Aplikasi Indoor Secured-Localization System Menggunakan Jaringan Sensor Nirkabel untuk Koordinasi Pasukan PMK pada Kondisi Darurat Kebakaran di dalam Gedung

Adam Surya Putra[1], Prima Kristalina[2], Amang Sudarsono[3]
Program Studi Teknik Telekomunikasi
Politeknik Elektronika Negeri Surabaya(PENS)
Surabaya, Indonesia
[1]adam115telkom@gmail.com , [2]prima@pens.ac.id , [3]amang@pens.ac.id

Abstrak—**Informasi lokasi suatu object penginderaan adalah salah satu hal yang penting dan menjadi tantangan dalam implementasi jaringan sensor nirkabel. Saat ini jaringan sensor nirkabel dapat digunakan dalam aplikasi pemantuan suatu object, pelacakan sasaran, koordinasi, dan masih banyak lagi. Karena jaringan sensor dapat berinteraksi dengan data sensitif dan / atau beroperasi di lingkungan tanpa pengawasan, maka sangat penting bahwa masalah sistem keamanan diperhatikan dari awal men-design system. Dalam makalah ini, kami mengusulkan suatu sistem lokalisasi node secara terdistribusi di lingkungan indoor dengan skema penentuan lokasi node dilakukan di setiap node dengan bantuan dari node refrensi. Setiap pengiriman paket data dalam jaringan sensor dilengkapi dengan sistem keamanan. Teknik lokalisasi node menggunakan metode trilaterasi dengan memanfaatkan 3 node refrensi. Sistem keamanan data terdiri dari AES (Advanced Encryption Standard) sebagai confidentiality dan Fungsi Hash MD5 sebagai authentication. Kami mengevaluasi kinerja secara komprehensif meliputi estimasi jarak antar node, kalkulasi posisi node, waktu dan keamanan pengiriman paket data. Hasil evaluasi sistem yang diusulkan menggunakan platform jaringan sensor perangkat waspmote. Hasil penelitian pada lingkungan indoor menunjukkan bahwa sistem yang diusulkan menghasilkan kinerja yang baik, meliputi penentuan posisi node, waktu komunikasi dan keamanan pengiriman paket data. Secara keseluruhan sistem yang di usulkan memiliki keandalan yang cukup baik dalam aplikasi real time tracking node.**

Kata kunci—Lokalisasi Terdistribusi; AES; Hash MD5; Range-Based.

I. PENDAHULUAN

Jaringan sensor nirkabel merupakan salah satu bentuk implementasi dan pengembangan dari komunikasi nirkabel. Dimana pada suatu kelompok node yang memiliki sensor-sensor tertentu disebar untuk memantau kondisi suatu area dan dapat berkomunikasi tanpa bantuan media fisik [1]. Sebagain dari node akan ditempatkan secara acak dan mengamati sisa-sisa lokasi yang tidak bisa dijangkau oleh teknologi GPS. Posisi node menentukan lokasi fenomena yang diamati. Masalah lokalisasi node akan menjadi semakin rumit jika diterapkan di lingkungan indoor, sebab teknologi GPS receiver tidak mampu menjangkau satelite.

Tujuan dari lokalisasi adalah menyediakan koordinat fisik untuk semua node sensor yang tidak diketahui posisinya (*unknown node*). Lokalisasi pada jaringan sensor nirkabel di lingkungan indoor memiliki banyak aplikasi baru di bidang monitoring dan kontrol. Contohnya dalam lingkungan taman kanak-kanak pintar, lokalisasi node dapat digunakan untuk memantau kemajuan anak-anak dengan melacak interaksi mereka dengan mainan dan juga sebaliknya. Hal ini juga dapat digunakan dalam lingkungan rumah sakit untuk melacak peralatan, pasien, dokter dan perawat [3]. Dan pada aplikasi pelacakan pasukan pemadam kebakaran dalam hal koordinasi dan kontrol.

Skema lokalisasi pada jaringan sensor nirkabel, sebagian didasarkan pada dua metode estimasi jarak. Pertama, jarak dapat diperoleh dengan mengukur kekuatan sinyal, interval waktu atau sudut yang tiba di node tertentu. Metode pengukuran ini dikenal sebagai teknik *range-based.* Metode lainnya, dikenal sebagai *range free,* pendekatan jarak node tertentu berdasarkan informasi yang dikirimkan oleh node lain [4].

Sebuah jaringan nirkabel umumnya dalam mengirim informasi menggunakan teknologi nirkabel. Karena kebutuhan fleksibilitas jaringan maka diperlukan adanya keamanan data. Dalam makalah ini kami mengusulkan skema lokalisasi node untuk aplikasi koordinasi pasukan pemadam kebakaran yang berada di lingkungan *indoor*. Dalam skema ini, perangkat node mampu mengkonfigurasi dan menentukan posisinya sendiri dengan menggunakan metode *range-based*. Proses Konfigurasi diri dimulai ketika sebuah node menerima paket informasi kekuatan sinyal dari node refrensi, kemudian membandingkan dengan kuat sinyal refrensi. Penentuan posisi node dihitung secara relatif terhadap posisi node refrensi terdekat. Disamping itu, proses pengiriman paket data pada jaringan sensor nirkabel dilengkapi dengan sistem keamanan data. Sistem keamanan data dibangun dengan 2 fitur, yaitu kerahasiaan dan otentikasi. Pada sisi kerahasiaan data menggunakan AES *(Advanced Encription Standard*) dan sisi otentikasi data menggunakan fungsi hash MD5. Kontribusi dari makalah ini adalah untuk mengembangkan skema lokalisasi secara terdistribusi yang

dilengkapi dengan sistem keamanan data. Kami menganalisa akurasi posisi node, waktu kinerja sistem mulai dari mengkonfigurasi diri hingga paket data diterima oleh server, ketahanan sistem terhadap serangan dari pihak ke tiga atau *man in the middle attack*, dan memvalidasi hasil menggunakan waspmote.

Selanjutnya makalah ini disusun sebagai berikut: Pada bagian II, kami meninjau konsep dan karakteristik teknik lokalisasi node, pada bagian III kami meninjau teknik keamanan data AES dan MD5, pada bagian IV, kami membahas gambaran arsitektur dan kerangka yang diusulkan, pada bagian ke V menyajikan hasil penelitian yang meliputi lokasi posisi unknown node dan ketahanan sistem terhadap serangan, dan akhirnya kami menyimpulkan hasil penelitian pada bagian ke VI.

II. KONSEP DAN KARAKTERISTIK LOKALISASI

Lokalisasi adalah perkiraan posisi melalui komunikasi antara *localized node* (node yg diketahui) dan *unlocalized node* (node yang tidak diketahui) [5].

Tahapan pada sistem lokalisasi terdiri dari tiga komponen penting yaitu [6]:

- Penentuan jarak/sudut estimasi :

Komponen ini bertanggung jawab untuk memperkirakan informasi tentang jarak dan sudut antara dua node. Informasi ini nantinya akan digunakan oleh komponen lain dari sistem lokalisasi.

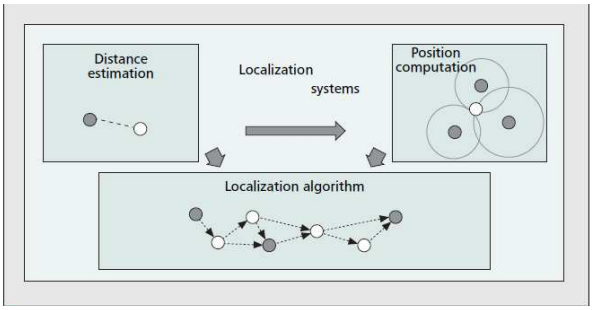
- Komputasi posisi :

Komponen ini bertanggung jawab untuk komputasi posisi node yang didapatkan berdasarkan informasi yang tersedia mengenai jarak / sudut dan posisi referensi node.

- Algoritma lokalisasi :

Komponen utama dari sistem lokalisasi. Komponen ini berfungsi untuk menentukan bagaimana informasi yang tersedia akan di manipulasi untuk memungkinkan sebagian atau semua node dari jaringan memperkirakan posisi mereka.

Gambar 1 menggambarkan pembagian komponen pada sistem lokalisasi.

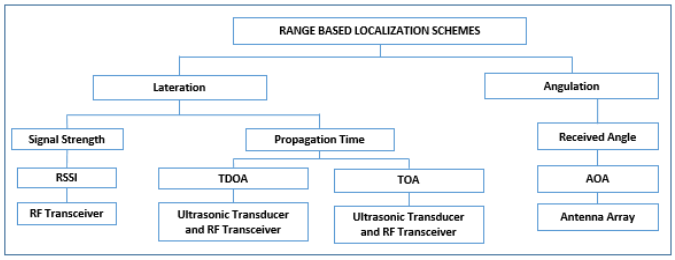


Gambar 1. Pembagian Komponen Penting Sistem Lokalisasi Jaringan Sensor Nirkabel

Kebutuhan untuk mengetahui posisi *unlocalized node* dalam sistem lokalisasi bergantung langsung pada masing-masing komponen tersebut. Setiap komponen juga memiliki tujuan dan metode sendiri-sendiri. Sehingga komponen tersebut dapat dipandang sebagai subareas dari masalah lokalisasi yang perlu dianalisis dan dipelajari secara terpisah.

A. Skema Lokalisasi Range-Based

Algoritma lokalisasi *range-based* berfokus pada estimasi jarak dan sudut antara *node sensor*. Algoritma ini menghitung jarak antar *node* dengan bantuan prinsip-prinsip geometris. Klasifikasi skema lokalisasi range-based ditunjukkan pada gambar 2. Algoritma ini menggunakan hardware canggih untuk mengetahui metrik kisaran seperti AOA (*Angle of arrival*), TOA (*Time of arrival*), TDOA (*Time Difference of arrival*), dan RSSI (*Received signal strength indication*). Harus ada komunikasi antara *localized node* dan *unlocalized node* disekitarnya untuk menentukan posisi *unlocalized node* [2].



Gambar 2. Klasifikasi Skema Lokalisasi-*Range Based*

Dalam makalah ini, kerangka yang kami usulkan untuk menentukan jarak antara node menggunakan metode RSSI.

B. RSSI

Penggunaan *Receive Signal Strength Indicator* (RSSI) menganggap daya yang diterima (P_{RX}) sebagai fungsi dari jarak pemancar ke penerima dengan kenaikan beberapa pangkat. Model ini adalah model propagasi deterministik dan hanya memberikan nilai rata-rata, dimana nilai RSSI adalah [7]:

$$RSSI = 10\ x\ \log\left[\frac{P_{RX}}{P_{ref}}\right] \quad (1)$$

Keterangan persamaan (1):

RSSI = Perbandingan kuat sinyal yang diterima terhadap kuat sinyal refrensi (meter).
P_{RX} = Daya yang diterima pada *receiver* (Watt)
P_{ref} = Daya yang diterima pada jarak refrensi (Watt)

Dimana kuat sinyal yang diterima (P_{RX}) diubah ke dalam bentuk RSSI yang didefinisikan sebagai rasio daya yang diterima terhadap referensi daya Pref (d_0). Sedangkan P_{RX} sendiri memiliki nilai seperti ditunjukkan oleh persamaan (2)

$$P_{RX} = P_{TX}\ x\ G_{TX}\ x\ G_{RX}\left[\frac{\lambda}{4\pi d}\right]^n \quad (2)$$

dimana:

P_{RX} = Daya yang diterima pada *receiver* (Watt)
P_{TX} = Daya yang dikirim oleh *transmitter* (Watt)
G_{TX} = Gain *transmitter* (Watt)
G_{RX} = Gain *receiver* (Watt)
λ = panjang gelombang (Meter)
d = Jarak *transmitter* dan *receiver* (Meter)
n = *path loss exponent*

Dari subtitusi antara persamaan (1) dan (2) didapatkan persamaan (3) dibawah ini:

$$RSSI = 10n\ x\ \log\left[\frac{d}{d_0}\right] \quad (3)$$

Berikut ini merupakan acuan tabel varian dari *exponent path loss* (n) untuk lingkungan yang berbeda ditunjukkan pada tabel 1 dibawah ini [8].

TABEL I. PATH LOSS EXPONENT UNTUK LINGKUNGAN BERBEDA

Environment	*Path Loss Exponent, n*
Free space	2
Urban area celluler radio	2.7 to 3.5
Shadowed urba celluler radio	3 to 5
In building Line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

Nilai koefisien pathloss juga bisa di dapatkan dengan menurunkan rumus RSSI sehingga di dapatkan persamaan (4).

$$n = \frac{P_{RX0} - P_{RX}}{10\log\frac{d}{d_0}} - X_\sigma \quad (4)$$

Setelah mendapatkan nilai *exponent path loss*, untuk mencari estimasi jarak antar node dapat menggunakan persamaan (5).

$$d = d_0 . 10^{\frac{P_{R0}-P_{Rx}}{10.n}} \quad (5)$$

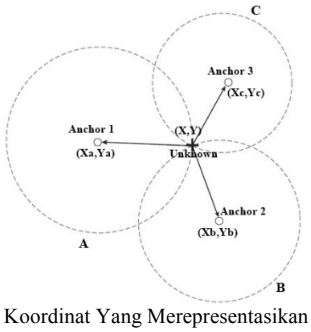
Keterangan persamaan:

n : Koefisien *pathloss*
P_{RXo} : Daya terima pada jarak acuan 1 meter (dB)
P_{RX} : Daya terima pada jarak d (dB)
d : Jarak pengukuran (meter)
d_0 : Jarak acuan = 1 meter.
X_σ : Sebuah variable *zero-mean Gaussian distributed random* (dalam dB) dengan standar deviasi σ. Variabel ini hanya digunakan ketika ada *shadowing effect*. Jika tidak ada *shadowing effect*, maka variabel ini adalah nol.

C. Komputasi Posisi

Ketika sebuah *node* sudah memiliki informasi yang cukup tentang jarak dan / atau sudut dan posisi, selanjutnya dapat menghitung lokasi posisinya dengan menggunakan salah satu metode lokalisasi. Beberapa metode dapat digunakan untuk menghitung posisi *node*. Metode tersebut yaitu *trilateration*, multilateration, triangulasi, pendekatan probabilistik, bounding box, dan posisi sentral. Pemilihan metode akan berdampak pada kinerja sistem lokalisasi, seperti informasi yang tersedia dan ketrebatasan prosesor [6].

Pada skema yang kami ajukan, metode untuk komputasi posisi menggunakan *trilateration*.



Gambar 3. Tiga Koordinat Yang Merepresentasikan Tiga Lingkaran Jangkar

Trilateration merupakan sebuah metode pencarian koordinat sebuah titik berdasarkan referensi jarak titik tersebut pada 3 buah koordinat yang sudah diketahui. Seperti ditunjukkan pada Gambar 3. Dimana kuadrat jarak antara unknown node dan anchor node i dapat dinyatakan sebagai [4]

$$d_i{}^2 = (x - x_i)^2 + (y - y_i)^2 \quad (6)$$

dengan i = 1 sebagai titik acuan, di mana $x_1 = y_1 = 0$ dengan demikian, untuk i > 1 Persamaan (6) dapat ditulis sebagai:

$$d^2{}_i - d^2{}_1 = x^2{}_i - 2xx_i + y^2{}_i - 2yy_i \quad (7)$$

Dalam bentuk matriks dengan i = 1 sampai 3 , terhadap persamaan (7) dapat ditulis sebagai:

$$2\begin{bmatrix}(x_2 - x_1) & (y_2 - y_1)\\ (x_2 - x_3) & (y_2 - y_3)\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix} = \begin{bmatrix}x^2{}_2 - x^2{}_1 + y^2{}_2 - y^2{}_1 + d^2{}_1 - d^2{}_2\\ x^2{}_2 - x^2{}_3 + y^2{}_2 - y^2{}_3 + d^2{}_3 - d^2{}_2\end{bmatrix}$$

d dan koordinat (x,y) adalah nilai estimasi.

III. KONSEP NETWORK SECURITY

Network security adalah Perlindungan yang diberikan untuk sistem informasi agar mencapai tujuan yang dimaksud, menjaga integritas, ketersediaan, dan kerahasiaan sumber daya sistem informasi (termasuk *hard-ware, software, firmware*, informasi, dan telekomunikasi). Definisi ini memperkenalkan tiga tujuan utama dari *network security* yaitu [9]:

1. *Confidentiality*: Istilah ini mencakup dua konsep yang saling terkait, yaitu kerahasiaan data dan privasi
2. Integritas: Istilah ini mencakup dua konsep yang saling terkait, yaitu Integritas data dan Integritas System
3. *Availability*: memastikan bahwa sistem bekerja secara cepat dan layanan tidak ditolak untuk pengguna yang berwenang.

A. Kriptografi

Kriptografi merupakan bidang ilmu yang berfungsi untuk menjaga agar pesan rahasia menjadi tetap aman. Terdapat beberapa komponen dalam kriptografi agar dapat mencapai tujuan dari kriptografi yaitu [9]:

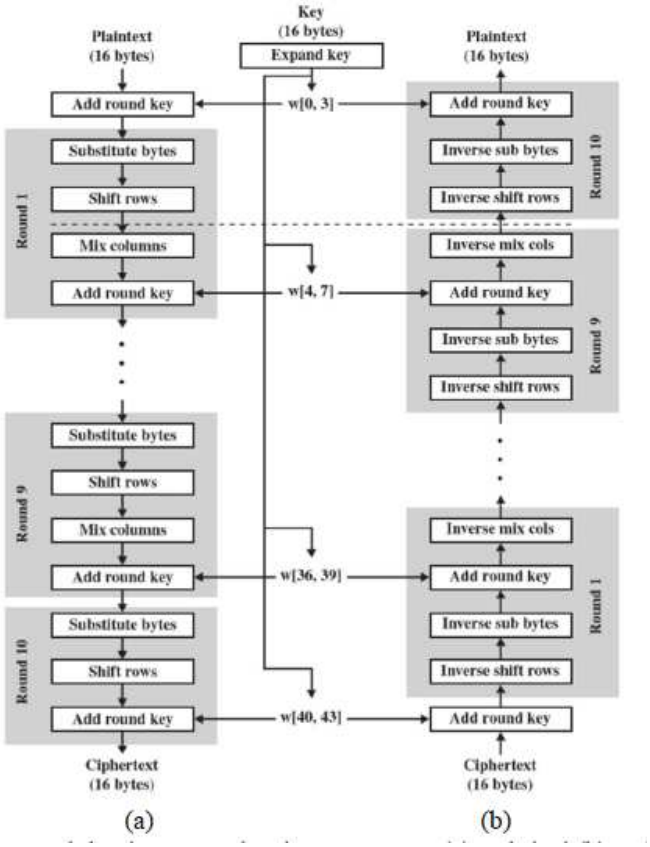
1. Plaintext, merupakan pesan atau data asli yang harus dijaga kerahasiaanya. Plaintext akan menjadi masukan algortima kriptografi untuk diubah menjadi ciphertext.
2. Ciphertext, merupakan pesan yang telah teracak yang dihasilkan sebagai keluaran dari algoritma enkripsi.
3. *Key* atau kunci, merupakan kunci yang digunakan sebagai masukan algoritma enkripsi atau dekripsi. Algoritma

enkripsi dan dekripsi menjalankan subtitusi dan transformasi bergantung pada *key* yang digunakan.

4. Enkripsi, merupakan algoritma yang menjalankan bermacammacam subtitusi dan transformasi berdasarkan key yang digunakan untuk mengacak pesan asli (plaintext). Keluaran dari algoritma enkripsi adalah ciphertext.
5. Dekripsi, merupakan algoritma enkripsi yang berjalan secara terbalik (*reverse*). Dalam kriptografi simetrik, algoritma dekripsi memerlukan key yang sama agar dapat mengembalikan ciphertext menjadi plaintext semula.

B. AES (Advanced Encryption Standard)

Advanced Encryption Standard atau AES merupakan algoritma kriptografi simetrik yang bersifat non-Feistel. Masing-masing blok proses yang digunakan dalam AES dapat dijalankan secara terbalik (*invertible*). Operasi yang digunakan dalam algoritma AES ada 4 yaitu *AddRoundKey, SubBytes, ShiftRows, MixColumns*. Proses secara lengkap algoritma AES ditunjukkan pada gambar 4.



Gambar 4. Blok Diagaram Algoritma AES 128 (a) Enkripsi (b) Dekripsi

Dari gambar 4 dapat dilihat bahwa sebelum *round* pertama, 1 blok data masuk proses *AddRoundKey* terlebih dahulu, proses ini sering disebut sebagai *initial round*. Kemudian pada *round* 1 sampai ronde ke Nr-1, dijalankan proses *SubBytes*, *ShiftRows, MixColumns,* dan *AddRoundKey*. Sedangkan pada *round* ke Nr (*Final Round*), prosesnya sedikit berbeda dengan round-round sebelumnya, yakni hanya dilakukan *SubBytes, ShiftRows*, dan *AddRoundKey* saja tanpa proses *MixColumns*. Proses tersebut dijalankan setiap 16 Bytes data untuk AES 128. Sedangkan untuk AES 192 setiap 24 Bytes data, dan AES 256 setiap 32 Bytes data. Proses sebaliknya dilakukan untuk mendekripsi. Proses initial round-nya adalah AddRoundKey, kemudian round pertama sampai round ke Nr-1 dijalankan proses *InvShiftRows, InvSubBytes, AddRoundKey*, dan *InvMixColumns*. Kemudian pada *round* ke Nr (Final Round) hanya dijalankan proses *InvShiftRows, InvSubBytes,* dan *AddRoundKey*.

C. Fungsi Hash MD5

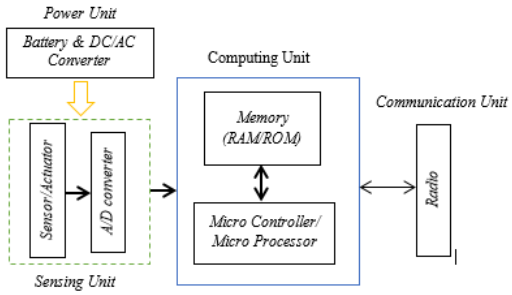
Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (*fixed*) [9]. Kegunaan dari *Hash function* dalam keamanan data adalah sebagai integritas data dan otentikasi. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Keluaran fungsi hash disebut juga nilai hash (*hash-value*) atau pesan-ringkas (*message digest*).

Algoritma MD5 adalah fungsi hash satu arah yang dibuat oleh Ron Rivest dan merupakan pengembangan dari algoritma MD4. Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan sebuah *message digest* dengan panjang 128 bit.

IV. GAMBARAN ARSITEKTUR DAN KERANGKA YANG DIUSULKAN

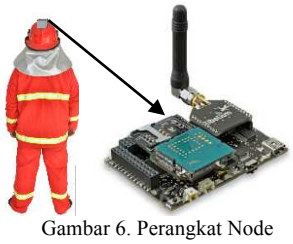
A. Perancangan Teknik Lokalisasi

Berdasarkan kemampuan dalam memperkirakan poisisi, ada dua jenis node: node yang memiliki koordinat posisi disebut node refrensi, biasanya lokasi node telah ditentukan sebelumnya. Node kedua disebut sebagai unknown node, ditempatkan secara acak pada daerah pengamatan. Arsitektur fundamental node sensor nirkabel , seperti yang diusulkan oleh [11] digambarkan pada Gambar 5. Ada empat unit dasar dalam node sensor nirkabel: *sensing unit, computing unit, communication unit and power unit*.



Gambar 5. Komponen yang Bekerja pada Sensor *Node*

Komponen dari perangkat *unknown node* ditunjukkan pada gambar 6.



Gambar 6. Perangkat Node

Waspmote merupakan perangkat elektronik buatan libelium yang bersifat open source terhadap pengembangan.

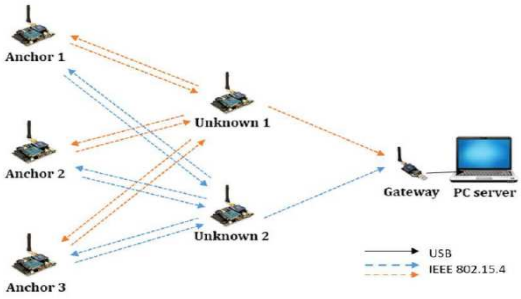
Perangkat waspmote menggunakan mikrokontroler ATmega 1281 sebagai otak untuk
mengolah tugas yang diberikan.

TABEL II. DATASHEET PERANGKAT WASPMOTE

Spesifikasi	Keterangan
Microcontroller	Atmega 1281
SRAM	8KB
EEPROM	4KB
FLASH	128KB
Dimensi/Uuran	7.35 x 51 x13 mm
Temparature Range	[-20°C , +65°C]
Konsumsi daya	ON: 9mA ; Sleep: 65 μA ; Deep Sleep: 62 μA
Inputs/Outputs	7 Analog (I), 8 Digtal (I/O), 1 PWM, 2 UART, 1 L2C, 1 USB.
Electrical Data	Battery voltage: 3.3 – 4.2 V

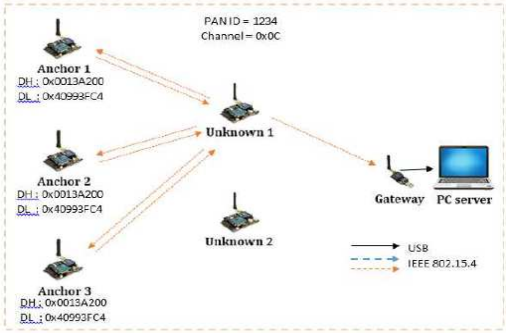
Komunikasi *anchor node* dan *unknown node* memanfaatkan perangkat ZigBee sebagai modul radio. Jenis Modul yang digunakan bekerja pada pita frekuensi ISM (Industrial, Scientific, and Medical) yaitu 2,4 GHz. IEEE 802.15.4 menetapkan terdapat 16 channel yang dapat digunakan pada pita frekuensi ISM 2,4 GHz. Suatu jaringan XBee biasa disebut dengan PAN (Personal Area Network). Setiap jaringan ditetapkan dengan sebuah PAN identifier (PAN ID) yang unik.

Pada design yang kami usulkan, metode routing sistem digambarkan pada gambar 7.



Gambar 7. Metode *Routing Sistem*

Metode routing dimulai dari unknown node menjalankan fungsi **SendRequest()** yaitu send data request ke semua anchor node dalam satu PAN ID yang sama. Selanjutnya, jika Anchor node menerima data request yang sesuai dengan inisialisasinya, maka anchor node mengirimkan paket data yang berisi informasi posisinya ke unknown node secara unicast dengan cara menyesuaikan alamat DL anchor node dan SL unknown node melalui fungsi ATDL 40C2923D command. Pada sisi unknown node, akan terjadi proses RSSI dan konversi data sinyal yang diterima menjadi jarak dilakukan pada fungsi **PerhitunganRSSI() dan PembacaanRefrensiRSSI()**. Selanjutnya memilih 3 anchor node berdasarkan jarak terdekat. Kemudian melakukan komputasi posisi unknown node menggunakan metode trilaterasi. Hasil dari komputasi tersebut, kemudian dibentuk satu paket data pada fungsi **AddPacketInfo()** dan dikirimkan ke server. Agar tidak terjadi collision data, maka unknown node memiliki kemampuan untuk mengubah PAN ID untuk menyesuaikan PAN ID server melalui fungsi **SwitchPAN()**. Untuk setting alamat DL, SL, dan PAN ID ditunjukkan pada gambar 8.



Gambar 8. Konfigurasi Pengalamatan Anchor node dan Unknown Node

Ketika *unknown node* akan mengirimkan paket data ke *server*, maka *unknown node* terlebih dahulu melakukan perubahan alamat DL agar sesuai dengan alamat DH gateway ATDL *command*.

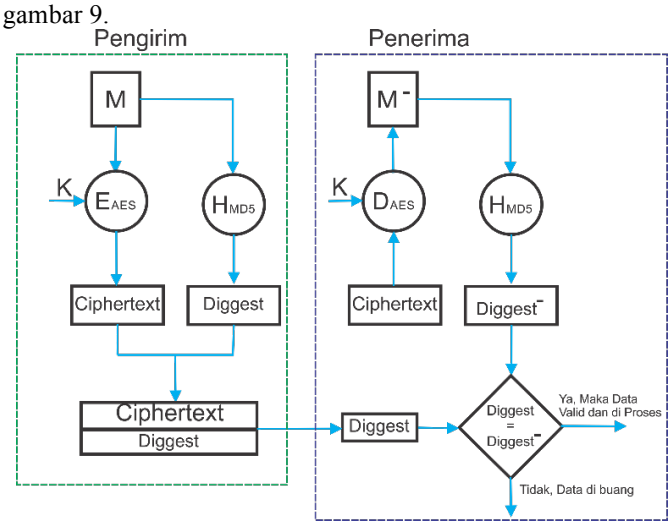
TABEL III. ALGORITMA TEKNIK LOKALISASI TERDISTRIBUSI

Algoritma Lokalisasi Terdistribusi
1: SendRequest()
2: p=PerhitunganRSSI()
3: z=PembacaanRefrensiRSSI()
4: epz=EvaluasiError(p,z)
5: while inBoundary do
6: SelectDistanceMeasurement()
7: if numberofReference >=3, then
8: CalculatePosition()
9: end if
10: AddPacketInfo()
11: SetDLGateway()
12: SendUnicast()
13: end while

Setelah paket dikirimkan ke server dengan fungsi **SendUnicast()**, Unknown node melakukan switch PAN ID nya kembali menjadi 221 untuk melakukan komputasi posisi kembali.

B. Perancangan Keamanan Data

Berikut konsep keamanan data dapat ditunjukkan pada gambar 9.



Gambar 9. Ilustrasi Keamanan Data

Secara garis besar keamanan data meliputi AES dengan *secret key* sebagai *confidentiality* (kerahasiaan) dan hash MD5 sebagai *integrity and authentication*. Pesan berupa frame data bersama dengan *key* menjadi input dari fungsi enkripsi AES sehingga menghasilkan ciphertext. Selanjutnya pesan juga menjadi input dari fungsi Hash MD5 sehngga menghasilkan message diggest. Hasil frame data setelah dilengkapi oleh sistem keamanan ditunjukkan pada gambar 10.

1	2	3	4	5	6	7
Header	@@	Ciphertext	@@	Diggest	@@	Tail

Gambar 10. Format Frame Data Setelah di Lengkapi Keamanan Data

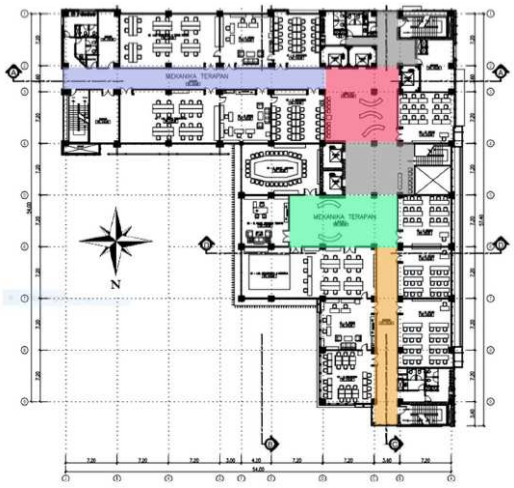
Pada sisi penerima, frame data diterima dan dilakukan *separated* frame data. Chipertext bersama *key* menjadi input fungsi dekripsi AES. *Key* yang digunakan harus sama dengan *key* yang digunakan saat enkripsi. Hasil dari proses dekripsi berupa plaintext. Plaintext tersebut menjadi input fungsi hash MD5 sehingga menghasilkan *diggest*. Hasil *diggest* di bandingkan dengan *diggest* dari frame data yang diterima. Jika hasil perbandingan menunjukkan nilai yang sama, maka data dapat dikatakan valid. Jika tidak sama, maka data bisa dianggap tidak berasal dari pihak yang semestinya.

V. HASIL PENGUJIAN DAN DISKUSI

Ada tiga skema pengukuran yang telah dilakukan. Pertama, kami mengukur kekuatan sinyal untuk mencapai pemodelan karakteristik lingkungan observasi. Kedua, kami melakukan lokalisasi/perkiraan posisi *unknown node* dengan menerapkan kerangka sistem lokalisasi terdistribusi. Dan ketiga, kami melakukan uji ketahanan sistem keamanan terhadap serangan-serangan yang mungkin dilakukan oleh pihak ketiga atau *Man in the middle attack*.

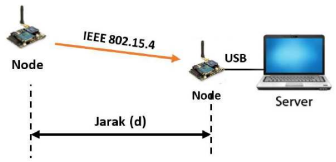
A. Pengujian Kuat Sinyal/RSSI

Pada percobaan pertama, kami meletakkan sepasang *node* yang merupakan *anchor node* dan *unknown node*. Lingkungan observasi ditampilkan pada gambar 11.



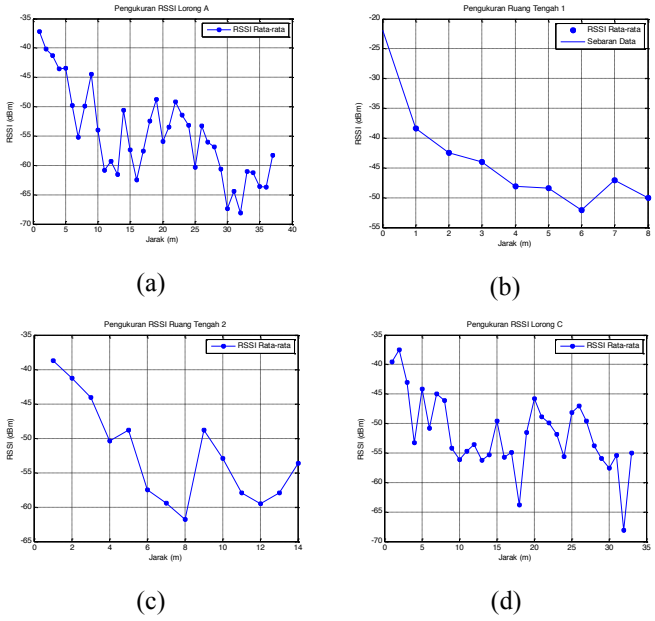
Gambar 11. Lokasi Area Pengukuran

Anchor node mengirimkan karakter ASCII ke *unknown node*. Kemudian di *Unknown node* mengolah karakter yang diterima menjadi kuat sinyal melalui ATDB *command*. Hasil kuat sinyal berupa bilangan heksadesimal akan dikonversi menjadi bilangan desimal. Jarak antar node pengirim dan penerima dibuat secara logaritmik. Pengukuran diulang selama 10 kali dalam posisi yang sama.



Gambar 12. Skenario Pengukuran Pemodelan Karakteristik Lingkungan

Kami juga menggunakan waspmote untuk memvalidasi data pengukuran hasil dari pengembangan prototipe node. Pada gambar 11 ruangan gedung pascasarjana lantai 3 PENS dibagi menjadi 4 area. 4 area tersebut diberi tanda dengan warna yang berbeda. Warna biru adalah pada area lorong A, warna merah pada area ruang tengah 1, warna hijau pada area ruang tengah 2, dan warna kuning pada area lorong C. Pengukuran dilakukan dengan skenario 1 pada keempat area tersebut. Percobaan hasil dari kekuatan sinyal yang diterima di berbagai jarak dari pengukuran digambarkan sebagai grafis pada gambar 13.



Gambar 13. Hasil Pengukuran RSSI (a) Lorong A, (b) Ruang Tengah 1, (c) Ruang Tengah 2, (d) Lorong C

Pada gambar 13, semakin jauh perpindahan jarak antar node, maka kuat sinyal yang diterima semakin kecil. Dengan menggunakan persamaan (4), berdasarkan hasil rata-rata nilai RSSI maka di dapatkan nilai *exponent path loss* (n) sebagai berikut

TABEL IV. HASIL PERHITUNGAN EXPONENT PATH LOSS

Area	n (Exponent Pathloss)
Lorong A	1,63545
Ruang tengah 1	1,73121
Ruang tengah 2	1,77563
Lorong C	1,04918

Dari hasil perhitungan *exponent path loss* untuk lorong A, ruang tengah 1 dan ruang tengah 2 memiliki nilai yang sesuai dengan tabel 1. Dimana nilai *exponent path loss* pada kondisi LOS

dalam ruangan adalah berkisar antara 1,6 sampai 1,8. Sedangkan nilai *exponent path loss* yang didapatkan nilainya masih mendekati range tersebut. Hal ini dapat disebabkan karena nilai RSSI hasil pengukuran pada lorong C bersifat fluktuatif pada jarak-jarak tertentu.

B. Pengujian Estimasi Posisi Unknown Node

Setelah mendapatkan nilai *exponent path loss*, maka dapat digunakan untuk menentukan komputasi posisi dengan persamaan (6). Berikut ini sample Pengujian dilakukan pada area ruang tengah 2 yang berukuran 15,6 x 7,2 meter. Pengujian ini dilakukan pada tanggal 31 desember 2015 pukul 10.00 di gedung Pasca Sarjana PENS. Berikut adalah koordinat posisi anchor node yang di letakkan pada area pengujian.

Anchor node 1 : (3,6 , 1)

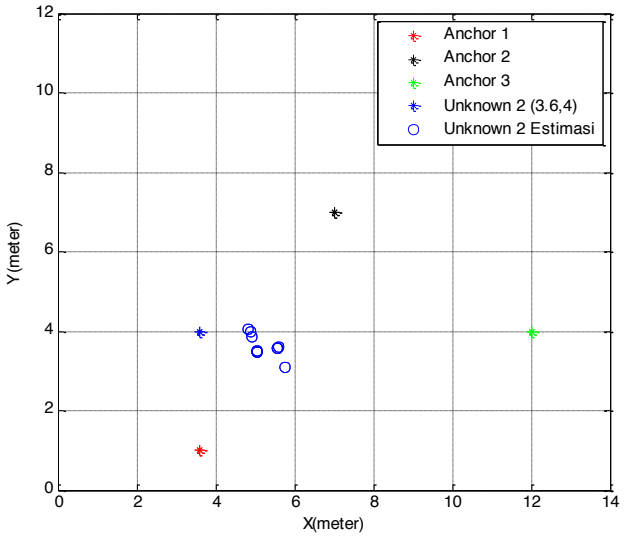
Anchor node 2 : (7, 7)

Anchor node 3 : (12, 4)

Pengujian dilakukan selama 10 kali pada posisi yang sama ditunjukkan pada tabel 5.

TABEL V. PENGUJIAN ESTIMASI POSISI UNKNOWN NODE

	RSSI1 (dBm)	RSSI2 (dBm)	RSSI3 (dBm)	d1 (m)	d2 (m)	d3 (m)	X(m) 3.6	Y(m) 4	MSE (meter)
1	-48	-55	-65	0.706	1.752	6.408	4.831	4.051	0.857
2	-51	-57	-65	1.043	2.27	6.408	4.93	3.87	1.09
3	-50	-59	-65	0.916	2.943	6.408	5.052	3.488	1.581
4	-50	-56	-65	0.916	1.994	6.408	4.877	3.977	0.944
5	-51	-56	-64	1.043	1.994	5.629	5.587	3.596	0.957
6	-50	-56	-64	0.916	1.994	5.629	5.577	3.58	0.886
7	-50	-56	-64	0.916	1.994	5.629	5.577	3.58	0.886
8	-51	-59	-65	1.043	2.943	6.408	5.061	3.503	1.54
9	-50	-59	-64	0.916	2.943	5.629	5.752	3.091	0.825
10	-50	-59	-65	0.916	2.943	6.408	5.052	3.488	1.581



Gambar 14. Estimasi Posisi *Unknown Node* Pada Ruang Tengah 2

Dari hasil pengujian tersebut, nilai MSE terbesar diperoleh pada percobaan ke-3 dan ke-10 yaitu sebesar 1,581 meter. Posisi hasil estimasi nya adalah x = 5,052m dan y = 3,488m. Sedangkan nilai MSE terkecil adalah pada percobaan ke-9 yaitu sebesar 0,825 meter, hasil estimasinya adalah x = 5,752m dan y = 3,488m. Dari 10 percobaan estimasi posisi unknown node pada ruang tengah 2 diperoleh rata-rata MSE sebesar 1,115 meter.

Dari pengujian estimasi posisi menggunakan unknown node 1 dan unknown node 2 diperoleh rata-rata nilai MSE untuk masing-masing lokasi adalah seperti pada tabel 6.

TABEL VI. PERBANDINGAN NILAI MSE PADA LOKASI PENGUJIAN

Lokasi Pengujian MSE	MSE (Unknown Node 1)	MSE (Unknown Node 2)
Ruang Tengah 1	1,008 meter	0,567 meter
Ruang Tengah 2	0,486 meter	1,115 meter
Lorong C	2,892 meter	1,431 meter
Lorong A	7,322 meter	9,284 meter
Rata-rata	2,927 meter	3,099 meter

C. Pengujian Keamanan Data

Sistem keamanan yang digunakan pada komunikasi antara node ke node dan antara node ke PC server adalah menggunakan algoritma AES-128. Panjang kunci yang digunakan oleh AES-128 adalah sebesar 16 byte. Kunci tersebut diambil dari variabel karakter dimana setiap karakternya berukuran 1 byte, sehingga kunci yang diperlukan adalah sepanjang 16 karakter.

TABEL VII. ENKRIPSI DATA ESTIMASI POSISI UNKNOWN NODE

Plaintext	Ciphertext	Waktu Enkripsi
Unknw1@8.225@0.959@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	34BBDF3769EE96809CC89FDB4 69C269E9B2CE24C92A7B41DEA 08508ABE65129FCB56B682A8C6 96D34852D41818FB864C4EAA41 71C8870D0F1BF6D3C8157ABAA3	6 ms
Unknw1@8.198@0.914 @A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	D6174E8B7C62C711F6AF59AE3B 7C10590FFC96846350F813528FD 20DBC188B4CCB56B682A8C696D 34852D41818FB864C4EAA4171C8 870D0F1BF6D3C8157ABAA3	7 ms
Unknw1@8.664@0.390@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	DAC759DDEF87D81B1E6F80DD8 27B14139CB74ED012AF38ED228 0FA88F1762726CB56B682A8C696 D34852D41818FB864C4EAA4171 C8870D0F1BF6D3C8157ABAA3	6 ms
Unknw1@7.921@1.691@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	B2B39A8658565DF3DF9DA91C45 DE1349EC0FE139A23DBD45309C B3E61C97CD63CB56B682A8C696 D34852D41818FB864C4EAA4171C 8870D0F1BF6D3C8157ABAA3	7 ms
Unknw1@7.987@1.653@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	671105C5B6ABEE7954CA339C91 4CD60C650B2BFC1962685898BF6 11DBA2DBB19CB56B682A8C696 D34852D41818FB864C4EAA4171C 8870D0F1BF6D3C8157ABAA3	6 ms
Rata-rata		6,4 ms

TABEL VIII. DEKRIPSI DATA ESTIMASI POSISI UNKNOWN NODE 1

Ciphertext	***Plaintext***	**Waktu Dekripsi**
34BBDF3769EE96809CC89FDB469C 269E9B2CE24C92A7B41DEA08508 ABE65129FCB56B682A8C696D348 52D41818FB864C4EAA4171C8870D 0F1BF6D3C8157ABAA3	Unknw1@8.225@0.959@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	1 ms

Ciphertext	*Plaintext*	Waktu Dekripsi
0590FFC96846350F813528FD20DBC 188B4CCB56B682A8C696D34852D41 818FB864C4EAA4171C8870D0F1BF6 D3C8157ABAA3	Unknw1@8.198@0.914@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	1 ms
DAC759DDEF87D81B1E6F80DD827B 14139CB74ED012AF38ED2280FA88F1 762726CB56B682A8C696D34852D4181 8FB864C4EAA4171C8870D0F1BF6D3 C8157ABAA3	Unknw1@8.664@0.390@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	1 ms
B2B39A8658565DF3DF9DA91C45D E1349EC0FE139A23DBD45309CB3 E61C97CD63CB56B682A8C696D348 52D41818FB864C4EAA4171C8870D 0F1BF6D3C8157ABAA3	Unknw1@7.921@1.691@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	1 ms
671105C5B6ABEE7954CA339C914C D60C650B2BFC1962685898BF611DB A2DBB19CB56B682A8C696D34852 D41818FB864C4EAA4171C8870D0F 1BF6D3C8157ABAA3	Unknw1@7.987@1.653@ A1@3.599@1.000@ A2@7.000@7.000@ A3@12.00@4.000#	1 ms
Rata-rata		1 ms

Pada proses enkripsi, plaintext dan key merupakan input proses enkripsi menghasilkan ciphertext yang merupakan pesan acak yang akan dikirimkan. Waktu yang dibutuhkan dalam proses enkripsi rata-rata selama 6.4 ms. Sedangkan waktu yang dibutuhkan proses dekripsi rata-rata selama 1 ms. Proses komputasi dekripsi lebih cepat dikarenakan dekripsi dilakukan di PC server.

TABEL IX. OTENTIKASI DATA ESTIMASI POSISI UNKNOWN NODE

h'	h	Waktu Eksekusi (ms)	Keterangan
AA87C4AA86BBEE7 4BBB69DB32CFB0965	AA87C4AA86BBEE7 4BBB69DB32CFB0965	4	Valid
D129367006958EAF6 225DEA144B2706B	D129367006958EAF6 225DEA144B2706B	4	Valid
1F2264EF5ED664C8D 25E07FC0F238314	1F2264EF5ED664C8D 25E07FC0F238314	4	Valid
D16220748E3B8FB6D 3578D76778AA653	D16220748E3B8FB6D 3578D76778AA653	4	Valid
E99B8DCFAFD95F379 C431BA35CD0856E	E99B8DCFAFD95F379 C431BA35CD0856E	4	Valid

Proses otentikasi berfungsi untuk memvalidasi data. Hal ini dilakukan supaya data yang diterima merupakan data yang berasal dari pihak yang diharapkan. Waktu proses otentikasi rata-rata selama 4 ms.

TABEL X. WAKTU EKSEKUSI RATA-RATA PROGRAM UNKNOWN NODE

Proses	Waktu Eksekusi
Inisialisasi	161 ms
Kriptografi antar *node*	8,64 ms
Kriptografi *node* dengan *server*	11,48 ms
Pengiriman data	185,24 ms
Estimasi Jarak	1 ms
Trilaterasi	1 ms
Waktu Total	384,40 ms

Setiap *unknown node* bergerak, akan terjadi komputasi posisi yang melibatkan peristiwa komunikasi antara anchor node, unknown node, hingga ke server. Rata-rata unknown node membutuhkan waktu 384,40 ms untuk melakukan estimasi posisi. Dalam proses estimasi posisi, perangkat menunjukkan hasil yang cukup baik dengan rata-rata MSE error sebesar 2 hingga 4 meter.

VI. KESIMPULAN

Pada pekerjaan ini, kami mengusulkan kerangka kerja sistem lokalisasi node yang dilengkapi sistem keamanan data dan mengembangkannya sebagai prototipe dengan memanfaatkan perangkat waspmote. Selama pengujian estimasi lokasi, hasil menunjukkan kinerja yang cukup baik. Selama pengujian sistem keamanan data, hasil menunjukkan kinerja yang cukup cepat dan aman jika *man in the midle attack* tidak memiliki kunci. Meskipun man in the midle attack mengirimkan pesan yang menyerupai pesan sesungguhnya, sistem tetap aman karena terdapat fitur otentikasi data yang menggunakan fungsi has MD5.

Kekurangan dalam sistem yang kami usulkan terletak pada penentuan exponent pathloss sebagai karakteristik lingkungan yang dapat membuat error estimasi posisi. Oleh karena itu, di masa penentuan posisi unknown node hendaknya menempatkan anchor node di lokasi yang tidak terhalang oleh object tertentu sehingga mampu meminimalkan error untuk pengembangan selanjutnya.

UCAPAN TERIMA KASIH

Para penulis ingin mengucapkan terima kasih kepada rekan-rekan mahasiswa PENS yang fokus di bidang lokalisasi node untuk kerja sama dalam membantu perancangan prototipe dan melakukan pengujian hingga mendapatan data experiment..

DAFTAR PUSTAKA

[1] Putra, Bimantara Kesatria, "*Analisa dan Evaluasi Secure Localization Indoor Menggunakan Platform Jaringan Sensor Waspmote*", Proyek Akhir, PENS-ITS, 2016.

[2] S. Singh, Ravi Shakya, Yaduvir Singh, "Localization Techniques in Wireless Sensor Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 844-850.

[3] Amitangshu Pal, "Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges", Network Protocols and Algorithms ISSN 1943-3581, 2010, Vol. 2, No. 1.

[4] P. Kristalina, Wirawan, Gamantyo H., "DOLLY: An Experimental Evaluation of Distributed Node Positioning Framework in Wireless Sensor Networks", IEEE Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore 2014.

[5] Nabil Ali Alrajeh, Maryam Bashir, and Bilal Shams, "Localization Techniques in Wireless Sensor Networks",International Journal of Distributed Sensor Networks Volume 2013 (2013).

[6] Azzedine Boukerche, Horacio A. B. F. Oliviera, Eduardo F. Nakamura, Antonio A. F. Loureiro, "Secure Localization Algorithm for Wireless Sensor Networks", IEEE Communication Magazine, 2008.

[7] Nebe S.U., "Pathloss Prediction Model of a Wireless Sensor Network in an Indoor Environment", IJAREEIE, September 2014.

[8] Okumbor N. Anthony and Raphael, "Characterization of Signal Attenuation using Pathloss Exponent in South-South Nigeria",International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume 3, Issue 3, May – June 2014

[9] J Stallings, Willian dan Lawrie Brown, Computer Security Principles and Practice Second Edition, United States of America, 2012.

[10] R. Roshdy, M. Fouad, M. Aboul-Dahab, "Design and Implementation a New Security Hash Algorithm Based on MD5 and SHA-256", International Journal of Engineering Sciences & Emerging Technologies, August 2013.

[11] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.

[12] JerilKuriakose, Sandeep Joshi and V.I. George, "Localization in Wireless Sensor Networks: A Survey", CSIR Sponsored X Control Instrumentation System Conference - CISCON-2013.

[13] Amitangshu Pal, "Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges", Network Protocols and Algorithms ISSN 1943-3581, 2010, Vol. 2, No. 1.