

**PENGESANAN PENCEROBOHAN TRAFIK PENEROWONGAN IPV6
BERASASKAN RANGKAIAN NEURAL PERAMBATAN BALIK**

NAZRULAZHAR BIN BAHAMAN

**TESIS YANG DIKEMUKAKAN UNTUK MEMPEROLEH IJAZAH
DOKTOR FALSAFAH**

**FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI**

2014

PENAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang setiap satunya telah saya jelaskan sumbernya.

11 September 2014

NAZRULAZHAR BIN BAHAMAN
P 50007

PENGHARGAAN

Syukur Alhamdulillah kepada Allah S.W.T kerana memberikan saya kesihatan yang cukup, masa dan kematangan fikiran untuk menyiapkan penyelidikan ini. Jutaan terima kasih yang rasanya tidak saya mampu untuk balas kembali hingga ke akhir hayat saya kepada penyelia utama Prof. Madya Dr. Anton Satria Prabuwono atas bantuan yang begitu besar, bimbingan, teguran dan nasihat yang begitu berguna sepanjang kajian ini. Tidak lupa juga kepada Prof. Madya Dr. Mohd. Faizal Abdollah dan Dr. Robiah Yusof dengan kepakaran masing-masing yang banyak membantu menguatkan lagi semangat saya untuk menyiapkan kajian ini. Terima kasih juga saya ucapkan kepada pihak KPM dan UTeM atas kebenaran mengikuti pengajian ini serta skim bantuan SLAI yang banyak membantu dari segi kewangan pada kajian ini.

Sumber data bagi penulisan ini telah diperoleh dari trafik rangkaian UTeM. Penulis ingin mengucapkan ribuan terima kasih kepada pegawai-pegawai UTeM khususnya pegawai dari Pusat Komputer kerana membantu saya dari segi pengurusan serta kebenaran dalam proses penyediaan data. Tidak lupa juga pegawai-pegawai dari FTMK, UTeM kerana membenarkan saya menggunakan peralatan dengan semaksimumnya. Begitu juga dengan pegawai yang bertanggungjawab terhadap sumber maklumat di perpustakaan FTSM, UKM. Sekalung penghargaan juga tidak saya lupakan buat NAV6, USM yang telah banyak menyediakan input dari segi data dan maklumat terkini dari luar negara.

Terima kasih yang tidak terhingga juga ditujukan kepada ayahanda serta bonda tercinta Haji Bahaman Kaba dan Hajah Saoma Zakaria yang telah banyak memberi sokongan dan dorongan bagi menyiapkan pengajian ini. Juga kepada isteri serta anak-anak tersayang Elia Erwani Hassan, Muhammad Adeeb Amsyar, Nur Aeen Insyirah dan Nur Aimee Irdyindah atas pengorbanan yang ditempuhi bersama.

ABSTRAK

Setelah melaksanakan mekanisme peralihan IPv6 sebagai pemangkin peralihan protokol Internet, telah memberi kesan terhadap prestasi sebahagian daripada teknik anti pencerobohan. Sistem Pengesanan Pencerobohan (SPP) adalah antara yang amat terkesan di mana kadar janaan penggera palsu yang meningkat ekoran corak ancaman yang berubah. Sebagai tindakan, tesis ini mencadangkan suatu penerbitan corak dan permodelan serangan implikasi penggunaan mekanisme peralihan iaitu penerowongan 6to4. Perolehan maklumat dari permodelan tersebut digunakan bagi mereka bentuk Sistem Pengesanan Pencerobohan Rangkaian Penerowongan (SPP-RP) yang memfokuskan kepada serangan DoS yang tersembunyi di dalam paket kapsul penerowongan yang dikenali sebagai protokol-41. Objektif penyelidikan ini adalah (i) menganalisis tahap keberkesanan SPP semasa terhadap serangan DoS pada model medan uji penerowongan, (ii) menerbitkan corak dan model serangan DoS Alihan Penerowongan (SeDAP), (iii) menggubal kaedah pengelasan corak dengan bantuan algoritma pengelasan RN, dan (iv) menilai serta mengesahkan pembangunan kaedah pengelasan corak mampu meningkatkan pengesanan dan mengurangkan kadar bilangan penggera palsu. Pembangunan medan uji berpandukan model Makmal Lincoln MIT yang melalui beberapa kaedah pengujian bagi memastikan jenis peralatan dan tatarajah tidak mempengaruhi hasil keputusan penyelidikan. SPP-RP terdiri daripada 3 peringkat utama dan setiap darinya terdapat beberapa bahagian. Pertama, peringkat input mengandungi bahagian penangkapan. Kedua, peringkat Pengesanan yang mengandungi bahagian pemprosesan, bahagian pengelasan dan bahagian penggera. Ketiga ialah peringkat output mewakili bahagian tindak balas. Kaedah pengelasan RNPB ini turut disepadukan dengan teknik pengesanan bagi menentukan status data. Tiga jenis algoritma latihan iaitu *Levenberg-Marquardt*, *Bayesian Regulation* dan *Scaled Conjugate Gradient* dibandingkan bagi memilih yang terbaik. Kesimpulannya, SPP-RP berkebolehan di dalam mengenal pasti trafik penerowongan yang mengandungi paket normal dan anomali dan turut berjaya membantu mengurangkan janaan penggera palsu.

IPV6 TUNNELING TRAFFIC INTRUSION DETECTION BASED ON BACK PROPAGATION NEURAL NETWORK

ABSTRACT

After implementing of IPv6 transition mechanism (TM) as IP catalyst transition has influences the performance on anti-intrusion system. IDS is one of the greatly affected where there is an increasing rate of false alarms generated due to changing patterns of threat. As an action, this thesis proposes new formulation of attack pattern and model lead by implication of TM named 6to4 tunneling. The outcomes from the model are used to develop SPP-RT that focuses on DoS attack that hiding in encapsulating tunneling packet known as protocol-41. The objectives of the research are (i) analysis the performance of IDS on the testbed model, (ii) formulate SeDAP pattern and model, (iii) ability to extract packet features from IPv4 and IPv6 header, and (iv) capable to increase detection rate and decrease false alarm using BPNN. The development of testbed refers to MIT Licoln Lab model was experimented through several testing methods. This accomplishment was done to ensure that the type of equipment and figure will maintain the accurate results. The SPP-RP formed by 3 major parts containing various modules individually. In first, Information Processing consists of capture module, status labeling module and features extraction module. Secondly, Detection part involved with preprocessing module and classification module. The third part called Output with alert notification module. Furthermore, the BPNN method has been integrated into classification module in determining the normal and anomaly status. Then, this BPNN module applied with 3 dissimilar training algorithms named as Levenberg-Marquardt, Bayesian Regulation and Scaled Conjugate Gradient. As a conclusion the highlighted SPP-RP perform capable to recognize tunneling traffic with normal or anomaly packet and a successful tool in reducing false alarm.

KANDUNGAN

		Halaman
PENGAKUAN		ii
PENGHARGAAN		iii
ABSTRAK		iv
ABSTRACT		v
KANDUNGAN		vi
SENARAI JADUAL		xii
SENARAI ILUSTRASI		xv
SENARAI SINGKATAN PERKATAAN		xxii
BAB I	PENDAHULUAN	
1.1	Latar Belakang	1
1.2	Penyataan Masalah	4
1.3	Objektif Penyelidikan	8
1.4	Skop Penyelidikan	9
1.5	Sumbangan Penyelidikan	9
1.6	Garis Panduan Tesis	10
1.7	Ringkasan	14
BAB II	KAJIAN KEPUSTAKAAN	
2.1	Pengenalan	15
2.2	Keselamatan Maklumat	15
2.3	Sistem Pengesan Pencerobohan	18
	2.3.1 Komponen asas	19
	2.3.2 Klasifikasi	21
	2.3.3 Sumber set data	25
	2.3.4 Kaedah pengesanan	26
	2.3.5 Teknik pengelasan corak	32
	2.3.6 Amaran	34
	2.3.7 Tindak balas	37
2.4	Pengelasan Umum Serangan Komputer	38
2.5	Ancaman DOS IPv6	39
	2.5.1 Jenis Serangsan DoS	40

2.5.2	Teknik serangan	41
2.6	Mekanisme Peralihan IPv6	43
2.6.1	Keperluan media peralihan	43
2.6.2	Kategori media peralihan	45
2.6.3	Trafik penerowongan 6to4	50
2.7	Pendekatan Kecerdasan Buatan Untuk Teknik Pengesanan	53
2.7.1	Rangkaian Neural dalam domain penyelidikan	54
2.7.2	Keberkesanan pengelasan Rangkaian Neural	55
2.8	Ringkasan	58
BAB III	METODOLOGI PENYELIDIKAN	
3.1	Pengenalan	60
3.2	Struktur Penyelidikan	60
3.2.1	Fasa I – Kajian literasi	62
3.2.2	Fasa II – Reka bentuk	63
3.2.3	Fasa III – Analisis	63
3.2.4	Fasa IV – Pembangunan	64
3.2.5	Fasa V – Pengujian	65
3.2.6	Fasa VI – Keputusan	65
3.3	Seni Bina SPP-RP	65
3.4	Rangka Kerja Perkakasan	66
3.4.1	Medan uji	67
3.4.2	Prestasi Sistem Pengesanan Pencerobohan semasa	69
3.4.3	Corak serangan penerowongan	70
3.4.4	Set data trafik	70
3.5	Rangka Kerja Perisian	71
3.5.1	Bahagian pemprosesan data	72
3.5.2	Bahagian pengelasan corak	74
3.5.3	Bahagian penggera	75
3.6	Ringkasan	76
BAB IV	IMPLIKASI PENEROWONGAN TERHADAP SISTEM PENGESANAN PENCEROBOHAN	
4.1	Pengenalan	77
4.2	Pembangunan Medan Uji Penerowongan	77
4.3	Matlamat	78
4.4	Penentuan Komponen	80
4.4.1	Hos dan sistem pengoperasian	81

4.4.2	Perkakasan rangkaian	82
4.4.3	Perisian keselamatan rangkaian	83
4.5	Pembangunan Rangkaian	84
4.5.1	Reka bentuk logik	85
4.5.2	Reka bentuk fizikal	87
4.5.3	Konfigurasi peralatan	88
4.6	Pengujian Rangkaian	90
4.6.1	Keputusan pengujian	92
4.6.2	Kesimpulan pengujian	96
4.7	Pengujian Sistem Pengesanan Pencerobohan	97
4.7.1	Penyediaan persekitaran	97
4.7.2	Tatarajah peralatan	98
4.7.3	Reka bentuk serangan	98
4.7.4	Perlaksanaan	99
4.7.5	Keputusan	102
4.7.6	Rumusan masalah dan isu-isu keselamatan	104
4.7.7	Perbincangan keputusan	106
4.8	Ringkasan	107
BAB V	SERANGAN DOS PENEROWONGAN DAN ALIHAN PENEROWONGAN	
5.1	Pengenalan	108
5.2	Permodelan Serangan	109
5.2.1	Tetapan persekitaran rangkaian	110
5.2.2	Perlaksanaan serangan pilihan	115
5.2.3	Pengumpulan log pemantau	117
5.2.4	Analisis hasil	118
5.3	Dapatan Serangan Banjir	120
5.3.1	Pemantauan aliran paket serangan banjir	121
5.3.2	Senario serangan banjir	130
5.3.3	Analisis serangan banjir secara umum	131
5.4	Dapatan Serangan Mengeksploitasi Protokol	134
5.4.1	Pemantauan aliran paket serangan	135
5.4.2	Senario serangan mengeksploitasi protokol	137
5.4.3	Analisis serangan mengeksploitasi protokol secara umum	138
5.5	Dapatan Eksperimen Serangan Paket Palsu	141
5.5.1	Pemantauan aliran paket serangan paket palsu	142
5.5.2	Senario serangan paket palsu	147
5.5.3	Analisis serangan paket palsu secara umum	148

5.6	Dapatan Serangan Balikan	151
	5.6.1 Pemantauan aliran paket serangan balikan	152
	5.6.2 Analisis serangan balikan secara umum	161
5.7	Analisis Corak Serangan Secara Umum	163
5.8	Cadangan Corak Serangan	166
5.9	Cadangan Model Serangan	167
	5.9.1 Model Serangan Dos Penerowongan	167
	5.9.2 Model Serangan DoS Alihan Penerowongan	169
5.10	Ringkasan	171
BAB VI	SISTEM PENGESANAN PENCEROBOHAN RANGKAIAN PENEROWONGAN	
6.1	Pengenalan	172
6.2	Rangka Kerja Sistem Cadangan	172
6.3	Modul Penangkapan Trafik	175
	6.3.1 Penyelarasan perkakasan	176
	6.3.2 Penyelarasan perisian	176
6.4	Modul Penyaringan Trafik	178
	6.4.1 Pemilihan trafik	179
	6.4.2 Pengasingan paket	180
6.5	Modul Pengekstrakan Ciri	183
	6.5.1 Pengekstrakan ciri dari pengepala IPv4	185
	6.5.2 Pengekstrakan ciri dari muatan IPv4	186
	6.5.3 Pengekstrakan ciri dari pengepala protokol	187
6.6	Modul Perubahan Nilai	188
6.7	Modul Pelabelan	193
6.8	Modul Penormalan Data	195
6.9	Modul Rangkaian Neural	197
	6.9.1 Pembangunan RN	197
	6.9.2 Penentuan matlamat dan data	198
	6.9.3 Penentuan topologi	199
	6.9.4 Fungsi pengaktifan	200
	6.9.5 Mengawal pemberat dan pincang	201
	6.9.6 Penentuan kadar pembelajaran	202
	6.9.7 Metrik prestasi	202
	6.9.8 Melatih RN	202
	6.9.9 Pengujian RN	204
6.10	Modul Amaran	204

6.11	Modul Tindak Balas	205
6.12	Ringkasan	206
BAB VII	PERBINCANGAN KEPUTUSAN	
7.1	Pengenalan	207
7.2	Penyediaan Set Data	207
	7.2.1 Data simulasi	208
	7.2.2 Data nyata	209
7.3	Tatacara Pengujian	210
7.4	Pengujian Bahagian Penangkapan	211
	7.4.1 Keputusan modul penangkapan trafik	211
7.5	Pengujian Bahagian Pemrosesan	214
	7.5.1 Keputusan modul penyaringan trafik	214
	7.5.2 Keputusan modul pengekstrakan ciri	215
	7.5.3 Keputusan modul penukaran nilai	216
7.6	Pengujian Bahagian Pengelasan	218
	7.6.1 Keputusan modul pelabelan	218
	7.6.2 Keputusan modul penormalan	221
	7.6.3 Keputusan modul rangkaian Neural	221
7.7	Pengujian Bahagian Penggera	224
	7.7.1 Keputusan modul amaran	224
7.8	Pengujian Sistem Keseluruhan	228
	7.8.1 Keputusan pengujian SPP Bro	229
	7.8.2 Keputusan pengujian SPP Snort	232
	7.8.3 Keputusan pengujian SPP-RP	236
	7.8.4 Perbandingan keputusan	239
7.9	Pengesahan Sistem Keseluruhan	242
	7.9.1 Keputusan	243
7.10	Ringkasan	245
BAB VIII	PENUTUP	
8.1	Pengenalan	247
8.2	Perbincangan	247
8.3	Sumbangan Penyelidikan	248
8.4	Kekangan Penyelidikan	252
8.5	Cadangan Masa Hadapan	253

8.6	Kesimpulan	254
RUJUKAN		256
LAMPIRAN		
A	SENARAI PENERBITAN DAN PERSIDANGAN	267
B	Akta Rahsia Rasmi	268
C	Data Ujian Prestasi Rangkaian IPv4 bagi Trafik TCP	269
D	Data Ujian Prestasi Rangkaian IPv6 bagi Trafik TCP	270
E	Data Ujian Prestasi Rangkaian Penerowongan bagi Trafik TCP	271
F	Data Ujian Prestasi Rangkaian IPv4 bagi Trafik UDP	272
G	Data Ujian Prestasi Rangkaian IPv6 bagi Trafik UDP	273
H	Data Ujian Prestasi Rangkaian Penerowongan bagi Trafik UDP	274
I	MIT Lincoln Laboratory	275

SENARAI JADUAL

Jadual		Halaman
1.1	Ringkasan permasalahan penyelidikan	7
1.2	Ringkasan persoalan penyelidikan	7
1.3	Ringkasan objektif penyelidikan	8
1.4	Ringkasan sumbangan penyelidikan	10
2.1	Sumber set data yang diperoleh mengikut jenis protokol	27
2.2	Antara kaedah Pengesanan Pencerobohan yang diguna pakai oleh penyelidik terdahulu	31
2.3	Jenis RN dalam meningkatkan teknik pengesanan pada SPP	55
2.4	Ringkasan perbandingan komponen oleh penyelidik terdahulu.	58
4.1	Ringkasan pembahagian hos mengikut OS dan bilangannya	82
4.2	Senarai ringkasan perkakasan dan perisian yang digunakan di dalam eksperimen	84
4.3	Contoh antara alamat IP yang di konfigurasi pada penghala	88
4.4	Nilai TO bagi TCP and UDP	96
4.5	Ringkasan keputusan keseluruhan yang diperoleh daripada eksperimen.	104
5.1	Cadangan kategori teknik dan matlamat serangan penerowongan	112
5.2	Ringkasan nod-nod yang terlibat mengikut penggunaannya	114
5.3	Senarai ringkasan aplikasi serangan rangkaian IPv6	116
5.4	Ringkasan keputusan eksperimen pelaksanaan serangan Banjir.	121
5.5	Ringkasan maklumat serta aliran corak serangan Banjir bagi Situasi 4, 5 dan 6	132
5.6	Ringkasan keputusan eksperimen pelaksanaan serangan Mengeksploitasi Protokol.	134
5.7	Ringkasan maklumat serta aliran corak serangan Mengeksploitasi Protokol bagi Situasi 12	140

5.8	Ringkasan keputusan eksperimen pelaksanaan serangan Paket Palsu.	142
5.9	Ringkasan maklumat serta aliran corak serangan Paket Palsu bagi Situasi 14 dan 15	149
5.10	Ringkasan keputusan eksperimen pelaksanaan serangan Balikkan.	152
5.11	Ringkasan maklumat serta aliran corak serangan Balikkan bagi Situasi 19,20 dan 21	162
5.12	Ringkasan Serangan DoS Alihan Penerowongan dari sudut penggunaan jenis IP oleh Komponen Serangan	164
5.13	Ringkasan serangan dari sudut status alamat IP yang digunakan	165
5.14	Ringkasan Serangan dari sudut gabungan teknik serangan	165
6.1	Ringkasan modul-modul yang terlibat dalam pembangunan Sistem Pengesanan Pencerobohan Rangkaian Penerowongan	175
6.2	Antara arahan atur cara yang terlibat.	179
6.3	Ringkasan bagi ciri-ciri yang diekstrak dari lokasinya	184
6.4	Senarai ciri-ciri dan jenis nilai kandungan	189
7.1	Ringkasan set data kasar yang telah dijana dan dihimpunkan kepada jenis keadaannya.	209
7.2	Ringkasan set data nyata yang telah ditangkap dan dihimpunkan sebelum dibahagikan kepada 4 set.	210
7.3	Sampel data Anomali dan Normal untuk latihan dan pengujian	220
7.4	Bilangan sampel data anomali mengikut teknik serangan	220
7.5	Pengujian regresi bagi penggunaan algoritma PB yang berlainan	224
7.6	Jumlah janaan amaran berbanding jumlah paket sebenar.	225
7.7	Keputusan bagi pengujian pengesanan bagi paket anomali	226
7.8	Keputusan bagi pengujian pengesanan bagi paket normal	227
7.9	Keputusan pengujian bagi SPP Bro mengikut jenis SeDAP	229
7.10	Senarai jumlah Amaran ⁽⁺⁾ oleh Bro mengikut kesahihan tulen atau palsu.	231
7.11	Senarai jumlah Amaran ⁽⁻⁾ mengikut kesahihan tulen atau palsu oleh Bro.	231

7.12	Keputusan pengujian bagi SPP Snort mengikut jenis SeDAP	233
7.13	Senarai jumlah Tulen ⁽⁺⁾ dan Palsu ⁽⁺⁾ bagi Amaran ⁽⁺⁾ yang dikeluarkan oleh Snort.	234
7.14	Senarai jumlah Amaran ⁽⁻⁾ mengikut kesahihan tulen atau palsu oleh <i>Snort</i> .	235
7.15	Keputusan pengujian bagi SPP-RP mengikut jenis SeDAP	236
7.16	Senarai jumlah Tulen ⁽⁺⁾ dan Palsu ⁽⁺⁾ bagi Amaran ⁽⁺⁾ yang dikeluarkan oleh SPP-RP.	238
7.17	Senarai jumlah Amaran ⁽⁻⁾ mengikut kesahihan tulen atau palsu oleh SPP-RP.	239
7.18	Nilai perkadaran yang menjelaskan keupayaan dan kebolehpercayaan sistem.	241
7.19	Perbandingan keputusan antara Bro, Snort dan SPP-RP dalam pengesanan serangan menerusi penerowongan.	244
7.20	Bilangan Tulen ⁽⁺⁾ (penggera tulen) mengikut jenis serangan.	245

SENARAI ILUSTRASI

Rajah		Halaman
1. 1	Statistik jumlah kejadian serangan DoS yang direkodkan oleh CyberSecurity Malaysia Tahun 1998 – 2011.	3
1. 2	Kejadian serangan DoS yang dikesan sebanyak 2 kali pada hari yang sama pada rangkaian penerowongan.	4
1. 3	Struktur penyelidikan menggambarkan metodologi secara keseluruhan	10
2.1	Ringkasan Teknik Anti Pencerobohan semasa	17
2.2	Model umum bagi Sistem Pengesanan Pencerobohan	20
2.3	Sistem Pengesanan Pencerobohan diklasifikasikan berdasarkan pengaruh sumber maklumat.	22
2.4	Jenis data yang digunakan oleh SPP	26
2.5	Jenis pengesanan pencerobohan mengikut kaedah perlaksanaannya	26
2.6	Model pengesanan salah guna	28
2.7	Model pengesanan anomali	30
2.8	Penglibatan kejadian dan amaran dalam proses pengesanan pencerobohan	35
2.9	Jenis amaran yang dijana oleh pengesanan pencerobohan	36
2.10	Jenis tindak balas oleh SPP	37
2.11	Pengelasan jenis serangan rangkaian	38
2.12	Pengkapsulan IPv6 ke dalam muatan IPv4	44
2.13	Komponen asas teknologi Mekanisme Peralihan	45
2.14	Kategori Mekanisme Peralihan	46
2.15	Mekanisme Dwi Tindakan	46
2.16	Mekanisme Penterjemahan	47
2.17	Mekanisme Penerowongan	47
2.18	Penerowongan hos-ke-hos	48

2.19	Penerowongan penghala-ke-penghala	49
2.20	Penerowongan Hos ke Penghala / Penghala ke Hos	50
2. 21	Senario Mekanisme Peralihan Penerowongan 6to4	52
3.1	Rangka kerja penyelidikan secara keseluruhan	61
3.2	Seni bina Sistem Pengesanan Pencerobohan Rangkaian Penerowongan	66
3.3	Rangka kerja perkakasan SPP-RP	67
3.4	Rangka kerja bagi pembangunan medan-uji penerowongan	68
3.5	Susun atur peralatan bagi medan-uji	69
3.6	Rangka kerja bagi pengujian prestasi SPP	69
3.7	Rangka kerja eksperimen bagi menjejak aliran trafik serangan untuk menghasilkan corak serangan.	70
3.8	Rangka kerja bagi proses penangkapan trafik	71
3.9	Rangka kerja perisian SPP-RP	72
3.10	Modul-modul dalam Bahagian Pemprosesan Data	73
3.11	Modul-modul dalam bahagian pengelasan corak	74
3.12	Modul Amaran pada bahagian penggera	75
4.1	Rangka kerja pembangunan medan-uji	78
4.2	Matlamat pembangunan medan-uji	79
4.3	Penentuan komponen berdasarkan model asas komunikasi data	80
4.4	Ringkasan bentuk pembangunan rangkaian medan-uji	85
4.5	Reka bentuk logikal rangkaian medan-uji secara berhierarki	86
4.6	Reka bentuk fizikal rangkaian medan-uji	87
4.7	Salah satu bahagian himpunan perkakasan yang asingkan mengikut rangkaian.	88
4.8	Konfigurasi alamat IP pada hos	89
4.9	Konfigurasi penerowongan 6to4 pada penghala	90
4.10	Konfigurasi penerowongan 6to4 pada penghala geganti	90

4.11	Kaedah pengujian rangkaian medan-uji	92
4.12	Keputusan pengujian penyambungan antara nod merentasi rangkaian	93
4.13	<i>Round trip time (RTT)</i> terhadap TCP	94
4.14	<i>Round trip time (RTT)</i> oleh UDP	94
4.15	TCP <i>throughput</i>	95
4.16	UDP <i>throughput</i>	95
4.17	<i>Tunneling Overhead</i>	96
4.18	Kaedah pengujian Sistem Pengesan Pencerobohan.	97
4.19	Carta alir pembangunan serangan secara umum	99
4.20	Antara muka baris arahan untuk serangan oleh packETH	100
4.21	Senario pengujian pengesanan	100
4.22	Senario pengujian serangan menerusi penerowongan	101
4.23	Sebahagian daripada IDS berjaga-jaga muncul di syslog	102
4.24	Maklumat trafik serangan yang ditangkap oleh PR	102
4.25	Contoh antara sekatan yang dilakukan terhadap paket penerowongan	103
4.26	Maklumat trafik serangan melalui terowong yang ditangkap oleh PR	103
4.27	Senario pelaksanaan keselamatan rangkaian terhadap trafik penerowongan.	105
5.1	Rangka kerja permodelan serangan DoS penerowongan	110
5.2	Langkah-langkah yang terlibat dalam persediaan persekitaran rangkaian	110
5.3	Kategori serangan DoS yang mengeksploitasi kelemahan.	111
5.4	Reka bentuk rangkaian secara umum bagi melaksanakan eksperimen	113
5.5	Perlaksanaan serangan penerowongan secara umum	117
5.6	Corak serangan DoS tradisional	118

5.7	Contoh penggunaan IPv6 dengan perkhidmatan mekanisma penerowongan	119
5.8	Corak aliran serangan Banjir dari nod rangkaian <i>6to4</i>	123
5.9	Corak aliran serangan Banjir dari nod rangkaian IPv6 asli	125
5.10	Corak aliran serangan Banjir dari nod rangkaian IPv4	128
5.11	Senario oleh 3 jenis serangan Banjir yang dilaksanakan terhadap mangsa nod rangkaian <i>6to4</i>	130
5.12	Corak aliran serangan Mengeksploitasi Protokol dari nod H-10 kepada R-1	136
5.13	Senario Serangan Mengeksploitasi Protokol yang dilaksanakan terhadap mangsa nod rangkaian <i>6to4</i>	138
5.14	Corak aliran serangan Paket Palsu dari nod rangkaian IPv6 asli	144
5.15	Corak aliran serangan Paket Palsu dari nod rangkaian IPv4	146
5.16	Senario Serangan Paket Palsu yang dilaksanakan terhadap mangsa nod rangkaian <i>6to4</i>	148
5.17	Corak aliran serangan Paket Balikkan dari nod rangkaian <i>6to4</i>	153
5.18	Corak aliran serangan Paket Balikkan dari nod rangkaian IPv6 asli	156
5.19	Corak aliran serangan Paket Balikkan dari nod rangkaian IPv4	158
5.20	Senario Serangan Paket Balikkan yang dilaksanakan terhadap mangsa nod rangkaian <i>6to4</i>	160
5.21	Corak Serangan Dos Alihan Penerowongan	166
5.22	Model asas serangan DoS merujuk Model komunikasi data	167
5.23	Model SDP	168
5.24	Model umum serangan DoS Alihan	169
5.25	Model SeDAP	170
6.1	Struktur prototaip bagi pembangunan sistem cadangan	174
6.2	Rangka kerja penangkapan trafik	175
6.3	Carta alir bagi modul penangkapan trafik	177
6.4	Struktur kedudukan ruang dalam pengepala dan muatan IP Protokol-41	178

6.5	Contoh himpunan paket yang telah melalui modul saringan	179
6.6	Carta alir saringan trafik	180
6.7	Ruangan Pengepala Depan dalam pengepala IPv6	181
6.8	Ruangan Port Sumber di dalam pengepala TCP	182
6.9	Ruangan Jenis yang terdapat pada Pengepala ICMPv6	182
6.10	Carta alir pengasingan paket	183
6.11	Carta Alir Modul Pengekstrakan Unsur	185
6.12	Perbezaan nilai ciri-ciri sebelum dan selepas proses penyeragaman	191
6.13	Carta alir bagi modul penyeragaman nilai unsur.	192
6.14	Gambaran proses pelabelan menerusi teknik perbandingan	194
6.15	Penterjemahan matematik ke bentuk rajah euler	194
6.16	Carta Alir Modul Audit Status Trafik	195
6.17	Carta Alir Modul Rangkaian Neural	198
6.18	Carta alir bagi modul amaran	205
7.1	Jenis data dan penggunaannya dalam kajian	208
7.2	Tatacara bagi pengujian peringkat bahagian	211
7.3	Contoh data bagi setiap kadar penangkapan	212
7.4	Graf peratusan penangkapan mengikut kandungan paket	212
7.5	Graf purata penangkapan dengan bilangan paket dalam 1 saat	213
7.6	Graf perbandingan bilangan paket setiap saat sebelum dan selepas penyaringan.	214
7.7	Perbezaan kandungan maklumat sebelum dan selepas pengekstrakan dan pemilihan ciri	215
7.8	Graf perbezaan jumlah kandungan pada setiap paket sebelum dan selepas melalui modul pengekstrakan ciri.	216
7.9	Perbezaan nilai ciri-ciri sebelum dan selepas proses penukaran nilai	217
7.10	Graf perbezaan jumlah kandungan pada setiap paket implikasi daripada perlaksanaan modul pengekstrakan ciri.	217

7.11	Contoh nilai bagi ciri terbitan yang digunakan bagi proses pelabelan	218
7.12	Pelabelan bagi setiap data yang terlibat.	219
7.13	Pelabelan data mengikut status	220
7.14	Pecahan bilangan data anomali terkumpul mengikut teknik serangan	221
7.15	Data diubah pada satu julat melalui proses penormalan	221
7.16	Prestasi Kaedah Latihan <i>Levenberg-Marquardt</i>	222
7.17	Prestasi Kaedah Latihan dan Regresi Pengujian <i>Scale Conjugate Gradient</i>	222
7.18	Prestasi Kaedah Latihan dan Regresi Pengujian <i>Bayesian Regularization</i>	223
7.19	Perbezaan jumlah amaran antara jenis Perambatan Balik	225
7.20	Kadar janaan Amaran ⁽⁺⁾ serta tahap ketulenan dan kepalsuannya	226
7.21	Kadar janaan Amaran ⁽⁻⁾ serta tahap ketulenan dan kepalsuannya	227
7.22	Tatacara proses pengujian sistem pengesanan	228
7.23	Graf peratusan kadar Amaran bagi data anomali SeDAP dan setiap data normal oleh Bro	230
7.24	Graf kesahihan Amaran ⁽⁻⁾ oleh Bro dari segi ketulenan dan kepalsuannya.	232
7.25	Tambahan tatacara bagi mengubah tatacara lalai	232
7.26	Graf peratusan kadar Amaran bagi data anomali SeDAP dan setiap data normal oleh Snort	234
7.27	Graf kesahihan Amaran ⁽⁺⁾ oleh Snort dari segi ketulenan dan kepalsuannya.	235
7.28	Graf kesahihan Amaran ⁽⁻⁾ oleh Snort dari segi ketulenan dan kepalsuannya.	236
7.29	Graf peratusan kadar Amaran bagi data anomali SeDAP dan setiap data normal oleh SPP-RP	237
7.30	Graf kesahihan Amaran ⁽⁺⁾ oleh SPP-RP dari segi ketulenan dan kepalsuannya.	238

7.31	Graf kesahihan Amaran ⁽⁻⁾ oleh SPP-RP dari segi ketulenan dan kepalsuannya.	239
7.32	Graf perbezaan keupayaan dan kebolehpercayaan sistem-sistem yang diuji.	242
7.33	Tatacara proses pengesahan keputusan	243
7.34	Graf perbandingan keputusan antara Bro, Snort dan SPP-RP dalam pengesanan serangan menerusi penerowongan.	244

SENARAI SINGKATAN PERKATAAN

DoS	Serangan Penafian Perkhidmatan
ICMP	<i>Internet Control Message Protocol</i>
IETF	<i>Engineering Task Force</i>
IPv4	Protokol Internet Versi 4
IPv6	Protokol Internet Versi 6
KB	Kecerdasan Buatan
KDD	<i>Knowledge Discovery in Database</i>
MPIIPv6	Mekanisme Peralihan IPv6
NGTRANS	<i>Next Generation TRANSition</i>
P41	Protokol 41
Palsu ⁽⁻⁾	Negatif Palsu
Palsu ⁽⁺⁾	Positif Palsu
RN	Rangkaian Neural
RNPB	Rangkaian Neural Perambatan Balik
SDP	Serangan DoS Penerowongan
SeDAP	Serangan DoS Alihan Penerowongan
SPP	Sistem Pengesanan Pencerobohan
SPPH	Sistem Pengesanan Pencerobohan berasaskan Hos
SPPR	Sistem Pengesanan Pencerobohan berasaskan Rangkaian
SPP-RP	Sistem Pengesanan Pencerobohan Rangkaian Penerowongan
SPR	Sistem Pemantauan Rangkaian
TA	Tembok Api
TCP	<i>Transmission Control Protocol</i>
Tulen ⁽⁻⁾	Negatif Tulen

Tulen⁽⁺⁾ Positif Tulen
UDP *User Datagram Protocol*

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Kebergantungan terhadap perkhidmatan berasaskan teknologi maklumat bukan lagi satu fenomena asing. Teknologi ini mendapat kepercayaan oleh pengguna kerana telah terbukti dengan kesahihan dan kejituan perkhidmatan yang ditawarkan. Tambahan pula dengan tersedianya rangkaian komunikasi terkini, telah menjadikannya lebih efisien. Justeru itu, pelbagai pihak telah menjadikan teknologi ini sebahagian besar daripada urusan perkhidmatan harian mereka. Pelbagai maklumat umum mahu pun yang sulit, telah dimuatkan ke alam maya. Oleh itu penglibatan teknologi komunikasi secara tidak langsung turut mendapat perhatian oleh kebanyakan pihak. Keadaan ini telah menjadikan teknologi komunikasi salah satu elemen yang sangat penting dalam era ini.

Sejak awal perkhidmatannya, Protokol Internet Versi 4 (IPv4) merupakan pendukung utama dan tunggal bagi teknologi komunikasi data berinternet. Namun hingga ke hari ini, alamat IP yang tidak terpakai telah mengalami penyusutan amat ketara. Perkara ini diperakui oleh Karpilovsky et al. (2009), di mana menurut beliau dalam beberapa tahun terdekat, permintaan untuk memperoleh alamat IP ini akan terbatas ekoran bilangannya hampir kehabisan. Implikasi daripada kekusutan ini, pengguna Internet telah mula beralih kepada alternatif protokol yang lain iaitu Protokol Internet Versi 6 (IPv6). Sungguhpun IPv6 masih di peringkat asas perlaksanaannya, namun keupayaannya untuk memenuhi keperluan jumlah alamat Internet telah mengatasi kelemahan asas IPv4.