IMPLEMENTASI DAN ANALISA SISTEM KEAMANAN DI JARINGAN SENSOR NIRKABEL PADA STANDAR ZIGBEE

IMPLEMENTATION AND ANALYSIS OF SECURITY SYSTEM IN WIRELESS SENSOR NETWORK BASED ON ZIGBEE STANDARD

Jorjiana Aminatus SIP[1], Dr. Ir. Rendy Munadi, M.T.[2], Gustommy Bisono, S.T., M.T.[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Univesitas Telkom

[1]jorjiana.asip@gmail.com, [2]rendymunadi@telkomuniversity.ac.id, [3]bisono.telu@gmail.com

Abstrak

Wireless Sensor Network (WSN) atau Jaringan Sensor Nirkabel (JSN) merupakan teknologi yang sedang hangatnya digunakan baik untuk riset maupun untuk mempermudah kehidupan sehari-hari. Sistem keamanan adalah salah satu hal penting yang harus diperhatikan baik dalam wireless network maupun wireline network. Jaringan sensor nirkabel semakin berkembang yang mengakibatkan mudah diserang dan sebab itu membutuhkan mekanisme keamanan yang efektif. Jaringan sensor nirkabel memiliki beberapa kendala seperti memori terbatas, energi dan kemampuan komputasi yang menimbulkan kendala bila ditambah dengan keamanan di node sensor.

Untuk menyelesaikan masalah diatas, tugas akhir ini akan mengimplementasikan dan menganalisa sistem keamanan di jaringan sensor nirkabel mengacu pada standar ZigBee. Skema ZigBee dapat disetarakan dengan protokol baru yang ditargetkan pada low rate, perangkat dengan daya kecil, dan node sensor. ZigBee membutuhkan kriptografi yang diharapkan bisa menghemat daya, kemampuan komputasi, dan sumber penyimpanan. Untuk itu, sistem keamanan yang dipilih adalah menggunakan algoritma enkripsi AES (Advanced Encryption Standard) yang diimplementasikan langsung pada ZigBee.

Pada tugas akhir ini berhasil mengimplementasikan algoritma enkripsi dekripsi AES128 pada jaringan sensor nirkabel. Pengujian yang digunakan adalah passive attacks yang hanya bisa melihat dan meng-capture packet saja. Pada analisa performansi keamanan, parameter confidentiality tidak terpenuhi jika tidak menggunakan keamanan. Parameter integrity terpenuhi menggunakan atau tanpa menggunakan keamanan. Nilai throughput terbesar adalah 1122 bytes/s pada jarak 21 meter. Dan nilai delay terbesar pada jarak 49,5 meter dengan nilai 4,1483 s.

Kata Kunci : WSN, ZigBee, AES128

Abstract

Wireless Sensor Network (WSN) is a technology that is being warmly used both for research and to help human activities. System security is one of the important things that must be considered both in wireless network and wireline network. Wireless sensor networks are expanding which are vulnerable and therefore require an effective security mechanism. Wireless sensor networks have several constraints such as limited memory, energy and computational capabilities that create constraints when coupled with security at sensor nodes.

To solve the above problem, this final project will implement and analyze security system in wireless sensor network refers to ZigBee standard. ZigBee schemes can be synchronized with new protocols targeted at low rates, small power devices, and sensor nodes. ZigBee requires cryptography that is expected to save power, computing power, and storage resources. To that end, the chosen security system is using AES encryption algorithm (Advanced Encryption Standard) which is implemented directly on ZigBee.

In this final project successfully apply AES128 decryption and encryption algorithm on wireless sensor network. The test used is a passive attack that can only see and capture the package only. In a security performance analysis, the confidentiality parameter is not fulfilled if it does not use security. Integrity parameters are fulfilled using or without using security. The largest throughput value is 1122 bytes / s at a distance of 21 meters. And the last delay at a distance of 49.5 meters with a value of 4.1483 s.

Keyword : WSN, ZigBee, AES128

1. Pendahuluan

Wireless Sensor Network (WSN) atau Jaringan Sensor Nirkabel (JSN) merupakan teknologi yang sedang hangatnya digunakan baik untuk riset maupun untuk mempermudah kehidupan sehari-hari. WSN adalah jaringan dengan infrastruktur yang bisa mendeteksi, menghitung dan mempunyai elemen komunikasi yang dapat mengirimkan data kepada administrator untuk mengukur, mengobservasi, dan memberikan perintah jika ada suatu kondisi tertentu. Salah satu tujuan dari wireless sensor network adalah untuk membawa informasi yang dapat dipercaya dari satu node ke node yang lain dalam jaringan tersebut [1]. Wireless sensor setwork adalah aspek krusial yang ada dalam pengimplementasian IoT karena sensor merupakan perangkat kecil, portable, dan bisa diimplementasikan di banyak aplikasi [2].

Sistem keamanan adalah salah satu hal penting yang harus diperhatikan baik dalam wireless network maupun wireline network. Jaringan sensor nirkabel semakin berkembang yang mengakibatkan mudah diserang dan sebab itu membutuhkan mekanisme keamanan yang efektif [1]. Pengguna WSN seharusnya percaya bahwa informasi yang mereka terima dari jaringan dapat dipercaya, akurat, dan tidak dirusak oleh pihak yang tidak bertanggung jawab. Contohnya jika seorang petani menggunakan WSN untuk sistem irigasi otomatis harus percaya bahwa sensor tidak rusak yang dapat mengakibatkan tanah akan kering atau tanaman kering sebelum memperingatkan petani [2]. Jaringan sensor nirkabel memiliki beberapa kendala seperti memori terbatas, energi dan kemampuan komputasi yang menimbulkan kendala bila ditambah dengan keamanan di node sensor. Untuk mengirimkan informasi yang telah dibaca oleh node sensor membutuhkan ZigBee untuk mengirim sehingga informasi tersebut sampai kepada pengguna WSN tersebut. ZigBee merupakan standar yang diatur dalam IEEE 802.15.4, yang terdiri dari physical (PHY) layer, medium access control (MAC) layer, network (NWK) layer, dan application layer [3].

Untuk menyelesaikan masalah diatas, tugas akhir ini akan mengimplementasikan dan menganalisa sistem keamanan di jaringan sensor nirkabel mengacu pada standar ZigBee. ZigBee seperti standar yang mana sepanjang konfigurasi sensor mikro dari ZigBee yang dapat saling berhubungan satu sama lain dari Adhoc [3]. ZigBee adalah standar yang muncul untuk low power, low rate komunikasi nirkabel dimana dengan tujuan dua sistem dapat bekerjasama dan dapat mencakup seluruh perangkat dalam cakupan WSN walaupun daya pada node sensor rendah [4]. ZigBee membutuhkan kriptografi yang diharapkan bisa menghemat daya, kemampuan komputasi, dan sumber penyimpanan. Algoritma enkripsi AES pernah dilakukan pada standar IEEE 802.15.4 tetapi menggunakan perangkat TelosB [5]. Untuk itu, sistem keamanan yang dipilih adalah menggunakan algoritma enkripsi AES (Advanced Encryption Standard) yang diimplementasikan langsung pada ZigBee.

2. Dasar Teori

2.1 Keamanan pada WSN

Lingkungan WSN mungkin dapat terkena serangan *Internet-originated* seperti *Denial of Service* (DoS), dan dalam konteks ini *availability* dan *resilience* merupakan syarat yang penting [5]. Jaringan yang aman menggunakan trust center, yang mana mempedulikan kuci. Jaringan yang aman tidak menggunakan satu kuci detiap saat, tetapi menggunakan beberapa kunci dan merubah kunci secara kontinyu [10].

Mengamankan jaringan sensor nirkabel membutuhkan jaringan yang dapat mendukung semua aspek keamanan: confidentiality, integrity, authenticity, dan availability. Untuk memilih algoritma enkripsi yang paling efisien dalam semua aspek seperti kecepatan operasi, penyimpanan dan daya konsumsi. Kunci kriptografi simetris lebih cepat prosesnya dibanding dengan kriptografi menggunakan kunci asimetris. Mekanisme kriptografi kunci simetris menggunakan satu kunci bersama antara pengirim dan penerima yang digunakan baik untuk enkripsi dan dekripsi. algoritma kunci simetris dapat dibagi lagi cipher blok inti untuk transformasi pada data plain-text, dan streaming cipher untuk waktu transformasi yang bervariasi. Kunci kriptografi simetris yang digunakan pada jaringan sensor nirkabel seperti AES, DES, CAST, dan RC5 [1].

2.2 Zigbee

ZigBee Alliance didukung member seperti Siemens, Philips, Texas Instruments, dan Samsung mempromosikan spesifikasi nirkabel yang menawarkan komunikasi *low power* dan transmisi data jarak pendek-medium up to 250 kbps

pada band frekuensi 2,4 GHz. ZigBee dikembangkan oleh IEEE untuk perangkat jarak jauh yang berdaya rendah. Serta menawarkan mekanisme keamanan yang sangat tinggi untuk melindungi kebenaran data melalui enkripsi [2]. ZigBee mencakup atribut umum yaitu: *low performance, short to medium range, low power*, dan *low cost*. ZigBee bedasarkan standar IEEE 802.15.4-2006 dan IEEE 802.15.4-2003, dimana menetapkan menggunakan operasi *Direct Sequence Spread Spectrum* (DSSS) pada beberapa band tidak berlisensi: 868 MHz, 915 MHz, dan 2,4 GHz [7].

ZigBee terdiri dari *physical layer* (PHY), *medium access control* (MAC) *layer, network layer* (NWK), dan application layer [3]. PHY layer seperti fungsi untuk mengaktifkan atau menonaktifkan *radio transmitter, energy detecion* (ED), *link quality instruction* (LQI), *idle channel assessment* (ICA), seleksi kanal, dan pengiriman/penerimaan data. MAC layer bertanggung jawab dalam pembangkit tower jaringan, sinkronisasi antar tower, mengkoneksi/diskoneksi PAN, menyediakan CSMA-CA mekanisme akses, dan membangun komunikasi yang dapat diandalkan dalam menghubungkan antara entitas rekan MAC.

Network layer pada ZigBee mendukung topologi *star, tree,* dan *mesh.* Layer ini memberikan alamat untuk perangkat, yang dapat bergabung dan meninggalkan jaringan. Layer ini bertanggung jawab membangun dan mempertahankan daftar routing, dan melakukan *routing* untuk data frame. *Application* layer dibagi ke dalam *application support sub-layer* (APS), APL *layer framework*, dan ZigBee *device objects* (ZDO). Jaringan ZigBee terdiri dari *coordinator, Full Function Device* (FFD) dan *Reduced Function Device* (RFD) [3].

Mekanisme keamanan ZigBee bukanlah protokol independen tunggal, tetapi satu set unsur-unsur keamanan pada IEEE 802.15.4. Hal ini untuk realisasi lebih mudah pada platform yang dengan daya komputasi yang lemah, maka dari itu AES dipilih. Kebanyakan chip ZigBee saat ini memiliki built-in perangkat sirkuit akselerasi AES untuk mempercepat proses mekanisme ini [3]. IEEE 802.15.4 merekomendasikan menggunakan skema enkripsi 128-bit AES [4].

ZigBee menyediakan dua keamanan yang berbeda: keamanan standar yaitu profil keamanan dasar, keamanan ini jarang diadopsi karena dapt terkena serangan. Dan *high security*, kebanyakan digunakan karena menjamin keamanan yang lebih besar selama komunikasi. *Link keys* adalah salah satu kunci keamanan yang diadopsi oleh ZigBee [18]:

1) *Master Keys* biasanya *hardcoded* pada perangkat atau *shared out-of-band*. Hal ini diperlukan agar bisa mengambil kembali kunci lainnya tapi tidak pernah langsung dikirim ke jaringan.
2) *Netwok Keys* adalah kunci yang dimiliki oleh semua perangkat terhubung ke jaringan yang sama. Kunci ini dihasilkan oleh *Trust Center* dan kunci ini bisa dikirim ke jaringan dalam bentuk teks biasa atau dalam bentuk terenkripsi, tergantung pada yang diadopsi profil keamanan
3) *Link Keys* adalah kunci yang dihasilkan dengan menggunakan *master key* dan diadopsi untuk komunikasi antar dua perangkat yang berbeda dan pada jaringan yang sama.

Dalam jaringan ZigBee, jika komunikasi tidak terenkripsi, penyerang dapat mengakses semua informasi jaringan dan bahkan mungkin *sniff/capture* paket yang bertukar. Layer MAC bertanggung jawab atas pemrosesan keamanannya sendiri, namun layer atas menentukan tingkat keamanan mana yang akan digunakan. Ketika perlindungan integritas layer MAC digunakan, seluruh bingkai MAC terlindungi, termasuk *header* MAC yang berisi sumber perangkat keras dan alamat tujuan. Dengan mengaktifkan integritas frame MAC, alamat MAC layer *source* dapat diautentikasi. Tindakan ini dapat mengatasi serangan *spoofing* dan memungkinkan perangkat untuk memproses secara lebih efektif dan membandingkan frame MAC yang diterima dengan menggunakan Access Control List (ACL).

Kriptografi dalam spesifikasi ZigBee didasarkan pada penggunaan kunci 128-bit dan standar enkripsi AES. Enkripsi, integritas, dan autentikasi dapat diterapkan pada lapisan *Application, Network*, dan MAC untuk mengamankan frame pada masing-masing level tersebut. Dalam hal tipe kunci, ZigBee menentukan penggunaan tombol *Master, Link,* dan *Network* untuk mengamankan frame yang dikirimkan. *Network key* adalah kunci bersama di antara semua node dalam jaringan ZigBee. Standar ini juga menentukan *Alternate Network Key* sebagai bentuk rotasi kunci yang dapat digunakan untuk keperluan pembaruan kunci. Minimal, jaringan ZigBee harus diamankan dengan menggunakan *network key* yang digunakan oleh semua perangkat untuk melindungi semua frame jaringan (*routing messages, network join requests*, dan sebagainya) dan mencegah penggabungan dan penggunaan jaringan ZigBee oleh perangkat tidak sah. *Link keys* adalah kunci sesi rahasia yang digunakan antara dua perangkat ZigBee yang berkomunikasi dan unik untuk perangkat tersebut. Perangkat menggunakan *master key* mereka untuk menghasilkan *link key*. *Master, Link* dan *Network Key* dihasilkan, disimpan, diproses, dan dikirim ke perangkat ZigBee yang menentukan efektivitas dan tingkat keamanan keseluruhan implementasi jaringan ZigBee [9].

2.3 AES

AES (Advanced Encryption Standard) adalah blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) infoermasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES is mengunkan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 bits.

AES memiliki ukuran block yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal.

2.4 Parameter yang Digunakan

Parameter yang digunakan dalam pengujian analisa performansi keamanan WSN ini berupa :

a. Confidentiality of Information, mensyaratkan bahwa data atau informasi hanya bisa diakses oleh pihak berwenang saja. sifat komunikasi nirkabel antara sensor dan perangkat memudahkan serangan, apalagi tidak ada batas fisik yang ketat dari media transmisi. Isi paket yang bisa diungkap ke penyerang yang bisa mendapatkan keuntungan dari informasi tersebut bisa berupa data konfigurasi jaringan untuk serangan lebih lanjut.
b. Integrity of Information, mensyaratkan bahwa informasi hanya bisa diubah oleh pihak berwenang. Selain kerahasiaan informasi yang dipertukarkan, integritasnya bisa terancam oleh penyerang yang menambahkan fragmen tambahan ke paket atau memanipulasi data. Namun manipulasi paket bisa juga disebabkan oleh kesalahan karena lingkungan. Memodifikasi isi paket memungkinkan dapat menyebabkan perangkat tersebut tidak bekerja sebagai mana mestinya.

Seharusnya parameter yang digunakan pada pengujian performansi keamanan ada dua lagi yaitu *Authenticaty of Communication Peers* dan *Avaibility of Information*, tetapi pada jurnal referensi [17] mengatakan bahwa penyerangan dengan parameter avaibility dan authenticaty masih dalam topik penelitian masa depan. Sehingga, pada tugas akhir ini menggunakan dua parameter yang sudah dilakukan yaitu integrity dan confidentiality.

Parameter kualitas jaringan yang digunakan adalah sebagai berikut :

1. Throughput, adalah kecepatan rata-rata data yang diterima dalam selang waktu pengamatan tertentu.

$$Throughput = \frac{ukuran\ frame}{total\ waktu\ pengiriman\ frame} \quad \text{[Pers 2.1]}$$

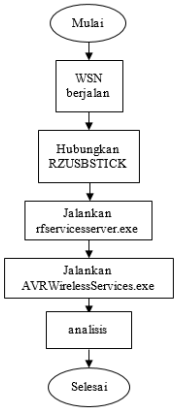
2. Delay, adalah lama waktu yang diperlukan paket saat dikirim oleh pengirim sampai diterima oleh penerima
3. RSSI (*Received Signal Strenghth Indication*), adalah parameter yang yang menunjukkan daya terima dari seluruh sinyal pada band frekuensi channel pilot yang diukur [19].

$$r = 3(RSSI - 91) \quad \text{[Pers 2.2]}$$

4. LQI (*Link Quality Indication*), adalah metrik yang digunakan untuk memperkirakan kualitas tautan dari transmisi RF

3. Skenario *Sniffing*

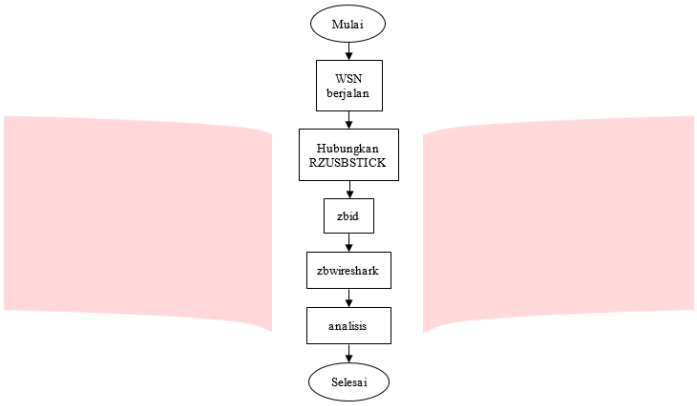
3.1 Menggunakan AVR Wireless Service



Gambar 1 Diagram Alir *Sniffing* Menggunakan AVR Wireless Services

Gambar 1 menunjukkan diagram alir penyerangan dalam jaringan sensor nirkabel. Setelah jaringan ini berjalan dengan baik, maka akan dilakukan penyerangan untuk membuktikan apakah dengan menggunakan security pada Arduino dan xbee bisa membuat jaringan menjadi aman. Pertama, kita harus menguhubungkan Raven USB Stick pada laptop. Setelah itu hubungkan dengan RF server melalui perintah pada command prompt. Selanjutnya buka aplikasi AVR Wireless Server dan klik tool *sniffing* untuk mulai merekam jaringan sensor nirkabel tersebut. Penyerangan ini hanya *listening* dan *capturing* saja. Pada softrware aplikasi ini kita bisa melihat RSSI jaringan sensor nirkabel tersebut.

3.2 Menggunakan KillerBee



Gambar 2 Diagram Alir *Sniffing* Menggunakan KillerBee

Gambar 2 menunjukkan diagram alir penyerangan dalam jaringan sensor nirkabel. Setelah jaringan ini berjalan dengan baik, maka akan dilakukan penyerangan untuk membuktikan apakah dengan menggunakan security pada Arduino dan xbee bisa membuat jaringan menjadi aman. Pertama, kita harus menguhubungkan Raven USB Stick pada PC yang sudah terinstall Kali Linux dan firmware KillerBee. Lalu ketikkan command zbid untuk mengetahui alat tersebut sudah terpasang dengan baik atau belum. Setelah itu, ketikkan command zbwireshark untuk menganalisis jaringan sensor nirkabel. Penyerangan ini hanya *listening* dan *capturing* saja.

3.4 Konfigurasi Kunci Keamanan pada XBee S2 Wire Antenna

XBee S2 befungsi sebagai pengirim dan penerima. Pada jaringan sensor nirkabel ini, XBee S2 digunakan sebagai kordinator dan *endnode* yang akan dikonfigurasi dengan bantuan *software* XCTU. Ketiga Xbee S2 ini menggunakan *operating channel* dari 11-26. Pada sisi XBee S2 sendiri mempunyai tiga skenario untuk pengamanan sendiri. Pertama tanpa keamanan, kedua *pre-configured link keys*, dan yang ketiga adalah *obataining keys during joining*.

- Pre-configures link keys
  Koordinator :
  a. ID = 1235
  b. EE = 1
  c. NK = 0
  d. KY = 4455
  Node sensor :
  a. ID = 1235
  b. EE = 1
  c. KY = 4455

- Obataining keys during joining
  Koordinator :
  a. ID = 1235
  b. EE = 1
  c. EO = 1
  d. NK = 0
  e. KY = 0
  Node sensor :
  a. ID = 1235
  b. EE = 1
  c. KY = 0

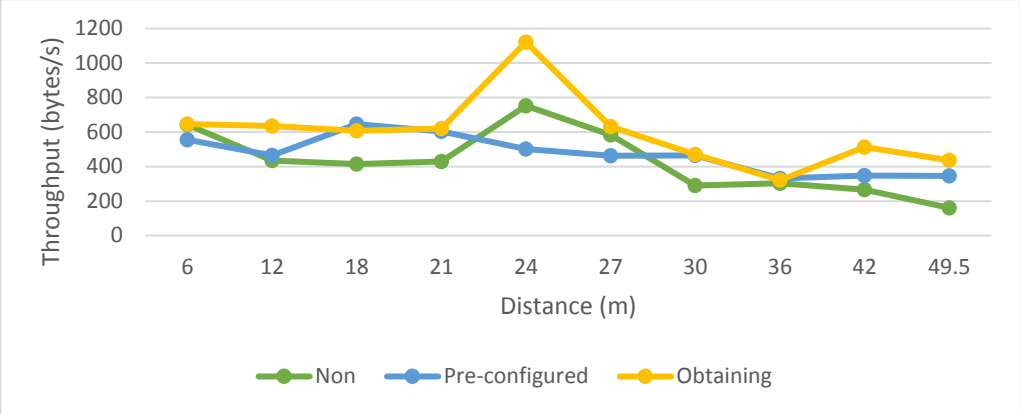
Pre-configure link keys mengatur perintah EE, ID, dan KY yang sama pada semua perangkat. Setelah berhasil bergabung dengan jaringan yang aman, kunci jaringan mengenkripsi semua transmisi data aplikasi. Karena NK ditetapkan ke 0 pada koordinator, perangkat akan memilih kunci jaringan acak. Karena KY dikonfigurasikan ke nilai non-nol pada semua perangkat, kunci pengenal pra-konfigurasi KY mengirim kunci jaringan yang dienkripsi saat perangkat digabungkan [15].

Sedangkan, *obtaining keys during joinin*g mengatur perintah EE, ID, dan KY yang sama pada semua perangkat. Karena NK ditetapkan ke 0 pada koordinator, perangkat akan memilih kunci jaringan acak. Karena KY diset ke 0 pada semua perangkat, kunci jaringan dikirim tidak terenkripsi saat perangkat digabungkan. Dan memberi EO angka 1, itu artinya menjadikan koordiantor sebagai trust center [15].

4. Pembahasan

4.1 Throughput

Throughput adalah kecepatan rata-rata data yang diterima dalam selang waktu pengamatan waktu tertentu. Throughput ini dihitung pada sisi node koordinator yang terhubung dengan node sensor PIR dan node sensor DHT11. Dapat dilihat dari gambar 3 dapat disimpulkan bahwa 25 meter adalah jarak optimal XBee S2 bekerja. Dan mulai menurun pada jarak 30 meter serta menurun drastic pada jarak 40 m. Serta semakin tinggi throughputnya, maka semakin banyak daya pada WSN yang digunakan.

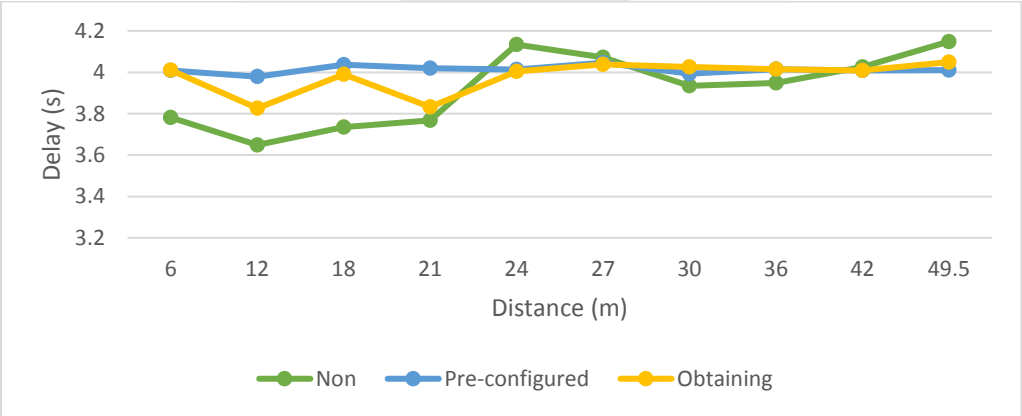


Gambar 3 Grafik Throughput

Nilai throuhput tertinggi terdapat pada jarak 24 meter dengan kondisi tanpa keamanan dan obtaining keys during joining. Pada kondisi tanpa keamanan nilai throughput mencapai 752,4 bytes/s dan pada kondisi obtaining keys during joining mencapai 1122 bytes/s. Sedangkan pada kondisi pre-configured link keys pada jarak 24 meter tidak mencapai nilai throughput maksimum. Pada kondisi ini nilai throughput maksmimum terjadi pada jarak 18 meter dengan nilai throughput 645,9 bytes/s. Ini bisa terjadi karena daya baterai pada sensor node sudah mulai berkurang, dan sensor mengalami kondisi kadang data terikirim ke node kordinator kadang tidak terkirim. Sehingga besarnya nilai throughput berpengaruh pada konsumsi daya jaringan sensor nirkabel tersebut.

4.2 Delay

Delay adalah waktu yang diperlukan oleh paket data saat dikirim oleh pengirim dan diterima oleh penerima. Pada pengujian delay ini dilakukan diruang terbuka. Pengujian kali ini dibantu dengan software Advances Serial Port Monitor. Pada gambar 4 dapat dilihat bahwa tidak ada selisih besar antara kondisi satu dengan kondisi lainnya. Semakin jauh node sensor maka semakin lama node koordinator menerima paket data dari kedua sensor node. Tidak ada selisih besar antara kondisi satu dengan lainnya dapat disimpulkan bahwa menggunakan atau tidak menggunakan keamanan enkripsi dekripsi AES128 tidak berpengaruh dalam kedatangan informasi yang dikirimkan.

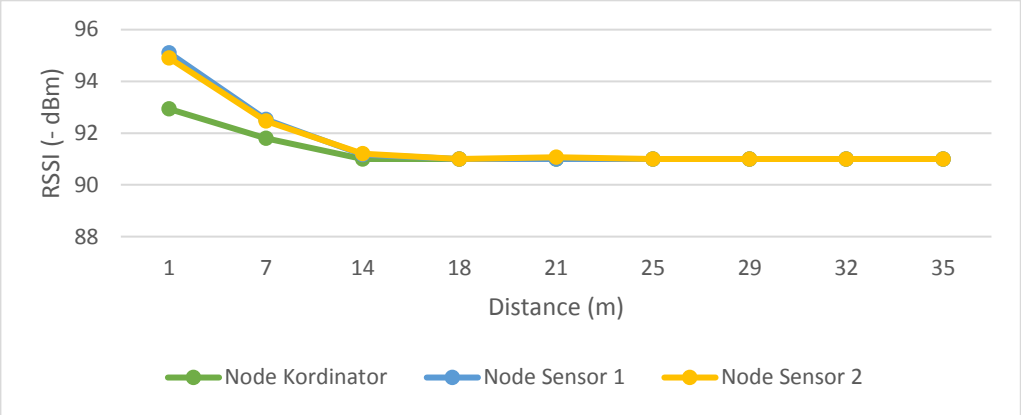


Gambar 4 Grafik Delay

Pada grafik diatas dapat dilihat nilai delay paling tinggi adalah 49,5 meter, karena merupakan jarak terjauh. Pada kondisi tanpa keamanan nilai delay pada jarak 49 mencapai delay 4,1483 s, pada kondisi pre-configured link keys nilai delay pada jarak 49 mencapai delay 4,0096 s, dan pada kondisi obtaining keys during joining nilai delay pada jarak 49 mencapai delay 4,0491 s. Tingginya nilai delay pada jaringan sensor nirkabel ini selain jarak antar node dan obstacle yang ada, ini juga dimungkinkan karena adanya tambahan kodingan enkripsi pada sensor node

4.3 RSSI

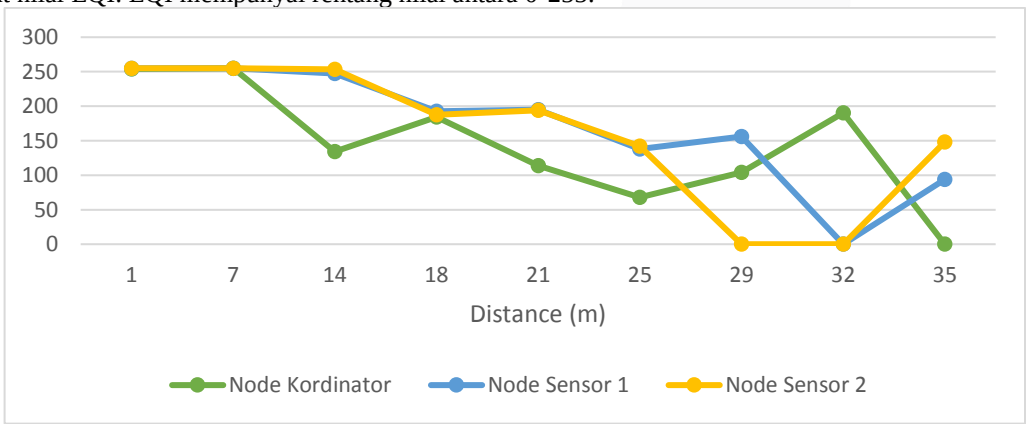
RSSI (*Received Signal Strength Indicator*) merupakan parameter yang menunjukan daya terima dari seluruh sinyal pada *band frequency channel pilot* yang diukur. Pada skenario pengujian ini, didapat RSSI masing-masing node. Pada gambar 5 dibawah ini menunjukkan RSSI pada ketiga node. RSSI paling besar terletak pada satu meter pertama. Node kordinator dengan RSSI -94,9 dBm, node sensor 1 dengan RSSI -95,1 dBm, dan node sensor 2 dengan RSSI 92,933 dBm. Serta, pada gambar 4.16 menunjukkan grafik RSSI, dapat dilihat semakin jauh sniffer maka semakin rendah RSSI. Pada tabel 4.4 dan gambar 4.12 adalah nilai RSSI yang sudah dirubah ke dBm.



Gambar 5 Grafik RSSI

4.4 LQI

Link Quality Indication (LQI) adalah metrik yang digunakan untuk memperkirakan kualitas tautan dari transmisi RF. Seperti yang didefinisikan di IEEE802.15.4, LQI dihitung oleh lapisan fisik dan memberikan sinyal kekuatan dan kualitas link ke jaringan dan diatas layer setelah setiap frame data diterima. LQI salah satu alternatif yang digunakan untuk mengetahui nilai RSSI. Jika nilai RSSI pada software AVR Wireless Services sudah mencapai nilai 0 maka kita bisa melihat nilai LQI. LQI mempunyai rentang nilai antara 0-255.



Gambar 6 Grafik RSSI

Pada gambar 6 dapat dilihat mulai pada jarak 29 meter LQI sudah tidak menampilkan nilai yang artinya tidak ada komunikasi pada jaringan sensor tersebut. Dan pada jarak 35 meter node sensor masih terlihat nilai RSSI dan LQI

4.5 Performansi Keamanan

Pada analisa performansi keamanan dapat disimpulkan bahwa menggunakan keamanan lebih aman karena sniffer tidak bisa melihat data yang dikirim pada jaringan sensor nirkabel. Sedangkan, tanpa keamanan sniffer bisa

melihat data yang dikirimkan seperti ?PIR#0! dan ?DHT#58$20!. Sehingga dapat disimpulkan pada kondisi tanpa keamanan parameter confidentiality tidak bisa dipenuhi dan pada kondisi dengan keamanan menggunakan pre-configured ataupun obtaining parameter confidentiality dapat dipenuhi. Dan, parameter integrity dapat dipenuhi oleh semua kondisi baik yang menggunakan keamanan maupun tidak menggunakan keamanan data tetap utuh tidak bisa dirubah karena pengujian hanya menggunakan serangan pasif saja.

Nilai RSSI dan LQI juga dapat mempengaruhi keamanan jaringan sensor nirkabel. Contohnya, jika nilai RSSI dan LQI semakin besar menandakan bahwa ada perangkat ZigBee disekitarnya. Jika sniffer digunakan untuk hal yang merugikan orang lain, maka perangkat ZigBee tersebut akan diambil dan digunakan untuk keperluan jahatnya.

.

5. Kesimpulan

Setelah melakukan proses perancangan, pengujian, dan analisa dapat disimpulkan bahwa :

1. Jaringan sensor nirkabel menggunakan kunci enkripsi dekripsi AES128 berjalan dengan baik
2. Raven USB Stick dapat berfungsi baik sebagai passive attack yang hasilnya dapat dilihat menggunakan software Wireshark dan Wireless Sensor Services
3. Pada kondisi tanpa keamanan parameter confidentiality tidak bisa dipenuhi dan pada kondisi dengan keamanan menggunakan pre-configured ataupun obtaining parameter confidentiality dapat dipenuhi.
4. Parameter integrity dapat dipenuhi oleh semua kondisi baik yang menggunakan keamanan maupun tidak menggunakan keamanan data tetap utuh tidak bisa dirubah karena pengujian hanya menggunakan serangan pasif saja.
5. Waktu enkripsi dan dekripsi AES128 juga berpengaruh pada nilai delay, jika semakin lama waktu enkripsi dan dekripsi maka semakin lama informasi sampai kepada penerima.
6. Semakin tinggi delay, maka semakin rendah nilai throughput.
7. Throughput tertinggi terdapat pada jarak 24 meter dengan nilai 1122 bytes/s
8. Delay tertinggi pada jarak 49,5 meter dengan nilai 4,1483 s
9. Pada analisa performansi jaringan, pada parameter RSSI dan LQI jika jarak semakin jauh maka nilai RSSI dan LQI semakin kecil juga
10. Nilai RSSI dan LQI berbanding terbalik dengan nilai delay. Jika semakin jauh jarak maka semakin turun nilai RSSI dan LQI, sedangkan akan makin naik nilai delay jaringan sensor nirkabel.

Daftar Pustaka :

[1] Panda, Madhumita. (2015). *Data Security in Wireless Sensor Network via AES Algorithm.* ISCO. India

[2] Maphats'oe, Ts'itso dan Muthoni Masinde. (2016). *A security Algorithm for Wireless Sensor Networks in the Internet of Things Paradigm.*IST-Africa.South Africa

[3] Yang, Bin. (2009). *Study on Security of Wireless Sensor Network Based on ZigBee Standard.* International Conference Computational Intelligence and Security. China

[4] Dini, Gianluca dan Marco Tiloca. (2010). *Considerations on Security in ZigBee Networks.*International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. Italia

[5] Granjal, Jorje., Edmundo Monteiro, dan Jorge Sa Silva. (2015). *Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues.* IEEE Communications Surveys and Tutorials

[6] Candra, Shalahuddin Kartika. "Desain dan Implementasi WSN pada Tempat Sampah dalama Gedung Berbasis Mikrokontroler Menggunakan RF Modul Zigbee dengan Topologi Cluster Tree". Universitas Telkom. Bandung. 2015

[7] Geier, Jim. *"Designing and Deploying 802.11n Wireless Networks".* Cisco Press. Indianapolis USA. 2010

[8] Masica, Ken. (2007). *Recommended Prectices Guide for Securing ZigBee Wireless Networks in Process Control System Envireonments*. DHS US CERT Control Systems Security Program (CSSP). Amerika Serikat

[9] Blonter, Melissa., dan Chow Ming. (2015). *Smart Home Technology : The ZigBee Protocol*. Computer Systems Security. Tufts University. Amerika Serikat

[10] Daemen, Joan., dan Vincent Rijmen. *"The Design of Rijndael AES – The Advanced Encryption Standard"*. Springer. Belgium. 2001

[11] Johnstone, Michael N., dan Jeremy A. Jarvis. (2011). *Penetration of ZigBee-based Wireless Sensor Networks*. Australian Information Warfare and Security Conference. Edith Cowan University. Australia

[12] Stelte, Bjorn., dan Gabi Dreo Rodosek. (2013). *Thwaeting Attacks on ZigBee – Removal of the KillerBee Stinger.* IFIP. Germany

[13] Soleimay, Kiana. (2011). *Security in IEEE 802.15.4/zigbee.* University of Mazandaran. Iran

[14] Olawumi, Olayemi., Keijo Haataja, Mikko Asikainen, Niko Vidgren, dan Pekka Toivanen. (2014). *Three Practical Attacks Against ZigBee Security: Attacks Scenario Definitions, Practical Experiments, Countermeasures, and Lesson Learned*. IEEE. Finlandia

[15] Digi International Inc. (2017). *"XBee/Xbee-PRO® S2C Zigbee® RF Module"*. [Online]. Tersedia: https: //www.digi.com/resources/ documentation/DigiDocs/ 90002002/default.htm#Containers yang direkam pada 13 September 2017

[16] Riverloopsec. (2017). *"IEEE 802.15.4/ZigBee Security Research Toolkit".* [Online]. Tersedia: http://www.riverloopsecurity.com yang direkam pada 20 Juni 2017

[17] J.Market, M.Massoth, K-P.Fischer-Hellmann, S.M.Furnell, dan C.Bolan. (2011). *Attack Vectors to Wireless ZigBee Network Communications – Analysis and Countermeasures*. Proceedings of SEIN. Jerman

[18] Vaccari, Ivan., Enrico Cambiaso, and Maurizio Aiello. (2017). *Remotly Exploiting AT Command Attacks on ZigBee Networks.* Hindawi. Mesir

[19] Seitz, Andrew., dan Benjamin Ramsey. (2016). *Z-Ranger : An Improved Tool Set for ZigBee Warwalking*. 11th International Conference on Cyber Warfare & Security Boston University. USA