P-12

TESTBED SECURE INDOOR LOCALIZATION SYSTEM MENGGUNAKAN *CLUSTER BASED PATHLOSS EXPONENTIAL* UNTUK ESTIMASI POSISI DI LINGKUNGAN *INDOOR* PADA *WIRELESS SENSOR NETWORK*

TESTBED SECURE INDOOR LOCALIZATION SYSTEM USING CLUSTER BASED PATHLOSS EXPONENTIAL FOR INDOOR POSITIONING SYSTEM IN WIRELESS SENSOR NETWORK

Cindha Riri Pratiwi[1*], Prima Kristalina[2], Amang Sudarsono[3]
[1]Sekolah Tinggi Teknologi Bontang, Jalan Raya S.Parman, Bontang
[2-3]Politeknik Elektronika Negeri Surabaya, Jalan Raya ITS, Surabaya

[*]E-mail: akucindha@gmail.com

Diterima 05-09-2018	Diperbaiki 12-11-2018	Disetujui 03-012-2018

ABSTRAK

Jaringan Sensor Nirkabel menjadi salah satu topik yang banyak di teliti akhir-akhir ini, baik untuk aplikasi indoor positioning system (IPS), tracking object dan monitoring system. Akan tetapi, upaya yang dilakukan untuk menghasilkan nilai akurasi yang lebih baik pada IPS menggunakan received signal strength value masih belum optimal. Selain itu, ketika terjadi proses pengiriman data dari satu perangkat ke perangkat lainnya, data yang diterima perlu untuk dijaga keaslian dan kerahasiaanya. Dengan demikian pada IPS diperlukan penambahan skenario Secure Indoor Localization System (SI-LOCS) untuk menjaga kerahasiaan informasi saat proses pengiriman data berlangsung. Pada penelitian ini dilakukan analisa SI-LOCS dengan Raspberry PI 3 menggunakan Cluster Based Pathloss Exponential (CBPLE) untuk meningkatkan nilai akurasi dari proses estimasi posisi menggunakan received signal strength value serta Algoritma Security AES 128 dan MD5 Hash Function. Hasil pengujian menunjukkan bahwa nilai akurasi pada Indoor Positioning System menggunakan CBPLE sebesar 99,89 % sementara jika dibandingkan dengan skenario sebelumnya tanpa menggunakan CBPLE sebesar 93,85%. Algoritma security yang digunakan untuk mengamankan data posisi dari node-node referensi dan node objek saat proses pertukaran data menunjukkan performansi yang memuaskan serta telah memenuhi persyaratan confidentiality dan data integrity. Diharapkan SI-LOCS dapat diimplementasikan untuk berbagai aplikasi IPS.

Kata kunci: Indoor Positioning System, Cluster Based, Pathloss Exponential, Algoritma Sekuriti

ABSTRACT

Wireless Sensor Network has become one of the topics that has been researched lately, both for indoor positioning system applications (IPS), tracking objects and monitoring systems. However, efforts made to produce better accuracy values on IPS using the received signal strength value are still not optimal. In addition, when the process of sending data from one device to another device, the data received needs to be maintained in its originality and confidentiality. Thus, the IPS required the addition of a Secure Indoor Localization System (SI-LOCS) scenario to maintain the confidentiality of information during the data transmission process. In this study, SI-LOCS analysis with Raspberry PI 3 was conducted using Cluster Based Pathway Exponential (CBPLE) to increase the accuracy value of the position estimation process using received signal strength values and AES 128 and MD5 Hash Function Security Algorithms. The test results show that the accuracy of the Indoor Positioning System uses a CBPLE of 99.89% while compared to the previous scenario without using CBPLE of 93.85%. The security algorithm used to secure position data from reference nodes and object nodes when the data exchange process shows satisfactory performance and has fulfilled the requirements of confidentiality and data integrity. It is expected that SI-LOCS can be implemented for various IPS applications.

Keywords:Indoor Positisoning System, Cluster Based, Pathloss Exponential, SecurityAlgorithm

PENDAHULUAN

Wireless Sensor Network saat ini banyak digunakan dalam berbagai aplikasi-aplikasi baik pada lingkungan *outdoor* maupun lingkungan *indoor*. Seiring berjalannya waktu, WSN lebih banyak dipergunakan untuk *monitoring system* di lingkungan *indoor* seperti pada pasien di sebuah rumah sakit, personel pemadam kebakaran, polisi maupun *tracking object* bergerak seperti hewan peliharaan dan deteksi sumber api maupun kebocoran gas di sebuah gedung [1]-[3].

Hal ini dikarenakan, pada lingkungan *outdoor*, *positioning system* dapat menggunakan informasi yang diperoleh melalui Global Positioning System (GPS) untuk menunjukkan posisi dari objek, namun pada lingkungan *indoor* GPS tidak dapat dipergunakan untuk mendeteksi lokasi dari objek tersebut, sehingga untuk medapatkan estimasi posisi dari sebuah objek pada lingkungan *indoor* dapat dilakukan dengan algoritma *range based* [4]-[5] dan algoritma *range free* [6]-[7]. Dimana algoritma *range based* menggunakan estimasi jarak atau estimasi sudut dalam proses estimasinya, sementara pada aloritma *range free* terdapat 2 komponen utama yakni *unknown node* dan *anchor node*. *Anchor node* akan menunjukkan posisi sebenarnya sehingga *unknown node* dapat memperoleh informasi berupa posisi dari *anchor node* dan nilai kuat sinyal untuk kemudian dicari jarak estimasi dari *anchor node* dan *unknown node*. Kemudian pada tahap akhir, jarak estimasi yang telah diperoleh akan dibandingkan dengan jarak sesungguhnya untuk mendapatkan posisi estimasi dari *unknown node* terhadap beberapa *anchornode*. Berikut ini beberapa *ranging method* pada lokalisasi menggunakan estimasi jarak ataupun estimasi orientasi, diantaranya RSSI [8]-[9], ToA [8][10], TDOA [8][11] dan AoA [8][12].

Penelitian sebelumnya yang berjudul SCLoc [13] pada lingkungan *indoor* menggunakan *received signal strength* antara *anchor node* dengan *unknown node* untuk kemudian diperoleh estimasi jarak, kemudian dengan menggunakan metode trilaterasi diperoleh posisi estimasi dari *unknown node* tersebut. Untuk mengamankan proses pertukaran data antara *anchor node* dan *unknown node* dipergunakan algoritma sekuriti AES 128 dimana platform ini menggunakan perangkat Waspmote. Proses komunikasi antar *anchor node* dengan *unknown node*merupakan proses komunikasi secara *peer to peer*menggunakan Zigbee radio modul. Kelemahan dari SCLoc platform terletak pada akurasi dari nilai estimasi posisi yang dihasilkan, mengingat bahwa estimasi posisi menggunakan *received signal strength* pada lingkungan *indoor* sangat dipengaruhi oleh kondisi lingkungan pengamatan dan material penyusunnya, sehingga mengakibatkan permasalahan pada *signal reflection, attenuation and absorption.*

Fluktuasi *received signal strength* pada lingkungan pengamatan [14] memiliki pengaruh yang cukup besar terhadap nilai estimasi jarak menggunakan *received signal strength*. Dengan demikian pada lingkungan *indoor* diperlukan metode untuk memperbaiki nilai estimasi jarak menggunakan *Cluster Based Pathloss Exponential* (PLE)[15].

Pada penelitian ini, kami melakukan pengujian*Secure Indoor Localization System*menggunakan *Cluster Based* PLE untukestimasi posisi di lingkungan *indoor*pada WSN. Platform ini diharapkan dapat dipergunakan untuk *secure monitoring system* pada objek bergerak seperti pemadam kebakaran, pekerja pada oil and gas serta pasien rumah sakit. *Testbed* dilakukang menggunakan *Raspberry pi 3* untuk menguji waktu komputasi dan waktu transmisi dari metode security AES *(Advanced Encrypted System)* 128 bit dengan *hash function* MD5. Dari hasil pengujian yang dilakukan penambahan metode security pada *indoor positiong system* tidak mengakibatkan penurunan performasi pada system, sementara dengan menambahkan *Cluster Based* PLEpada metode estimasi posisi multilaterasi diperolehnilai estimasi posisi sebesar 97,36 %.

Penelitian ini terdiri dari beberapa bagian yakni pendahuluan yang dijelaskan di awal bagian membahas tentang *state of art* dari penelitian ini, kemudian di bagian selanjutnya pembahasan metodologi penelitianmeliputi metode pengumpulan data, pengujian, pengolahan dan penarikan kesimpulan serta cara melakukan penhujian, selanjutnya di bagian ketiga dilakukan pembahasan pada hasil penelitian serta analisa singkat terkait hasil penelitian. Di akhir bagian, penulis akan membuat kesimpulan dan rencana terkait kelanjutan dari penelitian ini.

METODOLOGI

Metodologi penelitian meliputi metode pengumpulan data, studi lapangan dan pengujian yakni sebagai berikut:

1) Studi Pustaka
Studi pustaka dalam penelitian ini berasal dari literatur-literatur penelitian yang ada hubungannya dengan penelitian ini.

2) Studi lapangan
Melakukan observasi atau pengamatan tentang implementasi metode keamanan pada *raspberry pi 3* dalam proses komunikasi menggunakan socket programming dan melakukan pengamatan tentang pengaruh metode cluster based PLE terhadap peningkatan nilai akurasi.

3) Pengujian *(Testbed System)*
Melakukan pengujian sistem dengan melihat waktu transmisi, waktu enkripsi dan waktu deskripsi pada sistem tanpa penyerang dan dengan penyerang.

Setelah dilakukan proses pengujian maka, data akan di analisa berdasarkan data hasil pengujian yang meliputi waktu transmisi, waktu enkripsi dan waktu deskripsi serta berapa prosentase keberhasilan saat dilakukan pengujian dengan *attacker* (penyerang). Berikut ini tahapan dalam proses analisa sistem:

a. Pengujian Sistem
Meliputi pembuatan *node anchor, node unknown, gateway* dan juga *security+hash function* pada ketiga perangkat yang terlibat.

b. Rekapitulasi Data Pengujian Sistem
Meliputi pencatatan nilai kuat sinyal antar 2 node dengan jarak sama, pencatatan nilai kuat sinyal antar 2 node dengan jarak berbeda dan pencatatan nilai kuat sinyal dengan scenario cluster based PLE, pencatatan waktu transmisi antara 2 node, kemudian pencatatan waktu enkripsi pada *node anchor* danpencatatan waktu dekripsi pada *node unknown*.

c. Penarikan Kesimpulan
Keseluruhan hasil akan dituangkan ke dalam laporan hasil penelitian dan dituangkan kedalam artikel ilmiah.

Perangkat keras yang dibutuhkan dalam penelitian ini adalah 1 buah komputer, 3 buah Raspberry Pi 3, Monitor HDMI dengan spesifikasi sebagai berikut :

1. Komputer :
   - Intel Pentium Core I3
   - Memori RAM kapasitas 2 GB
   - Hardisk 500 GB
   - Monitor
   - Mouse&Keyboard USB

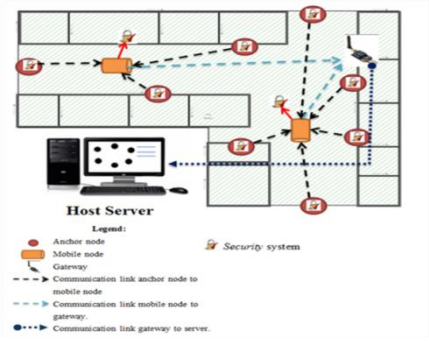
2. Raspberry Pi 3 :
   - SoC : Broadcom BCM2837
   - CPU : 4x ARM Cortex-A53, 1.2 GHz
   - GPU : Broadcom VideoCore IV
   - RAM : 1 GB LPDDR2 (900 MHz)
   - Networking : 10/100 Ethernet, 2.4 GHz 802.11n wireless
   - Bluetooth : Bluetooth 4.1 Classic, Bluetooth Low Energy
   - Storage : MicroSD
   - GPIO: 40-pin header, populated
   - Ports : HDMI, 3.5 mm analogue audio-video jack, 4x USB 2.0, Ethernet, Camera Serial Interface (CSI), Display Seriaal Interface (DSI).

3. Monitor Sharp Aquos LC-24LE170I
   - Port : HDMI dan USB

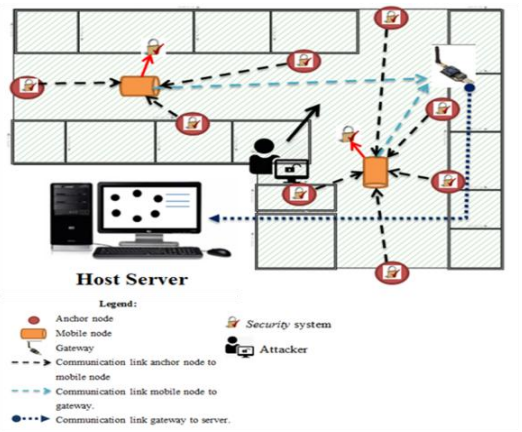
Kemudian untuk menujang pembuatan aplikasi dalam penelitian ini diperlukan juga beberapa perangkat lunak seperti ;

- Komputer sistem operasi Windows 7 atau 8
- OS Rasbian
- Wireshark
- Bahasa Pemrograman
  Bahasa pemrograman yang digunakan dalam pembuatan aplikasi adalah Bahasa C dan Library Security.

Adapun gambaran umum proses pengujian untuk *Testbed Secure Indoor Localization Sistem* menggunakan *Cluster Based PLE* untuk Estimasi Posisi di Lingkungan *Indoor* pada *Wireless Sensor Network*adalah seperti yang terdapat pada gambar 1 dan gambar 2 dibawah ini



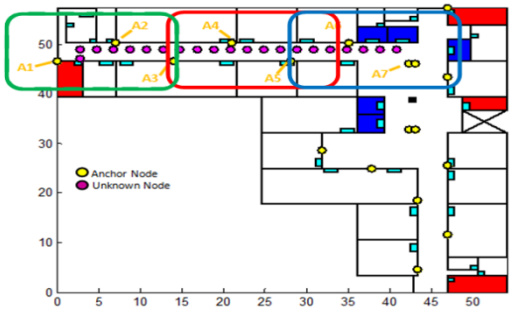
Gambar 1. Skenario Pengujian *Secure Indoor Localization System* tanpa menggunakan *attacker* (penyerang)



Gambar 2. Skenario pengujian*Secure Indoor Localization System* dengan menggunakan *attacker* (penyerang)

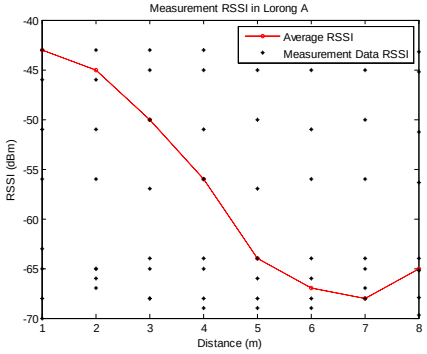
HASIL DAN PEMBAHASAN

Skenario peletakkan *Anchor Node* dan *Unknown Node* pada lingkungan pengamatan ditunjukkan pada gambar 3 di bawah ini. Pengukuran nilai kuat sinyal seperti gambar 3 dibawah ini dilakukan di Gedung Pascasarjana PENS Lantai 3. Pada scenario ini, digunakan 18 *Anchor Node*yang diletakkan di koordinat-koordinat tertentu sesuai Gambar 3 dan *Unknown Node* yang bergerak dari titik pertama hingga titik ke 21 dengan jarak perpindahan dari titik pertama ke titik selanjutnya sebesar 2 meter.



Gambar 3. Skenario Peletakkan *Anchor Node* dan *Unknown Node*

Selanjutnya dilakukan pengukuran nilai RSSI terhadap fungsi jarak di area berwarna hijau, merah dan biru, kemudian diperoleh sebaran nilai RSSI terhadap fungsi jarak yang ditunjukkan pada Gambar 4 dimana perubahan jarak memiliki pengaruh terhadap nilai RSSI yang didapatkan. Semakin besar jarak antara *anchor node* dan *unknown node* maka nilai RSSI yang didapatkan juga semakin besar. Akan tetapi pada titik-titik pengamatan tertentu, nilai RSSI yang didapatkan terkadang tidak konstan mengalami penurunan, Hal ini diakibatkan oleh kompleksitas dari area pengukuran yang memiliki dinding rapat kombinasi antara batu bata dan kaca sehingga kemungkinan terjadinya *multipath fading*. Anomali ini yang mengakibatkan pengerjaan penelitian ini memiliki kompleksitas yang sangat tinggi, dikarena jika besarnya nilai RSSI yang diperoleh tidak sesuai dengan yang seharusnya maka akan berakibat pada kesalahan estimasi jarak yang dihasilkan. Oleh karena itu, untuk menyelesaikan permasalahan tersebut, pada penelitian ini kami menguji 4 metode untuk memperoleh nilai koefisien path loss. Keempat metode tersebut adalah nilai koefisien path loss hasil regresi linier, nilai koefisien path loss kondisi 1 (per anchor node) kondisi 2 (sub cluster) dan kondisi 3 (cluster).



Gambar 4. Grafik Pengukuran jarak terhadapNilai RSSINilai RSSI di Lorong A

Pengamatan dengan kondisi 1 menghasilkan nilai koefisien path loss dari anchor yang terpasang seperti pada Gambar 3.Kemudian untuk menghitung masing-masing koefisien pathloss (n) pada setiap anchor, diperlukan pengukuran nilai RSSI *anchor node* terhadap *unknown node*.Sehingga diperoleh nilai koefisien pathhlos pada anchor 1, anchor 2 dan anchor 3 untuk titik 1-7 (area 1 pada Lorong A) kemudian anchor 3, 4 dan 5 untuk titik 8-14 dan seterusnya seperti pada Tabel 1 dibawah ini.

Tabel 1.Nilai Koefisien Path loss Kondisi 1

Anchor	n1(koef path loss kondisi real)	n2 (koef path loss kondisi chamber)	Nilai koef path loss rata-rata
1	1,38227	1,189462	1,285866
2	1,753125	4,534681	3,143903
3	1,281218	1,493506	1,387362
3.1	2,092367	2,494722	2,293544
4	1,600513	3,234614	2,417563
5	0,912555	1,168296	1,040426
5.1	1,503675	2,352547	1,928111

6	3,472792	3,563745	3,518269
7	1,802321	2,69173	2,247026

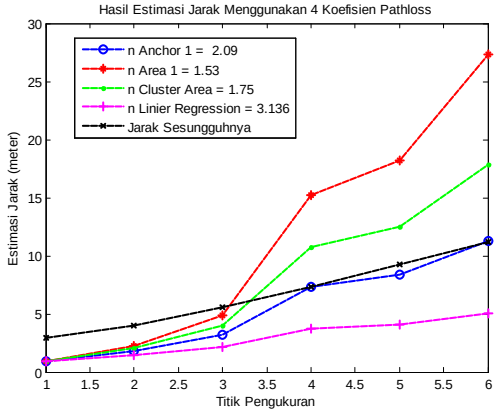
Pada Kondisi 2, merujuk pada nilai koefisien pathloss per anchor node (Kondisi 1) yang ditunjukkan oleh Tabel 1, kemudian dihitung nilai koefisien pathloss per *sub cluster* (Kondisi 2) dengan mencari nilai rata-rata koefisien pathloss per *anchor* yang terdapat pada Gambar 3 dimana *sub cluster* area 1 ditunjukkan dengan warna hijau, *sub cluster* area 2 ditunjukkan dengan warna merah dan *sub cluster* area 3 ditunjukkan dengan gambar biru. Nilai koefisien pathloss Kondisi 2 (Sub Cluster dapat dilihat pada Tabel 2 dibawah ini.

Tabel 2. Nilai Koefisien Path Loss Kondisi 2 (Sub Cluster) dan Kondisi 3 (Cluster)

Area	**Anchor**	**n1**	**n1 sub cluster**	**n1 Cluster**
Area 1	1	1,38227	1,472204	1,7556484
	2	1,753125		
	3	1,281218		
Area 2	3.1	2,092367	1,535145	
	4	1,600513		
	5	0,912555		
Area 3	5.1	1,503675	2,259596	
	6	3,472792		
	7	1,802321		

Pada Kondisi 3, merujuk pada nilai koefisien pathloss Kondisi 2 (Sub Cluster) yang ditunjukkan oleh Tabel 2, kemudian dihitung nilai koefisien pathloss Kondisi 3 (Cluster) dengan mencari nilai rata-rata koefisien pathloss sub cluster area.

Gambar 5 dibawah ini menunjukkanpengujian hasil estimasi jarak pada Lorong A sub cluster area 2 dengan menggunakan 4 macam koefisien *path loss.*



Gambar 5. Grafik hasil estimasi jarak menggunakan empat koefisien *path loss* dan jarak sesunggunya di Lorong A area 2

Terdapat 5 grafik yakni grafik berwarna magenta yang menggambarkan hasil estimasi jarak dengan koefisien path loss regresi linier, grafik berwarna biru yang menggambarkan hasil estimasi jarak dengan koefisien path loss kondisi 1 (Per Anchor), grafik berwarna merah yang menggambarkan hasil estimasi jarak dengan koefisien *path loss* kondisi 2 (Sub Cluster Area), grafik berwarna hijau yang menggambarkan hasil estimasi jarak dengan dengan koefisien path loss kondisi 3 (Cluster Area), dan grafik berwarna hitam yang menggambarkan jarak sesungguhnya pada pengukuran.

Dengan melihat gambar 5 diatas, terlihat bahwa grafik berwarna biru yang merupakah hasil estimasi jarak menggunakan koefisien *path loss* kondisi 1 lebih mendekati grafik berwarna hitam (jarak sesungguhnya) jika dibandingkan dengan grafik-grafik lainnya. Hal ini berbeda dengan hasil estimasi jarak pada lorong A area 1 dimana hasil estimasi jarak menggunakan regresi linier lebih mendekati jarak sesungguhnya.

Sehingga pada Lorong A area 2 dapat disimpulkan bahwa hasil estimasi jarak menggunakan koefisien *path loss* kondisi 1 (per anchor) memiliki prosentase akurasi sebesar 99,89 % lebih tinggi dibandingkan dengan hasil estimasi jarak lainnya. Untuk prosentase akurasi lainnya dapat dilihat pada Tabel 3 dibawah ini.

Tabel 3. Tabel Prosentase Akurasi (%) Hasil Estimasi Jarak Menggunakan empat Koefisien *path loss* di Lorong A area 2

No	**Jenis Kondisi Koefisien *Pathloss***	***Mean Square Error***	**Prosentase Akurasi (%)**
1.	Kondisi 1 (Per Anchor)	0,103	99,89
2.	Kondisi 2 (Per Sub Cluster)	16,1793	83,8
3.	Kondisi 3 (Per Cluster)	6,7079	93,29
4.	Regresi Linier	6,1427	93,85

Setelah melakukan pengujian untuk mengetahui keakurasian estimasi jarak, kemudian dilakukan pengujian estimasi posisi menggunakan metode *range based* yakni Trilaterasi dan Multilaterasi dengan

menggunakan nilai RSSI hasil pengukuran yang dilakukan di Lorong A, Gedung Pascasarjana PENS lantai 3. Pengujian menggunakan nilai koefisien pathloss dengan kondisi 1 (per anchor), kondisi 2 (per sub cluster area) dan kondisi 3 (per area). Hasil pengujian ditampilkan pada tabel 4 dibawah ini.

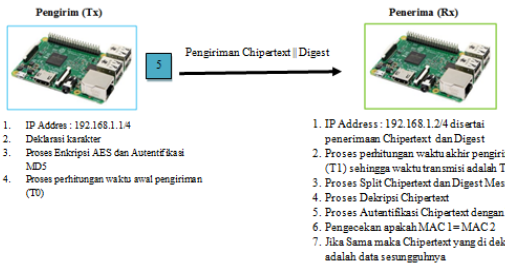
Dari keseluruhan hasil pengujian, dengan melihat tabel 4 dibawah ini dapat disimpulkan bahwa Metode Multilaterasi memiliki keakurasian lebih baik jika dibandingkan dengan Metode Trilaterasi baik menggunakan nilai koefisien pathloss kondisi 1 (per anchor), kondisi 2 (per sub cluster) dan Kondisi 3 (per cluster). Hal ini dikarenakan pada metode multilaterasi terdapat 4 *anchor node* yang menjadi node referensi, sementara pada metode trilaterasi hanya terdapat 3 *achor node* yang menjadi node referensi. Hal inilah yang mengakibatkan estimasi posisi dengan Metode Multilaterasi memiliki nilai rata-rata MSE (*Mean Square Eror*) lebih kecil jika dibandingkan dengan Metode Trilaterasi.

Tabel 4. Prosentase Akurasi (%) Hasil Estimasi Posisi dengan Multilaterasi dan Trilaterasi

No	Kondisi	Metode Estimasi Posisi	Mean Square Error	Prosentase Akurasi (%)
1.	Kondisi 1 (Per Anchor)	Multilaterasi	2,64	97,36
		Trilaterasi	3,19	96,81
2.	Kondisi 2 (Sub Cluster)	Multilaterasi	6,827	93,173
		Trilaterasi	11,137	88,86
3.	Kondisi 3 (Cluster)	Multilaterasi	4,42	95,58
		Trilaterasi	7,553	92,447

Selanjutnya setelah sistem mengimplementasikan metode estimasi posisi multilaterasi dengan *Cluster Based Pathloss*Kondisi 1,dilakukan juga implementasi sistem keamanan data yang sebelumnya telah berhasil disimulasikan menggunakan *socket programming* pada satu PC.

Tahapan pertama yang dilakukan untuk mengimplementasikan sistem keamanan data adalah membangun jaringan ad-hoc antara 2 buah *raspberry* pi agar keduanya dapat saling berkomunikasi. Dari kedua raspberry tersebut salah satu bertugas sebagai pengirim (Tx) dan sebagai penerima (Rx), yang tampak pada gambar 6, dikarenakan jenis protokol yang digunakan adalah UDP, maka data yang dikirimkan berupa pesan yang telah dienkripsi. Pada sistem ini terdapat 1 jenis *data* yang akan dikirim.Tx melakukan proses enkripsi pesan yang akan dikirimkan menggunakan algoritma AES yang menghasilkan *ciphertext* AES. Outputan dari *ciphertext* AES selanjutnya diautentikasi menggunakan MD5 dan menghasilkan MAC. Proses enkripsi AES dan autentifikasi MD5 menggunakan *key* yang sudah tersedia.



Gambar 5. Ilustrasi implementasi sistem keamanan pada Raspberry Pi 3

Pada Rx *file* tersebut akan diterima serta dilakukan proses autentifikasi terhadap ciphertext yang diterima menggunakan key MD5 dan menghasilkan MAC'. Kemudian dilakukan perbandingan antara MAC yang diterima dengan MAC' apakah sesuai, jika ya maka proses dekripsi AES dapat dilakukan, jika tidak maka sistem dihentikan. Ketika dalam kondisi "ya", ciphertext AES yang diterima akan didekrip untuk mendapatkan pesan sebenarnya.

Kemudian untuk menampilkan waktu *start* dari tiap-tiap proses baik proses yang terjadi pada Tx maupun Rx dilakukan print waktu langsung pada terminal dan dicatat secara manual. Selanjutnya untuk mensikronisasi waktu antara Tx dan RX, maka antara Tx dan Rx perlu dilakukan pengaturan waktu jaringan (*localtime*) menggunakan ntp server. Kemudian setelah waktu keduanya sinkronmaka Tx dan Rx dapat membaca waktu dimulainya proses pengiriman data (T_0). Selanjutnya pada sisi Rx, juga menampilkan waktu diterimanya file (T_1). Kedua parameter T_0 dan T_1 tersebut nantinya akan digunakan sebagai parameter perhitungan waktu transmisi dari tiap-tiap file yakni $T_t = T_1 - T_0$. Berikut ini hasil pengujian waktu transmisi antara Tx dan Rx ditunjukkan pada tabel 5 dibawah ini.

Tabel 5. Waktu Transmisi antara Tx dan Rx

No.	Karakter	Waktu Transmisi 1 (ms)	Waktu Transmisi 2 (ms)
1.	1/0/47/1.4/-51/	19,015	23,194
2.	1/0/47/1.4/-51/	22,500	17,757
3.	1/0/47/1.4/-51/	29,471	15,978
4.	1/0/47/1.4/-51/	21,415	13,550
5.	1/0/47/1.4/-51/	24,827	13,838
6.	1/0/47/1.4/-51/	21,146	13,333
7.	1/0/47/1.4/-51/	23,469	13,479
8.	1/0/47/1.4/-51/	22,281	13,518
9.	1/0/47/1.4/-51/	24,012	14,560
10.	1/0/47/1.4/-51/	20,949	18,449
11.	1/0/47/1.4/-51/	23,344	32,627
12.	1/0/47/1.4/-51/	23,060	13,872
13.	1/0/47/1.4/-51/	23,907	13,262
14.	1/0/47/1.4/-51/	20,732	33,500
15.	1/0/47/1.4/-51/	18,969	13,420
Rata-rata		**22,606**	**17,622**

Selanjutnya Tabel 6 dibawah ini, menunjukkan bahwa waktu persiapan yang diperlukan oleh Tx antara 0,005 - 0,007 ms dan waktu persiapan di sisi Rx antara0,078 – 0,083 ms. Dengan demikian waktu persiapan atau dikenal dengan *preparation time* pada sisi Rx jauh lebih lama dibandingkan dengan waktu persiapan pada sisi Tx. Hal ini dikarenakan pada sisi Rx terdapat proses pemisahan data yang diterima, baru kemudian dilanjutkan proses dekripsi, sementara pada sisi Tx data *plain text* langsung masuk ke dalam proses enkripsi.

Tabel 6. Waktu Komputasi untuk Proses Preparasi dan Sinkronisai

No	Karakter	Waktu Perp1 (ms)	Waktu Perp2 (ms)	Waktu Sinkron 1 (ms)	Waktu Sinkron 2 (ms)
1.	1/0/47/1.4/-51	0,005	0,08	0,27	0,34
2.	1/0/47/1.4/-51	0,005	0,082	0,27	0,36
3.	1/0/47/1.4/-51	0,006	0,082	0,27	0,37
4.	1/0/47/1.4/-51	0,006	0,083	0,22	0,32
5.	1/0/47/1.4/-51	0,005	0,081	0,26	0,34
6.	1/0/47/1.4/-51	0,006	0,08	0,28	0,34
7.	1/0/47/1.4/-51	0,007	0,078	0,27	0,32
8.	1/0/47/1.4/-51	0,005	0,081	0,25	0,32
9.	1/0/47/1.4/-51	0,005	0,08	0,21	0,34
10.	1/0/47/1.4/-51	0,005 5	0,081	0,24	0,34
Rata-rata		**0.005**	**0,080**	**0,26**	**0,36**

Keterangan: Perp = Persiapan ; Sinkron= Sinkronisasi; 1 = Tx dan 2 = Rx

Kemudian untuk waktu sinkronisasi ini merupakan proses penentuan port serta IP address yang dapat terhubung serta menerima pesan yang akan dikirim oleh Tx. Sehingga mengakibatkan waktu antara keduanya hanya selisih 0,1 ms lebih lama disisi Rx. Pada bagian Rx hanya perlu menunggu untuk dapat menerima pesan yang akan dikirim.

Kemudian dari sisi waktu komputasi sistem keamanan jaringan terdapat dua parameter waktu komputasi yang dapat dihitung, yaitu waktu enkripsiyang tersaji pada Tabel 7 dan waktu dekripsi yang tersaji pada Tabel 8.

Tabel 7. Waktu Komputasi Proses Enkripsi

No.	Karakter	Waktu Enkripsi (ms)	Waktu Autentifikasi (ms)	Waktu Preparasi (ms)	Waktu Total 1 (ms)
1.	1/0/47/1.4/-51/	0,008	0,047	0,005	0,06
2.	1/0/47/1.4/-51/	0,008	0,045	0,005	0,058
3.	1/0/47/1.4/-51/	0,009	0,046	0,006	0,061
4.	1/0/47/1.4/-51/	0,009	0,045	0,006	0,06
5.	1/0/47/1.4/-51/	0,009	0,046	0,005	0,06
6.	1/0/47/1.4/-51/	0,009	0,046	0,006	0,061
7.	1/0/47/1.4/-51/	0,008	0,046	0,007	0,061
8.	1/0/47/1.4/-51/	0,01	0,046	0,005	0,061
9.	1/0/47/1.4/-51/	0,009	0,047	0,005	0,061
10.	1/0/47/1.4/-51/	0,009	0.047	0,005	0,061
Rata-rata		**0,0088**	**0,0461**	**0,0055**	**0,0604**

Tabel 8. Waktu Komputasi Proses Dekripsi

No.	Karakter	Waktu Preparasi (ms)	Waktu Verifikasi (ms)	Waktu Dekripsi (ms)	Waktu Total 1 (ms)
1.	1/0/47/1.4/-51/	0,08	0,048	0,021	0,149
2.	1/0/47/1.4/-51/	0,082	0,043	0,021	0,146
3.	1/0/47/1.4/-51/	0,082	0,046	0,019	0,147
4.	1/0/47/1.4/-51/	0,083	0,044	0,021	0,148
5.	1/0/47/1.4/-51/	0,081	0,044	0,021	0,146
6.	1/0/47/1.4/-51/	0,08	0,045	0,02	0,145
7.	1/0/47/1.4/-51/	0,078	0,043	0,021	0,142
8.	1/0/47/1.4/-51/	0,081	0,046	0,019	0,146
9.	1/0/47/1.4/-51/	0,08	0,043	0,021	0,144
10.	1/0/47/1.4/-51/	0,081	0,044	0,02	0,145
Rata-rata		0,0808	0,0446	0,0204	0,1458

Pada Tabel 8 tampak bahwa lama rata-rata waktu untuk proses dekripsi AES jauh lebih lama yakni mencapai 0,0204 ms dibanding dengan rata-rata waktu enkripsi AES hanya 0,0088 ms.Pada proses enkripsi, proses yang ada melibatkan fungsi enkripsi, autentikasi serta fungsi penggabungan key AES dan key MD5 yang kemudian akan dikirimkan. Sedangkan pada proses dekripsi meliputifungsi splitting (pemisahan karakter) berupa pemisahan key AES dan key MD5 serta pemisahan ciphertext AES serta MAC, kemudian fungsi dekripsi autentifikasi, selanjutnya juga terdapat fungsi perbandingan (*comparing*) guna membandingkan hasil autentifikasi di sisi Rx = MAC' apakah sama dengan MAC yang dikirim oleh Tx, jika sama maka proses dapat dilanjutkan menuju enkripsi AES. Sehingga lamanya waktu yang dibutuhkan untuk proses dekripsi disisi Rx mengakibatkan waktu komputasi total disisi Rx juga lebih lama hingga 0,1458 ms sedangkan disisi Tx hanya 0,0604 ms.

Dengan melihat hasil pengujian keamanan data pada Raspberry Pi 3 berupa waktu komputasi dan transmisi yang di dapatkan, dapat di simpulkan bahwa waktu komputasi dan transmisi yang terjadi bisa dikatakan tidak membebani sistem estimasi posisi pada lingkungan *indoor*.Hal ini dikarenakan waktu komputasi dan waktu transmisi yang diperlukan masih dalam hitungan satuan waktu dibawah second yakni mili second atau dikenal dengan (ms).

KESIMPULAN

Pada penelitian ini, untukmeningkatkan nilai akurasi dari proses estimasi jarak menggunakan level kuat sinyal pada lingkungan *indoor* diperlukan pengukuran nilai *Pathloss Exponential* berdasarkan pembagian luas area atau *Cluster Based Pathloss Exponentia (CBPLE)l.* Sementara itu hasil pengujian menunjukkan bahwa estimasi posisi dengan metode multilaterasi menggunakan *CBPLE* Kondisi 1 mampu menghasikan prosentase akurasi estimasi posisi lebih baik dibandingkan dengan menggunakan metode trilaterasi yakni sebesar 97,36 % untuk prosentase akurasi menggunakan metode multilaterasi dan 96,81 % untuk prosentase akurasi menggunakan metode trilaterasi.

Dari sisi keamanan, untuk menghindari penyerangan oleh*attacker* maka perlu ditambahkan skenario autentifikasi yang memerlukan rata-rata waktu komputasi sebesar 0,461 ms pada proses enkripsi, sementara pada proses dekripsi dilakukan terlebih dahulu proses autentifikasi dan verifikasi yang memerlukan waktu komputasi rata-rata sebesar 0,0446 ms. Pada proses enkripsi diperlukan rata-rata waktu komputasi sebesar 0,0604 ms lebih cepat dibandingkan dengan rata-rata waktu komputasi yang diperlukan untuk proses dekripsi yakni sebesar 0,1458 ms. Sementara untuk hasil pengujian sistem keamanan, diperoleh rata-rata waktu transmisi data sebesar 22,606 ms.Dengan demikian jika ditinjau dari waktu komputasi dan waktu transmisi yang telah diujikan, sistem keamanan ini dapat diimplemantasikan pada aplikasi *monitoring* dan *tracking object* karena terbukti tidak membebani sistem.

SARAN

Penelitian pada lingkup *wireless sensor network* di lingkungan *indoor* masih perludilakukan lebih lanjut, terutama pada pengamatan *pathloss exponential.*Hal ini dikarenakan karakteristik dari *pathloss exponential* pada lingkungan *indoor* satu dengan lainnya memiliki topologi ruang yang berbeda dan mengakibatkan terjadinya perubahan karakteristik dari *pathloss exponential*.Kemudian pada sistem keamanan, perlu dilakukan penelitian lebih lanjut pada metode Wrap AES agar kedepan segala proses dapat di amati dan dianalisa dengan baik.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada Lembaga Peneltian dan Pengabdian Masyarakat Sekolah Tinggi Teknologi Bontang atas bantuannya dalam mendukung penelitian ini.

DAFTAR PUSTAKA

[1] I. T.Haque and C. Assi,"Profiling-based indoor localization schemes,"IEEE System Journal, vol.9,no.1, pp. 76-85, 2015.

[2] Z. Hengjun and Q. Hanbiao,"Research on the mine personnel localization algorithm based on the background of week signal,"International Journal of Smart Home,vol. 10,no.7, pp. 47-56, 2016.

[3] Z. De and L. G. Yan, "Positioning system of underground coal mines based on zigbee technology," TELKOMNIKA Indonesian Journal of Electrical Engineering and Computer Science, vol.12, no. 5, pp. 3962-3968, 2014.

[4] W. Yan, S. Xinxin, and J. Wei, "The mobile nodes location technology in wireless sensor network," Chinese Journal of Sensor and Actuators, vol. 24, no.9, 2011.

[5] B.Zhou, Q. Chen, and P. Xiao, "The error propagation analysis of the received signal strength based simultaneos localization and tracking in WSN," IEEE Transaction on Information Theory, vol. 63, pp. 3943-4007, 2017.

[6] A.A Momtaz, F. Behnia, R. Amini, and F. Marvash,"NLOS Identification in range based scene localization : Statistical Approach," IEEE Sensor Journal, vol.18, pp. 3745-3751, 2017.

[7] M. Singh and P.M. Khilar, "Mobile beacon based range free localization method for Wireless Sensor Networks,"Journal of Mobile Communication, Computation and Information,vol.23, pp. 1285-1300, 2017.

[8] K. Z. Lu, X. H. Xiang, D. Zhang, R. Mao, and Y. H. Feng, "Localization algorithm based on maximum aposteriori in wireless sensor networks," International Journal of Distributed Sensor Networks, vol.2, no.3, pp.198-214, 2012.

[9] S. Tomic, M. Beko, R. Dinis, and P. Montezena, "Distributed algorithm for target localization in wireless sensor network using RSS and AOA measurement," Elsavier Journal : Pervasive and Mobile Computing, vol. 37, pp. 63-77, 2017.

[10] M. Salamah and E. Doukhnitch, "An efficient algorithm for mobile objects localization," International Journal of Communication Systems, vol.21, no. 3, pp. 301-310, 2008.

[11] A. Znaid, I. Idris, A. Wahab, L.K. Qabajeh, and O.A. Mahdi, "Sequential monte carlo localization method in mobile wireless sensor networks : a review," Hindawi Journal of Sensors, vol.1, 2017.

[12] H. Zou, L. Xie, Q.-S Jia,and H. Wang, "Platform and algorithm development for a RFID-based indoor positioning System,"Journal of Unmanned Systems,vol. 2, no.3, pp. 279-291, 2014.

[13] P. Kristalina, A. Sudarsono, M. Syafrudin, and B.K. Putra, "SCLoc :secure localization platform for Indoor wireless sensor network," Proc. 2016 International Electronics Symposium, 2016, pp. 420-425.

[14] N. U. Scholastica, "Path loss prediction model of a wireless sensor network in an indoor environment," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 4, pp. 11665-11673, 2012.

[15] C. R. Pratiwi, P. Kristalina, and A. Sudarsono,"Clusterbased Path Loss Exponentmodel for indoor estimation distance in wireless sensor network,"Proc. The 5th International Conference on Knowledge Creation and Intelligent Computing (KCIC), IEEE Xplore, 2016, pp. 89-102.