

BAB II

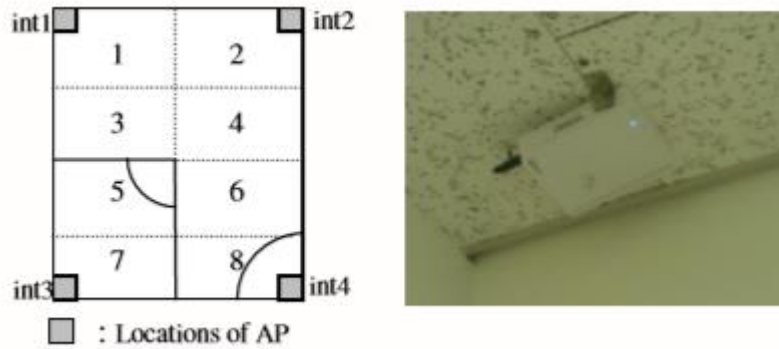
LANDASAN TEORI

2.1 Indoor Positioning System

Indoor Positioning System merupakan suatu system yang dapat menentukan lokasi *mobile device* di dalam sebuah ruangan maupun gedung. Ada beberapa teknik untuk menghitung posisi sebuah *mobile device*. Terdapat 2 teknik utama yang biasa digunakan, yaitu *signal strength (SS) cartography* dan *multilateration*. Tidak menutup kemungkinan kedua tehnik tersebut dapat digunakan secara bersamaan. Dalam system yang menggunakan *cartography*, akurasi posisi berkorelasi dengan *mesh granularity*, sedangkan system yang menggunakan *SS-multilateration* keakurasian bergantung pada model propagasi yang digunakan (Cypriani, Lassabe, Canalda, & Spies, 2009).

2.1.1 Indoor Wi-Fi Positioning System for Android

Dalam penelitian yang telah dilakukan (Beom, Kwang, Sun, Joo, Woo, & Hyung, 2010) menggunakan sebuah ruangan 6 x 12 m, smartphone OS Android 2.1, dan terdapat 4 *Access Point (AP)* yang diletakan disetiap pojok ruangan. Pada ruangan tersebut sudah dibagi menjadi 8 area, dan kekuatan signal setiap AP disetiap area sudah disimpan disebuah *database*.



Gambar 2.1 : Lokasi Access Point

Pada penelitian ini pengukuran lokasi smartphone menggunakan RSSI . pengukuran dilakukan dengan pengambilan data RSSI sebanyak 3 kali dan dirata – ratakan. Setelah dirata – ratakan apabila hasilnya kurang dari 16 dBm maka akan diambil rata – rata kembali. Setelah rata – rata lebih dari 16 dBm maka akan dibandingkan dengan data yang ada di database dan setelah itu area dapat di tentukan. Penentuan lokasi pada penelitian ini masih berdasarkan pembagian area dan belum bisa menentukan jarak pasti dalam satuan meter.

2.1.2 Robust Indoor Wi-Fi Positioning System for Android

Penelitian ini melanjutkan penelitian “*Indoor Wi-Fi Positioning System for Android*”. Penambahan yang dilakukan adalah penghitungan jarak *smartphone* ketiap AP (Lubbad, Alkurdi, & Samra, 2013). Formula yang digunakan untuk menghitung jarak :

$$Pr = Pt - Lu$$

$$Lu = 20\log_{10}(4\pi/\lambda) + 20\log_{10}(d) \times \mu$$

Dimana :

$$Pt \text{ [dBm]} = \text{Kekuatan sinyal yang dikirim AP}$$

P_r [dBm] = Kekuatan sinyal yang diterima Android

d [m] = Jarak antara AP dan *Smartphone*

λ [m] = Panjang gelombang

μ = Nilai index kualitas pengiriman sinyal.

Table 2.1 : Nilai μ

μ	Deskripsi
2	<i>Outdoor</i> dengan kondisi <i>clear</i>
2.5	<i>Indoors</i> dengan kondisi <i>clear</i>
3.0	<i>Indoors</i> dengan kondisi <i>not clear</i>
4.0	<i>Indoors</i> dengan kondisi yang buruk

Penelitian ini dilakukan dengan penempatan 3 AP di 3 lantai yang berbeda di gedung Gaza, Islamic University. Hasil dari penelitian ini, masih ada rata-rata perbedaan perhitungan sebesar 1.6 m dari perhitungan berdasarkan RSSI dengan jarak asli dan dengan tingkat akurasi pengukuran 83.5%.

2.1.3 Outdoor Localization System Using RSSI Measurement of Wireless Sensor Network

Penelitian ini melakukan pengukuran jarak menggunakan RSSI dan metode trilateration untuk pencarian koordinat (x,y) dilokasi *outdoor* (Okorogu, Oguejiofor, Adewale, & Osuesu, 2013). Formula yang digunakan dalam pengukuran jarak :

$$\text{RSSI [dBm]} = -10n \log_{10} (d) + A \text{ [dBm]}$$

Dimana :

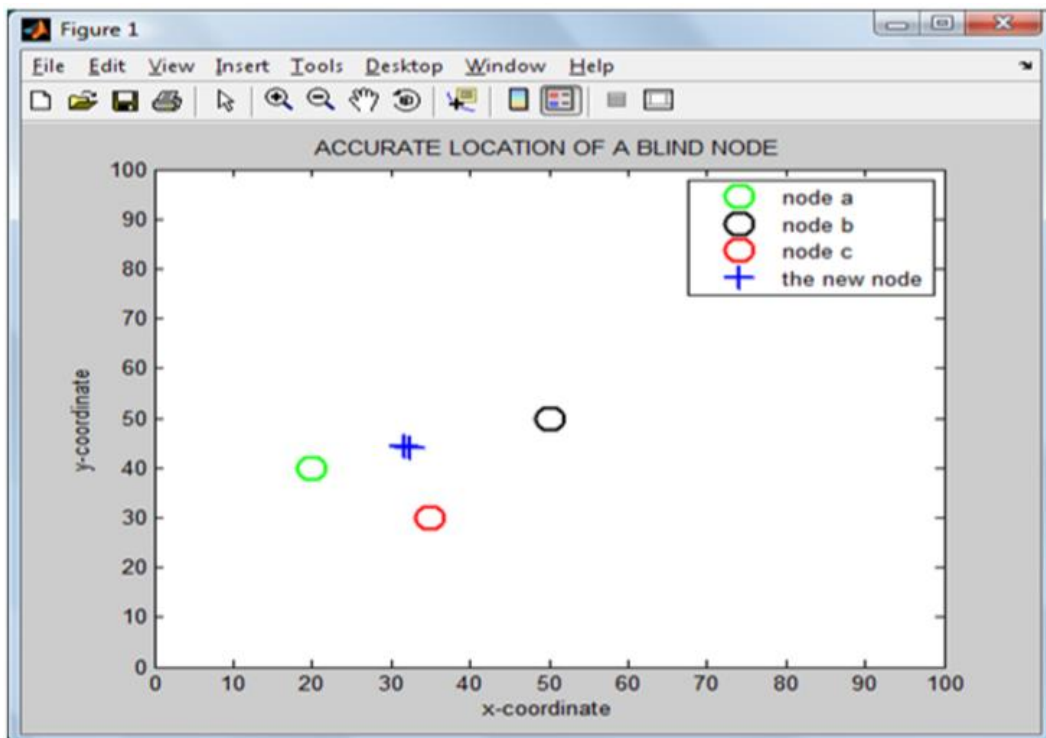
RSSI [dBm] = Kekuatan sinyal yang diterima pada jarak d .

n = *Propagation pathloss exponent*

d [m] = Jarak dari pengirim sinyal ke penerima sinyal

A [dBm] = Kekuatan sinyal pada jarak 1 meter.

Setelah mendapatkan nilai sinyal dan jarak tiap *anchor node* maka dilakukan penentuan koordinat (x,y) dengan menggunakan metode trilateration. Pada metode trilateration dibutuhkan minimal 3 *anchor node*. Dari penelitian ini dihasilkan bahwa apabila menggunakan 3 *anchor node* memiliki tingkat kesalahan pengukuran sebesar 0.74 meter, namun apabila anchor node ditambahkan menjadi 4 maka tingkat kesalahan pengukuran sebesar 0.56 meter. Dengan penambahan 1 *anchor node*, tingkat kesalahan berkurang 0.18 di lingkungan *outdoor*.



Gambar 2.2 : Estimasi Posisi dari Sebuah Node

2.2 Wi – Fi

Berdasarkan (Tim Penelitian dan Pengembangan Wahana Komputer, 2004) Wi-Fi merupakan kependekan dari *Wireless Fidelity* dan merupakan aliansi industri yang mempromosikan penggunaan jaringan nirkabel (Wireless LAN/WLAN) untuk jaringan yang didasari pada spesifikasi IEEE 802.11.

2.2.1 Spesifikasi Wi – Fi

Saat ini terdapat empat variasi dari 802.11, yaitu 802.11a, 802.11b, 802.11g dan 802.11n. Berikut detail dari masing-masing variasi tersebut :

Tabel 2.2 : Variasi 802.11

	Kecepatan	Frekuensi Band	Sesuai Spesifikasi
802.11b	11 Mbps	2.4 GHz	B
802.11a	54 Mbps	5 GHz	A
802.11g	54 Mbps	2.4 GHz	b, g
802.11n	100 Mbps	2.4 GHz	b, g, n

Menurut (Sofana, 2012) dalam pengembangan teknologi Wi-Fi terbaru berdasarkan spesifikasi Pre-802.11n terdapat teknologi yang disebut MIMO (*Multiple Input Multiple Output*) yang dapat meningkatkan throughput, reliabilitas serta jumlah client yang terkoneksi. Selain itu daya tembus terhadap penghalang lebih baik, jangkauan lebih luas dan menghasilkan kecepatan transfer data yang lebih besar.

Secara teknis operasional, Wi-Fi merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat WLAN (Wireless Local Area Network). Dengan kata lain, Wi-Fi adalah sertifikasi merek dagang yang diberikan pabrikan kepada perangkat telekomunikasi (Internet) yang bekerja di jaringan WLAN dan sudah memenuhi kualitas kapasitas interoperasi

yang dipersyaratkan sehingga produk yang telah mendapat persetujuan dari aliansi tersebut menerima sertifikat segel interoperabilitas Wi-Fi.

2.3 Access Point (AP)

Access point adalah peralatan yang digunakan *wireless* LAN. AP bertugas mengatur dan menghubungkan koneksi beberapa peralatan Wi – Fi. AP dapat dianalogikan dengan hub, hanya saja digunakan pada *wireless* LAN. AP juga dapat menghubungkan *wireless* LAN dengan *wired* LAN.

2.3.1 SSID

Di dalam peralatan Wi-Fi terdapat SSID (*Service Set Identifier*) merupakan *network* ID atau nama untuk jaringan *wireless*. Beberapa vendor menyebut SSID sebagai Domain ID. Setiap jaringan wi-fi harus memiliki SSID yang unik serta channel yang sama agar antar *device* dapat saling berkomunikasi.

2.3.2 Otentikasi dan Enkripsi *Wireless*

Di dalam jaringan *wireless* terdapat beberapa metode otentikasi dan enkripsi yaitu :

- WEP (Wired Equivalent Privacy)

Fitur keamanan standar untuk peralatan *wireless*. Dalam WEP menggunakan 64bit dan 128bit. Ada dua cara untuk memasukkan WEP key, disetkan sendiri atau generate menggunakan *passphrase*. *Passphrase* akan *generate automatic* WEP key untuk masukkan abjad. WEP hanya boleh memasukkan 0-9 dan A-F(hexadecimal). Kepanjangan *key* bergantung jenis *securiy*, jika 64bit memasukkan 10 *key*, dan untuk 128 bit memasukkan 26 *key*. Tak boleh kurang dan lebih.

- WPA - PSK (*Wi-Fi Protected Access – Pre Shared Key*)

WPA-PSK adalah securiti yang lebih update dari WEP. WPA-PSK mempunyai *decryption* yang ada pada WEP. Serta menambahkan *security* yang lebih pada *wireless* yaitu dengan menggunakan key yang akan diubah secara otomatis dan diotentikasi secara teratur. WPA-PSK masih bisa *dicrack* atau disadap, tetapi mengambil masa lebih lama dari WEP. Panjang key adalah 8-63, anda boleh memasukkan sama ada 64 hexadecimal atau ASCII.

- WPA2 – PSK (*Wi-Fi Protected Access 2*)

Dalam WPA2-PSK beberapa teknisnya hampir sama dengan WPA namun pada enkripsinya yang dipakai adalah *Advanced Encryption Standard* (AES) yaitu suatu enkripsi dengan menggunakan algoritma Rijndael. Dalam proses enkripsi input, diperlukanlah empat macam operasi yang dilakukan berulang-ulang dalam beberapa putaran dan menggunakan kunci *cipher*.

2.3.3 Metode Koneksi *Access Point*

Terdapat 2 metode koneksi pada AP, yaitu:

- Ad-hoc

Sistem ad-hoc adalah sistem *peer-to-peer*, dalam arti satu komputer dihubungkan dengan satu komputer lain secara langsung tanpa menggunakan AP. Pada sistem ad-hoc tidak lagi mengenal sistem *central* (yang biasanya difungsikan pada AP). Sistem ad-hoc hanya memerlukan satu buah komputer yang memiliki nama SSID (*Service Set Identifier*) atau sederhananya nama sebuah *network* pada sebuah card / komputer.

- **Infrastruktur**

Sistem infrastruktur menggunakan AP untuk menghubungkan komputer-komputer ke dalam suatu jaringan. Jadi setiap komputer yang hendak berhubungan satu sama lain harus melewati AP terlebih dahulu, baru kemudian dapat menggunakan sumber daya yang ada pada jaringan.