Analisis Efisiensi Energi Pada Protokol Keamanan Jaringan Sensor Nirkabel Menggunakan Teknik *Pairwise Keys Establishment* dan *Advanced Encryption Standard*

Analysis Of Energy Efeciency on Wireless Sensor Network Security Protocol with Pairwise Keys Establishment Technique and Advanced Encryption Standard

Saiful Anwar[1], Fazmah Arif Yulianto S.T., M.T.[2], Sidik Prabowo S.T., M.T.[3]

[1]Prodi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom
[1]saifulanwar3101@gmail.com, [2]fazmaharif@telkomuniversity.ac.id ,[3]prabowosidik@gmail.com

Abstrak

Dalam *Wireless Sensor Network (WSN),* keamanan dalam pengiriman data merupakan hal terpenting, melihat data yang didapat dan dikirim oleh *WSN* bersifat penting. Banyaknya berbagai macam serangan uyang ditujukan terhadap WSn sehingga perlunya ada penanganan terhadap serangan tersebut, salah satunya menggunakan protokol keamanan WSN. Salah satu protkol keamanan WSN yang ada sekarang adalah Minisec yang memiliki spesifikasi Authentication and Encryption. Tetapi minisec memiliki kelemahan salah satunya adalah enkripsinya yang merupakan enkripsi Skipjack yang sudah tidak memadai untuk digunakan sekarang. Dalam jurnal ini akan mencoba untuk mengurangi kelemahan minisec tersebut dengan ditambahkan algoritma AES 128 dan PKE yang selanjutnya akan dibandingkan dari sistem minisec sebelumnya sehingga dapat diketahui tingkat penurunan kelemahan dari kekurangan sistem sebelumnya. Hasil dari jurnal ini adalah perbandingan dari segi kemanan dan penggunaan energi dari protokol keamanan WSN yang diterapkan sebelum dan sesudah ditambahkan AES dan skipjack.

Kata Kunci: Enkripsi, Cooja, ContikOS, AES, Skipjack, WSN.

Abstract

In the Wireless Sensor Network (WSN), security of data delivery is paramount, see the data obtained and sent by WSN is important. The number of different kinds of attacks directed against WSN thus need no treatment against such attacks, one of which uses a security protocol WSN. One of the security protocols existing WSN is Minisec which has a specification Authentication and Encryption. But minisec has drawbacks one of which is the encryption which is an encryption Skipjack already inadequate for use now. In this paper will try to reduce the weaknesses minisec added with AES 128 algorithm and PKE which will then be compared from the previous minisec system so that it can be seen the rate of decline weaknesses of the previous system deficiencies. The results of this paper is the comparison in terms of security and energy usage of WSN security protocols were applied before and after add AES and skipjack.

Keyword*: Encryption, Cooja, ContikOS, AES, Skipjack, WSN.*

1. Pendahuluan

Wireless Sensor Network(*WSN*) atau Jaringan Sensor Nirkabel merupakan sejumlah besar *Node* yang digunakan untuk memantau sebuah fenomena. *WSN* secara luas digunakan untuk pengolahan data dalam skala besar yang sifatnya Real-Time. Jaringan Sensor Nirkabel yang awalnya diciptakan untuk memenuhi kebutuhan dunia ini akan teknologi sensor yang *Low-Cost* arsitektur [3]. Sehingga dengan kebutuhan tersebut, terciptalah *WSN* dengan spesifikasi *Low-Power, Limited Capacity, Short Range Transmitter*. Tapi meskipun begitu dengan jumlah yang banyak *WSN* dapat digunakan secara menyebar dilingkungan yang tak terjangkau. Tugas *WSN* adalah mengumpulkan data, dan data tersebut bersifat rahasia, sehingga keamanan dalam segi pengiriman data merupakan konsentrasi terpenting dalam *WSN*. Kerahasiaan merupakan tujuan utama dari sebuah keamanan, dengan begitu dapat dipastikan sebuah komunikasi tersebut tepat sesuai tujuan. Dengan begitu protokol keamanan yang menjamin kerahasiaan data yang dikirim antar *Node-to-Node* bahkan *Base Station* harus digunakan tetapi dengan memperhatikan melihat kapasitas daya energi dan *Bandwith* yang disediakan oleh sensor tersbut. Banyak riset yang telah dikembangkan untuk memenuhi kebutuhan keamanan pada Jaringan Sensor Nirkabel salah satunya ada lah protokol keamanan WSN Minisec. *Minisec* memperkenal diri dengan *Low-Cost Energy* dan *High Security* yang dalam penerapannya menggunakan metode keamanan Authentication and Encryption. Dalam penerapannya *Minisec* menggunakan enkripsi *Skipjack* untuk meningkatkan keamanannya. *Verheul* dan *Lnstra* yang merupakan developer menciptakan *Minisec* dengan implementasi enkripsi *Skipjack*, karena melihat spesifikasi *Node* saat itu yang tidak memadai untuk diterapkan enkripsi yang lebih tinggi. Tapi melihat dari spesifikasi yang dimiliki oleh *Skipjack*, yang hanya menggunakan sistem *block Size* 64-bit dan 80 bit *keys*, menjadi agak berbahaya karena dengan jumlah *Keys* tersebut masih terhitung sedikit dibandingkan dengan enkripsi yang lain. Oleh

karena itu Verheul dan Lnstra merekomendasikan untuk menggunakan AES. Dan untuk Autnetication menggunakan PKE sebagai penanganannya.

Hasil dari jurnal ini akan didapat dari dua buah pengujian, dari segi keamanan dan efisiensi daya. Dalam segi keamanan, akan dilakukan serangan *impersonate attack* untuk memperoleh hasil tingkat keamanan dari sistem enkripsi tersebut. Dalam segi efisiensi daya, akan dilakukan pembandingan jumlah daya yang digunakan sebelum dan sesudah enkripsi *AES 128* diterapkan.

2. Dasar Teori dan Perancangan

2.1 Dasar Teori

2.1.1. Contiki OS dan Cooja Simulator

Contiki diciptakan oleh Adam Dunkels pada tahun 2002 dan telah dikembangkan lebih lanjut oleh tim di seluruh dunia pengembang dari Texas Instruments, Atmel, Cisco, ENEA, ETH Zurich, Redwire, RWTH Aachen University, Oxford University, SAP, Sensinode, Swedish Institute Ilmu Komputer, ST Microelectronics, Zolertia, dan banyak lainnya. Nama Contiki berasal dari terkenal rakit Kon-Tiki Thor Heyerdahl.

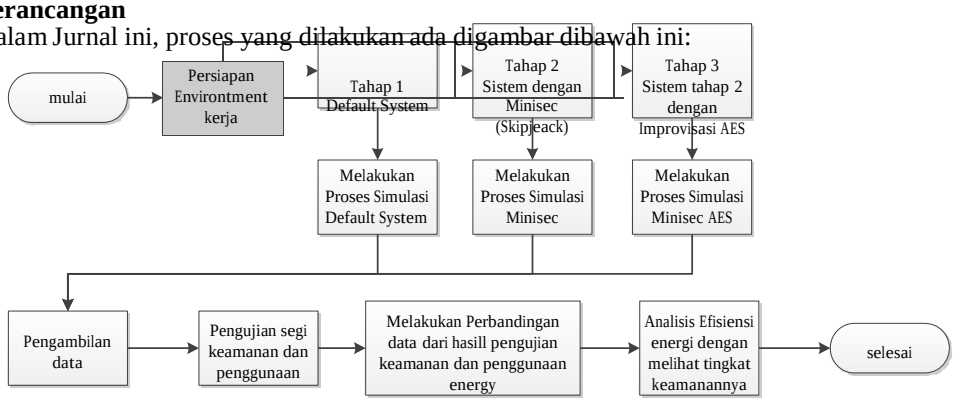
Dalam sistem operasi contiki tersedia simulator yaitu Cooja, yang dimana Cooja merupakan simulator berbasis java yang dibuat untuk Node – Node yang bekerja pada ContikiOS. Tetapi, ada beberapa yang menyebutkan bahwa Cooja bukan hanya sebuah simulator, melainkan emulator.

2.1.2. Minisec

MiniSec merupakan salah satu protokol keamanan yang ada pada Jaringan Sensor Nirkabel, yang bekerja dengan menggunakan dua jenis skema yaitu *Unicast* dan *Broadcast*. Dalam penerapan dua skema tersebut, *MiniSec* menerapkan pada dua buah operasi yaitu *MiniSec-U* dan *MiniSec-B*. Dengan sistem Enkripsi dan Autenifikasi, *MiniSec* memperkenalkan diri sebagai protokol keamanan yang *Low-Cost Energy* dan *High Security*.

2.2 Perancangan

Dalam Jurnal ini, proses yang dilakukan ada digambar dibawah ini:



Berikut merupakan tahapan perancangan

a. Tahap 1: *Default System*

   Default System merupakan keadaan dimana simulasi *WSN* biasanya bekerja. Proses kerja dari tahap ini adalah mengirimkan data dari hasil sensing *Node* menuju *Base Station*. Setelah data terkirim, akan diambil data penggunaan energi yang digunakan oleh tahap ini untuk dibandingkan dengan tahap – tahap lain.

b. Tahap 2: Penambahan Protokol *Minisec*

   Pada tahap ini, akan ditambahkan protokol keamanan *WSN Minisec* pada proses simulasi. Dalam proses kerja, *Minisec* bekerja untuk mengamankan data secara *authentication* dan e*ncryption*. Dalam tugas akhir ini, akan dikonsentrasikan dalam proses *encryption*-nya, karena akan dilihat seberapa aman dari proses enkripsi tersebut. Dalam *Minisec* Encryption yang digunakan adalah *skipjack*, dari enkripsi *skipjack* ini, yang nantinya akan dibandingkan tingkat keamananya dengan enkripsi pada tahap selanjutnya.

c. Tahap 3: Tahap 2, Dengan Mengubah *Skipjack* menjadi *AES*

   Pada tahap ini, sistem enkripsi *AES* akan diterapkan dengan menggantikan sistem enkripsi *skipjack*. Dalam tugas akhir ini, algoritma *AES* yang digunakan adalah algoritma *AES* 128 yang dibuat oleh openssl. Sebuah library standar yang digunakan dalam cryptography. Dalam implementasinya, openssl menyediakan source code *AES* dalam algoritma C, sehingga mudah diimplementasikan tanpa harus menginstal *library* baru dicontiki.

2.3 Pengujian dari segi efisiensi energi

Pada Jurnal ini, pengujian dari segi efisiensi enegri dilakukan dengan cara mengambil data yang telah dikeluarkan oleh *message*. data tersebut didapatkan dengan melakukan pengujian dari setiap tahapan yang sudah dirancang. Data energi yang diambil berdasarkan komputasi sistem dan trasnmisi data dalam bentuk mW. Setiap Node yang telah melakukan pengiriman data menuju *Base Station*(termasuk *Base Station*) akan diambil data penggunaan energinya. Jumlah data energi yang diambil pada pengujian ini dilakukan sebanyak 50 kali untuk setiap tahap. Data tersebut dibaca secara manual lalu diolah dengan menggunakan *microsoft excel* untuk disajikan dalam bentuk grafik 2D untuk selanjutnya dianalisis. Tujuan dari pengujian ini, untuk mendapatkan analisis perbandingan efisiensi energi yang digunakan oleh setiap tahapan untuk selanjutnya dibandingkan lagi dengan segi keamanan.

2.4 Pengujian dari Segi Keamanan

Pada pengujian dari segi keamanan, dilakukan dengan cara membuat serang terhadap simulasi ini. dilakukan serangan dikarenakan konsentrasi tujuan akhir ini adalah untuk melihat tingkat keamanan pada enkripsi data.

a. Impersonate Attack

Serangan yang dilakukan adalah serangan impersonating. Serangan *impersonating*, merupakan jenis serangan yang dimana untuk konteks tugas akhir yaitu memakasa Node untuk mengirim data yang seharusnya dikirim menuju Base Station tapi dikirim ke Node impersonate.

Dalam proses *impersonate data*, Node dibuat sedemikian mirip dengan Node yang akan dicuri datanya(*Base Station*) agar dapat dengan melakukan proses impersonate. Tujuan sebenarnya dari impersonate ini adalah untuk bisa masuk pada layer keamanan *authentication*-nya. Sehingga dengan begitu, proses transmisi data yang ada dalam simulasi WSN dapat dilihat dan dicuri. Proses *impersonate* dilakukan pada tiap tahapan, untuk melihat data yang ditransmisikan selama proses dilakukan.

Tujuan dari pengujian ini untuk dapat melihat dari proses PKE yang diterapkan simulasi itu, yang dimana proses PKE mewakili dari segi keamanan *Authentication* dari minisec.

b. Bruteforce Attack

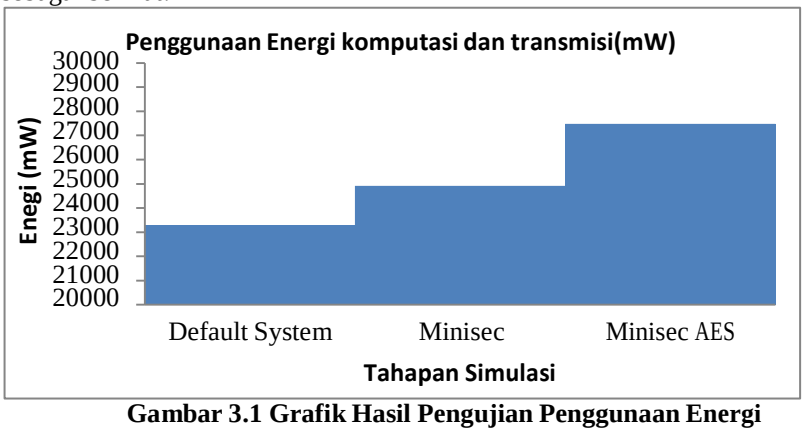
Pengujian bruteforce pada simulasi ini adalah dengan melakukan perhitungan matematis dari masing – masing kunci untuk mendapatkan nilai durasi proses untuk memecahkan kuncialgoritma AES 128 dan skipjack yang digunakan oleh tugas akhir ini yang akan dibandingkan. Yang dimana AES 128 memiliki panjang key 128 bit dan skipjack memiliki panjang keys 80-bit.

3. Pembahasan

Pada bagian ini akan menjelaskan hasil pengujian dari segi keamanan dan segi efisiensi energi.

3.1. Perhitungan Penggunaan energi

Perhitungan hasil penggunaan energi ini dicapture dari *message output contiki cooja*, dimana dari contiki cooja tersebut data diolah kedalam tabel dan untuk selanjutnya diolah dalam bentuk grafik. Data hasil penggunaan energi ini akan dikumpulkan berdasarkan penggunaan energi dari *Node* dari seluruh tahapan yang ada dalam perancangan pengujian. Data tersebut meliputi penggunaan energi komputasi dan transmisi dalam satuan mW dan selanjutnya akan dijumlahkan untuk selanjutnya dibuat grafik untuk dapat dibandingkan. Grafik hasil perhitungan data secara total sebagai berikut:



Gambar 3.1 Grafik Hasil Pengujian Penggunaan Energi

Dari gambar 4.6 dapat dilihat bahwa penggunaan energi pada simulasi ini jika diurutkan berdasarkan penggunaan terkecil ke terbesar yaitu tahap 1, tahap 2, dan tahap 3.

Tabel 3-1 hasil Pengujian Penggunaan Energi

No	Tahap Pengsimulasian	Penggunaan Energi(mW)
1	Tahap default system	23272
2	Tahap Minisec	24908
3	Tahap Minisec AES	27486

Tabel 3-2 Perubahan Energi dari tiap Tahap simulasi (%)

No	Simulasi	Jumlah Penigkatan Energi (dibandingkan sistem default)
1	Tahap Minisec	7,02%
2	Tahap Minisec AES	10,35%

a. Pengujian bagian kemanan

Pengujian bagian keamanan dilakukan dengan kondisi impersonating yang sudah dilakukan sehingga pengujian dari segi enkripsi dapat dilakukan. Berikut merupakan hasil impersonating dari simulasi tugas akhir ini.

Dari gambar tersebut dapat dilihat, *Node* default dari simulasi tugas akhir ini adalah *Node* dari 1 – 5 dan didalam gambar terlihat ada *Node* dengan id 6. *Node* dengan id 6 itu adalah *Node impersonate* yang gunanya untuk mencuri data. Berikut hasil dari impesonating *Node* terlihat dari gambar.

Setelah dari proses *impersonate* ini dilakukan, maka tujuan dari tugas kahir dapat dilakukan sesuai dengan bab 1 yaitu penenrapan enkripsi. Pada pengujian keamanan enkripsi pada tugas akhir ini, akan dilakukan pada enkripsi yang digunakan oleh seluruh tahapan yaitu *skipjack* dan *AES*. Pengujian dilakukan sesuai dengan skneraio yang sudah dijelaskan.

- *Brute force attack*

  Seperti yang sudah dijelaskan diskenario, bahwa *bruteforce attack* dilakukan dengan melakukan perhitungan matematis, perhitungan matematis dari dilakukan sebagai berikut:

  Dengan asumsi bahwa penggunaan flops per cek kombinasi *keys* adalah 1000

  Jadi jumlah kombinasi check/s adalah

  $125.435{,}9 \times 10^{12}/1000 = 125.435{,}9 \times 10^{9}$

  Dalam satu tahun ada sekitar =

  365 x 24 x 60 x 60 = 31536000 s

  Waktu yang dibutuhkan untuk dapat memecahkannya

  Skipjack

  Skipjack memiliki *keys* 80-bit

  $$\frac{1{,}2 \times 10^{24}}{125.435{,}9 \times 10^{9} \times 31536000} = 303 \text{ [illegible]}$$

  AES 128

  AES 128 memiliki *keys* 128-bit

  $$\frac{3{,}4 \times 10^{38}}{125.435{,}9 \times 10^{9} \times 31536000} = 85 \times 10^{15} \text{ [illegible]}$$

  Beikut tabel perbandingan nilai dari pengujian *brute force attack*:

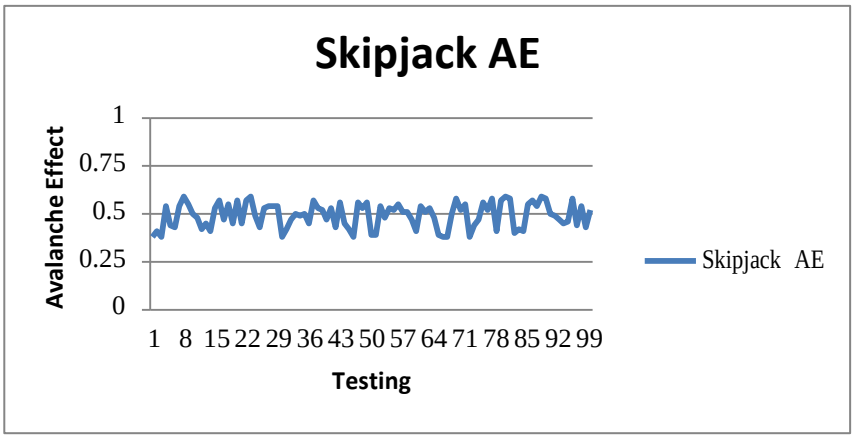
Tabel 3-3 Hasil Pengujian BruteForce

No	Enkripsi	Keys	Waktu untuk Bruteforce (tahun)
1	Skipjack	80-bit	303
2	AES 128	128-bit	85×10^{15}

- *Avalanche effect*

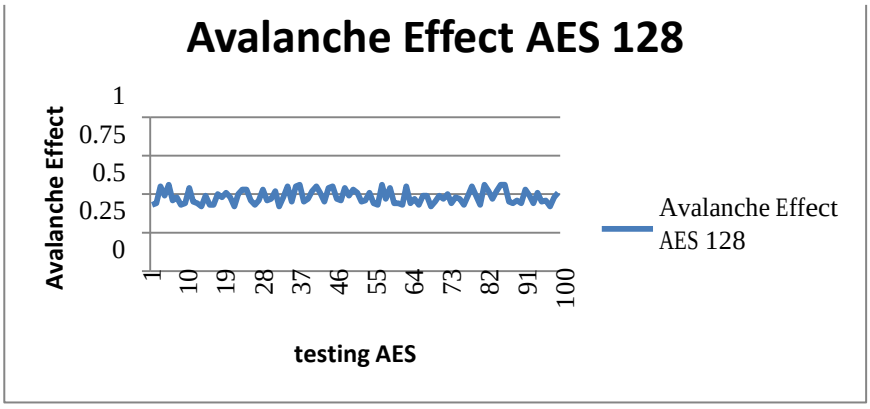
  Pengujian pada *avalanche effect* dilakukan sebanyak 100 kali. Hasil dari proses pengujian *avalanche effect* ada pada lampiran dan berikut merupakan ringkasan hasil pengujian *avalanche effect*.

  a. Pengujian Avalanche Effect Skipjack



Gambar 3.2 Grafik Hasil Pengujian Avalanche Effect Skipjack

b. Pengujian Avalanche Effect AES 128



Gambar 3.3 Grafik Hasil Pengujian Avalanche Effect AES 128

Dan berikut merupakan ringkasan hasil dari pengujian avalanche effect pada skipjack dan AES 128:

Tabel 3-4 Hasil Pengujian Avalanche Effect

No	Enkripsi	Rata – Rata Avalanche Effect (%)
1	Skipjack	45%
2	AES 128	48,23%

- *Impersonate* attack

  Hasil pengujian dari impersonate attack didapatkan dengan melakukan impersonate pada tahap yang ada PKE dan tidak ada PKE, hasil dari pengujian dilihat dari jumlah data yang didapatkan oleh Node impersonate melihat berapa sequensial yang telah dilakukan. Hasil impersonate terlihat pada tabel berikut:

  Tabel 3-5 Pengujian Imperosnate Attack

No	Pengujian	Presentase data yang didapat
1	Tanpa PKE	87%
2	Dengan PKE	2%

  Jadi setelah menggunakan PKE terlihat bahwa, tingkat keamanan terhadap authentication meningkat, yang membuat pencurian data semakin

4. Kesimpulan

Kesimpulan ini didasarkan hasil perhitungan dan pengujian yang telah dilakukan. Dari hasil perhitungan penggunaan energi terjadi penambahan penggunaan energi jika dibandingkan dengan tahap 1. Terlihat dari tabel 4.2, tahap 3 yang merupakan tujuan dari tugas akhir ini mengalami perubahan sebesar 10,35%. Dari perubahan penggunaan energi tersebut, akan menyebabkan durasi penggunaan *Node* akan berkurang, tetapi jika dilihat dari segi keamanan pada tabel 4-3, 4-4, 4-5, kemanan dari tahap minisec Aes mengalami peningkatan.

Dalam jurnal ini, bertujuan mengalisis seberapa efisien penggunaan energi yang terjadi jika dilakukann penmabahan fitur *PKE* dan *AES* 128. Setiap penambahan fitur keamanan akan

mengakibatkan penggunaan energi. Jika dilihat dari tabel 4.3 dan tabel 4.4, terlihat bahwa jika dibandingkan dengan *current system* yang sekarang ada yaitu tahap 2 dengan dibandingkan dengan usulan dari tugas akhir yaitu tahap 3, terlihat tingkat keamanan dari tahap 3 mengalami peningkatan dilihat dari serangan yang ditujukan terhadap sistem enkripsinya tetapi memiliki efek samping yaitu peningkatan penggunaan energi.

5. Daftar Pustaka

[1] Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, “Spins: security protocols for sensor networks,” in Proceedings of ACM Mobile Computing and Networking (Mobicom’01), 2001, pp.189–199.

[2] Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly-Secure Key Distribution for Dynamic Conferences,” Lecture Notes in Computer Science, vol. 740, pp. 471–486, 1993.

[3] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "TinySeRSync: Secure and resilient time synchronization inwireless sensor networks". In ACM CCS, November 2006.

[4] Jutla, "Encryption modes with almost free message integrity." Advances in Cryptology – EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045, B. Pfitzmann, ed., Springer-Verlag, 2001.

[5] V. Gligor, and P. Donescu, "Fast encryption and authentication: XCBC encryption and XECB authentication modes". Fast Software Encryption, Lecture Notes in Computer Science, Springer-Verlag, Apr2001.

[6] W. Zhang, M. Tran, S. Zhu, and G. Cao, "A Random Perturbation-Based Scheme for *Pairwise* Key *Establishment* in Sensor Networks", MobiHoc’07, September 9–14, 2007, Montréal, Québec, Canada. Copyright 2007 ACM 978-1-59593-684-4/07/0009 allow two nodes that can communicate (directly or indirectly)

[7] Youssef Sherin M., Mohamed Baith, “An Enhanced Security Architecture for Wireless Sensor Network”. In ACM, April 2014.

[8] Ren jian, “An Eficiency Link Layer Security Protocol for Wireless Sensor Network”, in IEEE, July 2014.

[9] Liu donggang, “Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks”, in IEEE, October 2003.

[10] L. Javier dan Z. Jianying, “Overview of Wireless Sensor Network Security,” IOS Press, 2008.

[11] Wei Liu dan Rong Luo, “Cryptography Overhead Evaluation and Analysis for Wireless Sensor Networks”, International Conference on Communications and Mobile Computing, 2009.

[12] European Network of Excellence in Cryptology II team, “ECRYPT II Yearly Report on Algorithms and *Keys*izes”, European Commission within the 7th Framework Programme, 2012.

[13] Dunkels, Adam, “Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors”, IEEE Coneference, 2004.

[14] Luk, Mark,“*Minisec*: A Secure Sensor Network Communication Architecture”, ACM, 2007.

[15] Liu, Donggang, “Establishing *Pairwise Keys* in Distributed Sensor Networks”, ACM, 2007.

[16] *Node*iv Team, “T*Node* Sky: Datasheet”, *Node*iv Corporation, 2006.

[17] Fieldman, Michael (20 juni 2016). China Races Ahead in TOP500 Supercomputer List, Ending US Supremacy. [Online] Tersedia di: http://www.top500.org/news/china-races-ahead-in- top500-supercomputer-list-ending-us-supremacy/ [Diakses pada tanggal 23 juni 2016].

[18] Z. Feng dan G. Leonidas, “Wireless Sensor Networks: An Information Processing Approach,” Morgan Kaufmann.

[19] Kumar, Amish, “Effective impelemntation and Avalanche Effect of AES”, IJSPTM, 2012.

[20] Matyas, Vaclav, “Biometric Authentication – Security and Usability”, Faculty of Informatics, Masaryk University Brno, Czech Republic.

[21] Poundstone, William (1983). Big Secrets. William Morrow. pp. 20–21. ISBN 0-688-04830-7.

[22] Abe, Masayuki, “Advances in Cryptology - ASIACRYPT 2010”, 16th International Conference on the Theory and Application of Cryptology and Information Security, 2010.

Stern, Jacques, “Advances in Cryptology — EUROCRYPT 1999”, International Conference on the Theory and Application of Cryptographic Techniques Prague, 1999.