ANALISIS PRESTASI PROTOKOL LEACH DALAM RANGKAIAN SENSOR TANPA WAYAR DENGAN SERANGAN DoS

Rozita Binti Mohd. Mokhtar

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor Malaysia.

rozzimm@gmail.com

ABSTRAK

Kemajuan teknologi sensor sejak dua puluh tahun lalu telah membawa transformasi pada pelbagai bidang industri melalui penggunaan rangkaian sensor tanpa wayar atau Wireless Sensor Network (WSN). Implementasi WSN bukan setakat di luar negara, tetapi juga di Malaysia. Namun begitu, terdapat isu dan kekurangan WSN yang menjadi fokus utama dalam kajian-kajian sedia ada iaitu pemuliharaan tenaga dan ancaman keselamatan seperti serangan Denial of Service (DoS). Ciri-ciri WSN iaitu tenaga, pemprosesan dan storan yang terhad menyebabkan kedua-dua isu ini sukar diatasi. Protokol Low Energy Adaptive Clustering Hierarchy (LEACH) merupakan protokol terbaik dan berkecekapan tenaga tinggi (high energy efficiency) untuk menjimatkan tenaga rangkaian. Kajian ini dijalankan untuk menganalisis prestasi protokol LEACH beserta dengan serangan DoS. Perbandingan juga dibuat berdasarkan kepadatan bilangan nod iaitu sebanyak dua puluh, empat puluh, enam puluh, lapan puluh dan seratus nod serta kedudukan stesen pangkalan (50, 175) dan (50, 50). Tujuan kajian ini dibuat adalah untuk mengenalpasti bilangan nod dan kedudukan stesen pangkalan yang bersesuaian serta memberi kesan minimum terhadap serangan DoS. Perisian simulasi NS-2.35 digunakan beserta dengan fail tampal LEACH dan kod Black Hole yang merupakan sejenis ancaman DoS. Metrik prestasi yang diukur adalah jangka hayat rangkaian, jumlah bilangan data yang dihantar ke stesen pangkalan dan jumlah tenaga yang digunakan. Hasil kajian mendapati bahawa kepadatan bilangan nod yang bersesuaian dan memberi kesan yang minimum terhadap serangan Black Hole bagi rangkaian berkeluasan 100 meter x 100 meter ialah lapan puluh nod. Manakala kedudukan stesen pangkalan yang memberi kesan minimum pula adalah (50, 175). Walaupun penggunaan tenaga bagi kedudukan ini agak tinggi sedikit, namun dari segi tempoh jangka hayat dan jumlah data yang dihantar pula meningkat berbanding kedudukan stesen pangkalan (50, 50). Hasil kajian ini dapat membantu dalam penilaian kesan serangan Black Hole, mengenalpasti tingkah laku rangkaian dan boleh dijadikan panduan untuk kajian lain seperti pengesanan serangan Black Hole, penambahbaikan keselamatan protokol dan lain-lain.

1. PENGENALAN

Peningkatan secara drastik aplikasi sensor sejak lebih dua puluh tahun lalu menunjukkan bahawa ia bakal mengalami revolusi sepertimana perkembangan mikrokomputer pada tahun 1980 an. Pelbagai industri dan bidang berkembang dan mengalami transformasi seiring dengan kemajuan teknologi sensor ini. Kini aplikasi rangkaian sensor tanpa wayar atau *Wireless Sensor Networks* (WSN) banyak digunakan dalam industri dan bidang seperti ketenteraan, pemantauan persekitaran, kediaman pintar, pemantauan kesihatan, pemantauan habitat, agrikultur dan lain-lain.

Di Malaysia, perkembangan WSN bermula sejak Rancangan Malaysia Kesembilan (RMK-9) dan Rancangan Malaysia Kesepuluh (RMK-10) (Junus (2013)). Antara implementasi WSN yang terdapat di Malaysia ialah penggunaan sensor untuk pertanian dengan teknologi fertigasi, sensor akuakultur berasaskan fiber optik, sensor untuk mengenalpasti punca keretakan di kondominium di Bukit Antarabangsa, pemantauan jambatan Pulau Pinang dan sensor pemantauan penanaman tembikai di rumah hijau Pulau Pinang, Terengganu dan Sabah (Zhin (2012)).

Oleh kerana penggunaan WSN yang meluas, maka kajian-kajian untuk penambahbaikan bagi mengatasi masalah serta kelemahan yang ada dapat dipertingkatkan. Terdapat juga kajian-kajian yang dilaksanakan oleh penyelidik tempatan seperti implementasi praktikal WSN untuk pemantauan

kawasan sawah padi (Goh et al. (2012)), implementasi WSN di ladang burung walit yang dijalankan oleh Al-Khalid Othman et al. (2009) dan lain-lain.

1. RANGKAIAN SENSOR TANPA WAYAR (WSN)

Sejak sepuluh tahun lalu, WSN telah mencetuskan aktiviti saintifik yang intensif. Banyak kesusasteraan telah dihasilkan untuk mengatasi cabaran-cabaran kajian dalam WSN. Antara cabaran-cabaran kajian yang menjadi fokus utama ialah isu pemuliharaan tenaga dan keselamatan rangkaian (Du & Li (2011)).

Pemuliharaan tenaga dalam WSN sangat penting untuk meningkatkan jangka hayat rangkaian. Oleh itu, kajian dan pembangunan protokol laluan yang berkecekapan tenaga tinggi (*high energy efficiency*) giat dijalankan untuk menangani isu tersebut. *Low Energy Adaptive Clustering Hierarchy* (LEACH) adalah salah satu protokol laluan berkecekapan tinggi yang terbaik (Ibrahim et al. (2011); Norouzi et al. (2013)) dan sangat popular serta banyak digunakan dalam rangkaian WSN (Tripathi et al. (2013); Almomani & Al-Kasasbeh (2015)). Sehingga kini LEACH menjadi topik hangat dan menjadi tumpuan para pengkaji untuk melaksanakan kajian dalam pelbagai aspek berkaitan dengannya.

Selain ciri yang dinyatakan di atas, WSN juga dianggap sebagai klasifikasi rangkaian ad-hoc yang luarbiasa dan tidak berinfrastruktur yang mampu beroperasi tanpa pengawasan pengguna (Bansal & Saluja (2016)). Nod dalam WSN boleh digunakan dalam persekitaran liar dan ganas serta kawasan yang terpencil, melaksanakan pengendalian-sendiri (*self-organized*) untuk membentuk rangkaian dan seterusnya menjalankan tugas yang ditetapkan (Xiaomei & Ke (2016)). Ciri-ciri ini menjadikan WSN digunakan secara meluas dan secara tidak langsung terdedah pada pelbagai jenis ancaman keselamatan. Serangan nafi khidmat atau *Denial of Service* (DoS) merupakan serangan utama yang berlaku dalam WSN (Patil & Chaudhari (2016)). Bansal dan Saluja (2016) juga menyatakan bahawa WSN cenderung pada ancaman keselamatan seperti *Jamming, Worm Hole, Sink Hole, Black Hole* dan serangan *Sybil*.

Menurut Conti dan Giordano (2014), terdapat keperluan kajian dalam isu tambahan rangkaian WSN. Salah satu isu tambahan tersebut ialah isu prestasi rangkaian. Oleh itu, kajian yang dijalankan ini menjurus pada analisis prestasi protokol laluan LEACH dalam rangkaian WSN beserta serangan *Black Hole*.

2. SIMULASI RANGKAIAN

Perlaksanakan kajian untuk analisis prestasi protokol dalam WSN adalah melalui simulasi peristiwa diskrit yang menggunakan perisian simulator rangkaian Network Simulator versi 2.35 (NS-2.35). Fail tampal bagi protokol LEACH digunakan kerana protokol tersebut tidak tersedia ada dalam perisian NS-2. Berikut adalah penerangan mengenai kaedah kajian menggunakan perisian simulator NS-2.35.

3.1 Perisian Simulator NS-2.35

Terdapat tiga langkah untuk melaksanakan simulasi dalam NS-2. Dalam langkah pertama, tujuan simulasi, senario rangkaian, andaian, ukuran prestasi serta jenis keputusan yang diingini perlu ditentukan.

Langkah kedua adalah untuk mengimplementasi rekabentuk simulasi rangkaian yang telah dibuat dalam langkah pertama. Terdapat dua fasa dalam langkah ini iaitu fasa konfigurasi rangkaian dan fasa simulasi. Dalam langkah ketiga pula, program terlebih dahulu perlu dinyahpepijat (*debug*). Kemudian, prestasi bagi simulasi rangkaian yang dilaksanakan diukur.

Mesin maya (*virtual machine*) Oracle VM Virtual Box digunakan untuk proses pemasangan (*installation*) sistem pengoperasian. NS-2.35 berserta fail tampal LEACH dipasang dalam sistem pengoperasian sumber terbuka CENTOS versi 6.7. Sistem pengoperasian ini dipilih kerana keserasiannya (*compatibility*) dengan fail tampal LEACH. Terdapat banyak isu serta konflik yang berlaku semasa pemasangan fail tampal LEACH ke dalam perisian NS-2.35. Tetapi kesemua masalah tersebut dapat diatasi dengan merujuk pada forum, blog dan laman web yang berkaitan.

3.2 Rekabentuk Simulasi

Rekabentuk simulasi rangkaian WSN yang dikaji adalah berdasarkan topologi dan parameter simulasi dalam Jadual 1. Rekabentuk yang digunakan adalah merujuk pada kajian Tian et al. (2012). Dalam kajian tersebut, parameter yang bersesuaian untuk rangkaian tanpa serangan bagi mencapai tahap prestasi optimum telah dikenalpasti. Berikut adalah penetapan parameter simulasi yang digunakan:

Jadual 1. Parameter Simulasi

Parameter Simulasi	Nilai
1. Jumlah Nod	20, 40, 60, 80 dan 100
2. Jumlah Klaster	1, 2, 3, 4 dan 5
3. Saiz Topografi	100m x 100m
4. Kedudukan Stesen Pangkalan	(50, 50) dan (50, 175)
5. Protokol Laluan	LEACH
6. Masa Simulasi	3600s
7. Tenaga Awalan (J)	2 dan 3
8. Jumlah Nod Hasad	1

3.3 Fasa Konfigurasi Dan Simulasi Rangkaian

Dalam fasa ini, konfigurasi untuk komponen rangkaian seperti nod-nod, agen trafik dan lain-lain perlu dibina berdasarkan rekabentuk simulasi yang telah dibuat. Konfigurasi serta pembinaan ini dibuat dalam kod *Tool command language* (Tcl) atau *Object-oriented Tool command language* (OTcl) dan disimpan sebagai fail Tcl.

Kod untuk serangan *Black Hole* tidak disediakan dalam NS-2.35 atau fail tampal protokol LEACH. Untuk mewujudkan serangan *Black Hole* dalam rangkaian WSN dalam simulasi ini, kod tambahan diperlukan. Pengubahsuaian pada beberapa fail protokol LEACH dilakukan.

Perlaksanaan simulasi dimulakan dalam fasa ini dengan memasukkan arahan ./leach_test di terminal. Arahan ini akan membaca kod yang terdapat dalam fail bash (*bash file*) terlebih dahulu. Dalam fail bash, terdapat kod yang memanggil fail Tcl untuk melaksanakan simulasi. Selepas arahan dilaksanakan, hasil simulasi akan dikeluarkan. Oleh kerana fail tampal protokol LEACH tidak menyokong animasi, maka output akan dikeluarkan melalui fail teks.

3.4 Pemprosesan selepas simulasi

Dalam langkah ini, proses pengesanan paket (objek) akan merekod butiran aliran paket semasa simulasi. Rekod ini boleh diklasifikasikan dalam dua bahagian iaitu pengesanan paket berdasarkan teks dan pengesanan paket *Network Animator* (NAM). Simulator akan menghasilkan kedua-dua fail ini bergantung pada peristiwa (*event*) yang ditetapkan dalam rangkaian. Oleh kerana fail tampalan LEACH yang digunakan tidak menyokong animasi, maka hanya terdapat rekod pengesanan paket berdasarkan teks.

Langkah pengesanan paket ini sangat penting kerana ia akan menghasilkan analisis prestasi yang menjadi fokus utama dalam kajian ini. Fail data pengesanan paket diproses melalui skrip AWK untuk mengekstrak data yang dikehendaki sahaja.

Metrik atau ukuran prestasi yang digunakan dalam kajian ini ialah jangka hayat rangkaian, jumlah bilangan data yang dihantar ke stesen pangkalan dan jumlah penggunaan tenaga dalam

rangkaian. Untuk membuat perbandingan prestasi, penjanaan graf dari skrip AWK dibuat. Penjanaan graf dihasilkan melalui aplikasi Gnuplot. Perbandingan yang dibuat adalah prestasi rangkaian tanpa serangan dan dengan serangan *Black Hole* dan tahap prestasi berdasarkan kedudukan stesen pangkalan.

3. DAPATAN KAJIAN

Analisis prestasi telah dilaksanakan untuk protokol LEACH terbahagi pada tiga bahagian iaitu:

a. Perbandingan prestasi untuk rangkaian tanpa serangan dan dengan serangan menggunakan kedudukan stesen pangkalan (50, 175).
b. Perbandingan prestasi untuk rangkaian tanpa serangan dan dengan serangan menggunakan kedudukan stesen pangkalan (50, 50).
c. Perbandingan prestasi untuk rangkaian dengan serangan antara kedudukan stesen pangkalan (50, 175) dan (50,50).

4.1 Kesan Serangan *Black Hole* Terhadap Jangka Hayat Rangkaian

Jangka hayat rangkaian memainkan peranan yang sangat penting dalam rangkaian WSN. Sekiranya sesebuah rangkaian mempunyai jangka hayat yang pendek, maka penyenggaraan dan pemantauan yang kerap perlu dilakukan. Pengumpulan data juga tidak dapat dilakukan dengan efisyen. Ini akan menjurus pada peningkatan kos dan tenaga.

Kesan jangka hayat rangkaian WSN semasa serangan *Black Hole* bergantung kepada bilangan nod yang terdapat dalam rangkaian tersebut, pemilihan ketua klaster dan juga kedudukan stesen pangkalan. Daripada analisis yang dijalankan, terdapat tiga keadaan jangka hayat rangkaian iaitu jangka hayat paling rendah, paling tinggi dan negatif.

Jika perbezaan tempoh jangka hayat antara rangkaian tanpa serangan dan dengan serangan adalah rendah, maka rangkaian tersebut tidak memberi kesan yang ketara atau minimum sekiranya berlaku serangan. Tetapi jika perbezaan adalah tinggi, maka rangkaian tersebut mendapat kesan yang ketara atau maksimum akibat dari serangan. Perbezaan negatif pula terjadi apabila jangka hayat rangkaian dengan serangan adalah lebih tinggi berbanding tanpa serangan. Seperti yang telah diterangkan sebelum ini, keadaan ini terjadi kerana kesan dari aktiviti nod hasad yang menyebabkan lebihan tenaga pada nod biasa sekaligus memanjangkan jangka hayat rangkaian tersebut.

Jadual 2. Perbandingan dan Perbezaan Nilai Jangka Hayat Rangkaian

Kedudukan Stesen Pangkalan	**Metrik Prestasi**	**Jangka Hayat Rangkaian (Saat)**				
	Senario	**Bilangan Nod**				
		20	**40**	**60**	**80**	**100**
(50, 175)	Tanpa serangan	182.3	374.5	292.8	550.9	505.3
	Dengan Serangan	109.3	275.6	302.0	531.9	413.6
	Perbezaan	**73.0**	**98.9**	**-9.2**	**19.0**	**91.7**
(50, 50)	Tanpa serangan	234.5	272.6	448.2	412.6	526.1
	Dengan Serangan	170.2	361.1	257.5	388.0	211.4
	Perbezaan	**64.3**	**-88.5**	**190.7**	**24.6**	**314.7**

Dari pemerhatian berdasarkan Jadual 2, perbezaan yang paling tinggi adalah pada empat puluh nod bagi kedudukan stesen pangkalan (50, 175). Manakala yang paling rendah adalah lapan puluh nod dan terdapat tempoh jangka hayat negatif pada enam puluh nod.

Pada kedudukan stesen pangkalan (50, 50) pula, perbezaan yang paling tinggi adalah pada seratus nod. Yang paling rendah pada lapan puluh nod dan nilai negatif pada empat puluh nod.

4.2 Kesan Serangan *Black Hole* Terhadap Jumlah Data Yang Dihantar

Salah satu kriteria rangkaian berprestasi tinggi adalah dengan mempunyai kadar penghantaran data yang tinggi. Dalam analisis jumlah data yang dihantar ke stesen pangkalan ini, terdapat tiga kadar yang diperolehi iaitu kadar tinggi, rendah dan negatif. Perbezaan kadar jumlah penghantaran data telah dilakukan seperti dalam Jadual 3.

Jadual 3. Perbandingan dan Perbezaan Nilai Jumlah Data Yang Dihantar Ke Stesen Pangkalan

Kedudukan Stesen Pangkalan	**Metrik Prestasi**	**Jumlah Data Yang Dihantar (Paket)**				
	Senario	**Bilangan Nod**				
		20	**40**	**60**	**80**	**100**
(50, 175)	Tanpa serangan	243,784	723,764	528,430	1,506,855	1,380,352
	Dengan Serangan	73,654	431,976	514,470	1,458,195	886,119
	Perbezaan	**170,130**	**291,788**	**13,960**	**48,660**	**494,233**
(50, 50)	Tanpa serangan	178,174	430,511	1,173,018	884,508	1,491,218
	Dengan Serangan	183,543	796,742	346,608	776,562	189,612
	Perbezaan	**-5369**	**-366231**	**826,410**	**107,946**	**1,301,606**

Didapati bahawa jika kedudukan stesen pangkalan (50, 175), perbezaan paling tinggi ialah pada seratus nod. Ini bermakna terdapat banyak paket yang digugurkan semasa serangan berlaku. Perbezaan paling rendah pula adalah enam puluh nod.

Pada kedudukan (50, 50) pula, perbezaan kadar penghantaran yang paling tinggi ialah seratus nod, manakala yang paling rendah adalah lapan puluh nod. Terdapat kadar negatif iaitu pada dua puluh nod dan empat puluh nod.

Walaupun terdapat hanya satu nod hasad yang ditetapkan, tetapi sekiranya nod ini tidak dilantik sebagai ketua klaster, maka ketua klaster yang lain masih berkomunikasi dengan stesen pangkalan. Ini akan menyebabkan kadar penghantaran data dalam rangkaian dengan serangan lebih tinggi dari tanpa serangan.

4.3 Kesan Serangan *Black Hole* Terhadap Jumlah Penggunaan Tenaga

Dalam rangkaian WSN, penggunaan tenaga yang rendah menunjukkan bahawa rangkaian tersebut adalah yang terbaik. Ini merupakan salah satu isu penting dalam WSN di mana penjimatan tenaga diperlukan untuk memanjangkan jangka hayat rangkaian. Jadual 4 menunjukkan perbandingan dan perbezaan yang dilakukan.

Jadual 4. Perbandingan dan Perbezaan Nilai Jumlah Penggunaan Tenaga

Kedudukan Stesen Pangkalan	**Metrik Prestasi**	**Jumlah Penggunaan Tenaga (Joule)**				
	Senario	**Bilangan Nod**				
		20	**40**	**60**	**80**	**100**
(50, 175)	Tanpa serangan	476	1529	1894	5027	5385
	Dengan Serangan	274	1353	2642	4908	4651
	Perbezaan	**202**	**176**	**-748**	**119**	**734**
(50, 50)	Tanpa serangan	810	1581	2908	3008	5673
	Dengan Serangan	511	1661	2012	4328	2619
	Perbezaan	**299**	**-80**	**896**	**-1320**	**3054**

Perbezaan penggunaan tenaga yang paling tinggi adalah pada seratus nod bagi kedudukan stesen pangkalan (50, 175). Yang paling rendah pula adalah pada empat puluh nod. Nilai negatif berlaku pada enam puluh nod. Kedudukan stesen pangkalan (50, 50) pula menunjukkan perbezaan tinggi pada

seratus nod, paling rendah pada dua puluh nod dan nilai negatif pada empat puluh dan lapan puluh nod.

4.4 Perbandingan Dapatan Kajian Dengan Kajian Terdahulu

Perbandingan dapatan kajian ini dilakukan dengan kajian yang telah dilaksanakan oleh Tripathi et al. (2013) serta Almomani dan Al-Kasasbeh (2015). Perbandingan juga dibuat berdasarkan kesetaraan dan persamaan nilai parameter. Kajian yang telah dilaksanakan ini menggunakan hanya satu nod hasad. Kesan yang dilihat adalah berdasarkan kepadatan bilangan nod.

a. Perbandingan jangka hayat rangkaian

Perbandingan jangka hayat rangkaian adalah seperti yang dipaparkan dalam Jadual 5.4. Dapatan kajian ini menunjukkan bahawa tempoh jangka hayat rangkaian dengan serangan adalah lebih singkat. Ini berbeza dengan hasil kajian Tripathi et al. (2013) di mana tempoh jangka hayat rangkaian dengan serangan adalah lebih panjang. Kepadatan bilangan nod yang digunakan dalam kajian ini adalah dua puluh, lima puluh, seratus dan dua ratus nod. Manakala bilangan nod hasad yang digunakan adalah satu sahaja.

Dalam kajian Almomani dan Al-Kasasbeh (2015) juga menunjukkan hasil yang sama tetapi menggunakan kepadatan bilangan nod sebanyak seratus sahaja dan intensiti bilangan nod hasad sebanyak sepuluh peratus, tiga puluh peratus dan lima puluh peratus. Menurut mereka, ini kerana nod hasad menghalang paket data dari dihantar ke stesen pangkalan. Bilangan paket yang dihantar ke stesen pangkalan berkurangan dan menyumbang pada penjimatan tenaga nod.

Perbezaan tempoh jangka hayat ini kemungkinan dipengaruhi oleh bilangan nod hasad serta nilai tenaga awalan yang ditetapkan untuk nod sensor dan juga nod hasad. Dalam kajian ini, tenaga awalan yang digunakan ialah 2J untuk nod sensor dan 3J untuk nod hasad. Tripathi et al. (2013) tidak menyatakan nilai tenaga awalan yang mereka gunakan manakala Almomani dan Al-Kasasbeh (2015) menggunakan nilai 5J dan 50J untuk nod sensor dan nod hasad.

Selain itu, kedudukan stesen pangkalan dan jarak antara nod-nod juga menyumbang pada jangka hayat rangkaian. Sekiranya jarak antara ketua klaster lebih jauh dari stesen pangkalan, maka lebih tenaga diperlukan untuk menghantar data. Tetapi sekiranya jaraknya berhampiran dengan stesen pangkalan, maka tenaga yang digunakan juga adalah kurang. Perkara yang sama akan terjadi pada nod-nod biasa yang menghantar data ke ketua klaster. Tripathi et al. (2013) tidak menyatakan kedudukan stesen pangkalan yang mereka tetapkan. Manakala Almomani dan Al-Kasasbeh (2015) menggunakan kedudukan (50, 175).

Jadual 5. Perbandingan Tempoh Jangka Hayat

Kajian	**Tempoh Jangka Hayat**	
	Bilangan Nod	
	20	**100**
Tripathi et al. (2013)	Meningkat	Meningkat
Almomani dan Al-Kasasbeh (2015)	-	Meningkat
Kajian Semasa - Kedudukan Stesen Pangkalan (50, 157)	Menurun	Menurun
Kajian Semasa - Kedudukan Stesen Pangkalan (50, 50)	Menurun	Menurun

b. Perbandingan jumlah data yang dihantar ke stesen pangkalan

Dua kajian yang terdahulu menunjukkan bahawa jumlah data yang dihantar ke stesen pangkalan dalam rangkaian dengan serangan adalah berkurangan berbanding tanpa serangan seperti yang dipaparkan dalam Jadual 6.

Jadual 6. Perbandingan Jumlah Data Yang Dihantar

Kajian	**Jumlah Data Yang Dihantar**
	Bilangan Nod

	20	100
Tripathi et al. (2013)	Menurun	Menurun
Almomani dan Al-Kasasbeh (2015)	-	Menurun
Kajian Semasa - Kedudukan Stesen Pangkalan (50, 157)	Menurun	Menurun
Kajian Semasa - Kedudukan Stesen Pangkalan (50, 50)	Sama	Menurun

Hasil yang sama diperolehi bagi dapatan kajian ini dengan kedudukan stesen pangkalan (50, 175). Pada kedudukan stesen pangkalan (50, 50), nilai bagi bilangan nod dua puluh adalah sama seperti yang terdapat dalam Jadual 5.4. Perbezaan berlaku pada bilangan empat puluh nod di mana nilainya adalah lebih tinggi.

Perbezaan yang berlaku kemungkinan disebabkan oleh faktor pemilihan ketua klaster. Sekiranya nod hasad tidak dilantik sebagai ketua klaster dipermulaan tempoh simulasi, maka nod lain dapat menghantar data ke stesen pangkalan.

c. Perbandingan jumlah tenaga yang digunakan

Hasil kajian Tripathi et al. (2013) menunjukkan pengurangan jumlah tenaga dalam rangkaian dengan serangan. Manakala Almomani dan Al-Kasasbeh (2015) pula tidak menyatakan hasil analisis bagi bahagian ini.

Perbandingan mengikut bilangan nod yang setara menunjukkan hasil yang sama seperti yang dipaparkan dalam Jadual 7. Tetapi jumlah tenaga yang digunakan adalah lebih tinggi pada bilangan nod-nod tertentu dalam rangkaian dengan serangan. Ini terjadi pada kedudukan stesen pangkalan (50, 175) dengan enam puluh nod dan kedudukan (50, 50) dengan empat puluh, enam puluh dan lapan puluh nod.

Jadual 7. Perbandingan Jumlah Tenaga Yang Digunakan

Kajian	**Jumlah Penggunaan Tenaga**	
	Bilangan Nod	
	20	**100**
Tripathi et al. (2013)	Menurun	Menurun
Almomani dan Al-Kasasbeh (2015)	-	-
Kajian Semasa - Kedudukan Stesen Pangkalan (50, 157)	Menurun	Menurun
Kajian Semasa - Kedudukan Stesen Pangkalan (50, 50)	Menurun	Menurun

4.5 FAKTOR PERBEZAAN HASIL KAJIAN

Setelah membuat perbandingan hasil dapatan kajian dengan dua kajian terdahulu, terdapat persamaan dan perbezaan nilai prestasi yang diukur. Perbezaan nilai ini disebabkan oleh beberapa faktor yang mempengaruhi hasil simulasi.

a. Bilangan kepadatan nod yang digunakan
   Hasil kajian Tripathi et al. (2013) menunjukkan bahawa kesan serangan akan meningkat seiring dengan peningkatan saiz rangkaian. Jika menggunakan kepadatan dengan sela yang lebih kecil, kesan untuk kepadatan-kepadatan nod yang lain dapat dilihat dengan lebih terperinci berbanding kepadatan dengan sela yang besar.

b. Penetapan nilai tenaga awalan
   Nilai tenaga awalan yang tinggi akan meningkatkan peluang nod untuk menjadi ketua klaster. Jika penetapan nilai tenaga bagi nod biasa dan nod hasad tidak begitu ketara atau sama nilainya, pemilihan ketua klaster akan berlaku secara normal. Hasil analisis akan menjadi lebih tepat dan tidak dominan pada nod hasad. Dalam dua kajian terdahulu, pemilihan ketua klaster adalah cenderung pada nod hasad dengan menggunakan nilai tenaga awalan yang tinggi.

c. Bilangan nod hasad
   Hasil kajian Almomani dan Al-Kasasbeh (2015) menunjukkan bahawa kesan serangan yang teruk akan berlaku dengan peningkatan kecenderungan bilangan nod hasad. Bilangan nod hasad yang

mereka gunakan ialah sepuluh, tiga puluh dan lima puluh. Bilangan nod hasad yang banyak sudah pasti akan meningkatkan kesan pada rangkaian, tetapi kesan untuk satu nod hasad juga perlu dikaji kesannya.

d. Penjanaan kedudukan nod-nod dalam kawasan rangkaian
Kedudukan nod boleh dijana sama ada secara sebaran rawak atau grid. Kedua-dua kedudukan ini akan mempengaruhi cara pembentukan klaster dan jarak antara nod-nod dalam klaster. Nod yang berada lebih jauh dari ketua klaster akan menggunakan tenaga yang lebih berbanding nod yang lebih dekat. Begitu juga dengan keadaan nod yang bergerak (mobil) dimana tenaga yang digunakan adalah lebih berbanding nod yang statik. Ini secara tidak langsung memberi kesan terhadap jangka hayat rangkaian.

e. Kedudukan stesen pangkalan
Kedudukan stesen pangkalan yang terletak jauh dari kawasan rangkaian akan menyebabkan penggunaan jumlah tenaga yang lebih berbanding dalam kawasan rangkaian. Jika kedudukan ketua klaster jauh dari stesen pangkalan, maka lebih tenaga diperlukan untuk penghantaran data dan jangka hayat akan menjadi lebih singkat.

f. Perbezaan model serangan
Sumber untuk mewujudkan serangan *Black Hole* bukan dari sumber dan rujukan yang sama. Kajian-kajian terdahulu menggabungkan pelbagai jenis serangan dalam satu kod serangan yang sama. Modifikasi yang dilakukan pada fail-fail tampal juga mungkin berbeza. Ini akan mempengaruhi perbezaan hasil analisis kajian yang dilakukan.

4. KESIMPULAN

Kajian yang telah dilaksanakan menunjukkan bahawa serangan *Black Hole* memberi kesan pada prestasi rangkaian WSN. Metrik prestasi yang digunakan untuk kajian iaitu tempoh jangka hayat rangkaian, jumlah penghantaran data ke stesen pangkalan dan jumlah tenaga menunjukkan tindak balas terhadap serangan yang berlaku. Perbandingan yang dibuat adalah berdasarkan kepadatan bilangan nod serta kedudukan stesen rangkaian. Berikut adalah rumusan dari hasil analisis prestasi yang telah dilaksanakan dan dapatan kajian yang diperolehi.

a. Jangka hayat rangkaian secara purata akan menurun semasa serangan *Black Hole* kecuali pada kepadatan bilangan nod sebanyak enam puluh pada kedudukan stesen pangkalan (50, 175) dan empat puluh nod pada kedudukan (50, 50).

b. Jumlah data yang dihantar ke stesen pangkalan berkurangan semasa serangan *Black Hole* kecuali pada kepadatan empat puluh nod pada kedudukan stesen pangkalan (50, 50).

c. Jumlah tenaga yang digunakan meningkat pada kepadatan empat puluh nod bagi kedudukan stesen pangkalan (50, 175) dan pada kepadatan empat puluh, enam puluh dan lapan puluh nod di kedudukan stesen pangkalan (50, 50).

d. Jumlah nod yang sesuai bagi kedudukan stesen pangkalan (50, 175) dan (50, 50) adalah lapan puluh nod. Ini kerana perbezaan jangka hayat, jumlah penghantaran data dan jumlah penggunaan tenaga rangkaian tanpa serangan dan dengan serangan adalah rendah. Secara ringkasnya, sekiranya berlaku serangan *Black Hole* ke atas rangkaian yang mempunyai lapan puluh nod, maka impaknya adalah minima berdasarkan ketetapan parameter senario kajian ini.

e. Kesan maksima terhadap serangan *Black Hole* untuk kedudukan stesen pangkalan (50, 175) adalah pada kepadatan dua puluh nod. Manakala untuk kedudukan stesen pangkalan (50, 50) pula adalah pada kepadatan seratus nod.

Ringkasan perbandingan antara kepadatan bilangan nod dalam rangkaian dan kedudukan stesen pangkalan dengan serangan *Black Hole* seperti yang dipaparkan dalam Jadual 8.

Jadual 8. Ringkasan Hasil Kajian

Bilangan Nod	Kedudukan Stesen Pangkalan	Tempoh Jangka Hayat	Jumlah Data Yang Dihantar	Jumlah Tenaga Yang Digunakan
20	**(50, 175)**	Menurun	Menurun	Rendah
	(50, 50)	Meningkat	Meningkat	Tinggi
40	**(50, 175)**	Menurun	Menurun	Rendah
	(50, 50)	Meningkat	Meningkat	Tinggi
60	**(50, 175)**	Meningkat	Meningkat	Tinggi
	(50, 50)	Menurun	Menurun	Rendah
80	**(50, 175)**	Meningkat	Meningkat	Tinggi
	(50, 50)	Menurun	Menurun	Rendah
100	**(50, 175)**	Meningkat	Meningkat	Tinggi
	(50, 50)	Menurun	Menurun	Rendah

Dengan implementasi WSN yang semakin meluas berserta dengan kepesatan aplikasi yang menggunakan teknologi sensor, maka kajian-kajian berkaitan dengannya perlu diteruskan. Terdapat pelbagai aspek kajian yang boleh diterokai dan dikaji untuk membuat penambahbaikan dan meningkatkan tahap prestasi dan keselamatan teknologi rangkaian ini.

Hasil yang diperolehi dari kajian yang telah dilaksanakan ini hanyalah sebahagian kecil dari kajian-kajian besar yang lain. Kajian lanjutan perlu dilakukan untuk mendapat maklumat yang lebih terperinci dan lengkap dengan menggunakan pelbagai nilai parameter dan metrik prestasi yang berbeza. Ini adalah untuk melihat kesan serangan Black Hole secara menyeluruh.

Diharap maklumat dan hasil yang diperolehi dalam kajian ini dapat sedikit sebanyak memberi input dan idea untuk meneruskan kajian-kajian yang akan datang.

RUJUKAN

Almomani, I. & Al-Kasasbeh, B. 2015. Performance analysis of LEACH protocol under Denial of Service attacks. *IEEE* 978-1-4799-7349-1/15.

Bansal, V. & Saluja, K. K. 2016. Anomaly based detection of black hole attack on leach protocol in WSN. *IEEE* 978-1-4673-9338-6/16.

Conti, M. & Giordano, S. 2014. Mobile ad hoc networking: milestones, challenges, and new research directions. *IEEE* Communications Magazine 0163-6804/14: 85-96.

Du, J. & Li, J. 2011. A study of security routing protocol for Wireless Sensor Network. *IEEE* DOI 10.1109/IMCCC.2011.68: 236-240

Ibrahim, A., Sis, M. K. & Cakir, S. 2011. Integrated comparison of energy efficient routing protocols in Wireless Sensor Network: a survey. *IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA), Langkawi, Malaysia* 978-1-4577-1549-5/11: 237-242.

Laupa Junus. 2013. Pacu teknologi sensor. *Utusan Malaysia*, 19 Ogos: 10 & 11.

Norouzi, A., Zaim, A.H. & Sertbas, A. 2013. A comparative study based on power usage performance for routing protocols in Wireless Sensor Network. *IEEE* ISBN: 978-1-4673-5613-8: 10-15.

Patil, S. & Chaudhari, S. 2016. DoS attack prevention technique in Wireless Sensor Networks. *Procedia Computer Science* 79 (2016) 715 – 721.

Tian, L., Du, H. & Huang, Y. 2012. The simulation and analysis of LEACH protocol for wireless sensor network based on NS2. *IEEE* 978-1-4673-0945-5/12.

Tripathi, M., Gaur, M.S. & Laxmi, V. 2013. Comparing the impact of black hole and gray hole attack on LEACH in WSN. *Procedia Computer Science* 19: 1101 – 1107.

Xiaomei, Y. & Ke, M. 2016. Evolution of Wireless Sensor Network security. *IEEE*.

Zhin, C. M. 2012. Condo to be fitted with sensors. *The Star*, 27 November: Property News.