Analisis Perbandingan Protokol Keamanan MiniSec dan *Sensor Network Encryption Protocol* (SNEP) Pada Jaringan Sensorik Nirkabel

Analytical Comparison of MiniSec Security Protocol and Sensor Network Encryption Protocol (SNEP) in *Wireless Sensor Network*

Kevin Bastian Sirait[1], Fazmah Arif Yulianto[2], Sidik Prabowo[3]

Prodi S1 Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

[1]kbastian26@gmail.com [2]fazmaharif@telkomuniversity.ac.id
[3]pakwowo@telkomuniversity.ac.id

Abstrak

Sensor Jaringan Nirkabel adalah jaringan nirkabel yang berisikan sekumpulan sensor untuk menganalisa kondisi suatu lingkungan seperti tingkat kelembapan, suhu udara dan tingkat kebisingan akan tetapi pesan yang dikirimkan mempunyai pengamanan yang rendah terhadap serangan yang dapat diberikan oleh *attacker*. Protokol keamanan pada jaringan sensorik nirkabel mempunyai pengaruh yang besar untuk menjaga integritas, kerahasiaan data serta kemampuan pengiriman data untuk menghadapi kendala yang sering ditemukan pada pengiriman data di jaringan sensorik nirkabel yang dapat menyebabkan sensor tidak dapat diakses oleh user dan hilangnya kemampuan untuk mengirimkan informasi lingkungan yang dianalisa oleh sensor pada suatu lingkungan. Analisis protokol ini dilakukan untuk menentukan protokol manakah yang mempunyai performa yang lebih baik dalam penanganan serangan pada jaringan sensorik nirkabel dengan membandingkan protokol keamanan MiniSec dan *Sensor Network Encryption Protocol* (SNEP). Simulasi protokol dilakukan dengan menggunakan aplikasi NS-3 dan perbandingan protokol keamanan menggunakan metoda studi literatur. Pada akhir penelitian ditemukan pada aspek *confidentiality*, *integrity* dan *authentication* MiniSec mempunyai kinerja yang lebih fleksibel daripada SNEP pada tahapan autentikasi enkripsi dan MiniSec menggunakan energi lebih rendah dari pada SNEP dikarenakan MiniSec melakukan enkripsi serta autentikasi pada tahapan yang sama tidak seperti SNEP dengan dua tahapan yang terpisah untuk autentikasi dan enkripsi.

Kata kunci: Sensor Jaringan Nirkabel, NS-3, MiniSec, *Sensor Network Encryption Protocol* (SNEP)

Abstract

Wireless Sensor Network is a wireless network that has numbers of sensors in it to analyse the condition of certain environment for example humidity, temperature and noise level but every packets that are sent is not safe due to lack of security. Security Protocol in wireless sensor network has major influence to protect the integrity, confidentiality and the capability to transmit data like an attack to the wireless network which can result the loss of capability of the sensors to be accessed by the user and the loss of the capability to transmit data about the condition of the environment and also can damage the performance in wireless network. Protocol analysis are meant to decide which protocol that have better performance by comparing MiniSec security protocol and Sensor Network Encryption Protocol (SNEP). The simulation of the protocols used NS-3 Application and literature study for the analytical comparison of each protocols. At the end of the research, the result shows that in confidentiality, integrity and authentication point of view, MiniSec works better than SNEP due to its capability to work in flexible manner at authenticated encryption and also MiniSec has the upper hand at the energy consumption because MiniSec done its encryption and authentication in a single stage unlike SNEP for encryption and authentication are done in two separate stages.

Keywords: Wireless Sensor Network, NS-3, MiniSec, Sensor Network Encryption Protocol (SNEP)

1. Pendahuluan

Keamanan dalam pengiriman suatu informasi maupun data mempunyai peranan yang penting untuk menjaga kerahasiaan serta integritas informasi pada jaringan sensorik nirkabel. Setiap jaringan nirkabel maupun bukan nirkabel mempunyai potensi untuk tidak bekerja secara optimal serta memenuhi ekspektasi dikarenakan berbagai kendala yang muncul pada jaringan tersebut baik dimana kendala tersebut muncul secara internal mapun eksternal. Kendala tersebut dapat menimbulkan dampak merugikan seperti hilangnya kemampuan untuk mengirimkan informasi, pencurian data sampai kondisi jaringan secara keseluruhan berada dalam kondisi tidak aktif.

Protokol keamanan dibuat untuk memberikan penanganan terhadap segala efek yang merugikan kepada jaringan nirkabel dan non-nirkabel. Protokol keamanan tersebut mempunyai tujuan untuk mempertahankan originalitas informasi serta memastikan informasi tersebut tetap dapat dikirimkan untuk dapat memberikan analisa secara mendalam dan akurat. Jaringan sensor nirkabel menggunakan sensor yang mempunyai

keterbatasan pada sumber daya, kemampuan komputasi serta kemampuan untuk mengirimkan informasi dan sensor tersebut ditempatkan pada kondisi lingkungan yang tidak kondisif [1], sehingga menimbulkan kemungkinan terjadinya berbagai kendala pada jaringan sensorik nirkabel.

Berdasarkan penjelasan tersebut dilakukan perbandingan protokol keamanan jaringan MiniSec [12] dan *Sensor Network Encryption Protocol* (SNEP) [13] di jaringan sensorik nirkabel. Parameter utama dalam melakukan perbandingan protokol keamanan pada jaringan sensor nirkabel merupakan kerahasisaan data, integritas informasi, originalitas dan penggunaan energi serta simulasi serangan [1] pada jaringan sensorik nirkabel. Simulasi protokol keamanan dilakukan dengan aplikasi NS-3 dan perbandingan protokol keamanan antara MiniSec dan SNEP dilakukan dengan melakukan studi literatur.

2. Dasar Teori dan Perancangan Simulasi

2.1 MiniSec

MiniSec merupakan protokol keamanan yang mempunyai tingkat keamanan yang lebih tinggi dari pada ZigBee dengan menggunakan sumber daya yang lebih rendah daripada TinySec [12]. Protokol keamanan MiniSec mempunyai dua operasi yang digunakan untuk melakukan transmisi yaitu MiniSec-U untuk transmisi unicast dan MiniSec-B untuk transmisi broadcast, berikut merupakan format packet yang digunakan untuk MiniSec-U dan MiniSec-B:

1		2	1	2	2	1	2	0..28	4
Ctr[0:2]	Len	FCF	DSN	DstPAN	DstAddr	AM	SrcAddr	Enc Dta	Tag/MIC

Gambar 1. MiniSec-U packet format [12]

1		2	1	2	2		1	2	0..28	4
Ctr[0:2]	Len	FCF	DSN	DstPAN	Ctr[3:7]	DstAddr	AM	SrcAddr	Enc Dta	Tag/MIC

Gambar 2. MiniSec-B packet format [12]

Berikur merupakan penjelasan dari bagian bagian yang ada pada operasi *MiniSec-U* dan *MiniSec-B* saat pengiriman packet ke tujuan, yang dijelaskan sebagai berikut [12]:

a. DstAddr → *node* tujuan.
b. AM → *active message*.
c. Len → Panjang data.
d. SrcAddr → Alamat *node* asal.
e. Ctr → bit *Counter*
f. FCF → *Frame Control Field*
g. DSN → *Data Sequence Number*
h. MIC → *Message Integrity Code*
i. DstPAN → *Destination Personal Area Network*
j. Enc Dta → *Encrypted data.*

Notasi yang digunakan untuk menjelaskan cara kerja dari protokol keamanan MiniSec dijelaskan sebagai berikut:

Tabel 1. Notasi dan Definsi Protokol Keamanan MiniSec [12]

Notasi	Definisi
A, B	*Node* yang saling berkomunikasi
K_{AB}	Enkripsi OCB yang digunakan untuk komunikasi dari node A ke B, dimana kunci K_{AB} digunakan untuk meng-enkripsi data dari B ke A.
C_{AB}	*Counter* yang akan bertambah sesuai dengan kunci K_{AB}
$(C, tag) = OCB_K(N, M, H)$	Enkripsi yang ter-autentifikasi oleh OCB dimana M merupakan *plaintext*, H merupakan *header* optimal yang harus di autentifikasi, N merupakan 64 bit *nonce* dan K merupakan kunci dari OCB
N_A	*Nonce* yang dibuat oleh node A

2.2 *Sensor Network Encryption Protocol* (SNEP)

Sensor Network Encryption Protocol (SNEP) merupakan salah satuprotokol keamanan yang digunakan pada jaringan sensorik nirkabel. SNEP mempunyai kelebihan pada aspek keamanan yang

menyangkut *data confidentiality*, *authentication*, *integrity* dan *freshness* [13]. Aspek pengamanan tersebut bertujuan untuk mencegah terjadinya penyerangan dengan jenis *denial-of-service* (DoS) dikarenakan apabila sebuah sensor terkena serangan tersebut maka jaringan tersebut akan kehilangan kemampuan untuk menghasilkan fungsi dan kinerja yang seharusnya dilakukan untuk melakukan pengiriman informasi dari daerah atau lokasi yang dianalisa. SNEP mempunyai fitur utama dalam memberikan keamanan terhadap serangan yang mungkin terjadi yaitu: *sematic security*, *data authentication*, *replay protection*, *low communication overhead* dan mempunyai *weak freshness* [13].

Notasi yang digunakan pada SNEP untuk menjelaskan protokol keamanan dan operasi kriptografi dijelaskan sebagai berikut:

Tabel 2. Operasi Kriptografi SNEP [13]

Notasi	Definisi
A,B	*Node* sensor.
N_A	*Nonce* yang dihasilkan oleh A (*nonce* merupakan string bit yang tidak dapat diperkirakan.
X_{AB}	*master secret key* yang bertujuan untuk dibagikan pada A dan B.
K_{AB}	*secret encryption key* yang diberi pada A dan B.
K'_{AB}	*Secret MAC key* yang dibagikan pada A dan B, dimana A dan B merupakan turunan dari *master secret key*.
MK	pesan M yang dienkripsi serta *encryption key KAB*.
$M(K_{AB},IV)$	pesan M yang di enkripsi dengan kunci *KAB* serta inisialiasi vector (IV) yang digunakan untuk mode enkripsi.
$MAC(K_{AB},M)$	komputasi dari kode autentifikasi (MAC) dari pesan M dengan kunci MAC K'_{AB}

Mekanisme SNEP yang diberikan untuk penerimaan pesan dari node sensor yang akan menerima datadari *node* sensor yang mengirimkan data tersebut menggunakan notasi sebagai berikut:

$$A \rightarrow B : D\,(K_{AB}, C_A), MAC\,(K'_{AB}\, C_A \,||\, D\,(K_{AB}, C_A)) \quad [13]\ (1)$$

Persamaan diatas mempunyai arti dimana D merupakan data, K merupakan kunci dari enkripsi, C merupakan *counter* serta MAC berisikan kunci untuk membuka data yang telah ditelah diterima dan dienkripsi serta berisikan data asli bersama *counter* yang berperan sebagai autentifikasi [13].

2.3 Perancangan Simulasi

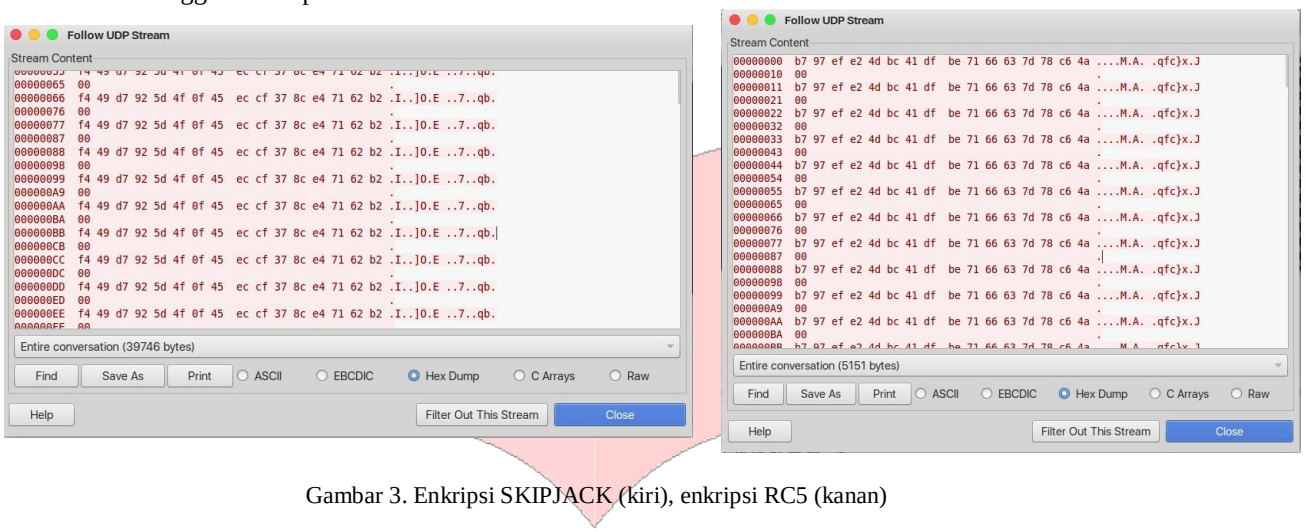
Tabel 3. Parameter skenario pengujian

Skenario Simulasi Jaringan Sensorik Nirkabel				
Waktu Simulasi	1500 detik			
Aplikasi Simulasi	NS-3 , Wireshark			
		MiniSec	SNEP	Serangan
Aspek pengujian simulasi	*Confidentiality*	SKIPJACK	RC5	-
	Integrity	OCB	HMAC	*Man-In-The-Middle*
	Authentication	OCB	CBC-MAC	*Replay Attack*
	Energy Consumption	OCB	CBC	-
Hasil output simulasi	*Confidentiality*	Ciphertext pada node base		
	Integrity	Packet yang tidak sesuai dari node tidak valid		
	Authentication	Drop packet dari node tidak valid		
	Energy Consumption	Rata -rata dan standar deviasi penggunaan energi pada sensor		
Analsis perbandingan protokol keamanan	*Confidentiality*	Studi Literatur		
	Integrity			
	Authentication			

3. Pembahasan

3.1 Simulasi *Message Confidentiality*

Ciphertext yang dihasilkan dengan menggunakan SKIPJACK dan RC5 ditemukan pada *node base* yang awalnya dikirimakan oleh sensor, berikut merupakan isi pesan yang dilihat dengan menggunakan apliksai wireshark:

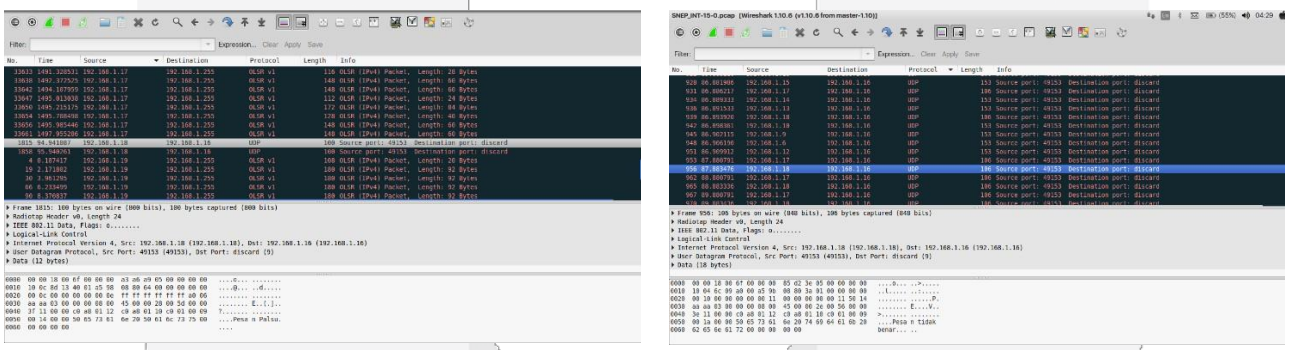


Gambar 3. Enkripsi SKIPJACK (kiri), enkripsi RC5 (kanan)

3.2 Simulasi *Message Integrity*

Pemeriksaan packet dilakukan untuk mengetahui apakah packet yang diterima mengalami perubahan atau tidak, hal tersebut dilakukan pada *node base* untuk melakukan menentukan packet yang salah dari *sender* yang mengirimkan packet tersebut.

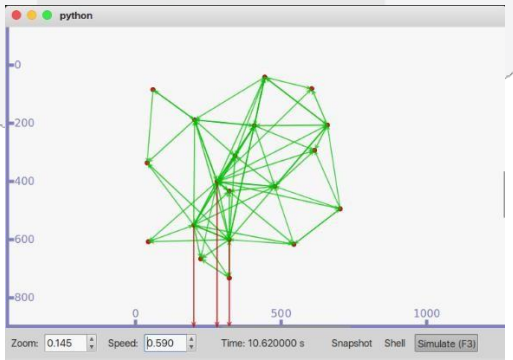
Jaringan sensorik dengan menggunakan protokol keamanan MiniSec dan SNEP menerima packet berisikan data *invalid* yang tidak berasal dari sumber yang bukan bagian dari jaringan sensorik nirkabel yang telah ditetapkan, IP dari *sender* yang bukan bagian dari jaringan tersebut merupakan 192.168.1.17 sampai dengan 192.168.1.19 , ditunjukan sebagai berikut:



Gambar 4. Cek Integritas MiniSec (kiri), SNEP (kanan)

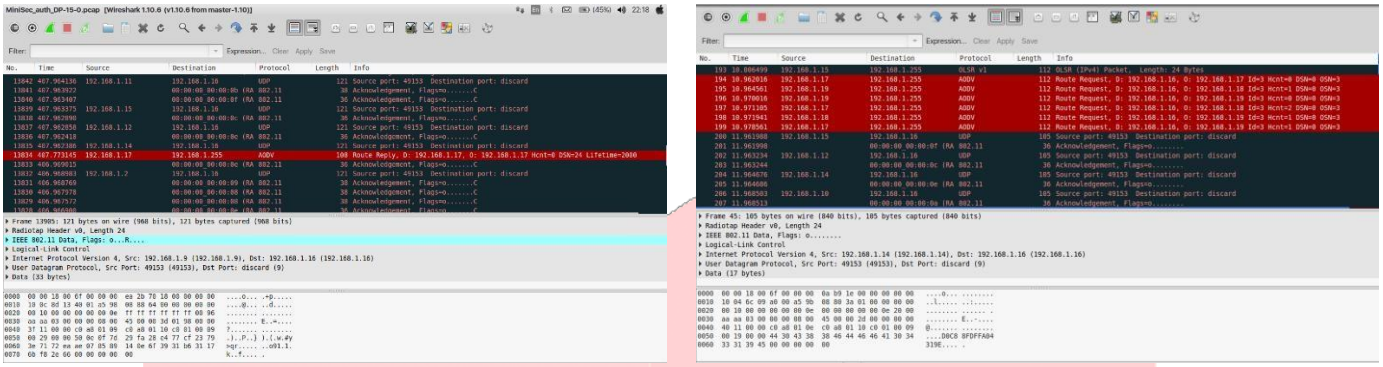
3.3 Simulasi *Message Authentication*

Paket yang di-drop ditunjukkan dengan menggunakan fitur PyViz pada NS-3. Topologi yang digunakan pada masing masing simulasi merupakan topologi yang sama, sehingga lokasi packet yang di-drop berada pada lokasi yang sama.



Gambar 5. Animasi drop packet PyViz.

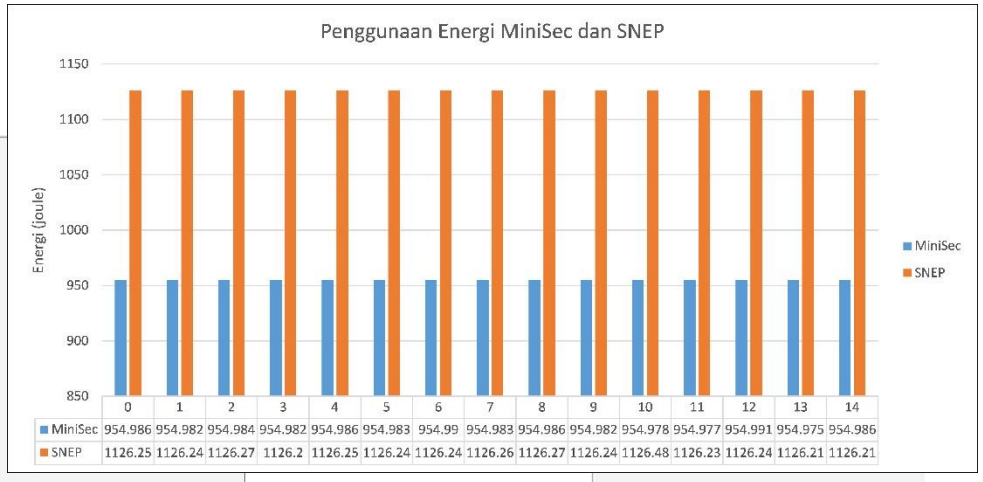
Berdasarkan hasil dari visualisasi yang telah didapat, maka digunakan apliksi wireshark untuk melihat paket yang didrop oleh *receiver*, diberikan sebagai berikut:



Gambar 6. MiniSec Auth (kiri), SNEP Auth (kanan)

3.4 Simulasi *Energy Consumption*

Hasil yang didapat terhadap penggunaan energi yang digunakan oleh sensor yang menggunakan protokol keamanan MiniSec dan SNEP diberikan sebagai berikut:



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
MiniSec	954.986	954.982	954.984	954.982	954.986	954.983	954.99	954.983	954.986	954.982	954.978	954.977	954.991	954.975	954.986
SNEP	1126.25	1126.24	1126.27	1126.2	1126.25	1126.24	1126.24	1126.26	1126.27	1126.24	1126.48	1126.23	1126.24	1126.21	1126.21

Gambar 7. Perbandingan energi secara keseluruhan MiniSec dan SNEP

Setelah simulasi selesai didapatkan hasil dari skenario dimana sensor melakukan pengiriman selama 1500 detik ditemukan bahwa MiniSec menggunakan rata - rata energi sebesar 954.9834 joule sedangkan SNEP menggunakan energi secara keseluruhan sebesar 1126.255 joule dengan standar deviasi MiniSec sebesar 0.004437 dan standar deviasi SNEP sebesar 0.065451.

Berdasarkan hasil yang didapat dapat disimpulkan bahwa MiniSec menggunakan energi lebih sedikit dari pada SNEP. Hal tersebut dapat dicapai dikarenakan MiniSec melakukan autentifikasi dan enkripsi dalam satu operasi yang berdampak komputasi yang dilakukan tidak memakan banyak sumber daya pada sensor dimana SNEP mempunyai dua operasi yaitu enkripsi dan autentifikasi yang merupakan dua tahapan yang berbeda yang mempunyai dampak memakan sumber daya yang lebih banyak dari pada MiniSec.

3.5 Studi literatur

3.5.1 *Message Confidentiality*

Aspek *Confidentiality* merupakan salah satu unsur untuk menjamin keamanan pada suatu pesan yang dikirimkan oleh *sender* terhadap *receiver* dengan cara meng-enkripsikan suatu pesan aslinya dengan tujuan pesan tersebut tidak dapat di baca oleh pihak yang tidak mempunyai kepentingan dengan data tersebut dengan kata lain pesan tersebut hanya dapat dibaca oleh *receiver*.

Simulasi terhadap aspek *confidentiality* terhadap protokol keamanan *Sensor network Encryption Protocol* (SNEP) dan MiniSec dilakukan dengan memberikan *ciphertext* kepada *receiver* dan membandingkan kenapa protokol yang menggunakan algoritma enkripsi tersebut lebih baik atau tidak dari protokol keamanan yang dibandingkan. Pada skenario pengujian aspek *confidentiality*

Minisec menggunakan OCB Skipjack dimana SNEP menggunakan CBC-RC5 untuk memfasilitsi pengamanan pesan.

Pada tahun 2009 Abu Shohel Ahmed [1] memberikan evaluasi terhadap protokol keamanan yang digunakan pada jaringan sensorik nirkabel yang didalamnya menjelaskan cara kerja dari SNEP dalam menangani serangan. Berdasarkan hasil dari evaluasi, SNEP tidak mempunyai mekanisme yang dapat membedakan *master key* yang mengalami modifikasi yang dilakukan oleh *attacker*.

Pada buku karangan G. Sen Gupta dan S. Chandra Mukhopadhyay tahun 2008 [8] menuliskan bahwa skipjack merupakan algoritma yang lebih aman dibandingkan dengan algoritma RC5 yang dapat digunakan pada sensor dikarenankan skipjack menggunakan 64 bit *blocks* serta 80 bit key dan menpunyai 32 *rounds* untuk melakukan enkripsi akan tetapi terdapat kemungkinan skipjack dapat di bongkar dengan menggunakan serangan *exhaustive key search*.

Pada tahun 2007 Mark Luk, Ghita Mezzour, Adrian Perrig dan Virgil Gligor [12] menyatakan bahwa MiniSec pengamanan terhadap aspek *confidentiality* dengan menggunakan dua mekanisme yaitu autentikasi serta menggunakan *Offset Code Book* (OCB) untuk melakukan enkripsi sedangkan SNEP hanya bergantung pada CBC-MAC dan skipjack atau RC5 untuk memberikan pengamanan. OCB-Skipjack lebih aman dibandingkan dengan CBC-RC5 dikarenakan Skipjack menggunakan komputasi dan memori yang rendah serta mempunyai fleksibilitas yang tinggi dengan menggunakan ukuran *block* sebesar 64 bits.

Buku karangan J. Lopez dan J. Zhou pada tahun 2008 [11] menuliskan bahwa SNEP mempunyai performa yang lebih baik terhadap enkripsi karena menggunakan RC5 dibandingkan dengan Skipjack akan tetapi RC5 tidak mempunyai primitif hash seperti MiniSec sehingga membutuhkan pengamanan lebih dengan menggunakan CBC-MAC sedangkan MiniSec menggunakan OCB-Skipjack dimana proses enkripsi dan autentikasi merupakan satu tahapan.

Pada tahun 2002 A. Perrig, R. Szewczyk, J. Tygar, V. Wen dan D. Culler [13] menuliskan bahwa SNEP memberikan pengamanan dengan cara memberikan nilai *counter* pada setiap node untuk membuka pesan yang telah di enkripsi yang dimana nilai *counter* tersebut berperan untuk meng-enkripsi dengan cara yang berbeda-beda pada saat menlakukan enkripsi pada *plaintext* yang akan dikirimkan.

Artikel yang dibuat oleh N. Jorstad dan T. Landgrave pada tahun 1997 [10] menuliskan bahwa RC5 menggunakan panjang dari *key* untuk memberikan fleksibilitas terhadap tingkat keamanan yang diinginkan dimana ukuran *key* dapat digunakan sampai dengan 255 bit. RC5 menggunakan parameter w sebagai ukuran *word*, r sebagai jumlah *rounds* yang digunakan untuk melakukan enkripsi dan b yang merupakan jumlah bits yang ada pada *key* sehingga tingkat keamanan harus ditentukan berelasi dengan panjang *key* dan jumlah iterasi atau *rounds* yang spesifik sedangkan Skipjack merupakan algoritma yang beroperasi pada 64 bit *blocks* yang dimana mempunyai parameter 80 bit *key* dan mempunyai 32 iterasi atau *rounds* untuk melakukan enkripsi.

3.5.2 *Message Integrity*

Aspek *integrity* merupakan salah satu unsur untuk mengetahui apakah konten dari suatu pesan telah mengalami perubahan atau tidak pada dikirimkan oleh *sender* ke *receiver*.

Simulasi terhadap aspek *integrity* dilakukan dengan memberikan serangan *man-in-the-middle* (MITM) pada MiniSec dan *Sensor Network Encryption Protocol* (SNEP), serangan tersebut bertujuan untuk melakukan perubahan isi pesan yang dikirimkan oleh *sender* kepada *receiver*. Skenario pengujian aspek *integrity* MiniSec menggunakan OCB sedangkan SNEP menggunakan *Hash Message Authentication Code* (HMAC) untuk memberikan integritas terhadap pesan yang dikirimkan.

Artikel yang ditulis oleh Y. Dodis, T. Ristenpart, J. Steinberger dan S. Tessaro pada tahun 2012 [5] menuliskan bahwa HMAC mempunyai dua kelemahan yang dimiliki oleh HMAC yaitu terdapatnya *colliding key pairs* dan *ambiguous key pair*. *Colliding keys pairs* muncul dikarenakan adanya perbedaan terhadap panjang dari *key* yang digunakan sehingga memberikan peluang kepada *attacker* untuk mencoba key yang didapat terhadap pesan yang telah diterima untuk menentukan fungsi yang digunakan untuk melakukan pengamanan pada pesan tersebut. *Ambiguous key pair* memberikan peluang kepada *attacker* untuk menemukan *key* yang digunakan dengan cara menghitung rantai *hash* diawal dan diakhir rantai dan menentukan *key* secara asal yang digunakan oleh *attacker* untuk memulai rantai hash serta menentukan *key* yang digunakan.

Pada tahun 2014 J. Guo, Y. Sasaki, L. Wang M. Wang dan L. Wen [7] menuliskan bahwa serangan MITM terhadap HMAC *attacker* mengumpulkan banyak pasangan *key* dikarenakan

tahapan *hash* tidak berurutan sehingga pada proses pertukaran *key* dapat ditemukan oleh *attacker* untuk menemukan *key* yang digunakan pada pesan untuk dikirimkan ke tujuan.

Buku karangan E. Pricop dan G. Stamatescu tahun 2016 [14] menuliskan bahwa MiniSec menggunakan OCB untuk memenuhi kebutuhan dari *confidentiality*, *integrity* dan *authencity* kelebihan dari MiniSec dari SNEP ialah dengan OCB proses enkripsi dan autentikasi dapat dilakukan dalam satu operasi dengan kata lain dilakukannya operasi *authenticaed encryption* yang dimana SNEP membutuhkan dua operasi.

Buku karangan F. Hu dan X. Cao tahun 2010 [9] menuliskan bahwa MiniSec memperoleh *authenticity* dan *integrity* dengan cara mengirimkan sedikit nilai bit *initialization vector* (IV) pada setiap packetnya akan tetapi tingkat keamanan packet yang dikirimkan dapat juga diperiksa dengan jumlah keseluruhan dari IV pada setiap packetnya tidak seperti protokol keamanan lainnya (seperti SNEP) yang membutuhkan nilai IV secara menyeluruh untuk dua operasi yaitu enkripsi dan auntentikasi.

Pada tahun 2009 Z. Gong, P. Hartel, S. Nikova dan B. Zhu [6] menuliskan bahwa MiniSec memberikanautentikasi dan integritas pada pesan. MiniSec dengan menggunakan OCB mempunyai waktu *message proccessing* yang lebih lambat dari pada HMAC dan ukuran *key* yang lebih sedikit dengan HMAC.

3.5.3 *Message Authentication*

Aspek *authentication* merupakan salah satu unsur untuk menjamin keamanan pada suatu pesan yang diterima oleh *receiver*, dimana *receiver* harus dapat memastikan bahwa pesan yang diterima berasal dari sumber yang valid dengan kata lain node yang merupakan bagian dari jaringan sensorik nirkabel tersebut.

Simulasi terhadap aspek *authentication* dilakukan dengan memberikan sebuah pesan yang tidak berasal dari node yang merupakan dari jaringan sensorik nirkabel yang telah ditentukan. *Receiver* akan melakukan pemeriksaan terhadap packet yang diterima dan membandingkan apakah packet tersebut sesuai dengan standar yang telah ditetapkan dengan menggunakan protokol keamanan MiniSec dan SNEP. Apabila packet yang diterima tidak sesuai maka packet tersebut akan di-drop.

Pada tahun 2013 Yazeed Alkhurayyif [2] melakukan komparasi terhadap *block cipher* OCB dan CBCMAC. Protokol keamanan MiniSec menggunakan OCB untuk memberikan jaminan terhadap autentifikasi pada pesan dikarenakan OCB melakukan operasi *authenticated encryption* dalam satu tahapan sedangkan protokol keamanan menggunakan CBC-MAC menggunakan dua tahapan yang berbeda dalam melakukan operasi autentikasi pesan dan operasi enkripsi pesan.

Pada tahun 2004 Tom Dennis [4] menuliskan bahwa OCB merupakan protokol enkripsi yang juga memberikan kemampuan autentifikasi pada pesan yang akan dikirimkan dimana menggunakan ukuran dari *key* dan *nonce* yang dipilih secara acak, akan tetapi *nonce* harus mempunyai ukuran yang sama pada *block cipher* yang digunakan.

Pada tahun 2007 Mark Luk, Ghita Mezzour, Adrian Perrig dan Virgil Gligor [12] menuliskan bahwaMiniSec merupakan protokol keamanan pertama yang mempunyai kemampuan untuk menangani serangan *replay attack* dalam pengaturan *broadcast* jaringan sensor nirkabel. MiniSec memberikan pengaman terhadap autentikasi dengan menggunakan ukuran dari *tag* yang digunakan sehingga *attacker* hanya mempunyai satu kesempatan dari 2^{32} kemungkinan untuk menemukan *tag* yang benar pada suatu pesan.

Pada tahun 2002 A. Perrig, R. Szewczyk, J. Tygar, V. Wen dan D. Culler [13] menuliskan bahwa SNEP tidak dapat melakukan autentifikasi apabila menggunakan *symmetric MAC key* dikarenakan pengirim dan penerima menggunakan *secret key* yang sama untuk melakukan autentifikasi, sehingga dibutuhkan mekanisme *asymmetric* untuk melakukan autentifikasi. CBC-MAC digunakan untuk melakukan perhitungan MAC untuk setiap packetnya untuk memeriksa autentifikasi dari suatu pesan.

Pada tahun 2010 W. Dargie dan C. Poellanbauer [3] menuliskan bahwa SNEP dengan CBC-MAC menggunakan *key* yang diturunkan untuk menjadi empat *key* dimana dua kunci berperan untuk proses enkripsi dan dua kunci lainnya berfungsi untuk menjaga integritas pada pesan dimana kunci tersebut didapat dengan menggunakan *pseudorandom function*. Akan tetapi dikarenakn SNEP

menggunakan CBC-MAC maka jenis mekanisme keamanan yang digunakan adalah *symmetric* sehingga autentifikasi menggunakan *key* yang sama untuk melakukan autentifikasi, oleh karena hal tersebut SNEP membutuhkan protokol lain untuk melakukan mekanisme *asymmetric* untuk menghindari *key* yang digunakan tidak diketahui oleh *attacker*.

4. Kesimpulan

Berdasarkan hasil simulasi dan studi literatur yang telah dilakukan, rancangan skenario simulasi dan studi literatur membuktikan bahwa protokol keamanan MiniSec lebih baik dari pada protokol keamanan *Sensor Network Encryption Protocol* (SNEP) pada aspek *energy consumption*, *authentication*, *confidentiality* dan *integrity*. Aspek *energy consumption* yang digunakan oleh MiniSec menggunakan rata-rata energi yang lebih sedikit daripada SNEP. Aspek *message authentication* pada MiniSec menggunakan nilai *nonce* yang berbeda sehingga menghasilkan hasil *ciphertext* yang berbeda juga daripada SNEP yang menggunakan mekanisme keamanan *symmetric* yang dapat diketahui oleh *attacker*. Aspek *message confidentiality* pada MiniSec mempunyai waktu pembongkaran yang lebih lama serta tahapan enkripsi dan autentifikasi berada dalam tahapan yang sama dibandingkan dengan SNEP dan pada aspek *message integrity* protokol keamanan MiniSec mempunyai kemampuan pemeriksaan integritas yang lebih baik dikarenakan penggunaan *Initialization Vector* yang lebih fleksibel dari pada SNEP.

Daftar Pustaka:

[1] AHMED, A. S. An evaluation of security protocols on wireless sensor network. In *TKK T-110.5190 Seminar on Internetworking*(2009).

[2] ALKHURAYYIF, Y. Security in wireless sensor network. *International Journal of Computing Science and Information Technology 1*, 3 (7 2013), 10–17.

[3] DARGIE, W., AND POELLABAUER, C. *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons,2010.

[4] DENIS, T. S. Libtomcrypt. *available online at libtom. org* (2004).

[5] DODIS, Y., RISTENPART, T., STEINBERGER, J., AND TESSARO, S. To hash or not to hash, again. *On the Indifferentiability of the Second Iterate and HMAC* (2012).

[6] GONG, Z., HARTEL, P., NIKOVA, S., AND ZHU, B. Towards secure and practical macs for body sensor networks. In *International Conference on Cryptology in India* (2009), Springer, pp. 182–198.

[7] GUO, J., SASAKI, Y., WANG, L., WANG, M., AND WEN, L. Equivalent key recovery attacks against hmac and nmac with whirlpool reduced to 7 rounds. In *International Workshop on Fast Software Encryption* (2014), Springer, pp. 571–590.

[8] GUPTA, G. S., AND MUKHOPDHYAY, S. C. *Smart Sensors and Sensing Technology*. Springer, 2008.

[9] HU, F., AND CAO, X. *Wireless sensor networks: principles and practice*. CRC Press, 2010.

[10] JORSTAD, N. D., AND LANDGRAVE, T. Cryptographic algorithm metrics. In *20th National Information Systems Security Conference* (1997).

[11] LÓPEZ, J., AND ZHOU, J. *Wireless sensor network security*, vol. 1. Ios Press, 2008

[12] LUK, M., MEZZOUR, G., PERRIG, A., AND GLIGOR, V. Minisec: a secure sensor network communication architecture. In *Proceedings of the 6th international conference on Information processing in sensor networks* (2007), ACM, pp. 479–488.

[13] PERRIG, A., SZEWCZYK, R., TYGAR, J. D., WEN, V., AND CULLER, D. E. Spins: Security protocols for sensor networks. *Wireless networks 8*, 5 (2002), 521–534.

[14] PRICOP, E., AND STAMATESCU, G. *Recent Advances in Systems Safety and Security*, vol. 62. Springer, 2016