Skema Peningkatan *Reciprocity* Kanal dengan Menggunakan Metode *Hierarchical Clustering*

Prima Kristalina[1], Florista Dewi[2], Mike Yuliana[3], Tri Budi Santoso[4], Amang Sudarsono[5], Reni Soelistijorini[6]

***Abstract*—Secret key generation scheme that utilizes the randomness of wireless channels is a very promising alternative to establish a secure communication path. Some wireless devices are used to obtain the channel parameters. But the problem that occurs is imprecise measurement results, causing a secret key difference between the two users. To overcome this problem, pre-processing method is used before the data is quantized, to increase the similarity (reciprocity) channel parameter measurement results. In this paper, the effect of the use of one pre-process method, which was hierarchical clustering, on the performance of secret key generation scheme in an indoor environment with two variations of scenario was investigated. The results show that the use of the pre-processing method can improve the similarity parameter of the channel measurement results as indicated by the increasing of correlation values up to 20%. In addition, the resulting bit mismatch also decreases with the value of key disagreement rate (KDR) maximum of 20%.**

***Intisari*—Skema pembangkitan *secret key* yang memanfaatkan keacakan kanal *wireless* merupakan alternatif yang sangat menjanjikan untuk membangun jalur komunikasi yang aman. Beberapa perangkat *wireless* digunakan untuk mendapatkan parameter kanal tersebut. Namun, permasalahan yang terjadi adalah pengukuran yang dihasilkan tidak presisi sehingga menimbulkan perbedaan *secret key* antara dua pengguna. Salah satu upaya yang dapat dilakukan adalah melakukan praproses data sebelum dikuantisasi sehingga dapat meningkatkan kemiripan (*reciprocity*) parameter kanal hasil pengukuran. Pada makalah ini dilakukan investigasi secara detail terhadap pengaruh penggunaan salah satu metode praproses, yaitu *hierarchical clustering,* terhadap kinerja skema pembangkitan *secret key* di lingkungan *indoor* dengan dua variasi skenario. Hasil pengujian yang dilakukan menunjukkan bahwa penggunaan metode praproses dapat meningkatkan kemiripan parameter kanal hasil pengukuran yang ditunjukkan dengan peningkatan nilai korelasi hingga 20%. Selain itu, ketidak-cocokan bit yang dihasilkan juga semakin menurun dengan nilai *key disagrement rate* (KDR) maksimal sebesar 20%.**

***Kata Kunci—secret key*, praproses, *reciprocity*, *hierarchical clustering*, KDR.**

I. PENDAHULUAN

Jaringan *mobile ad-hoc* telah berkembang sangat pesat dalam beberapa tahun terakhir ini. Tidak seperti komunikasi yang tradisional, *node wireless* dalam jaringan tersebut dapat berkomunikasi dengan *node* yang lain dalam jangkauan tertentu. Hal ini menyebabkan komunikasi *wireless* rentan terhadap adanya serangan, karena semua *node* lain yang berada dalam jangkauan pemancar dapat juga menerima sinyal dari pemancar tersebut. Karenanya, penyadapan merupakan salah satu masalah keamanan utama dalam komunikasi *wireless*. Secara intuitif, komunikator akan berbagi *secret key* sehingga komunikasi yang dilakukan dapat diacak dan aman dari penyadap.

Seperti yang telah didiskusikan pada penelitian-penelitian sebelumnya, persyaratan keamanan yang harus dipenuhi meliputi ketersediaan, kerahasiaan, integritas, autentikasi, serta tidak adanya penolakan dari *node* yang ada di jaringan *ad-hoc* [1], [2]. Kerahasiaan dari komunikasi antar *node* dijamin dengan skema enkripsi dan dekripsi pesan. Persyaratan keamanan tersebut membutuhkan implementasi manajemen *secret key* yang efisien. Sistem manajemen *secret key* dengan menggunakan variasi *reciprocity* kanal merupakan manajemen *secret key* antar *node* jaringan *ad-hoc* yang simpel dan efektif. Ide dasar yang digunakan adalah pemanfaatan variasi *reciprocity* dan keacakan kanal *wireless* dan membangun sistem manajemen *secret key* seperti yang ditunjukkan pada penelitian sebelumnya [3]-[11].

Prinsip dari *reciprocity* kanal merupakan dasar dari skema pembangkitan *secret key* menggunakan variasi dari kanal *wireless*. Oleh karena itu, skema pembangkitan *secret key* yang lebih baik dapat dikembangkan jika pengukuran kanal yang efisien dapat terpenuhi. Beberapa perangkat *wireless* diperlukan untuk mendapatkan parameter kanal hasil pengukuran. Permasalahan yang terjadi adalah penggunaan perangkat *wireless* yang digunakan di laptop sering menghasilkan pengukuran yang kurang presisi dibandingkan dengan penggunaan perangkat *wireless* yang khusus. Namun, penggunaan perangkat yang khusus tersebut juga akan meningkatkan kompleksitas dan biaya yang diperlukan. Salah satu upaya yang dapat dilakukan untuk mengatasi permasalahan tersebut adalah dengan melakukan praproses data pengukuran sebelum dikuantisasi sehingga dapat meningkatkan kemiripan (*reciprocity*) parameter kanal hasil pengukuran.

Pada makalah ini dilakukan investigasi pengaruh penggunaan salah satu metode praproses, yaitu *hierarchical clustering*, terhadap kinerja skema pembangkitan *secret key* di lingkungan *indoor*. Metode praproses ini diharapkan dapat meningkatkan *reciprocity* kanal tanpa menggunakan perangkat *wireless* yang khusus, sehingga akan menghasilkan parameter kanal *wireless* yang lebih presisi. Parameter kanal yang diukur adalah RSS. Alasan pemilihan metode *hierarchical clustering* sebagai metode praproses adalah

[1]*Staf Pengajar, Politeknik Elektronika Negeri Surabaya, Raya ITS Keputih Sukolilo Surabaya 60111 (tlp: 031-5947280; fax: 031-5946111; e-mail: prima@pens.ac.id)*

[2]*Mahasiswa, Politeknik Elektronika Negeri Surabaya, Raya ITS Keputih Sukolilo Surabaya 60111 (tlp: 031-5947280; fax: 031-5946111; e-mail: dewiflorista@gmail.com)*

[3,4,5,6] *Staf Pengajar, Politeknik Elektronika Negeri Surabaya, Raya ITS Keputih Sukolilo Surabaya 60111(tlp: 031-5947280; fax:0315946111;email:mieke@pens.ac.id,tribudi@pens.ac.id, amang@pens.ac.id, reni@pens.ac.id)*

adanya mekanisme pengelompokan titik-titik data untuk menghaluskan variasi data dari parameter kanal yang tidak teratur sehingga mampu meningkatkan *reciprocity*. Pengelompokan data dilakukan dengan menggunakan rata-rata atau nilai tengah dari titik yang berurutan. Hasil pengujian yang dilakukan menunjukkan adanya peningkatan *reciprocity* parameter kanal hasil pengukuran dengan rata-rata peningkatan hingga sebesar 20%

Sisa bagian dari makalah ini diatur sebagai berikut. Bagian II membahas tentang skema pembangkitan *secret key*. Bagian III mendiskusikan tentang desain sistem yang berisi tentang desain sistem yang diusulkan beserta mekanisme pengukuran. Bagian IV berisi hasil dan pembahasan, sedangkan kesimpulan ada pada bagian V.

II. SKEMA PEMBANGKITAN *SECRET KEY*

Secara umum terdapat empat tahapan yang digunakan dalam skema pembangkitan *secret key*, yang meliputi *channel probing*, kuantisasi, rekonsiliasi, dan *privacy amplification* [12]. Pada makalah ini ditambahkan tahapan yang digunakan pada skema pembangkitan *secret key* untuk meningkatkan *reciprocity* kanal. Tahapan yang ditambahkan adalah tahap praproses data sebelum dikuantisasi dengan menggunakan metode *hierarchical clustering*.

A. Tahapan Pembangkitan Secret Key

Terdapat lima tahapan pembangkitan *secret key* yang dilakukan untuk mendapatkan *secret key* sepanjang 256 bit, yaitu sebagai berikut.

1) Channel Probing: Tahap ini dilakukan untuk mengumpulkan nilai RSS dari Alice dan Bob. Pada tahap ini, Alice dan Bob bertukar *request/reply probing* sinyal satu sama lain dalam durasi waktu tertentu. Salah satu segera membalas jika menerima *request* dari lainnya. Di akhir proses *channel probing*, diasumsikan Alice dan Bob membuat *n* pasangan dari pengukuran RSS seperti yang ditunjukkan oleh (1) dan (2).

$$h_x = \{h_x(1), h_x(2), \dots, h_x(n)\} \quad (1)$$

$$h_y = \{h_y(1), h_y(2), \dots, h_y(n)\}. \quad (2)$$

Pada makalah ini, h_x adalah parameter kanal RSS yang diukur oleh *user x* ketika *user y* mengirim sinyal *probing*, sedangkan h_y adalah parameter kanal yang diukur oleh *user y* ketika *user x* mengirim sinyal *probing*.

2) Praproses Data: Praproses data dilakukan untuk meningkatkan *reciprocity* parameter kanal hasil pengukuran antara dua pengguna. Peningkatan *reciprocity* ditunjukkan dengan peningkatan korelasi yang diukur dengan menggunakan korelasi Pearson seperti ditunjukkan oleh (3).

$$\rho_{X,Y} = \frac{\mathrm{cov}(X,Y)}{\sigma_X.\sigma_Y} = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X.\sigma_Y} \quad (3)$$

dengan *cov* adalah kovarian, σ adalah standar deviasi, dan μ_A, μ_B adalah rata-rata pengukuran antara Alice dan Bob, sedangkan E adalah ekspektasi.

3) Kuantisasi: Tahap ini dilakukan untuk mengkuantisasi hasil praproses ke dalam bentuk bit. Kuantisasi dilakukan berdasarkan *threshold* yang telah ditentukan. Skema kuantisasi yang digunakan di sini adalah skema kuantisasi Aono. Skema ini menggunakan nilai median dari hasil pengukuran RSS sebagai *threshold* dan hasil kuantisasi akan bernilai 1 jika berada di atas *threshold* serta bernilai 0 jika dibawah *threshold* [13].

4) Rekonsiliasi: Rekonsiliasi adalah bentuk dari koreksi *error* yang dilakukan Alice dan Bob untuk memastikan bahwa kunci yang dibangkitkan secara terpisah di kedua sisi adalah identik. Akibat dari *reciprocity* yang tidak sempurna, bit yang dihasilkan Alice dan Bob setelah kuantisasi tidak selalu identik, meskipun bisa jadi berkorelasi tinggi. Ketidak-sempurnaan *reciprocity* tersebut diakibatkan oleh tidak simultannya pengukuran parameter kanal antara Alice dan Bob serta adanya *noise*. Digunakan metode BCH(255,199) untuk melakukan koreksi *error*. Alasan penggunaan metode ini adalah mudahnya penggunaan dan implementasi yang dilakukan.

5) Privacy Amplification: Tahap ini adalah langkah *post processing* yang digunakan untuk meyakinkan bahwa Eve belum mempelajari *key* yang telah terbentuk antara Alice dan Bob. Di sini digunakan fungsi hash SHA-256.

B. Hierarchical Clustering

Hierarchical clustering adalah metode yang digunakan untuk mengelompokkan titik-titik data. Dengan meng-gabungkan pasangan yang berurutan dari titik-titik data, maka bisa didapatkan pengelompokan titik-titik data baru. Tujuan dari pengelompokan ini adalah untuk meningkatkan *reciprocity* dengan menghaluskan variasi data dari parameter kanal yang tidak teratur. Pengelompokan data dilakukan dengan menggunakan rata-rata atau nilai tengah dari titik yang berurutan.

Pada makalah ini, metode pengelompokan yang digunakan adalah metode *Single Linkage* yang merupakan bagian dari metode pengelompokan secara Hierarki Aglomeratif. Untuk mendapatkan pengelompokan data baru dari parameter kanal sebanyak n perlu dilakukan penghitungan matriks jarak antar data dengan menggunakan *Manhattan Distance* seperti terlihat pada (4).

$$D(x,y) = \sum_{j=1}^{n} \left| x_j - y_j \right| \quad (4)$$

Beberapa metode pengelompokan secara Hierarki Aglomeratif terlihat pada (5) sampai (7), dengan d_{uv} merupakan jarak antara dua kelompok (*cluster*).

- *Single Linkage* (jarak terdekat)

$$d_{uv} = \min\{d_{\min}\}, d_{uv} \in D \quad (5)$$

- *Complete Linkage* (jarak terjauh)

$$d_{uv} = \max\{d_{\min}\}, d_{uv} \in D \quad (6)$$

- *Average Linkage* (jarak rata-rata)

$$d_{uv} = average\{d_{\min}\}, d_{uv} \in D \quad (7)$$

C. Evaluasi Kinerja Sistem

Terdapat tiga parameter kinerja sistem yang diuji dalam makalah ini, yaitu sebagai berikut.

1) Key Generation Rate (KGR): KGR mengacu pada jumlah bit yang dapat dibangkitkan dalam durasi waktu pengukuran tertentu. Matriks ini sering digunakan untuk menentukan kualitas dari protokol pembangkitan kunci. Pada makalah ini dievaluasi tiga jenis KGR, yaitu KGR setelah kuantisasi, rekonsiliasi, serta *privacy amplification*. KGR_{ik} adalah pengukuran kinerja yang menunjukkan banyaknya bit yang dihasilkan dalam durasi waktu pengukuran setelah proses kuantisasi, sedangkan KGR_r didapat dari banyaknya bit yang mampu dikoreksi dalam durasi waktu pengukuran setelah proses rekonsiliasi. Bit yang mampu dikoreksi dibagi menjadi beberapa blok, dengan masing-masing blok tersebut harus melewati persyaratan minimal dari tes keacakan entropi dan yang tidak memenuhi akan dibuang. Sisa bit yang didapat akan menghasilkan KGR_{pa}.

2) Key Disagrement Rate (KDR): KDR didefinisikan sebagai rasio dari jumlah bit yang tidak sesuai antara Alice dan Bob dengan total bit yang dihasilkan dari proses kuantisasi. Jika k_b adalah jumlah bit yang tidak sesuai dan l adalah total bit yang dihasilkan dari proses kuantisasi, maka KDR bisa didapatkan dengan menggunakan (8).

$$KDR = \frac{k_b}{l} \quad (8)$$

KDR digunakan untuk menentukan *error* dari *preliminary key* yang didapat setelah proses kuantisasi. Dengan penurunan KDR, maka upaya yang diperlukan untuk mendeteksi dan memperbaiki kesalahan juga menurun.

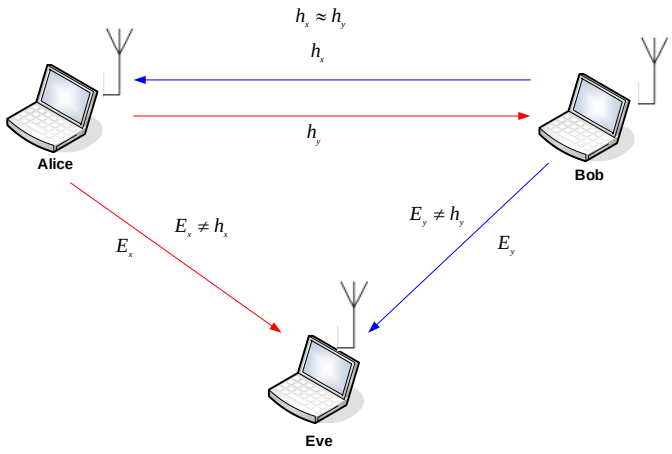
3) Keacakan (Randomness): Komponen yang paling penting dari perangkat kriptografi adalah pembangkit bilangan acak. Untuk melakukan validasi keacakan dari *Pseudo-Random Number Generator* (PRNG), dilakukan uji statistik dengan menggunakan *National Institute of Standards and Technology* (NIST), yang menyediakan lima tes. Masing-masing tes menghasilkan nilai p yang digunakan untuk menilai kualitas *secret key* yang dihasilkan. Tingkat signifikansi yang dinotasikan dengan α mendefinisikan batas antara acak dan tidak acak. Nilai p yang lebih atau sama dengan batasan $p \geq \alpha$ dikatakan sebagai acak. Jika tidak, maka nilai p dikatakan tidak acak. NIST merekomendasikan nilai α antara 0,001 hingga 0,1 ($0{,}001 \leq \alpha \leq 0{,}01$), yang menunjukkan bahwa keacakan rangkaian adalah benar dengan probabilitas 99%. Untuk aplikasi kriptografi nilai p yang dipilih adalah 0,01 [12]. Dalam makalah ini hanya digunakan enam tes keacakan dengan menggunakan NIST.

III. DESAIN SISTEM

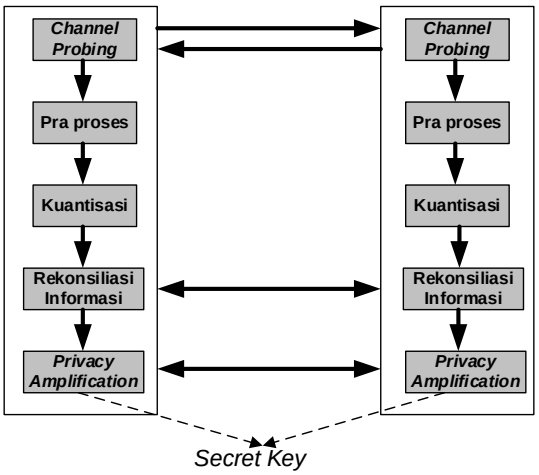
Pada bagian ini dibahas mengenai desain sistem yang diusulkan, serta mekanisme pengukuran yang digunakan.

A. Desain Sistem yang Diusulkan

Desain sistem yang digunakan untuk membangkitkan *secret key* antara dua pengguna yang sah, yaitu Alice dan Bob, ditunjukkan pada Gbr. 1, dengan salah satu pengguna bertindak sebagai inisiator untuk melakukan *channel probing*. Diasumsikan bahwa Alice bertindak sebagai inisiator dan Bob sebagai *responder*. Alice dan Bob harus mengirim sinyal *probe* satu sama lain untuk mendapatkan h_x dan h_y . Eve yang bertindak sebagai penyadap berjarak $\lambda/2$ dari Alice dan Bob juga mendengarkan sinyal *probing* tersebut (E_X dan E_Y), tetapi sulit bagi Eve untuk mendapatkan sinyal *probing* yang sama karena adanya sifat *spatial decorrelation* dari skema SKG yang memanfaatkan keacakan karakteristik kanal.



Gbr. 1 Desain sistem SKG.



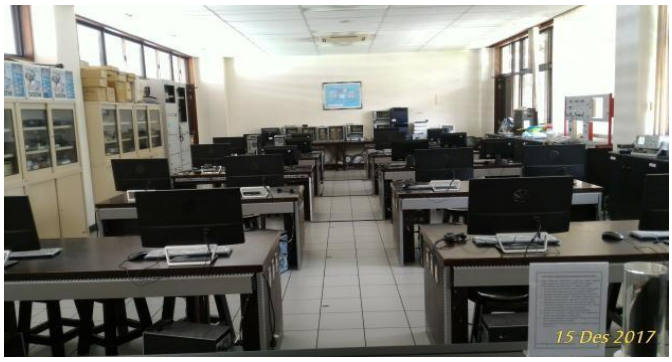
Gbr. 2 Tahapan pembangkitan *secret key*.

Lima tahapan yang digunakan untuk mendapatkan *secret key* meliputi *channel probing*, praproses data pengukuran, kuantisasi, rekonsiliasi informasi, *privacy amplification* sekaligus verifikasi seperti yang terlihat pada Gbr. 2. *Channel probing* merupakan salah satu tahapan yang bertujuan untuk mengumpulkan parameter kanal dengan mengirim sinyal satu sama lain antara dua pengguna yang sah. Parameter kanal yang didapatkan dari hasil pengukuran diproses terlebih

dahulu dengan menggunakan beberapa metode peningkatan *reciprocity*. Kuantisasi bertujuan untuk mengubah parameter kanal hasil praproses menjadi bit. Ketidakcocokan bit antara dua pengguna dikoreksi pada tahap rekonsiliasi informasi. Tahap akhir adalah *privacy amplification* dan verifikasi yang bertujuan untuk memastikan kecukupan entropi dan integritas dari *secret key* yang dihasilkan. Dalam skema enkripsi *hybrid* (gabungan antara skema enkripsi klasik dan PLS), *secret key* yang dihasilkan digunakan untuk mengacak pesan dan mengembalikan pesan teracak ke dalam bentuk pesan semula.

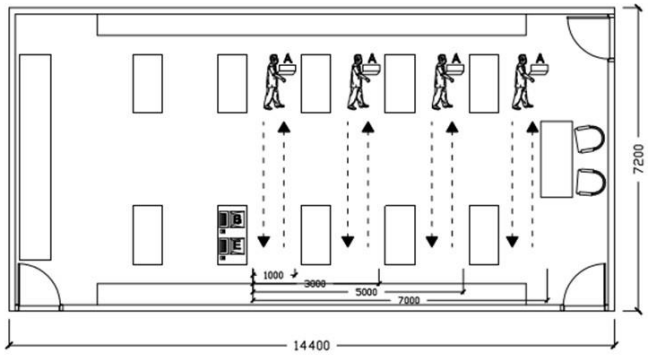
B. Mekanisme Pengukuran

Pengukuran dilakukan pada dua pengguna dengan 802.11 radio. Alice dikonfigurasi sebagai mode AP yang dilengkapi dengan *virtual monitor interface* untuk menangkap paket yang diterima. Bob dikonfigurasi sebagai klien yang juga dilengkapi dengan *virtual monitor interface*. Gbr. 3 menunjukkan urutan pengiriman paket dalam pengambilan data RSS. Aplikasi Wireshark sebagai *virtual monitor interface* berjalan di sisi klien dan AP untuk merekam semua paket yang diterima. Eksperimen dilakukan dengan mengirim 4.000 ICMP PING dari Alice ke Bob, dengan masing-masing paket *ping request* yang diterima oleh klien membangkitkan paket *Mac-layer acknowledgement (Ack)* yang dikirim kembali ke AP, diikuti oleh paket *ping response*. Setelah menerima paket *ping response*, AP juga membalas dengan paket *Mac-layer Ack*. Paket yang direkam dengan Wireshark difilter dengan menggunakan *Mac address* untuk mendapatkan paket yang telah disebutkan sebelumnya.

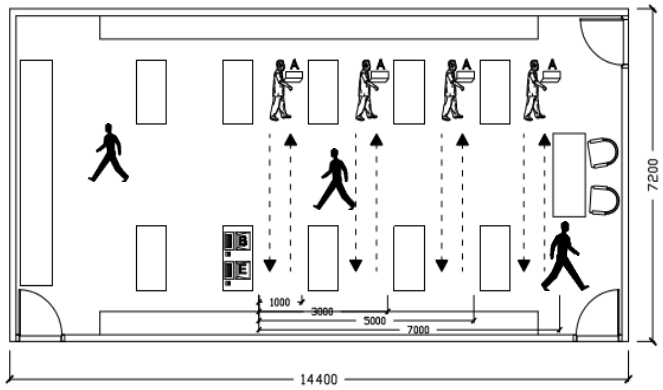


Gbr. 3 Ruang pengukuran.

Dalam makalah ini, dilakukan pengukuran di lingkungan *indoor*, yakni pada Lab E-107 Gedung D4 Politeknik Elektronika Negeri Surabaya (PENS). Terdapat dua jenis skenario dalam proses pengujian, yaitu skenario 1 dan 2, dengan perbedaan antara skenario 1 dan 2 adalah adanya lalu lalang manusia berjalan yang diasumsikan sebagai tempat ramai (skenario 2) dan kondisi sepi (skenario 1). Gbr. 3 menunjukkan ruang pengukuran, sedangkan Gbr. 4 dan Gbr. 5 menunjukkan gambaran skenario yang digunakan. Dengan menggunakan tiga buah laptop sebagai Alice, Bob, dan Eve, pengujian dilakukan hingga diperoleh 4.000 data parameter kanal RSS dengan interval pengukuran 50 ms. Bob dan Eve diam dengan jarak 5 cm, sedangkan Alice berjalan-jalan dengan variasi jarak 1 m hingga 7 m dari Bob.



Gbr. 4 Skenario 1.



Gbr. 5 Skenario 2.

IV. HASIL DAN PEMBAHASAN

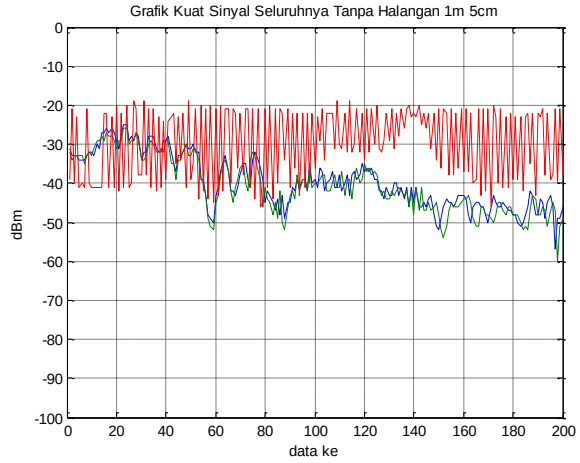
Pada bagian ini dibahas mengenai keberhasilan skema pembangkitan *secret key* yang dibangun, serta analisis kinerja sistem.

A. Keberhasilan Skema Pembangkitan Secret Key

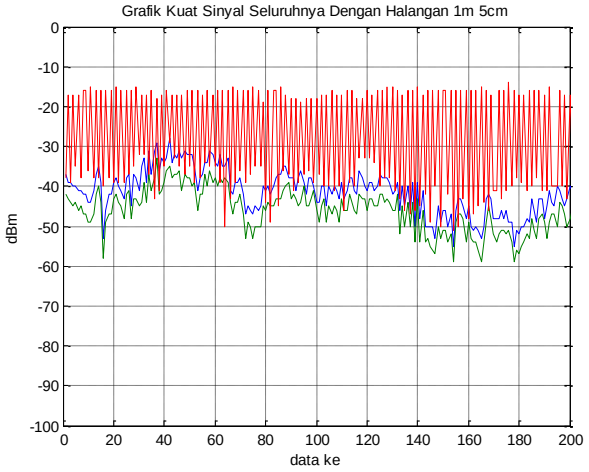
Keberhasilan sistem pembangkitan *secret key* dilihat dari keberhasilan masing-masing tahap yang digunakan. Detail keberhasilan yang akan dianalisis meliputi keberhasilan *channel probing* serta pengaruh penggunaan metode *hierarchical clustering* terhadap hasil pengukuran.

1) Keberhasilan Channel Probing: Pada tahap ini dilakukan pengujian korelasi untuk dianalisis sesuai kondisi dan skenario yang telah ditentukan. Gbr. 6 dan Gbr. 7 menunjukkan gambaran sinyal RSS dalam kondisi sepi dan ramai. Sinyal berwarna hijau merupakan sinyal RSS Alice, sinyal berwarna biru merupakan sinyal RSS Bob, sedangkan sinyal berwarna merah merupakan sinyal RSS Eve. Alice dan Bob memiliki tingkat kemiripan yang tinggi, terlihat dari miripnya sinyal RSS yang dihasilkan, sedangkan Eve memilki sinyal yang benar-benar berbeda. Detail korelasi sinyal yang dihasilkan ditunjukkan pada Tabel I. Dari korelasi yang dihasilkan, terlihat bahwa pada skenario 2 nilai korelasi yang diperoleh tidak setinggi skenario 1, bahkan pada kondisi tertentu sempat kehilangan paket data antara Alice dan Bob, sehingga nilai korelasinya tidak mampu dihitung karena panjang data antara Alice dan Bob tidak sama. Hal ini juga disebabkan karena banyaknya pantulan di sekitar ruangan dan adanya manusia yang beraktifitas, baik berjalan maupun

duduk dengan mengaktifkan ponselnya. Jika ditinjau dari segi ligkungan, di Lab E-107 terdapat banyak PC dan benda-benda sehingga menyebabkan pantulan sinyal antara pengirim (Bob) dan penerima (Alice) menyebar atau bahkan hilang.



Gbr. 6 Gambaran sinyal RSS pada skenario 1.



Gbr. 7 Gambaran sinyal RSS pada skenario 2.

2) Keberhasilan Praproses Data: Pada tahap ini dilakukan peningkatan *reciprocity* RSS yang dihasilkan dengan menggunakan metode *hierarchical clustering*. Praproses data dilakukan dengan membagi 4.000 data RSS menjadi beberapa variasi blok, yaitu 50, 100, 200 dan 1.000. Tabel II menunjukkan peningkatan korelasi dari penambahan tahap praproses data pada skenario 1 dan 2. Dari hasil pengujian terlihat bahwa rata-rata korelasi dari hasil praproses data pada skenario 1 mengalami peningkatan sebesar 15%, dengan peningkatan korelasi tertinggi untuk skenario 1 diperoleh saat jumlah blok data 200 yaitu 0,98853. Sedangkan pengujian pada skenario 2 menunjukkan rata-rata peningkatan korelasi sebesar 20%, dengan peningkatan korelasi tertinggi diperoleh saat jumlah blok data 100 yaitu 0,9796.

B. Kinerja Sistem

Terdapat tiga parameter sistem yang diuji dalam makalah ini, dengan parameter tersebut meliputi KDR, KGR, serta keacakan.

TABEL I
PENGUJIAN KORELASI

Skenario	Pengguna	Jarak (m)	Korelasi
Skenario 1	Alice-Bob	1	0,837239
		3	0,557072
		5	0,340374
		7	0,658612
	Alice-Eve	1	0,0352
		3	0,016509
		5	0,005216
		7	0,024294
	Bob-Eve	1	0,0116
		3	0,025304
		5	0,019041
		7	0,033536
Skenario 2	Alice-Bob	1	0,775515
		3	0,262295
		5	0,364664
		7	0,112
	Alice-Eve	1	0,045829
		3	0,029182
		5	0,021359
		7	0,003
	Bob-Eve	1	0,02842
		3	0,014837
		5	0,000756
		7	0,014460

TABEL II
PENINGKATAN KORELASI HASIL PRAPROSES DATA

Skenario	Jumlah blok data	Korelasi Awal	Korelasi hasil pra proses data
Skenario 1	50	0,83729	0,83724
	100		0,98641
	200		0,98853
	1000		0,98459
Skenario 2	50	0,775515	0,77552
	100		0,9796
	200		0,97543
	1000		0,9539

1) KDR: Pengujian KDR dilakukan untuk mengetahui besar perbedaan persentase bit yang dihasilkan dua pengguna. Dari hasil pengujian yang ditunjukkan oleh Tabel III terlihat bahwa skenario 2 memiliki nilai KDR yang lebih tinggi dibandingkan dengan skenario 1. Hal ini terjadi karena data pada skenario 2 memiliki rata-rata korelasi yang lebih rendah dibandingkan dengan skenario 1, sehingga mengakibatkan berkurangnya kemiripan (*reciprocity)* sinyal antara dua pengguna. Pada skenario 1 dan 2, KDR tertinggi didapat saat jumlah blok data 50 dengan nilai minimal adalah 20%.

2) KGR: KGR yang dihasilkan setelah kuantisasi KGR_{ik} berhubungan dengan mekanisme kuantisasi yang digunakan. Kuantisasi yang digunakan adalah kuantisasi Aono. Kuantisasi ini membuang data RSS yang terletak di median. Semakin banyak data yang terbuang, maka semakin rendah

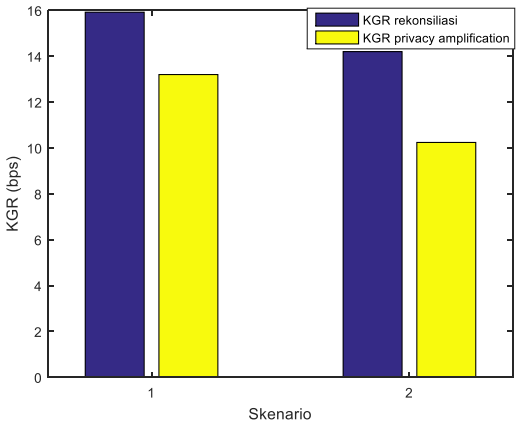
KGR yang dihasilkan. Hasil pengujian yang dilakukan, ditunjukkan pada Tabel IV, menunjukkan bahwa KGR tertinggi dengan menggunakan kuantisasi Aono diperoleh saat jumlah blok data 200 pada skenario 1, yaitu sebesar 19,98 bps dan jumlah blok data 100 pada skenario 2, yaitu sebesar 17 bps. Hasil pengujian juga menunjukkan bahwa KGR yang dihasilkan dengan kuantisasi Aono juga lebih tinggi jika dibandingkan dengan KGR yang dihasilkan dengan metode Mathur [14].

TABEL III
PENGUJIAN KDR

Skenario	Jumlah blok data	KDR (%)
Skenario 1	50	20
	100	10
	200	7
	1000	15
Skenario 2	50	22
	100	17
	200	18
	1000	18,5

TABEL IV
PENGUJIAN KGR

Skenario	Jumlah blok data	KGR setelah kuantisasi (bps)	
		Aono	Mathur
Skenario 1	50	16	2
	100	19	4
	200	19,98	3
	1000	18	2,4
Skenario 2	50	14	3
	100	17	1
	200	16,8	2
	1000	16,5	2,2



Gbr. 8 KGR setelah rekonsiliasi dan *privacy amplification*.

KGR setelah rekonsiliasi KGR_r diperoleh dengan memecah blok data menjadi 199 bit dan membuang blok data yang tidak mampu dikoreksi, sedangkan KGR setelah *privacy amplification* KGR_{pa} diperoleh dengan memecah blok data menjadi 256 bit (ukuran kunci yang diinginkan) dan membuang blok data yang memiliki nilai entropi di bawah persyaratan keacakan. Grafik pada Gbr. 8 menunjukkan KGR_r dan KGR_{pa} yang dihasilkan dengan skema kuantisasi Aono. Hasil pengujian yang dilakukan menunjukkan bahwa skenario 2 memiliki nilai KGR_r yang lebih rendah jika dibandingkan dengan skenario 1, demikian juga dengan KGR_{pa}. Hal ini disebabkan banyaknya gangguan yang berupa lalu lalang manusia serta adanya sinyal lain seperti sinyal ponsel pada skenario 2, yang mengakibatkan meningkatnya perbedaan sinyal antara dua pengguna sehingga banyak blok data yang dibuang karena tidak mampu diperbaiki.

TABEL V
PENGUJIAN KEACAKAN SKENARIO 1 DAN 2

Skenario	Entropi	Blok frek	*Cusum*	Frek	*Longest run*	*run*
1	0,64	0,41	0,85	0,90	0,95	0,80
2	0,92	0,66	0,68	0,38	0,4	0,56

3) Keacakan: Untuk memastikan keacakan bit yang dibangkitkan, dilakukan tes keacakan dengan menggunakan NIST *suite*. Hasil pengujian pada Tabel V menunjukkan bahwa data yang diperoleh dari skenario 1 dan 2 memenuhi keenam persyaratan keacakan dengan $p \geq 0{,}01$, sehingga dapat dikatakan bahwa bit *secret key* yang dihasilkan benar-benar acak dengan tingkat kepercayaan 99%. Tes frekuensi digunakan untuk menentukan jumlah 1 dan 0 dalam satu rangkaian bit kunci sama atau tidak, tes blok frekuensi digunakan untuk menguji frekuensi dari bit 1 pada blok M adalah $M/2$ atau tidak, tes *run* digunakan untuk menentukan osilasi dari 0 dan 1 terlalu cepat atau terlalu lambat, tes *longest run* digunakan untuk menentukan banyaknya bit 1 pada rangkaian kunci konsisten dengan panjang bit 1 pada bilangan acak atau tidak, tes entropi digunakan untuk membandingkan frekuensi dari blok yang *overlapping* dengan panjang yang berurutan, sedangkan tes *cusum* digunakan untuk menentukan jumlah kumulatif dari bit kunci yang dihasilkan relatif terlalu besar atau terlalu kecil terhadap jumlah kumulatif yang diharapkan dari sebuah bit kunci yang acak.

V. KESIMPULAN

Dalam makalah ini, telah dilakukan investigasi secara mendetail terhadap pengaruh penggunaan metode *hierarchical clustering* terhadap skema pembangkitan *secret key* di lingkungan *indoor* dengan dua variasi skenario. Hasil pengujian yang dilakukan menunjukkan adanya peningkatan korelasi dari dua data hasil pengukuran, dengan peningkatan yang signifikan terjadi pada skenario 2 dengan rata-rata peningkatan sebesar 20%. Selain itu, dari analisis kinerja terlihat bahwa penurunan korelasi juga dapat menurunkan KDR, sehingga nilai KDR maksimal yang diperoleh berada di bawah standar 50%, yaitu sebesar 20%. Bit *secret key* yang dihasilkan dari skenario 1 dan 2 juga telah memenuhi keenam persyaratan keacakan dengan nilai $p \geq 0{,}01$, sehingga dapat dikatakan bahwa bit *secret key* yang dihasilkan benar-benar acak dengan tingkat kepercayaan 99%.

UCAPAN TERIMA KASIH

Penelitian ini didanai oleh Kementrian Riset, Teknologi, dan Pendidikan Tinggi, Penelitian Dasar Terapan Unggulan Perguruan Tinggi Tahun 2018.

REFERENSI

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Upper Saddle River, NJ, USA: Prentice Hall, 2013.

[2] A. Karima, L.B. Handoko, dan A. Saputro, "Pemfaktoran Bilangan Prima pada Algoritma ElGamal untuk Keamanan Dokumen PDF," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, Vol. 6, No.3, hal. 252-258, Agustus 2017.

[3] A. Mukherjee, S. Fakoorian, J. Huang, dan A. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Commun. Surveys Tuts*., Vol. 16, No. 3, hal. 1550–1573, 2014.

[4] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, dan S. V. Krishnamurthy, "Secret Key Extraction from Wireless Signal Strength in Real Environments," *IEEE Trans. Mobile Comput*., Vol. 12, No. 5, hal. 917–930, 2013.

[5] S. Ali, V. Sivaraman, dan D. Ostry, "Eliminating Reconciliation Cost in Secret Key Generation for Body-Worn Health Monitoring Devices," *IEEE Trans. Mobile Comput*., Vol. 13, No. 12, hal. 2763–2776, 2014.

[6] B. Zan, M. Gruteser, dan F. Hu, "Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems," *IEEE Trans. Veh. Technol.*, Vol. 62, No. 8, hal. 4020–4027, 2013.

[7] M. Yuliana, Wirawan, dan Suwadi "Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment," *IJCNIS*, Vol. 9, No. 3, hal. 474–483, 2017.

[8] J. Zhang, R. Woods, T.Q.Duong, A. Marshall, dan Y. Ding, "Experimental Study on Channel Reciprocity in Wireless Key Generation", *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2016, hal. 1-5.

[9] L. Shi, J. Yuan, S. Yu, dan M. Li, "ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks," *Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC'13*, 2013, hal. 155–166.

[10] M. Edman, A. Kiayias, Q. Tang, dan B. Yener. "On the Security of Key Extraction from Measuring Physical Quantities," *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 8, hal. 1796-1806, Agustus 2016.

[11] A. Badawy, T. Khattab, T. Elfouly, A. Mohamed, D. Trinchero, "Secret Key Generation Based on Channel and Distance Measurements," *2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops*, ICUMT, 2014, hal. 136–142.

[12] J. Zhang, T. Q. Duong, A. Marshall, dan R. Woods, "Key Generation from Wireless Channels: A Review," *IEEE Access*, Vol. 4, hal. 614–626, 2016.

[13] M. Yuliana, Wirawan, dan Suwadi, "Performance Evaluation of the Key Extraction Schemes in Wireless Indoor Environment," *Proceedings - International Conference on Signals and Systems, ICSigSys 2017*, 2017, hal. 138-144.

[14] C. Ye, S. Mathur, A. Reznik, Y. Shah,W. Trappe, dan N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *IEEE Trans. Inf. Forensics Security*, Vol. 5, No. 2, hal. 240– 254, 2010.