianto, S.T., M.T.[2], Sidik Prabowo, S.T., M.T.[3]
Prodi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom
[1]ngalimatul@gmail.com, [2]fazmaharif@telkomuniversity.ac.id, [3]prabowosidik@gmail.com

Abstrak

Menjamin keamanan dan privasi merupakan salah satu prioritas tertinggi dalam WSN karena data yang dikumpulkan oleh sensor node tidak jarang merupakan data yang bersifat rahasia. Terdapat sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan berbasis nirkabel, yaitu *Wireless Intrusion Detection System* (WIDS). Namun, dari sekian banyak teknik pendekatan untuk WIDS belum ada yang dapat sepenuhnya terhindar dari kesalahan berupa *false negative*. Mekanisme cara kerja teknik pertahanan jaring laba – laba akan diterapkan pada alur kerja WIDS yang dibangun dengan tujuan mengurangi adanya *false negative*. Penerapannya dalam sistem nyata adalah memberikan *delay* untuk setiap paket yang masuk. Metode pengujian yang dilakukan berupa pengujian deteksi serangan dan perhitungan *false negative*. Pengujian deteksi serangan dilakukan dengan memberikan serangan *inside attack* berupa serangan *access point spoofing* dan serangan *de-authentication flood*. Hasil dari pengujian deteksi serangan menunjukkan bahwa WIDS mampu mendeteksi adanya serangan *inside attack*. Sementara perhitungan *false negative* mendapatkan hasil bahwa seiring ditambahkannya waktu *delay*, presentase *false negative* yang didapatkan mengalami penurunan namun kemudian dapat naik kembali. Pemberian waktu *delay* paling ideal kurang lebih 500 ms dengan tingkat presentase *false negative* berkurang hingga 66.37%.

Kata kunci: *false negative, Wireless Intrusion Detection System* (WIDS), sistem keamanan, teknik pertahanan jaring laba-laba, *Wireless Sensor Network* (WSN).

1. Pendahuluan

Wireless Sensor Network (WSN) dapat didefinisikan sebagai jaringan *wireless* yang terdiri dari ratusan hingga ribuan sensor node yang secara kooperatif memantau kondisi lingkungan [1]. Menjamin keamanan dan privasi merupakan salah satu prioritas tertinggi dalam WSN karena data yang dikumpulkan oleh sensor node tidak jarang merupakan data yang bersifat rahasia. Sensor node memiliki beberapa keterbatasan, seperti rendahnya ketersediaan sumber daya, ruang penyimpanan dan kemampuan komputasi [2]. Keamanan untuk WSN dapat dibangun menggunakan metode *authentication, cryptography* atau *key management*. Namun metode tersebut membutuhkan ruang penyimpanan dan kemampuan komputasi yang tinggi sehingga bertentangan dengan keterbatasan yang dimiliki oleh sensor node dalam WSN [3]. Terdapat sebuah aplikasi perangkat lunak yang dapat mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan nirkabel, disebut *Wireless Intrusion Detection System* (WIDS).

Berbagai teknik telah digunakan untuk merancang WIDS di dalam WSN. Salah satu teknik yang diterapkan menggunakan mekanisme *bio-inspired networking*. *Bio-inspired networking* merupakan suatu pendekatan terinspirasi dari berbagai struktur biologis yang mampu melakukan *self-organization* [4]. Namun, dari sekian banyak teknik pendekatan tidak ada yang sempurna, yang selalu benar membedakan perilaku abnormal dengan perilaku normal. WIDS mungkin melakukan kesalahan dengan mengidentifikasi aktivitas normal menjadi suatu aktivitas yang abnormal, disebut dengan *false positive*. Atau berlaku sebaliknya dengan *false negative*, mengidentifikasi aktivitas abnormal sebagai aktivitas normal.

Dalam tugas akhir ini akan dibangun WIDS yang mengadaptasi cara kerja jaring laba-laba ketika menangkap mangsa. WIDS akan menerapkan perilaku pertahanan jaring laba - laba dengan memberikan *delay* pada mekanisme sistem keamanan yang dibangun. *Delay* tersebut berfungsi untuk menahan paket yang masuk, kemudian dilakukan pengecekan apakah paket tersebut merupakan serangan atau bukan. Pengecekan ini ditujukan untuk mengurangi adanya *false negative*. Dengan tingginya nilai *false negative* menyebabkan sistem rentan terhadap serangan [5].

2. Landasan Teori

2.1. *Wireless Sensor Network* (WSN)

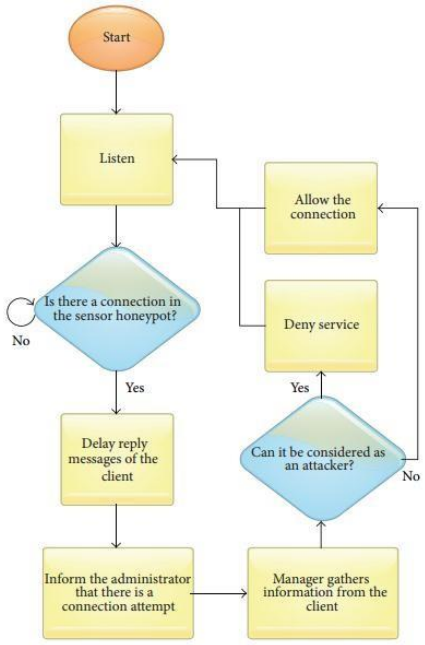
Wireless Sensor Network (WSN) merupakan jaringan nirkabel yang memiliki sensor untuk memantau kondisi fisik atau lingkungan dan mengumpulkan informasi seperti suhu, suara, tekanan dan secara kooperatif menyalurkan data hasil pantauan melalui jaringan nirkabel ke *server* [2]. Infrastruktur WSN dapat dibagi menjadi dua bagian, jaringan akuisisi data dan jaringan penyebaran data [6]. Jaringan akuisisi data terdiri node sensor dan *base station*. Sensor node memiliki tugas mengukur kondisi fisik. Sedangkan *base station* bertanggung jawab mengumpulkan data dari sensor serta menyampaikan perintah dari pengguna ke aktuator. Jaringan penyebaran data bertugas menyediakan hasil akuisisi data untuk pengguna dalam bentuk *interface.* Komponen utama yang dibutuhkan untuk membangun WSN berupa *memory*, *communication device* untuk mentransmisikan data, *controller* sebagai pengendali seluruh komponen, sensor dan akuator serta catu daya.

2.2. Sensor Node

Komponen utama sensor node terdiri dari unit sensor, *analog to digital converter* (ADC), *central processing unit* (CPU), unit sumber daya dan unit komunikasi [7]. Node sensor merupakan *micro-electro-mechanical-system* (MEMS) yang menghasilkan respon berupa data terhadap perubahan kondisi fisik lingkungan seperti suhu dan tekanan [7]. Sinyal analog yang didapatkan oleh sensor akan dirubah menjadi sinyal digital melalui *analog to digital converter*. Kemudian data digital tersebut dikirim ke *controller* untuk diproses lebih lanjut. Sensor node memiliki ukuran yang sangat kecil, mengkonsumsi energi yang sangat rendah dan adaptif terhadap lingkungan sekitar.

2.3. Teknik Pertahanan Jaring Laba – Laba

Pada referensi [8] mekanisme teknik pertahanan jaring laba – laba diadaptasi menjadi sebuah algoritma pertahanan pada WSN dengan mengkombinasikan *honeypot* dan *Intrusion Detection System* (IDS). Alur kerja algoritma teknik pertahanan jaring laba – laba pada sistem keamanan WSN dapat dilihat pada Gambar 2.1. Ketika ada koneksi yang masuk ke *honeypot*, *honeypot* akan memberikan *delay* ke koneksi tersebut karena seharusnya tidak ada yang perlu mengakses *honeypot*. Kemudian *honeypot* mengirimkan informasi ke administrator bahwa ada koneksi yang masuk. Admin mengumpulkan informasi mengenai *client* dan menentukan apakah koneksi tersebut dari penyusup atau bukan. Ciri khas dari mekanisme teknik pertahanan jaring laba – laba yang diadaptasi pada sistem keamanan adalah pemberian *delay* ke setiap koneksi yang masuk ke *honeypot*. Tujuan dari pemberian *delay* tersebut untuk mendapatkan informasi yang lebih mengenai penyusup. Karena penentuan sebuah koneksi merupakan suatu serangan atau bukan, dilakukan oleh seorang admin. Sehingga diperlukan informasi yang detail mengenai koneksi yang masuk ke *honeypot*. Berbeda dengan algoritma yang diusulkan pada referensi [8], dalam tugas akhir ini tujuan dari diberikannya *delay* terhadap sistem ingin mengurangi adanya *false negative* tanpa mengurangi nilai *true positive*. Selain itu, perancangan sistem yang dibangun menggunakan WIDS tanpa mengkombinasikan dengan *honeypot*.



Gambar 2.1 Algoritma Teknik Pertahanan Jaring Laba – Laba.

2.4. *Wireless Intrusion Detection System (*WIDS)

Wireless Intrusion Detection System (WIDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan [10]. WIDS akan memonitor lalu lintas data pada sebuah jaringan atau mengambil data dari berkas log. Intrusion sendiri adalah aktivitas tidak sah atau tidak diinginkan yang mengganggu konfidensialitas, integritas dan atau ketersediaan informasi yang terdapat di sebuah sistem. WIDS dapat dianggap sebagai sensor yang memproses informasi yang masuk ke dalam sistem. Perbedaan mendasar antara WIDS dan *Intrusion Detection System* (IDS) tradisional terletak pada layer yang menjadi konsentrasi pengamanannya. IDS fokus menangani ancaman untuk layer tiga ke atas. Sementara dalam jaringan nirkabel selain ancaman pada layer tiga ke atas, juga memiliki beberapa ancaman unik untuk layer satu dan dua. Ancaman tersebut berasal dari penggunaan *Radio Frequency* (RF) sebagai media komunikasi. IDS tradisional tidak dapat melakukan *monitoring* terhadap ancaman pada layer satu dan dua. WIDS membutuhkan *interface* khusus dimana *interface* tersebut harus dioperasikan pada mode monitor, disebut dengan mode RFMON. Dengan mode RFMON, suatu perangkat diperbolehkan menerima semua lalu lintas yang masuk.

2.5. Serangan dalam *Wireless Sensor Network* (WSN)

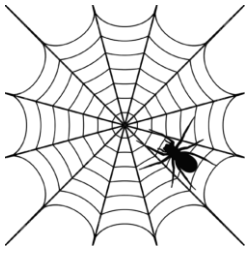
Dengan segala karakteristik yang dimiliki *Wireless Sensor Network*, mulai dari terbatasnya sumber daya hingga teknik *broadcast* yang digunakan untuk mengirimkan data, membuat WSN rentan terhadap beberapa ancaman keamanan. Beberapa serangan yang dapat menjadi ancaman bagi WSN, sebagai berikut [11]:

1. Hello Flood Attack
2. *Selective Forward Attack*
3. *Wormhole Attack*
4. *Sybil Attack*
5. *Denial of Service Attack*

3. Perancangan Sistem

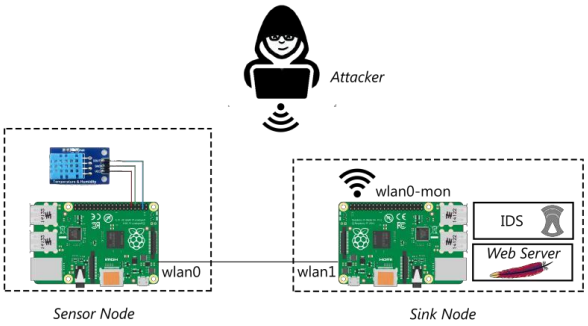
3.1. Gambaran Umum

Dalam tugas akhir ini terdapat beberapa aspek pada sistem keamanan yang dibangun terinspirasi dari teknik pertahanan jaring laba – laba. Aspek pertama, arsitektur laba – laba memiliki yang pola unik seperti yang digambarkan pada Gambar 3.1. Dimana pola yang dibangun oleh laba – laba memiliki banyak simpul yang saling terkait. Hal ini dianalogikan dengan WSN yang terdiri dari beberapa sensor node yang saling terhubung. Dari segi anatomi laba – laba sendiri, laba – laba memiliki indera peraba pada kakinya yang berjumlah delapan. Indera tersebut memiliki fungsi mendeteksi adanya getaran pada jaring yang menunjukkan adanya mangsa yang masuk ke dalam jaring. Indera peraba akan mengirimkan *impulse* ke sistem syaraf pusat apabila merasakan getaran. *Tools* WIDS yang digunakan dalam tugas akhir ini menyediakan fitur berupa Kismet *drone* dan Kismet *server*. Kismet *drone* memiliki fungsi layaknya indera peraba pada laba – laba yang akan mendeteksi adanya aktivitas abnormal pada WSN kemudian mengirimkan notifikasi ke kismet *server* apabila terdeteksi suatu aktivitas abnormal.



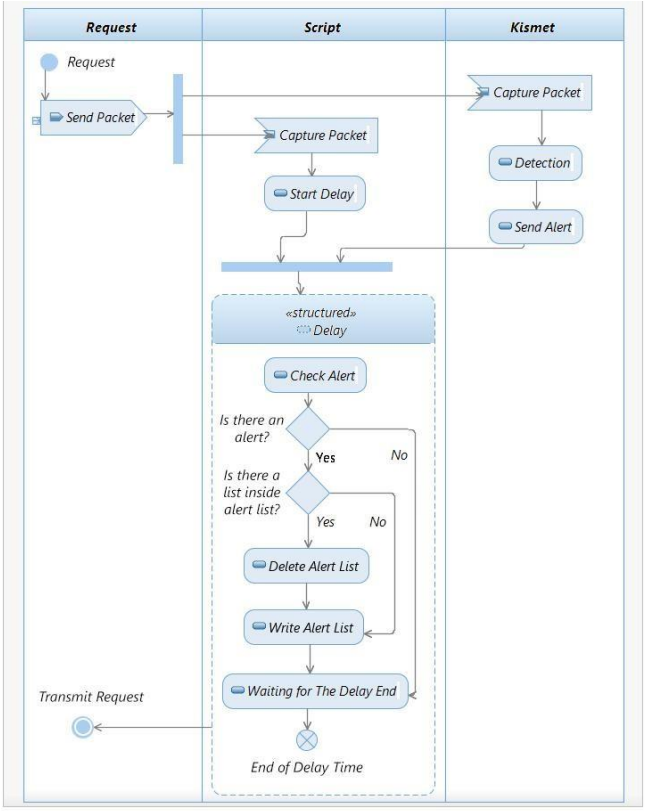
Gambar 3.1 Arsitektur Jaring Laba - Laba

Aspek lain yang diadaptasi dari jaring laba – laba adalah mekanisme cara kerja jaring laba – laba dalam menahan mangsa yang masuk ke jaring, bukan dari segi arsitektur jaring laba – laba. Arsitektur penerapan teknik pertahanan jaring laba – laba untuk keamanan WSN digambarkan pada Gambar 3.2. WIDS akan diletakkan di *sink node*. WIDS bekerja pada *interface* wlan dengan mode monitor. *Interface* wlan tersebut akan berubah menjadi *wlan0-mon.* Selain bertugas memantau keamanan sistem, *sink node* juga akan bertugas sebagai *web server*. Data yang berhasil dihimpun oleh sensor node ditransmisikan langsung ke *web server* yang berada di *sink node* untuk diolah. Seperti yang terlihat pada gambar 3.1., *sink node* dan sensor node berkomunikasi secara *wireless* menggunakan protokol 802.11 b/g melalui *interface* wlan.



Gambar 3.2 Desain Arsitektur Sistem.

3.2. Perancangan Sistem



Gambar 3.3 Diagram Aktivitas WIDS Menerapkan Teknik Pertahanan Jaring Laba – Laba.

Teknik pertahanan jaring laba – laba sendiri memiliki ciri khas pada tahap dimana mangsa dijebak dalam jaring laba – laba. Kemudian laba – laba akan menyuntikkan racun ke mangsa dengan tujuan memperlambat pergerakan mangsa hingga akhirnya mangsa lumpuh dan tidak dapat memberikan perlawanan. Penerapan teknik pertahanan jaring laba – laba dalam sistem nyata adalah diberikannya *delay* untuk setiap paket yang masuk. Seperti yang digambarkan pada diagram aktivitas Gambar 3.3., yang berwenang untuk memberikan delay adalah Script. Script merupakan *bash script* yang terdiri dari beberapa aktivitas. Aktivitas pertama, script akan menangkap paket yang masuk menuju *web server*. *Request* yang tertangkap, tidak akan langsung dikirimkan ke *web server* melainkan ditahan terlebih dahulu oleh script dengan memberikannya *delay*. Adanya *delay* berfungsi untuk memberikan waktu kepada sistem keamanan melakukan pengecekan apakah paket yang masuk dan terdeteksi serangan oleh WIDS benar – benar merupakan serangan atau bukan, berlaku juga sebaliknya. Selain bertugas memberikan delay, script juga menjadi penghubung antara *server* dan WIDS berupa aplikasi Kismet. Kismet merupakan perangkat lunak untuk mendeteksi serangan dalam jaringan

nirkabel. . Karena Kismet bekerja pada sistem nirkabel, maka setiap paket yang ditransmisikan selalu terdeteksi oleh Kismet tanpa perlu masuk ke *interface* Kismet. Oleh karena itu, pada Gambar 3.3., paket yang yang dikirimkan oleh r*equest* dapat ditangkap langsung oleh Kismet dan script secara bersamaan. Kismet mampu menangkap paket tersebut karena terdapat di lalu lintas dalam jaringan jangkauannya. Sedangkan script berada di *sink node* sama seperti *server*, sehingga script dapat menangkap adanya *request* yang masuk.

3.3. Fungsionalitas

Fungsionalitas sistem merupakan kemampuan yang harus terpenuhi untuk menentukan keberhasilan suatu sistem yang dibangun. Berikut beberapa indikator fungsionalitas sistem:

1. *Intrusion Dectection System* mampu mendeteksi adanya *inside attack*.
2. *Intrusion Dectection System* akan memberikan *alert* ketika ada serangan.
3. Memberikan *delay* untuk setiap *request* yang masuk ke *sink node* sebelum *request timeout*.
4. Mampu mengurangi jumlah *false negative* dari sebelum diberikannya *delay.*

3.4. Spesifikasi Kebutuhan Sistem

Untuk menunjang fungsionalitas sistem dan tujuan dari tugas akhir ini, maka dalam perancangan sistem diperlukan perangkat sebagai berikut:

3.4.1. Perangkat Keras

1. Raspberry Pi 2
2. Wi-Fi *Dongle*
3. Sensor DHT 11
4. Kabel *Jumper*
5. Laptop atau PC

3.4.2. Perangkat Lunak

1. Kismet
2. Wireshark

3.5. Tahapan Instalasi dan Konfigurasi

Tahapan instalasi dan konfigurasi dalam tugas akhir ini terbagi menjadi dua sisi, yaitu sisi WSN dan sisi WIDS. Sisi WSN berhubungan dengan instalasi sensor node dan *web server*. Sementara, WIDS berhubungan dengan instalasi sebuah perangkat lunak WIDS bernama Kismet dan penulisan *script*. Berikut tahapan instalasi dan konfigurasi yang dilakukan dalam membangun WIDS untuk WSN menerapkan teknik pertahanan jaring laba – laba.

1. Penyusunan Lingkungan Kerja
2. Instalasi Sensor Node
3. Instalasi dan Konfigurasi *Web Server*
4. Instalasi dan Konfigurasi Kismet
5. Konfigurasi *Shell Script*

4. Pengujian dan Analisa

4.1. Metode dan Skenario Pengujian

1. Pengujian Deteksi Serangan

   Pengujian deteksi serangan bertujuan untuk menguji apakah sistem keamanan yang dibangun sudah berfungsi dengan baik memenuhi salah satu kebutuhan fungsionalitas sistem yang sudah disebutkan dalam bab 3. Sistem keamanan yang dibangun diharapkan dapat mendeteksi adanya aktivitas abnormal dalam jaringan dan mampu memberikan *alert* apabila terdeteksi sebagai serangan. Dalam pengujian ini akan dilakukan pengujian terhadapserangan *access point spoofing* dan *de-authentication flooding.*

2. Perhitungan *False Negative*

   Perhitungan ini bertujuan menganalisis pengaruh pemberian *delay* pada sistem keamanan yang dibangun terhadap *false negative* yang dihasilkan oleh WIDS. Skenario pada metode pengujian ini dilakukan dengan mengubah besarnya waktu *delay* untuk koneksi yang masuk dari 0 ms hingga 900 ms. Skenario pengujian yang dijalankan akan dihadapkan pada serangan *de-authentication flood.* Serangan *de-authentication flood* dipilih karena *frame de-authentication* yang terdeteksi dari serangan ini dapat dianalisis melalui Wireshark.

4.2. Perhitungan dan Analisis

4.2.1. Pengujian Deteksi Serangan

1. Serangan *Access Point* (AP) *Spoofing*

   Serangan AP *Spoofing* dijalankan dengan membuat suatu AP palsu yang meniru MAC *address* AP yang sah. Untuk menjalankan serangan ini digunakan *tools* dari aircrack-ng berupa airbase-ng. Airbase-ng

berfungsi untuk menyediakan AP palsu. Airbase-ng memperbolehkan *user* untuk menentukan SSID serta channel sesuai keinginan *user*. Sehingga penyerang yang ingin melakukan serangan AP *Spoofing* dapat mengatur BSSID dan SSID agar serupa dengan AP yang sah.

Pada pengujian ini AP palsu akan meniru MAC *address* serta SSID dari AP dalam jaringan WSN yang dibangun. Akan tetapi, AP palsu yang dibuat tidak menggunakan enkripsi. *Spoofed* AP akan terdeteksi oleh Kismet dengan menganalisis adanya AP dengan MAC *Address* yang sama namun ada yang tidak menggunakan enkripsi. Sehingga AP tersebut diduga akan menipu *client* agar terhubug ke AP palsu. Kismet mengenali serangan ini sebagai CRYPTODROP. *Alert* yang di-*generate* oleh Kismet dapat dilihat pada Gambar 4.1.

```
Network BSSID FE:85:DE:31:DF:4D stopped advertising encryption
Network BSSID FE:85:DE:31:DF:4D stopped advertising encryption
Network BSSID FE:85:DE:31:DF:4D stopped advertising encryption
Network BSSID FE:85:DE:31:DF:4D stopped advertising encryption
```

Gambar 4.1 *Alert* untuk Serangan AP *Spoofing*

2. Serangan *De-Authentication Flood*

Dalam pengujian ini akan dilakukan serangan *de-authentication flood* dengan skenario memutuskan semua *client* yang terhubung dengan AP dalam WSN yang dibangun. Serangan *de-authentication* akan menyebabkan node – node dalam WSN terputus dari jaringan dan tidak dapat saling berkomunikasi. Serangan *de-authentication flood* dapat dijalankan menggunakan *tools* aireplay-ng yang merupakan bagian dari *package* aircrack-ng. Aireplay-ng memberikan keleluasaan bagi *user* untuk menentukan jumlah paket *de-authentication* yang akan diinjeksikan. Aireplay-ng akan menyamar sebagai AP yang akan mengirim paket *de-authentication* secara broadcast. Kismet akan mendeteksi adanya serangan *de-authentication flood* dengan menganalisis adanya paket *de-authentication* secara *broadcast*. Serangan ini dikenal oleh Kismet sebagai BCASTDISCON.

```
FE:85:DE:31:DF:4D broadcast deauthenticate/disassociation of all clients
FE:85:DE:31:DF:4D broadcast deauthenticate/disassociation of all clients
FE:85:DE:31:DF:4D broadcast deauthenticate/disassociation of all clients
FE:85:DE:31:DF:4D broadcast deauthenticate/disassociation of all clients
FE:85:DE:31:DF:4D broadcast deauthenticate/disassociation of all clients
```

Gambar 4.2 *Alert* untuk Serangan *De-Authentication Flood*

4.2.2 Uji Pengaruh *Delay* Terhadap *False Negative*

Pada pengujian ini akan dilakukan beberapa skenario pengujian dengan mengubah parameter *delay*. Tujuan dari pengujian yang dilakukan untuk mengetahui bagaimana pengaruh besarnya waktu *delay* yang diberikan pada alur kerja sistem keamanan terhadap nilai *false negative* yang dihasilkan oleh WIDS. Pemberian *delay* dilakukan oleh *script* yang berada pada node. Sehingga setiap ada *request* menuju node secara otomatis seluruh paket akan mengalami *delay*. Kemampuan sistem keamanan yang dibangun dalam memberikan *delay* ditunjukkan pada Gambar 4.3.

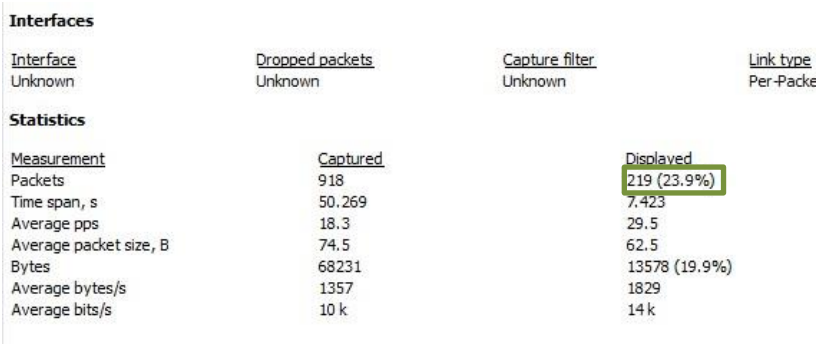
```
C:\Users\Maya>ping 192.168.138.106

Pinging 192.168.138.106 with 32 bytes of data:
Reply from 192.168.138.106: bytes=32 time=502ms TTL=64
Reply from 192.168.138.106: bytes=32 time=501ms TTL=64
Reply from 192.168.138.106: bytes=32 time=501ms TTL=64
Reply from 192.168.138.106: bytes=32 time=501ms TTL=64

Ping statistics for 192.168.138.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 501ms, Maximum = 502ms, Average = 501ms
```

Gambar 4.3 Hasil Pemberian *Delay* pada Node

Saat mendeteksi adanya serangan, Kismet akan menghasilkan beberapa *file* output. Salah satunya Kismet menghasilkan *file* keluaran berupa .pcapdump yang dapat dibaca dan dianalisis dengan Wireshark. Langkah analasis yang dilakukan, agar Wireshark hanya menampilkan *frame de-authentication* isilah kolom „Filter" dengan kata kunci "wlan.sa==FE-85-DE-31-DF-4D && wlan.fc.type_subtype==0x0c". FE-85-DE-31-DF-4D merupakan MAC *address* dari *access point* yang digunakan dalam WSN. 0x0c merupakan kode subtipe dari *management frame* untuk *frame de-authentication flood.* Gambar 4.4 memperlihatkan serangan *de-authentication flood* yang telah ter-*filter*.



Interfaces

Interface	Dropped packets	Capture filter	Link type
Unknown	Unknown	Unknown	Per-Packe

Statistics

Measurement	Captured	Displayed
Packets	918	219 (23.9%)
Time span, s	50.269	7.423
Average pps	18.3	29.5
Average packet size, B	74.5	62.5
Bytes	68231	13578 (19.9%)
Average bytes/s	1357	1829
Average bits/s	10 k	14 k

Gambar 4.4 Hasil Analisis Wireshark untuk *Frame De-authentication*

Parameter *delay* yang diberikan pada pengujian ini dimulai dari tanpa adanya *delay* atau *delay* = 0 ms kemudian bertambah dengan kelipatan 100 ms hingga mencapai 900 ms. Serangan *de-authentication flood* akan dikirimkan sebanyak 10 paket. Untuk setiap skenario, pengujian dilakukan sebanyak 30 kali. Rangkuman hasil akhir seluruh skenario pengujian dapat dilihat pada Tabel 4.1. yang menujukkan rata – rata *frame de-authentication* yang berhasil terdeteksi oleh Kismet untuk setiap skenario *delay*. Pada Tabel 4.1. terlihat bahwa *true positive* yang berhasil terdeteksi bertambah berbanding lurus dengan penambahan *delay* yang diberikan. Namun kenaikan tersebut berhenti saat *delay* sebesar 500 ms. Untuk *delay* di atas 500 ms, nilai *true positive* mengalami penurunan.

Tabel 4.1 Hasil Akhir Tiap Skenario *Perhitungan False Negative*

Waktu *Delay* (ms)	Rata–rata *frame de-authentication* yang berhasil terdeteksi (*frame*)
0	150.47
100	171.13
200	184.83
300	219.37
400	230.47
500	250.33
600	244.07
700	229.5
800	206.5
900	179.17

Presentase *false negative* dapat dihitung menggunakan persamaan:

Keterangan:

= Presentase *False Negative frame de-authentication* (*frame*)

= Rata – rata *frame de-authentication* saat delay = 0 (*frame*)

= Rata – rata *frame de-authentication* dari *delay* 250 ms atau 500 ms (*frame*)

Tabel 4.2 Jumlah Presentase *False Negative*

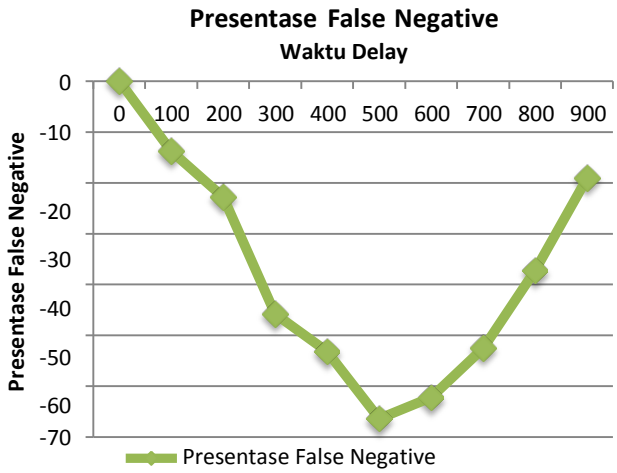
Presentase *False Negative* (%)								
100 ms	200 ms	300 ms	400 ms	500 ms	600 ms	700 ms	800 ms	900 ms
-13.74	-22.84	-45.79	-53.17	-66.37	-62.21	-52.53	-37.24	-19.07

Hasil perhitungan presentase *false negative* berdasar nilai rata - rata *frame de-athentication* yang terdeteksi oleh Kismet ditunjukkan pada Tabel 4.4. Hasil nominal negatif yang didapatkan pada Tabel 4.4 merupakan bentuk penurunan jumlah *false negative* dibandingkan dengan hasil deteksi saat tanpa adanya *delay*. Semakin besar nominal negatif yang dihasilkan maka semakin besar penurunan presentase *false negative*. Dari hasil pengujian menunjukkan bahwa terdapat penurunan presentase *false negative* untuk *delay* 100 ms hingga 500 ms. Kemudian presentase *false negative* menunjukkan kenaikan setelah *delay* 500 ms hingga 900 ms. Untuk gambaran lebih jelas mengenai penurunan dan kenaikan presentase *false negative*, grafik hasil perhitungan presentase *false negative* dapat dilihat pada Gambar 4.5.

False negative mengalami penurunan untuk *delay* 100 ms hingga 500 ms. Nilai penurunan presentase *false negative* bermula dari *delay* 100 ms -13.74%, -22.84% untuk 200 ms, -45.79% untuk 300 ms, -53.17% untuk 400 ms hingga mencapai nilai tertinggi -66.37% untuk waktu *delay* 500 ms. Sedangkan untuk *delay* di atas 500 ms, presentase *false negative* mulai mengalami kenaikan dibandingkan dengan nilai *false negative* yang berhasil dicapai pada waktu *delay* 500 ms. Saat diberikan *delay* sebesar 600 ms, presentase *false negative* bertambah menjadi -62.21 %, naik 4.16% dari presentase *false negative* saat *delay* 500 ms. Dan presentase *false negative* terus mengalami kenaikan untuk *delay* 700 ms hingga 900 ms.

Hasil perhitungan presentase *false negative* dalam pengujian ini menunjukkan bahwa pemberian *delay* memliki pengaruh mengurangi jumlah *false negative*. Akan tetapi agar *false negative* yang didapatkan seminimal mungkin terdapat waktu *delay* yang ideal, dengan *false negative* paling sedikit namun *frame* yang masuk belum mengalami *request timeout*. Dari pengujian ini didapatkan hasil waktu *delay* yang ideal yakni kurang lebih sebesar 500 ms. Dikarenakan presentase *false negative* untuk *delay* kurang dari 500 ms nilai yang didapatkan masih di bawah presentase *false negative* untuk *delay* 500 ms. Dan presentase *false negative* kembali menurun untuk *delay* di atas 500 ms.

Penambahan *delay* teruji mampu mengurangi adanya *false negative*. Dengan adanya *delay*, paket yang masuk ke node akan ditahan sementara waktu untuk menunggu giliran masuk. Mekanisme ini dapat mengurangi kepadatan *traffic* yang disebabkan oleh *frame de-authentication*. Sehingga Kismet dapat lebih jeli mengenali paket yang masuk. Di sisi lain, pemberian waktu *delay* yang terlalu lama dapat menyebabkan banyak *frame* mengalami *request timeout*. Sehingga *frame* yang ter-*drop* tersebut tidak dapat dikenali sebagai serangan dan menambah jumlah *false negative*.



Gambar 4.5 Grafik Presentase *False Negative*

5. Kesimpulan dan Saran

5.1. Kesimpulan

Berdasarkan hasil dari implementasi, pengujian dan analisis yang telah dilakukan terhadap penerapan teknik pertahanan jaring laba – laba untuk meningkatkan akurasi deteksi serangan pada WSN didapatkan kesimpulan sebagai berikut:

1. Implementasi teknik pertahanan jaring laba – laba untuk meningkatkan akurasi deteksi serangan pada WSN menggunakan WIDS dapat dibangun sesuai perancangan sistem.
2. Hasil dari pengujian deteksi serangan dan perhitungan *false negative* memperlihatkan bahwa sistem keamanan yang dibangun mampu mendeteksi adanya serangan *inside attack* berupa serangan AP *spoofing* dan *de-authentication flood*, menampilkan *alert*, memberikan *delay* untuk tiap paket yang masuk dan meningkatkan akurasi deteksi.
3. Dalam perhitungan *false negative*, hasil pengujian menunjukkan adanya penurunan presentase *false negative* saat diberikan *delay* 100 ms hingga 500 ms. Akan tetapi untuk *delay* lebih dari 500 ms presentase *false negative* yang dihasilkan mulai mengalami kenaikan kembali. Fenomena tersebut menunjukkan pemberian *delay* yang berlebihan sehingga beberapa paket mengalami *request timeout* kemudian ter-*drop* dan menyebabkan berkurangnya *frame* yang seharusnya terdeteksi sebagai serangan.
4. Teknik pertahanan jaring laba – laba mampu meningkatkan akurasi deteksi serangan pada WSN dengan waktu ideal pemberian *delay* kurang lebih sebesar 500 ms. Dengan pemberian *delay* 500 ms, dihasilkan pengurangan presentase *false negative* paling tinggi mencapai 66.37% dibandingkan saat tidak diberikan *delay*.

5.2. Saran

Beberapa saran pengembangan sistem yang dapat dilakukan berdasarkan pada tugas akhir ini, sebagai berikut:

1. Menambahkan konfigurasi pada *script* agar sistem keamanan yang dibangun dapat bekerja sama langsung dengan Kismet secara *real-time.*
2. Penerapan sistem keamanan pada tiap sensor node menggunakan Kismet-*drone*.
3. Melakukan analisa terhadap hasil deteksi berdasarkan nilai *true negative* dan *false positive.*
4. Melakukan analisis performansi lebih lanjut terhadap penerapan teknik pertahanan jaring laba – laba, seperti perhitungan *end-to-end delay*, *packet delivery ratio* dan *packet loss*.

6. Daftar Pustaka

[1] M. Garcia, D. Bri, S. Sendra dan J. Lloret, "*Practical deployments of wireless sensor networks : a survey*, " Journal On Advaces in Networks and Services, vol 3, 2010.

[2] Z. Feng dan G. Leonidas, "*Wireless Sensor Networks: An Information Processing Approach*," Morgan Kaufmann.

[3] B. Deependra, "*Intrusion Detection System for Wireless Sensor Network*," National Institute of Technology Rourkela, 2014.

[4] S. Binitha dan S. Siva "*A Survey of Bio Inspired Optimization Algorithms*," *International Journal of Soft Computing and Engneering* (IJSCE), 2012.

[4] L. Javier dan Z. Jianying, "*Overview of Wireless Sensor Network Security*," IOS Press, 2008.

[5] M. Asieh, F. Ahmad dan G. Arash, "*False Positives Reduction Techniques Intrusion Detection Systems - A Review*", *International Journal of COmputer Science and Network Security*, VOL. 13 No. 10, 2013.

[6] L. Javier dan Z. Jianying, "*Overview of Wireless Sensor Network Security*," IOS Press, 2008.

[7] S. Weilian, S. Yogesh dan C. Erdal, "*A Survey on Sensor Networks*,"*Georgia Institute of Technology, 2002.*

[8] Y. Harun, "*The Miracle in The Spider*", *Goodword Books*, 2010.

[9] C. Alejandro, L. Jaime, M. Elsa dan S. Alvaro, "*Web Spider Defense Technique in Wireless Sensor Networks*," 2014.

[10] Y. Maleh dan A. Ezzati, "*A Review of Security Attacks and Intrusion Detection Schemes in WIreless Sensor Network*," *International Journal of WIreless & Mobile Networks*, vol. 5, no. 6, 2013.

[11] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "*Intrusion Detection of Sinkhole Attacks in Wireless Sensor Network*," *Algorithmic Aspect of Wireless Sensor Networks*, Springer, 2008.