

Tugas Kuliah

EC-7010 Keamanan Sistem Lanjut

Sistem Keamanan pada Jaringan
Zigbee

Wawan
23203141



Jurusan Teknologi Informasi
Departemen Teknik Elektro
Institut Teknologi Bandung

Daftar Isi

	Halaman
Daftar Isi	i
Daftar Gambar dan Tabel	ii
Abstrak	iii
I. Pendahuluan	1
I.1. Latar Belakang	1
I.2. Tujuan	1
I.3. Lingkup Masalah	2
II. Zigbee.....	2
II.1 Arsitektir Zigbee	2
II.2 Lapisan Fisik (PHY)	3
II.3 Lapisan <i>Media Access Control</i>	4
II.4. Lapisan Jaringan (<i>NWK Layer</i>)	5
II.5. Lapisan Aplikasi	6
III. <i>Advanced Encryption Standard</i> (AES)	6
III.1 Penggunaan AES pada Zigbee	6
III.2. Algoritma AES	7
IV. Sistem Keamanan pada Zigbee	9
IV.1. Dasar Layanan Keamanan pada Zigbee	10
IV.1.1. Kontrol Akses (<i>access control</i>) dan Integritas Pesan (<i>message integrity</i>).....	10
IV.1.2. Kerahasiaan (<i>confidentiality</i>).....	11
IV.1.3. Perlindungan Pengulangan Pesan (<i>replay protection</i>).....	12
IV.2 Protokol Zigbee	12
IV.2.1. Standar IEEE 802.15.4	12
IV.2.2. Keamanan pada <i>Media Access Control</i>	13
IV.2.2.1 Kategori Rangkaian Keamanan	17
A. Null	17
B. AES-CTR	18
C. AES-CBC-MAC	19
D. AES-CCM	19
IV.3. Model Penguncian (<i>Keying Model</i>)	20
IV.3.1. Penguncian Jaringan berbagi (<i>Network shared keying</i>).....	20
IV.3.2. <i>Pairwise keying</i>	21
IV.3.3. <i>Grup Keying</i>	21
IV.3.4. Pendekatan Gabungan (<i>Hybrid approaches</i>)	21
IV.4 Implementasi	22
V. Penutup	22
Daftar Pustaka	23

Daftar Gambar dan Tabel

Halaman

Daftar Gambar

Gambar 1. Arsitektur Zigbee	3
Gambar 2. Topologi Jaringan pada Zigbee dengan RFD dan FFD	6
Gambar 3. Proses Enkripsi	7
Gambar 4. Format Paket Data dan Acknowledgment	15
Gambar 5. Format Field Data	15
Gambar 6. Format dari masukan ACL	16
Gambar 7. Format masukan (xi) untuk chiper blok pada rangkaian AES-CTR dan AES-CCM	19

Daftar Tabel

Tabel 1. Lebar Frekwensi dan Kecepatan Data pada Zigbee	4
Tabel 2. Pseudo Code Proses Enkripsi	8
Tabel 3. Pseudo Code Proses Dekripsi	9
Tabel 4. Rangkaian Keamanan yang didukung oleh Standar IEEE 802.15.4	14

Abstrak

Pemakaian frekwensi pada kisaran tanpa lisensi belum populer khususnya di Indonesia, berbeda dengan negara-negara seperti Amerika Serikat, Eropa dan Jepang yang sangat gencar mengembangkan frekwensi tanpa lisensi ini untuk pengembangan perangkat-perangkat industri, komersial dan rumah tangga.

Untuk mengetahui zigbee secara umum, dalam tulisan ini diuraikan tentang arsitektur zigbee standar yang telah ditetapkan oleh IEEE. 805.15.4 dan *Zigbee alliance* (aliansi perusahaan pengembang zigbee) yang meliputi lapisan fisik, lapisan jaringan dan lapisan aplikasi.

Sedangkan untuk keamanan jaringan pada zigbee yang akan dibahas pada lapisan lapisan fisiknya (MAC+PHY) saja.

Pembahasan yang rinci tentang keamanan zigbee meliputi keamanan pada lapisan *Media Access Control* dengan menggunakan algoritma inti kriptografi dari AES yang di dalamnya menyediakan pilihan rangkaian keamanan antara lain : Null, AES-CTR, AES-CBC-MAC-128, AES-CBC-MAC-64, AES-CBC-MAC-32, AES-CCM-128, AES-CCM-64 dan AES-CCM-32 serta menyediakan layanan kamanan antara lain kontrol akses (*access control*), integritas pesan (*message integrity*), kerahasiaan pesan (*message confidentiality*), dan perlindungan pengulangan pesan (*replay protection*).

Kata kunci: *Zigbee Alliance*, AES, CBC, CCM dan CTR

I. Pendahuluan

I.1. Latar Belakang

Zigbee mengalami perkembangan yang cukup pesat ini terbukti dari banyaknya artikel bisnis mingguan tentang zigbee, dan sebanyak 200 orang telah ikut mendaftarkan diri pada *Open House Marketing Presentation* di Seattle dan sekitar 430 orang telah ikut mendaftarkan diri pada *Open House Marketing Presentation* di Webinar dari 425 orang yang di harapkan hadir [11].

Pemakaian frekwensi pada kisaran tanpa lisensi belum populer khususnya di Indonesia, berbeda dengan negara-negara seperti Amerika Serikat, Eropa dan Jepang yang sangat gencar mengembangkan frekwensi tanpa lisensi ini untuk pengembangan perangkat-perangkat industri, komersial dan rumah tangga. Dengan demikian merupakan hal yang penting untuk mengetahui tentang teknologi dan sistem keamanan jaringan pada zigbee.

Alat-alat elektronik rumah tangga, mainan anak, perancangan penyaklaran lampu rumah tangga, sistem keamanan pada rumah dan perangkat-perangkat untuk personal komputer seperti *keyboard*, *mouse* merupakan contoh penggunaan teknologi zigbee.

Untuk mengetahui zigbee secara umum, dalam tulisan ini diuraikan tentang standar arsitektur zigbee yang telah ditetapkan oleh standar IEEE 805.15.4 dan *Zigbee alliance* yang meliputi lapisan fisik, lapisan jaringan dan lapisan aplikasi.

Sedangkan untuk kemaanan jaringan pada zigbee yang akan dibahas pada tulisan ini hanya keamanan pada lapisan fisiknya saja. Dimana untuk keamanan lapisan fisik ini menggunakan algoritma inti kriptografi AES 128 bit.

I.2. Tujuan

Berdasarkan latar belakang di atas tulisan tugas akhir EC7010 ini bertujuan untuk mempelajari keamanan jaringan pada zigbee dengan penggunaan AES 128 bit dan sistem keamanan pada lapisan *Media Access*

Control. Adapun tujuan yang lebih rinci dari penulisan tugas ini adalah sebagai berikut.

- a) Mengetahui sejauh mana arsitektur zigbee yang dikembangkan oleh standar IEEE 805.15.4 dan *zigbee alliance*.
- b) Memberikan pertimbangan-pertimbangan keamanan untuk zigbee yang meliputi : penerapan protokol zigbee, *Advance Encryption Standar (AES)*, keamanan pada lapisan *media acces control*, model penguncian (*keying model*), dan implementasi keamanan fisik zigbee.

I.3. Lingkup Masalah

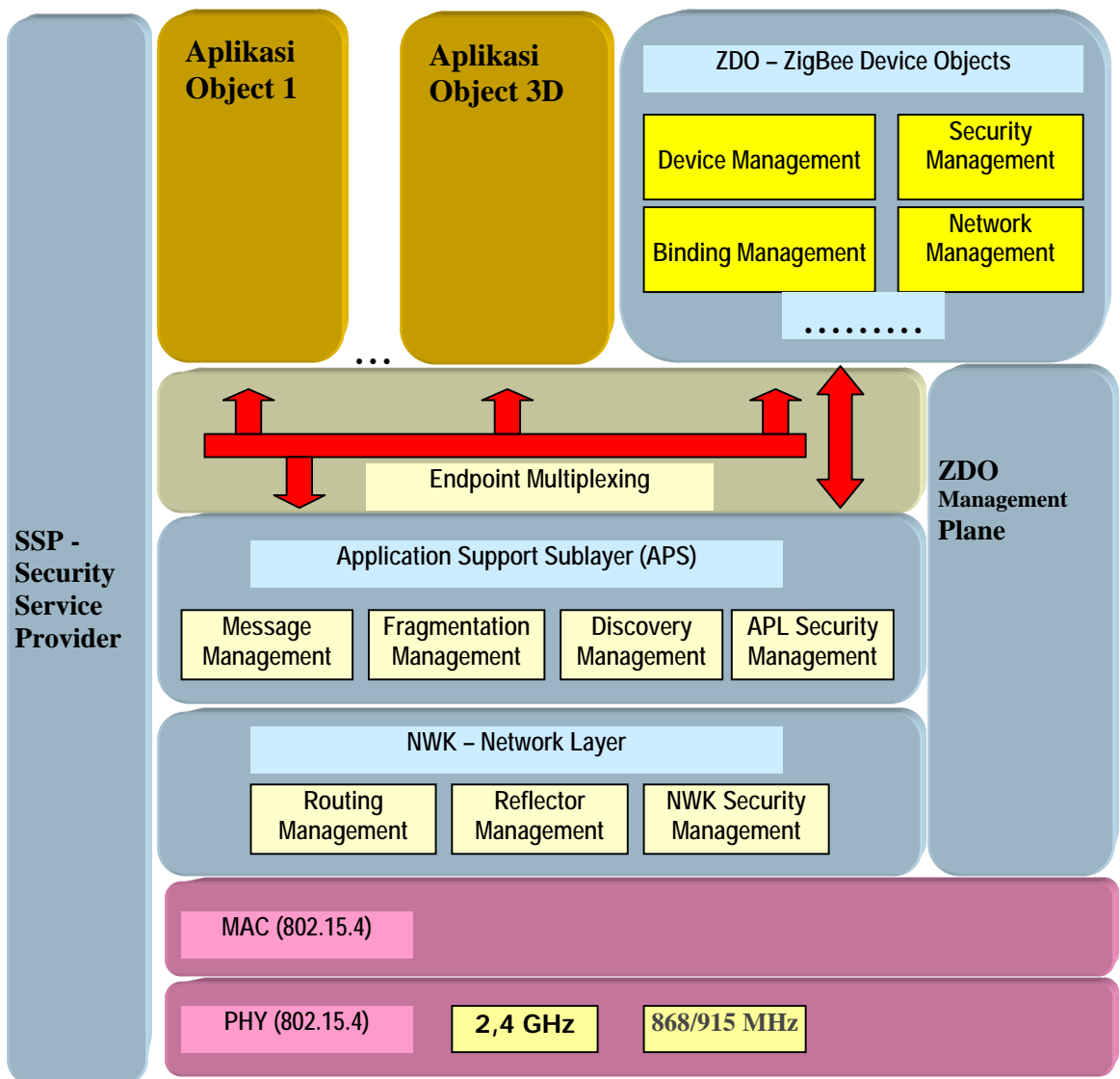
Masalah keamanan pada sistem zigbee dapat dipandang relatif luas dan rumit. Dalam tulisan tugas EL7010 ini yang dilakukan hanya studi pengamanan yang lebih menekankan pada protokol zigbee untuk standar IEEE 805.15.4 dan *zigbee alliance* serta teknik penerapan AES pada protokol lapisan *media acces control* untuk zigbee.

II. Zigbee

Standar lapisan jaringan pada zigbee telah di definisikan oleh *zigbee Alliance* yang meliputi : lapisan jaringan, lapisan aplikasi dan lapisan keamanan yang di dasarkan pada standar IEEE 802.15.4 untuk Lapisan fisik (MAC+PHY). Zigbee mempunyai beberapa kelebihan antara lain fleksibel dalam pengiriman data, biaya yang relatif murah serta rentang jaringan yang kurang dari 100 meter, yang memudahkan dalam instalasi jaringan.

II.1 Arsitektir Zigbee

Untuk memahami arsitektur zigbee ini tentunya harus mengacu pada standar IEEE 802.15.4, dimana arsitektur zigbee dibagi dalam beberapa lapisan , seperti terlihat pada Gambar 1. di bawah ini:



Gambar 1. Arsitektur Zigbee[2]

II.2 Lapisan Fisik (PHY)

Standar IEEE 802.15.4 mendefinisikan dua representasi dari lapisan fisik (PHYs) yang memiliki 3 lebar frekuensi tanpa lisensi yaitu 2,4 GHz dengan 16 channel, 902-928 MHz dengan 10 channel dan 868-870 MHz dengan 1 channel dengan kecepatan data masing-masing 250 kbps, 40 kbps dan 20 kbps. Seperti dapat dilihat pada Tabel 1.

PHY	Frequency Band	Channel Numbering	Spreading Parameters		Data Parameters		
			Chip Rate	Modulation	Bit Rate	Symbol Rate	Modulation
868/915 MHz	868-870 MHz	0	300 kchip/s	BPSK	20 kb/s	20 kbaud	BPSK
	902-928 MHz	1 to 10	600 kchip/s	BPSK	40 kb/s	40 kbaud	BPSK
2.4 GHz	2.4-2.4835 GHz	11 to 26	2.0 Mchips	O-QPSK	250 kb/s	62,5 kbaud	16-ary Orthogonal

Tabel 1. Lebar Frekwensi dan Kecepatan Data pada Zigbee

Kedua lapisan frekwensi pada lapisan fisik ini menggunakan teknik modulasi *Direct Sequence Spread Spectrum* (DSSS), Tipe modulasi dalam frekwensi 2,4 GHz menggunakan *Quadratutre Phase Shift Keying* (QPSK).

II.3 Lapisan *Media Access Control*

Lapisan *Media Access Control* ini didefinisikan oleh standar IEEE 802.15.4 antara lain, mempunyai tugas untuk pengaksesan saluran. Ada dua mekanisme untuk mengakses saluran yaitu mode beacon (*beacon mode*) dan mode non beacon (*non beacon mode*). Mode beacon menggunakan teknik *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA), sedangkan mode non beacon menggunakan teknik non CSMA/CA.

Tugas lain dari lapisan *Media Access Control* adalah untuk mendukung Jaringan dimana memiliki alamat 64 bit dan setiap node memiliki alamat yang unik, jumlah node bisa mencapai 254 untuk sebuah koordinator (untuk teknik Master-Slave), sedangkan jumlah node bisa mencapai 65534 jika menggunakan topologi jaringan peer-to-peer (*mesh*).

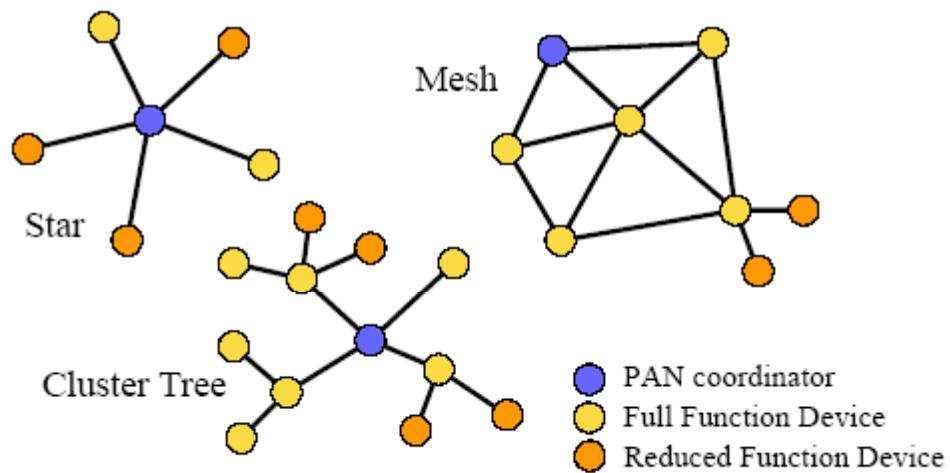
Lapisan *Media Access Control* menggunakan *frame acknowledgement*, dengan verifikasi data menggunakan CRC 16 bit dan untuk keamanan data menggunakan pilihan enkripsi dan autentifikasi 128 bit AES.

II.4. Lapisan Jaringan (*NWK Layer*)

Secara umum layanan manajemen jaringan dalam zigbee meliputi : konfigurasi perangkat, penetapan jaringan yang baru, keanggotaan jaringan, pengamalatan jaringan, pememilihan jenis keamanan jaringan, sinkronisasi, jaminan slot waktu, portabilitas, koordinator backup, resolusi konflik pengidentifikasi pada *Personal Area Network* (PAN), pemilihan saluran secara dinamis dan menghubungkan serta menggabungkan jaringan.

Lapisan jaringan zigbee mendukung tiga topologi jaringan yaitu *star*, *mesh* dan *cluster tree*. Topolgi *star* adalah topologi jaringan yang umum yang menyediakan operasi bertenaga baterai dengan kekuatan lama. Topolologi *mesh*, atau *peer-to-peer* memungkinkan keandalan dan skalabilitas yang sangat baik dengan menyediakan lebih dari satu jalur dalam jaringan untuk beberapa hubungan *wireless* (nir kabel). Topologi *Cluster-Tree* menggunakan gabungan topologi *star* dan topologi *mesh*, dengan menggabungkan keduanya mempunyai keuntungan keandalan tingkat tinggi dan dukungan node dengan bertenaga baterai.

Perangkat fisik zigbee membedakan perangkat kerasnya yang didasarkan pada definisi standar IEEE 802.15.4 yaitu *Reduced Function Device* (RFD) dan *Full Function Device* (FFD). RFD diterapkan dengan menggunakan *Random Access Memory* (RAM) dan *Read Only Memory* (ROM) dengan ukuran minimum dan dirancang untuk menjadi node pengirim dan atau penerima yang sederhana dalam sebuah jaringan yang berukuran sangat besar. Dengan ukuran *stack* yang kecil maka memori yang dibutuhkan sedikit dan harga untuk *Integreted Circuit* (IC)-nya pun yang diperlukan menjadi lebih murah. Perangkat RFD umumnya bertenaga baterai, RFD dapat mencari jaringan yang tersedia, memindahkan data, menentukan apakah data harus dipending, meminta data dari koordinator jaringan, dan akan *sleep* untuk periode waktu yang lama jika tidak ada yang menggunakan hal ini dilakukan untuk mengurangi konsumsi penggunaan baterai.



Gambar 2. Topologi Jaringan pada Zigbee dengan RFD dan FFD

II.5. Lapisan Aplikasi

Lapisan aplikasi pada arsitektur zigbee terdiri dari sub-layer aplikasi (APS), *Zigbee Device Object* (ZDO) dan definisi pembuat objek aplikasi. Tanggung jawab dari sub-layer APS meliputi memelihara tabel untuk menghubungkan, dimana memiliki kemampuan untuk mencocokkan dua perangkat secara bersama-sama yang didasarkan pada layanan dan kebutuhan pengguna, dan menyampaikan pesan antara perangkat yang terkait. Tanggung jawab yang lain dari sub-layer APS adalah melakukan pemulihan (*discovery*), serta menentukan tanggung-jawab dari ZDO yang meliputi penjelasan tentang aturan dari alat dalam jaringan, menginisialisasi dan atau merespon dan membuat suatu hubungan keamanan diantara perangkat jaringan.

III. *Advanced Encryption Standard* (AES)

III.1 Penggunaan AES pada Zigbee

Saat ini, AES digunakan sebagai standar algoritma kriptografi yang terbaru. AES menggantikan *Data Encryption Standar* (DES) yang pada tahun 2002 sudah berakhir masa penggunaannya. DES juga dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat

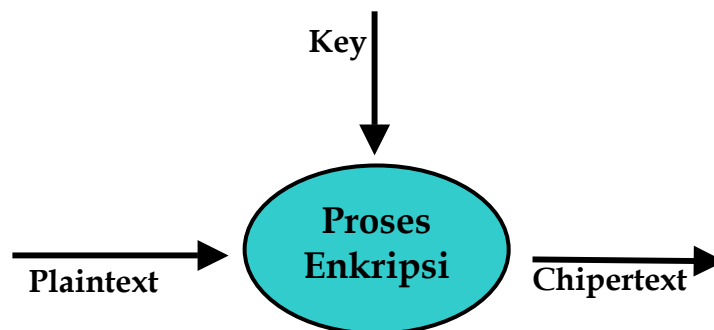
cepat. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit.

Algoritma inti kriptografi pada zigbee menggunakan AES yang didasarkan pada tiga mode operasi.

1. *Counter Mode* (CTR) digunakan untuk enkripsi
2. *Cipher Block Chaining Mode* (CBC) digunakan untuk Integritas
3. *CCM Mode* merupakan kombinasi dari CTR dan CBC

III. 2. Algoritma AES

Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *ciphertext* seperti pada Gambar 3. . *Cipher key* dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit



Gambar 3. Proses Enkripsi

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, input yang telah disalin ke dalam state akan mengalami transformasi byte *AddRoundKey*. Setelah itu, state akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak *Nr*. Proses ini dalam algoritma AES disebut sebagai *round function*. Round yang

terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi *MixColumns*. Tabel 2. berikut adalah *pseudo code* untuk masing fungsi tranformasi dalam proses *Chiper*.

```

Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
end

```

Tabel 2. *Pseudo Code* Proses Enkripsi

Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*. Tabel 3 berikut adalah *pseudo code* untuk masing fungsi tranformasi dalam proses *InvChiper*.

```

InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
for round = Nr-1 step -1 down to 1
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
InvMixColumns(state)
end for
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[0, Nb-1])
out = state
end

```

Tabel 3. *Pseudo Code* Proses Dekripsi

IV. Sistem Keamanan pada Zigbee

Pertumbuhan penting perangkat nir kabel yang berukuran kecil dan harga yang relatif murah membutuhkan suatu platform umum sedemikian sehingga alat dapat berkomunikasi satu sama lain dan saling berbagi sumber dengan biaya yang murah. Spesifikasi standar IEEE 802.15.4 menguraikan protokol nir kabel dan akses media untuk perangkat-perangkat PAN. Dalam lingkungan jaringan sensor telah memulai menggunakan protokol ini. Protokol ini dimaksudkan untuk diimplementasikan dalam perangkat keras berupa *chip* radio yang bersifat *dedicated*. Cakupan dari aplikasi zigbee ini cukup luas, meliputi : pengontrol game nir kabel, hal-hal yang berhubungan dengan lingkungan, medis, dan perangkat-perangkat pengontrol bangunan, untuk pemanas dan sensor ruang udara. Aplikasi ini seringkali menggunakan perangkat yang ditempelkan dan dikendalikan dengan mikrokontroler berukuran 8 atau 16 bit dengan maksud agar perangkat beroperasi tanpa campur tangan manusia untuk periode waktu yang lama.

Periode waktu yang lama pada operasi tanpa kendali dalam perangkat keras ini mempunyai dua implikasi ketika perancangan sistem yaitu perangkat

lunak yang berjalan pada perangkat ini harus memiliki metode yang benar dan sederhana, perangkat harus dibuat penggunaannya efisien dengan penggunaan energi yang terbatas.

Spesifikasi standar IEEE 802.15.4 dimaksudkan untuk mendukung berbagai aplikasi, dimana sebagian besar adalah sistem keamanan yang bersifat sensitif. Sebagai contoh, pertimbangan kasus dari suatu jaringan sensor yang digunakan untuk pengawasan kepemilikan dari sebuah bangunan dengan sistem alarm, ada suatu privasi yang terkait dengan jejak orang-orang dalam bangunan tersebut. Apalagi, jika jaringan tidak aman, musuh dapat memodifikasi dan menambahkan pesan lain ke dalam alarm, atau lebih parah lagi, mematikan sinyal alarm. Banyak aplikasi memerlukan kerahasiaan dan mempunyai suatu kebutuhan untuk perlindungan terpadu. Sehingga, spesifikasi standar 802.15.4 pengalamatannya melalui suatu paket keamanan link-layer .

IV.1. Dasar Layanan Keamanan pada Zigbee

Protokol keamanan lapisan *Link* menyediakan empat layanan keamanan dasar yaitu kontrol akses (*access control*), integritas pesan (*message integrity*), kerahasiaan pesan (*message confidentiality*), dan perlindungan pengulangan pesan (*replay protection*).

IV.1.1. Kontrol Akses (*access control*) dan Integritas Pesan (*message integrity*)

Maksud *access control* pada protokol lapisan *link* harus dapat mencegah pihak-pihak yang tidak berhak untuk ambil bagian dalam jaringan. Node yang mempunyai hak harus dapat mendeteksi pesan yang berasal dari node lain yang tidak mempunyai hak serta menolak untuk mengakses jaringan. Selain itu, jaringan yang aman harus menyediakan perlindungan terhadap integritas pesan, jika ada musuh yang memodifikasi suatu pesan, dimana pesan itu berasal dari pengirim yang diberi hak, sedangkan pesan dalam proses pemindahan, maka penerima harus dapat mendeteksi kerusakan pesan ini, termasuk kode pengesahan pesan *Message authentication code* (MAC)[1] dengan masing-masing paket menyediakan pengesahan dan integritas pesan.

MAC dapat dipandang sebagai sebagai suatu *checksum* kriptografi yang aman dari sebuah pesan. Perhitungannya memerlukan penerima dan pengirim pesan yang diberi hak untuk berbagi kunci kriptografi rahasia, dan kunci ini menjadi bagian dari masukan untuk perhitungan. Pengirim menghitung MAC yang ada pada paket dengan kunci rahasia dan termasuk MAC dengan paketnya. Penerima berbagi kunci rahasia yang sama untuk menghitung ulang MAC dan membandingkannya dengan MAC yang ada di dalam paket. Penerima menerima paket jika MAC-nya sama, dan menolaknya jika berbeda. MAC harus dibuat lebih susah untuk dipalsukan tanpa kunci rahasia. Sebagai konsekwensinya, jika musuh mengubah suatu pesan yang sah atau menyuntikan suatu pesan yang palsu, dia tidak akan mampu menghitung kersesuaian MAC, dan penerima akan menolak pesan yang dipalsukan itu

IV.1.2. Kerahasiaan (*confidentiality*)

Kerahasiaan dimaksudkan menjaga informasi dari pihak yang tidak berhak. Ini secara khusus dicapai dengan enkripsi. Skema enkripsi yang lebih disukai seharusnya tidak hanya mencegah pemulihan pesan, tetapi juga mencegah musuh untuk mempelajari sebagian informasi pesan yang telah dienkripsi. Sifat enkripsi yang kuat seperti itu dikenal dengan keamanan semantik.

Satu implikasi dari keamanan semantik adalah penyandian dua kali *plaintext* yang sama, memberi dua *ciphertexts* yang berbeda. Jika proses enkripsinya serupa untuk dua pekerjaan pada pesan yang sama, maka keamanan semantik telah dilanggar dimana menghasilkan *ciphertext* yang serupa. Teknik yang umum untuk memperoleh keberhasilan keamanan semantik adalah dengan menggunakan algoritma enkripsi untuk masing-masing pekerjaan dengan menggunakan waktu yang unik (*nonce*). *Nonce* tersebut dapat dijadikan ide sebagai masukan untuk algoritma enkripsi. Tujuan utama dari *nonce* tadi adalah untuk menambahkan variasi bagi proses enkripsi ketika hanya ada sedikit variasi dalam kumpulan pesan. Karena penerima harus menggunakan *nonce* tersebut untuk mendekripsi pesan, keamanan pada kebanyakan skema enkripsi

tidak bersandar pada *nonce* yang menjadi rahasia. *Nonce* secara khusus dikirim dan dimasukkan ke dalam paket yang sama dengan data yang telah di enkripsi.

IV.1.3. Perlindungan Pengulangan Pesan (*replay protection*).

Musuh yang menguping pesan yang sah yang telah dikirim di antara dua node yang diberi hak dan mengulangnya pada beberapa waktu kemudian yang mengakibatkan pengulangan serangan. Karena pesan asli berasal dari pengirim yang diberi hak, ini akan mempunyai MAC yang sah, sehingga penerima akan menerimanya lagi. Perlindungan pengulangan pesan mencegah jenis serangan ini. Pengirim secara khusus menentukan kenaikan nomor urutan secara terus-menerus ke masing-masing paket dan penerima menolak paket dengan nomor urutan yang lebih kecil.

IV.2 Protokol Zigbee

Secara garis besar arsitektur keamanan standar IEEE 802.15.4 akan dijelaskan lebih detil pada bagian ini yang meliputi standar IEEE 802.15.4 dan keamanan.

IV.2.1. Standar IEEE 802.15.4

Pengalamatan dalam standar IEEE 802.15.4 telah disempurnakan melalui pengenalan node 64 bit dan pengenalan jaringan 16 bit. Standar IEEE 802.15.4 mendukung beberapa pengalamatan node yang berbeda. Sebagai contoh, pemotongan alamat 16 bit mungkin digunakan sebagai pengganti pengenalan node 64 bit dalam kasus tertentu. Ini mengijinkan ukuran dari alamat sumber dan tujuan berubah-ubah antara 0 dan 10 bytes tergantung pada apakah alamat yang digunakan tersebut terpotong atau penuh, dan apakah node mengirimkan ke alamat lain secara tersebar. Sebagai bahan pertimbangan alamat pengenalan node cukup berukuran 64-bit.

Ada dua jenis paket yang penting yang terkait dengan keamanan pada standar IEEE 802.15.4 yaitu paket data dan paket *acknowledgment*. Paket data, dapat dilihat pada Gambar 4(a), mempunyai panjang variable (*variable length*)

dan digunakan pada sebuah node untuk mengirimkan pesan ke satu node atau untuk menyebarkan pesan ke banyak node. Masing-masing paket data mempunyai sebuah *Flagfield* yang menandakan jenis paket, apakah keamanannya enable atau tidak, mode pengalamatan yang digunakan, dan apakah pengirim meminta *acknowledgment*. 1 byte pertama melayani penentuan jumlah paket *acknowledgment*. Paket pilihannya meliputi alamat sumber dan tujuan. Seperti diuraikan di atas, masing-masing *field* berubah ukurannya antara 0 dan 10 bytes. *Payloadfield* data datang setelah *addressingfield*. Ini kurang dari 102 bytes. Dan bagian byte terakhir, 2 byte *checksumfield/Cyclic Redundancy Check* (CRC) melindungi paket yang digunakan untuk penanganan kesalahan-kesalahan pengiriman.

Paket *acknowledgment*, seperti pada Gambar 4(b), dikirimkan oleh penerima hanya jika paket data yang bersesuaian tidak mengirim ke alamat node secara tersebar dan membutuhkan *acknowledgment*. Formatnya sederhana: 2 byte *fieldflags* setara dengan satu paket data, nomor urutan (*sequent number*) yang berukuran 1 byte dari paket yang berisi *acknowledgment* dan 2 byte untuk CRC.

IV.2.2. Keamanan pada *Media Access Control*

Lapisan keamanan pada standar IEEE 802.15.4 ditangani oleh lapisan *media access control* yang berada di bawah kontrol aplikasi. Aplikasi menetapkan persyaratan keamanannya dengan pengaturan parameter kontrol yang sesuai ke dalam *stack* radio. Jika aplikasi tidak mengatur parameter apapun, maka nilai keamanan default-nya diatur dengan *disable*. Aplikasi harus tegas mengatur nilai keamanan dengan memberikan nilai *enable*, seperti diuraikan lebih rinci di bawah ini. Spesifikasi standar IEEE 802.15.4 mendefinisikan empat jenis paket yaitu paket beacon (*beacon packets*), paket data (*data packets*), paket *acknowledgments* (*acknowledgments packets*) dan paket kontrol (*control packets*) untuk lapisan *media access control*. Spesifikasi ini tidak mendukung keamanan untuk paket *acknowledgment*, jenis paket lain merupakan pilihan yang dapat

mendukung perlindungan integritas (*integrity protection*) dan perlindungan kerahasiaan paket *fielddata*.

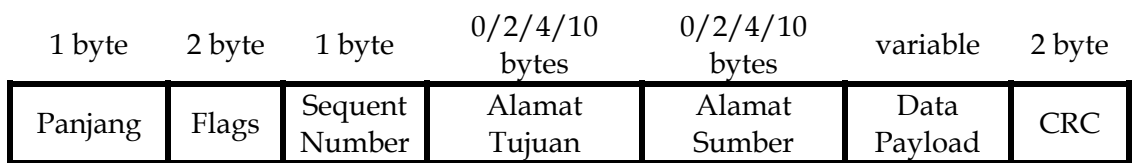
Aplikasi mempunyai sebuah pilihan rangkaian keamanan yang mengontrol jenis perlindungan keamanan yang disediakan untuk pengiriman data. Masing-masing rangkaian keamanan menawarkan *properties* dan jaminan keamanan yang berbeda, dan hal paling menarik adalah menawarkan format paket yang berbeda. Spesifikasi standar IEEE 802.15.4 mendefinisikan delapan rangkaian keamanan, seperti dapat dilihat dalam Tabel 4.

Nama	Deskripsi
Null	<i>No Security</i>
AES-CTR	<i>Encryption only, CTR Mode</i>
AES-CBC-MAC-128	<i>128 bit MAC</i>
AES-CBC-MAC-64	<i>128 bit MAC</i>
AES-CBC-MAC-32	<i>128 bit MAC</i>
AES-CCM-128	<i>Encryption & 128 bit MAC</i>
AES-CCM-64	<i>Encryption & 64 bit MAC</i>
AES-CCM-32	<i>Encryption & 32 bit MAC</i>

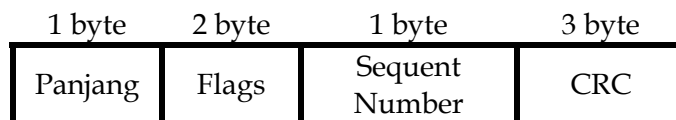
Tabel 4. Rangkaian Keamanan yang didukung oleh standar IEEE 802.15.4

Rangkaian keamanan yang didukung oleh standar IEEE 802.15.4 adalah sebagai berikut : tidak ada pengamanan (*no security*), enkripsi saja (*encryption only*)/AES-CTR, menjaga keaslian data saja (*authentication only*)/AES-CBC-MAC dan enkripsi dan menjaga keaslian data (*encryption and authentication*)/AES-CCM. Masing-masing kategori yang mendukung keaslian data (*authentication*) dibagi dalam tiga ukuran yang berlainan tergantung pada ukuran dari *media access control* yang di tawarkan.

MAC dapat memiliki panjang 4, 8, atau 16 bytes. Dengan ukuran MAC yang lebih panjang maka lebih kecil kesempatan musuh untuk memalsukan tebakan kode yang sesuai. Sebagai contoh, dengan ukuran MAC 8 byte, musuh mempunyai 2^{64} kesempatan memalsukan MAC.

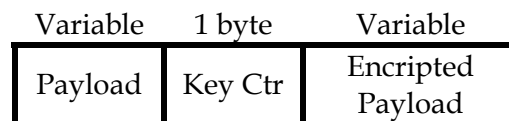


(a) Format Paket Data

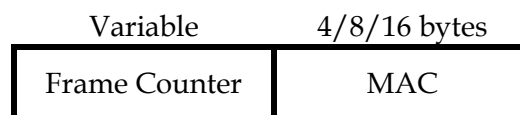


(b) Format Paket Acknowledgment

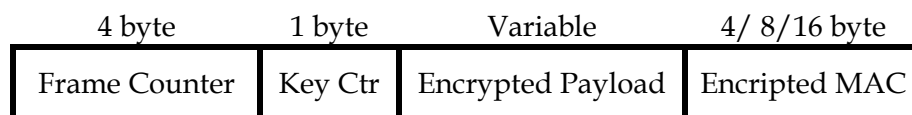
Gambar 4. Format Paket Data dan *Acknowledgment*



(a) AES-CTR



(b) AES-CBC-MAC- b , $b \in \{4,8,16\}$ ukuran MAC



(c) AES-CCM-MAC- b , $b \in \{4,8,16\}$ ukuran MAC

Gambar 5. Format dari Field Data

Tradeoff-nya adalah paket dengan ukuran yang lebih besar digunakan untuk meningkatkan perlindungan melawan serangan *authentication*. Apalagi, untuk masing-masing rangkaian yang menawarkan enkripsi, penerima dapat secara bebas mengaktifkan pilihan *enable* untuk *replay protection*. Para perancang radio tidak harus menerapkan seluruh rangkaian. Spesifikasi ini hanya memerlukan *chip* radio yang menyediakan dukungan untuk rangkaian *null* dan rangkaian AES-CCM-64.

Indikasi sebuah aplikasi memilih rangkaian keamanan berdasarkan pada alamat sumber dan tujuan pesan. *Chip* radio dengan standar IEEE 802.15.4 mempunyai suatu daftar pengontrol akses (*Access Control List*)/ACL yang mengendalikan rangkaian keamanan dan informasi kunci yang digunakan. Perangkat yang tersedia mendukung sampai 255 masukan ACL. Masing-masing masukan berisi sebuah alamat standar IEEE 802.15.4, sebuah pengenalan rangkaian keamanan dan material keamanan, seperti ditunjukkan pada Gambar 6.

Address	Security Suite	Key	Last Initialization Vector (IV)	Replay Counter
---------	----------------	-----	---------------------------------	----------------

Gambar 6. Format dari masukan ACL. Alamat tujuan dari paket yang keluar dicocokkan dengan *field* alamat dalam masukan ACL. Paket kemudian diproses menggunakan rangkaian keamanan yang ditandai dengan kunci dan *Initialization Vector* (IV) yang terdaftar di masukan ACL. Untuk paket yang datang, alamat sumber dicocokkan dengan *field address* masukan ACL. Kriptografi beroperasi menggunakan kunci dari masukan ACL dan *field counter replay* bertindak sebagai suatu *water mark*, jika *replay protection* diaktifkan dengan *enable*.

Material keamanan adalah status yang terus-menerus diperlukan untuk mengeksekusi rangkaian keamanan. Material keamanan ini terdiri dari kunci kriptografi untuk rangkaian yang menyediakan enkripsi, status *nonce* yang menyatakan bahwa harus dipelihara untuk bagian pekerjaan enkripsi dengan paket yang berbeda. Ketika *replay protection* dilibatkan, material keamanan juga sudah termasuk *water mark* untuk pengenalan paket yang baru akan diterima.

Sebagai bagian dari antar muka (*interface*) untuk paket pengiriman, Aplikasi harus menetapkan nilai *boolean* apakah keamanannya *enable*. Jika tidak ada keamanan (*no security*) yang dibutuhkan, paket dikirimkan seperti apa adanya. Jika keamanannya *enable*, lapisan MAC mencari (*lookup*) ke alamat tujuan dalam tabel ACL. Jika ada masukan ACL yang cocok, rangkaian keamanan, kunci, dan *nonce* yang ditetapkan dalam masukan ACL itu digunakan untuk mengenkripsi dan atau membuktikan keaslian paket yang keluar, dan *fieldflags* pada paket keluar yang sesuai dengan kelompoknya. Jika alamat tujuan tidak terdaftar dalam tabel ACL, maka masukan ACL dengan nilai *default* digunakan sebagai gantinya; masukan ACL dengan nilai *default* yang mirip dengan masukan ACL, kecuali kalau masukan ACL cocok untuk seluruh alamat tujuan. Jika masukan ACL nilai *default* kosong dan aplikasi membutuhkan keamanan, Lapisan *media acces control* mengembalikan kode kesalahan.

Pada tempat penerima paket, lapisan *media access control* memeriksa *fieldflags* dalam paket untuk menentukan jika ada beberapa rangkaian keamanan yang telah diberlakukan untuk sebuah paket. Jika keamanan tidak digunakan (*no security*), paket dilewatkan kepada aplikasi seperti apa adanya. Jika tidak, lapisan *media access control* menggunakan suatu proses yang mirip untuk menemukan masukan ACL yang sesuai, untuk waktu berdasarkan pada alamat pengirim. Kemudian menggunakan rangkaian keamanan yang sesuai, kunci, dan *counter replay* untuk paket kedatangan, memberikan aplikasi dengan pesan kesalahan jika tidak ada masukan ACL yang sesuai untuk ditempatkan.

IV.2.2.1. Kategori Rangkaian Keamanan

Berikut akan diuraikan lebih rinci tentang kategori dari rangkaian keamanan:

A. Null

Null merupakan rangkaian keamanan yang paling sederhana. Pencantumannya wajib dalam semua *chip* radio. Null tidak mempunyai material keamanan dan beroperasi seperti fungsi identitas dan tidak menghasilkan jaminan keamanan apapun.

B. AES-CTR

Rangkaian ini menyediakan perlindungan kerahasiaan yang menggunakan *AES block cipher* [7] dengan *counter mode*. Untuk mengenkripsi data pada *counter mode*, pengirim mengelompokkan paket *cleartext* ke dalam block berukuran 16-byte $p_1; \dots; p_n$ dan menghitung *chipper* dengan rumus $c_i = p_i \oplus E_x(X_i)$. Masing-masing blok yang berukuran 16 byte menggunakan *counter* sendiri yang berbeda-beda, dimana disebut x_i . Penerima mengembalikan *plaintext* asli dengan rumus $p_i = c_i \oplus E_x(X_i)$. Dengan Jelas, penerima memerlukan nilai *counter* X_i secara berurut untuk merekonstruksi p_i . *Counter* X_i disebut dengan *nonce* atau *Initialization Vector (IV)*, yang terdiri atas susunan *fieldflags* statis, alamat pengirim, dan 3 *counter* terpisah : 4 byte *frame counter* yang merupakan paket, 1 byte *fieldcounter* kunci, dan 2 byte *block counter*, yang jumlahnya 16 byte blok dalam paket seperti ditunjukkan dalam Gambar 7.

Pengelolaan *frame counter* dilakukan dengan radio perangkat keras. pengirim menaikkan nilai *frame counter* setelah mengenkripsi masing-masing paket. Ketika mencapai nilai maksimum, radio mengembalikan kode kesalahan dan tidak memungkinkan untuk melakukan enkripsi. *counter* kunci adalah *counter* yang berukuran satu byte yang berada di bawah kontrol aplikasi. *Counter* ini dapat dinaikan nilainya jika *frame counter* belum mencapai nilai maksimumnya. Persyaratannya adalah bahwa *nonce* harus tidak pernah mengulangi dalam *lifetime* dari *single key*, dan tugas dari *frame counter* dan *key counter* adalah untuk mencegah *nonce* digunakan kembali. *Block counter* yang berukuran 2 byte menjamin masing-masing blok akan menggunakan nilai *nonce* yang berbeda; pengirim tidak harus menggabungkannya dengan paket, karena penerima dapat memperkirakan nilainya untuk masing-masing blok.

Kesimpulannya, dalam pengirim sudah meliputi *frame counter*, *counter key* dan enkripsi *payload* yang telah yang ada dalam *payloadfiled* dari sebuah paket, seperti pada Gambar 5(a).

1 byte	8 byte	4 byte	1 byte	2 byte
Flags	Source Address	Frame Counter	Key Counter	Block Counter

Gambar 7. Format masukan (ξ) untuk *Block cipher* pada rangkaian AES-CTR dan AES-CCM. *flagsfield* adalah suatu konstanta untuk mode AES-CTR; nilainya ditentukan oleh spesifikasi CCM untuk AES-CCM.

C. AES-CBC-MAC

Rangkaian ini menyediakan perlindungan integritas (*integrity protection*) dengan menggunakan CBC-MAC [8]. Pengirim dapat menghitung MAC dengan ukuran yang berlainan yaitu 4, 8, atau 16 Byte dengan algoritma CBC-MAC, yang muncul untuk tiga AES-CBC-MAC yang berbeda. MAC hanya dapat dihitung oleh pihak yang memiliki kunci simetrik (*symmetric key*). MAC melindungi *headers packet* sama seperti halnya melindungi data *payload*. Pengirim melampirkan data *plaintext* dengan MAC, seperti pada gambar 5(b). Penerima memeriksa MAC dengan menghitung MAC dan membandingkannya dengan nilai yang dimasukkan di dalam paket.

D. AES-CCM

Rangkaian keamanan ini menggunakan mode CCM untuk mengenkripsi dan menjaga keaslian data [8]. Lebih luas lagi, AES-CCM merupakan rangkaian pertama yang menggunakan *integrity protection* pada *payload* data dan header dengan menggunakan CBC-MAC kemudian mengenkripsi *payload* data dan MAC menggunakan mode AES-CTR. AES-CCM memiliki dua bentuk *field* dari dua operasi enkripsi dan menjaga keaslian data: yaitu MAC, *frame counter* dan *counter key*. *Field* ini melayani fungsi yang sama seperti di atas. Sebagaimana AES-CBC-MAC mempunyai tiga jenis yang berbeda tergantung dengan ukuran MAC, AES-CCM juga mempunyai tiga jenis yang berbeda. Format pakatnya ditunjukkan dalam gambar 5(c)

Penerima dapat memilih *enable* untuk *replay protection* ketika menggunakan rangkaian keamanan yang menyediakan perlindungan kerahasiaan (*confidentiality protection*). Rangkaian ini meliputi AES-CTR dan semua varian dari AES-CCM. Penerima menggunakan *frame counter* dan *key counter* yang berukuran 5 byte, *replay counter* dengan *key counter* menempati (*Most Significant Byte*) MSB dari nilai ini. Penerima membandingkan *replay counter* dari kedatangan paket untuk nilai yang paling tinggi, yang disimpan dalam masukan ACL. Jika kedatangan paket mempunyai *counter replay* lebih besar dibanding salah satu yang disimpan, maka paket diterima dan *counter replay* baru disimpan. Akan tetapi, Jika kedatangan paket nilainya lebih kecil, paket tersebut ditolak dan aplikasi diberitahu tentang penolakan tersebut. Dengan mengacu pada *counter* ini seperti *counter replay*, sungguhpun ini merupakan *counter* yang sama seperti *nonce*. *Counter* ini secara logika melayani tujuan yang berbeda dari *nonce*, dimana digunakan untuk menjaga kerahasiaan. *Counter replay* tidak terbuka bagi aplikasi untuk digunakan.

IV.3. Model Penguncian (*Keying Model*)

Kriptografi simetrik (*symmetric cryptography*) mempercayakan pada kedua *endpoints* yang menggunakan kunci yang sama ketika berkomunikasi ingin aman. Dalam kelompok node, model penguncian mengurus apakah kunci sebuah node digunakan untuk berkomunikasi dengan node lain. Model penguncian yang paling sesuai untuk suatu aplikasi tergantung pada model ancaman pada aplikasi dan apa jenis sumber dayanya serta keinginan dari pihak manajemen kunci. Sebagai contoh, dalam *Network shared keying*, tiap-tiap node menggunakan kunci yang sama untuk berkomunikasi dengan node lain.

IV.3.1. Penguncian Jaringan berbagi (*Network shared keying*)

Dalam penguncian jenis ini masing-masing node dalam sistem memproses kunci yang sama dan menggunakannya untuk berkomunikasi dengan semua node. Manajemen kunci menjadi hal sepele dengan pendekatan ini, karena semua komunikasi menggunakan kunci yang sama. Tambahannya

adalah bahwa memori yang dibutuhkan minimal. Oleh karenanya aplikasi dapat menggunakan *network shared keying*.

Bagaimanapun, kesederhanaan manajemen ini menghadapi biaya dari rentan serangan orang dalam. Ini lebih rentan daripada model penguncian yang lain untuk kesepakatan *single key*, seperti terjadi ketika musuh mensepakati sebuah node. Musuh dapat menggunakan node yang disepakati untuk merusak keamanan jaringan yang sudah dijamin secara keseluruhan. Sebuah node dapat merusak kerahasiaan terhadap pesan yang telah dikirim dalam sistem dan memalsukan pengakuan terhadap pesan yang di timbulkan dari beberapa node.

IV.3.2. Pairwise keying

Pairwise keying tahan terhadap node yang disepakati dengan ruang lingkup yang terbatas pada masing-masing kunci. Dengan *Pairwise keying* masing-masing pasangan node berbagai kunci yang berbeda. Jadi, hanya node yang disepakati yang mempengaruhi pesan sebelum dan sesudah dikirim ke atau dari node itu. Lalulintas lainnya tidak diterima. *Pairwise keying* menyediakan keamanan yang lebih baik dibanding *network shared keying*.

IV.3.3. Grup Keying

Sekelompok kunci yang mensepakati antara *network shared keying* dan *pairwise keying*. Sebuah *single key* dibagi antara kumpulan node dan digunakan pada semua hubungan diantara dua node dalam kelompok itu. Pemisahan dalam kelompok mungkin dibuat didasarkan pada tempat, topologi jaringan, atau persamaan fungsi. Keuntungan dari *Group keying* adalah bahwa *Group keying* menyediakan suatu *tradeoff* diantara *network shared keying* dan *pairwise keying*, dengan hambatan yang memihak pada kesepakatan node untuk biaya yang lebih rendah dibanding *pairwise keying*.

IV.3.4. Pendekatan Gabungan (*Hybrid approaches*)

Beberapa sistem dapat menggunakan gabungan dari model penguncian secara bersma-sama dalam aplikasi yang sama. Sebagai contoh, kita mungkin

menggunakan *pairwise keying* untuk seluruh hubungan antara node dan pangkalan basis (*base station*) dan menggunakan *network shared keying* untuk hubungan yang lainnya.

IV.4 Implementasi

Peralatan yang sesuai dengan harapan keamanan diatas adalah *Atmel Z-Link transceiver*[1] dan *Motorola MC13192*[6] dimana mendukung standar IEEE 802.15.4 untuk lapisan fisik yang menentukan format dan frekwensi paket radio, walaupun tidak seluruhnya merupakan bagian standar *media access control*. Hal yang harus diterapkan dengan operasi keamanan pada mikrokontroler adalah berinteraksi dengan perangkat keamanan IEEE 802.15.4. Chipcon CC2420 merupakan perangkat keras yang mendukung primitif kriptografi yang mengizinkan operasi bagi lapisan perangkat standar IEEE 802.15.4 yang mengikuti spesifikasi tersebut.

Implementasi perangkat keras dari standar ini mempunyai nilai yang lebih untuk menyederhanakan pekerjaan pembuat aplikasi. Penanganan operasi kriptografi dalam perangkat keras memberikan kebebasan mikrokontroler dari permintaan kebutuhan akan sistem yang *real time* untuk mendekripsi dan mengenkripsi paket.

V. Penutup

Lapisan *media access control* pada lapisan fisik dari standar IEEE 802.15.4 merupakan benteng dari keamanan pada zigbee dengan menggunakan algoritma kriptografi dari AES. Dengan banyak pilihan rangkaian keamanan memberikan kemudahan untuk para pengguna perangkat zigbee dalam mengamankan data yang ada melalui aplikasi zigbee tersebut.

Tapi ada hal penting yang perlu penulis sampaikan bahwa keamanan pada zigbee ini masih rentan terhadap serangan dikarenakan standar dari spesifikasi IEEE 802.15.4 yang masih cacat ini terbukti dari beberapa penelitian yang dilakukan terhadap aplikasi yang berjalan pada zigbee tersebut. Oleh

karena itu perancang aplikasi zigbee di harapkan dapat memperbaiki kekurangan yang ada pada sistem keamanan zigbee tersebut.

Daftar Pustaka

- [1] Atmel at86rf210 z-link transceiver data sheet.
<http://www.atmel.com/dyn/resources/proddocuments/doc5033.pdf>, 2004.
- [2] Callaway, Ed., *"Low Power Consumption Features of the IEEE 802.15.4/Zigbee LR-WPAN Standar"*, Motorola Lab, Florida, 2004.
- [3] Craig, Wiliam C. *"Wireless control that simply work"*, Boston ,April 2004.
- [4] Jon Adams (Motorola), *"What you should know about the ZigBee alliance"*
[http://www.zigbee.org/resources/documents/Adams Heile_SensorsExpo AnaheimSept03_V1_000.ppt](http://www.zigbee.org/resources/documents/Adams_Heile_SensorsExpoAnaheimSept03_V1_000.ppt).
- [5] Joan Daemen, Vincent Rijmen, *"Note on naming"*
<http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf>.
- [6] Motorola mc13192 datasheet.
http://e-www.motorola.com/files/rf_if/doc/data_sheet/MC13192DS.pdf, 2004.
- [7] Pedersen, Morten and Thong, Than Kim *"Formation of Secure Wireless Ad-hoc Sensor Networks"*, Master Thesis in Information and Communication Technology, Agder University College, Grimstad, June 2004.
- [8] Sastry, Naveen and Wagner, David *"Security Considerations for IEEE 802.15.4 Networks"*, University of California, Berkeley, 2004.
- [9] Tanebaum, Andrew S., *"Computer Networks"*, 4th, Prentice-Hall of India, New Delhi, 110001 2003.
- [10] The Zigbee alliance.
<http://www.zigbee.org>
- [11] ---, *"Introduce potential members on the target markets of ZigBee and benefits of joining"*, Ember Corporation, Boston, May 2004.

