WEBINAR SERIES : NETWORK AND SECURITY

WI-FI SIGNAL FOR SECURITY APPLICATION

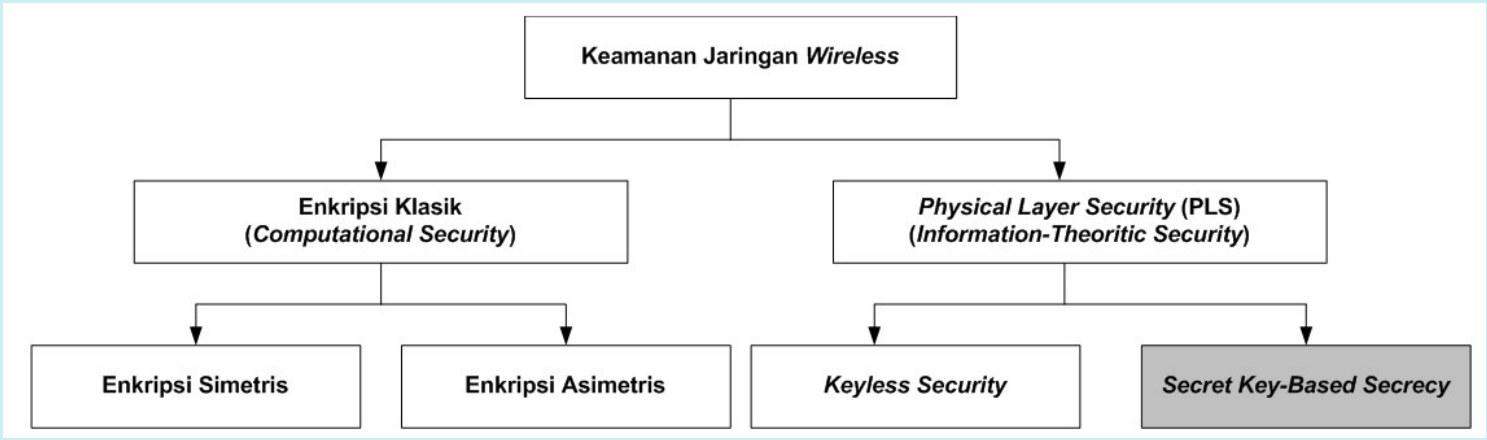
OLEH :

Dr. Mike Yuliana

Keamanan Jaringan Wireless (1)

- Teknologi *wireless* atau jaringan tanpa kabel telah berkembang sangat pesat saat ini
- Semua perangkat dapat saling berkomunikasi dalam jangkauan tertentu
- Rentannya komunikasi *wireless* terhadap adanya *passive attack* diantaranya penyadapan, analisa trafik serta monitoring maupun *active attack* diantaranya *jamming*, *spoofing*

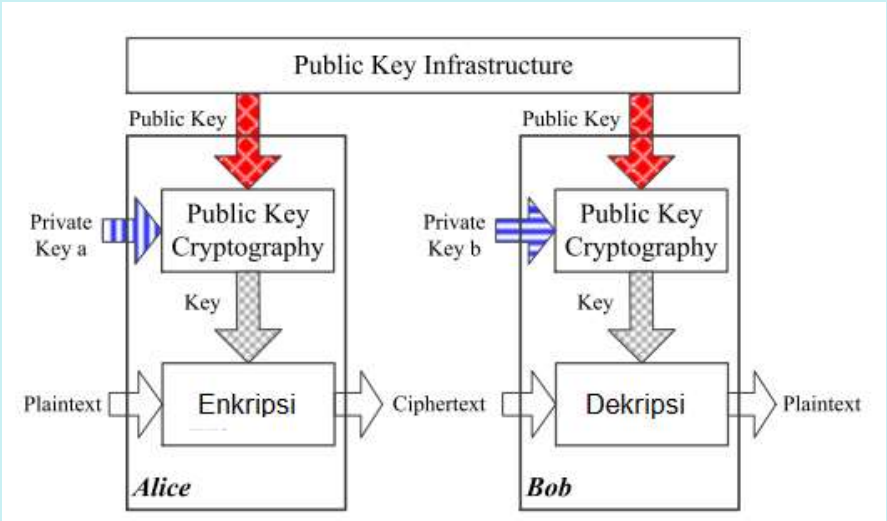
Keamanan Jaringan Wireless (2)



Taksonomi keamanan jaringan wireless

Permasalahan Enkripsi Klasik:

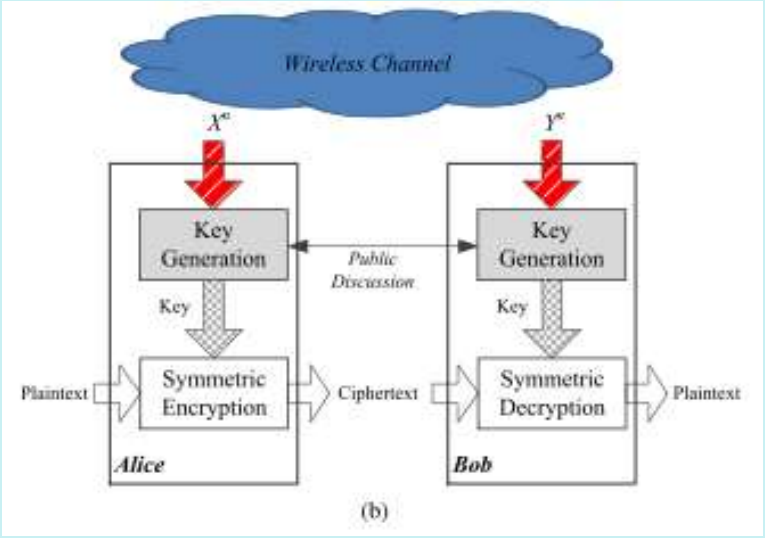
1. Ketergantungan pada kompleksitas komputasi
2. Ketergantungan pada infrastruktur manajemen kunci



Sumber : J. Zhang et.al, 2016

Enkripsi Klasik

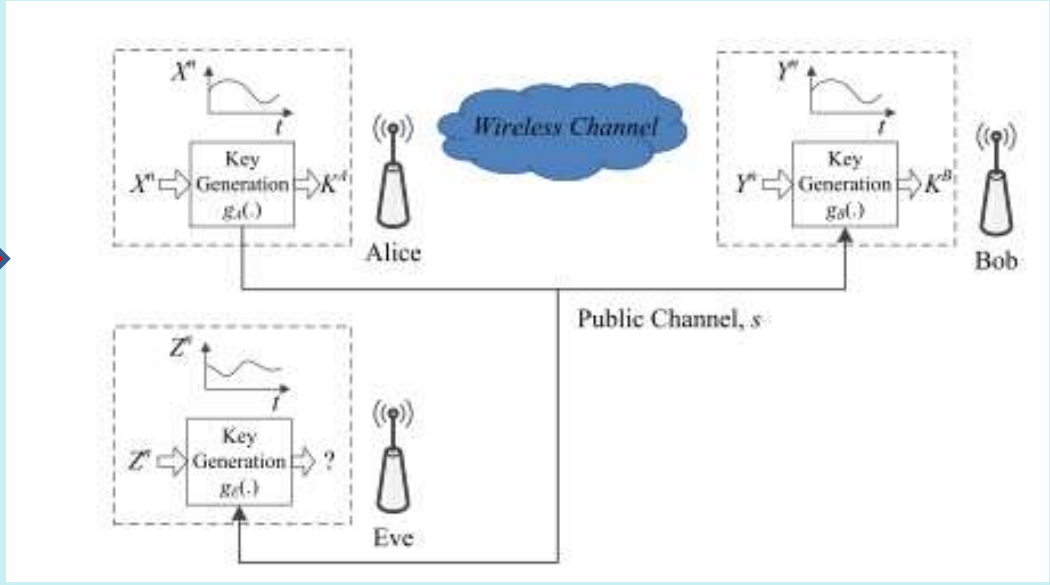
Keamanan Jaringan Wireless (3)



Sumber : J. Zhang et.al, 2016

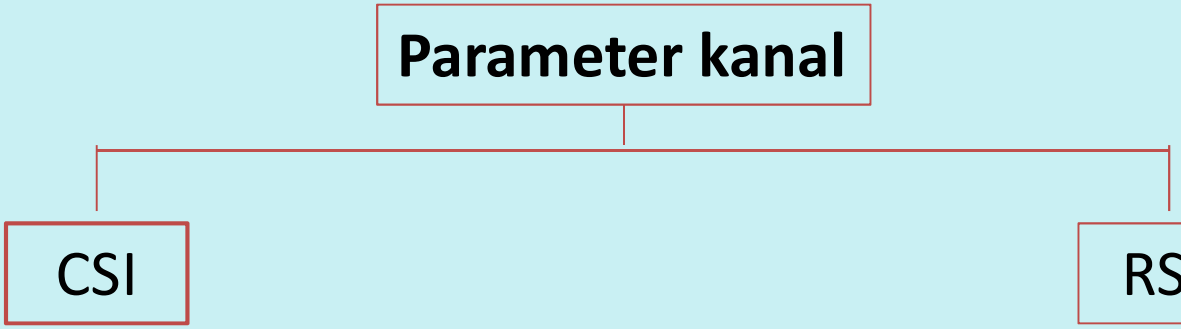
Hybrid cryptosystem

Pemodelan key generation



Sumber : J. Zhang et.al, 2016

Kanal Wireless (1)



Parameter kanal paling populer

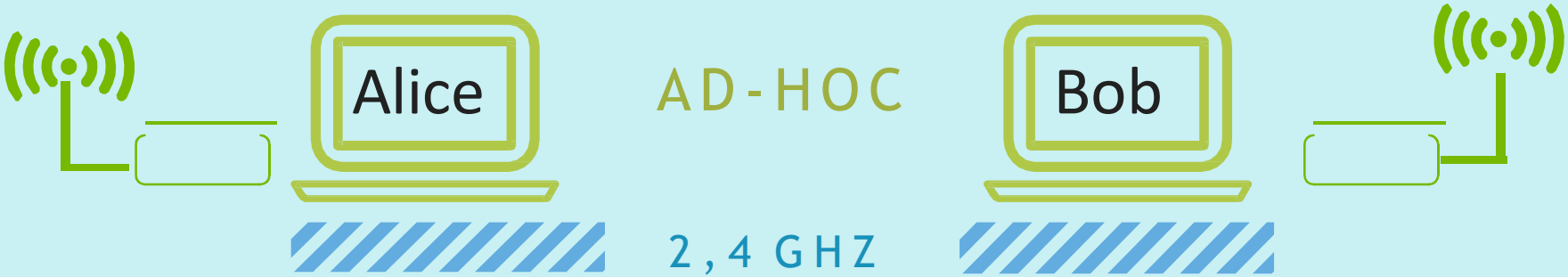
- Intel Wifi Link 5300 Wireless NIC
- universal software radio peripheral (USRP)
- wireless open-access research platform (WARP)

- Semua NIC

Kanal Wireless (2)

WiFi Adapter TP-Link

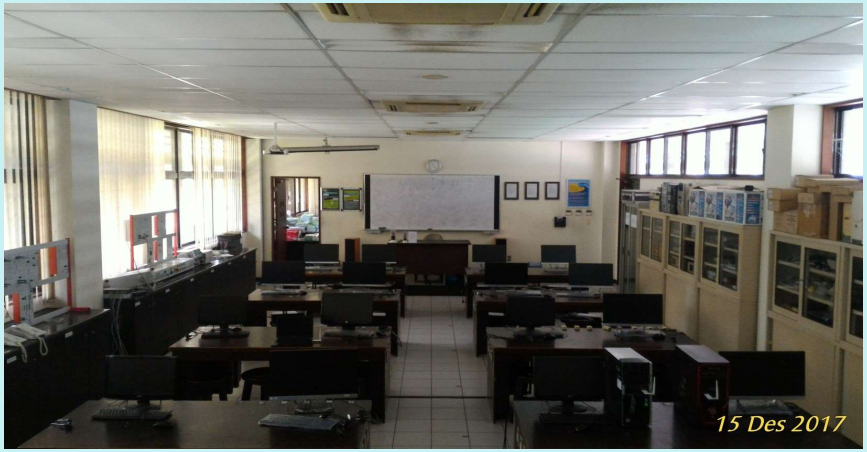
WiFi Adapter TP-Link

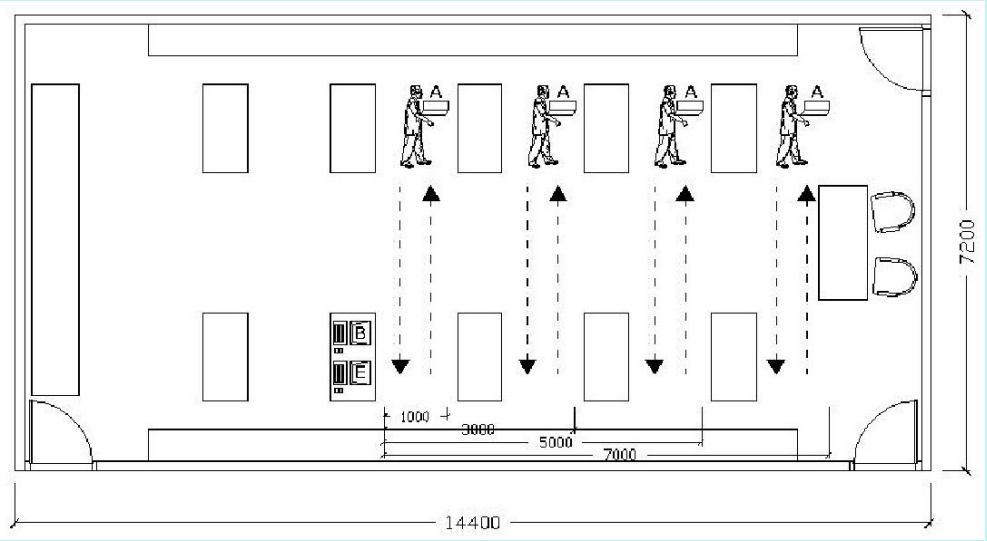


Perangkat yang digunakan

Kanal Wireless (3)

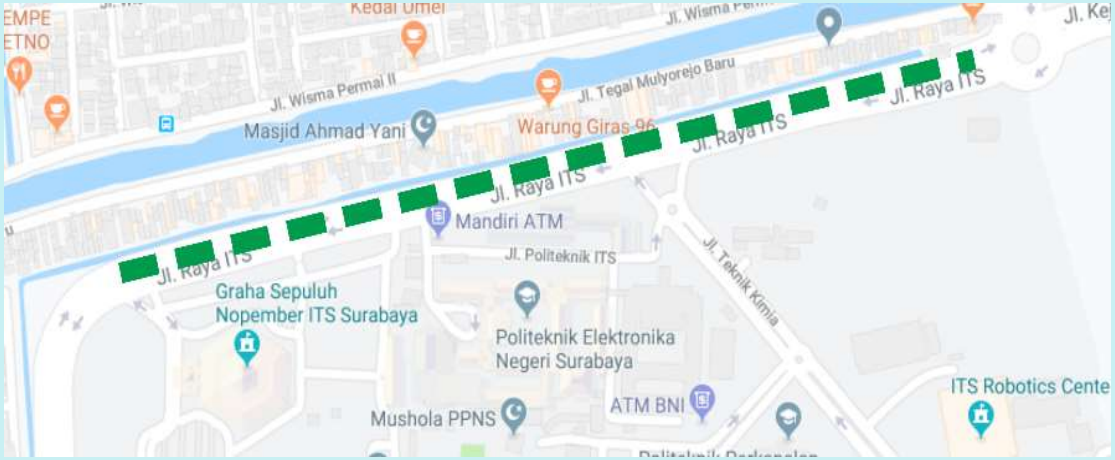
Lingkungan pengukuran (indoor)



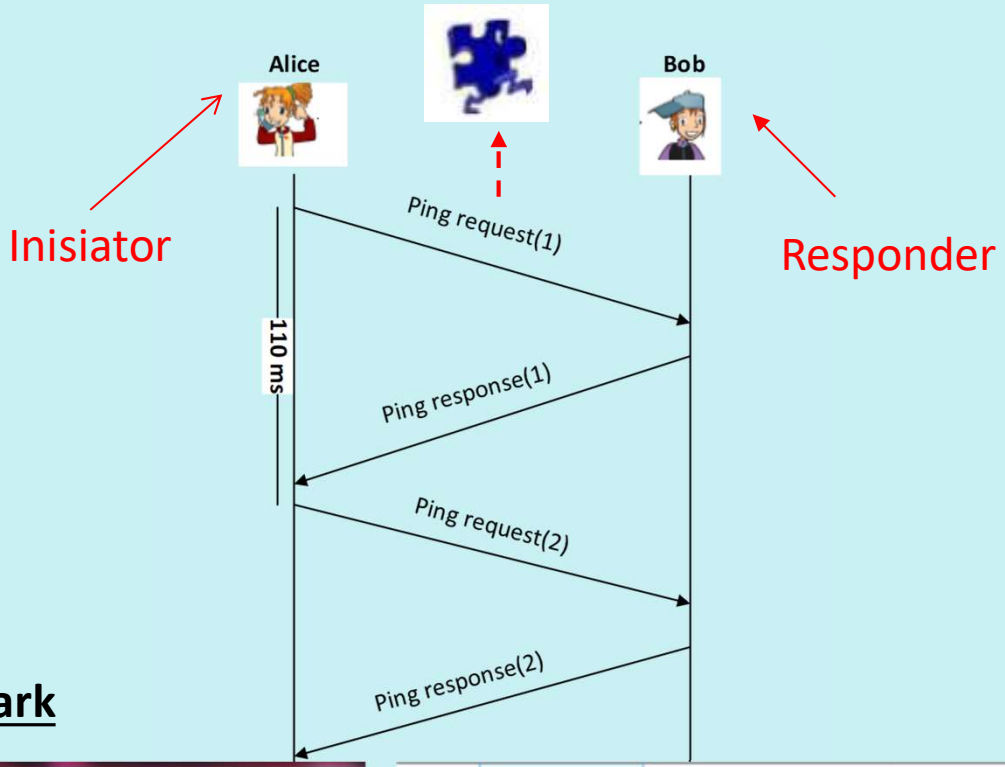


Kanal Wireless (4)

Lingkungan pengukuran (outdoor)



Kanal Wireless (3)



Capture dengan Wireshark

alice1m5cm.pcapng

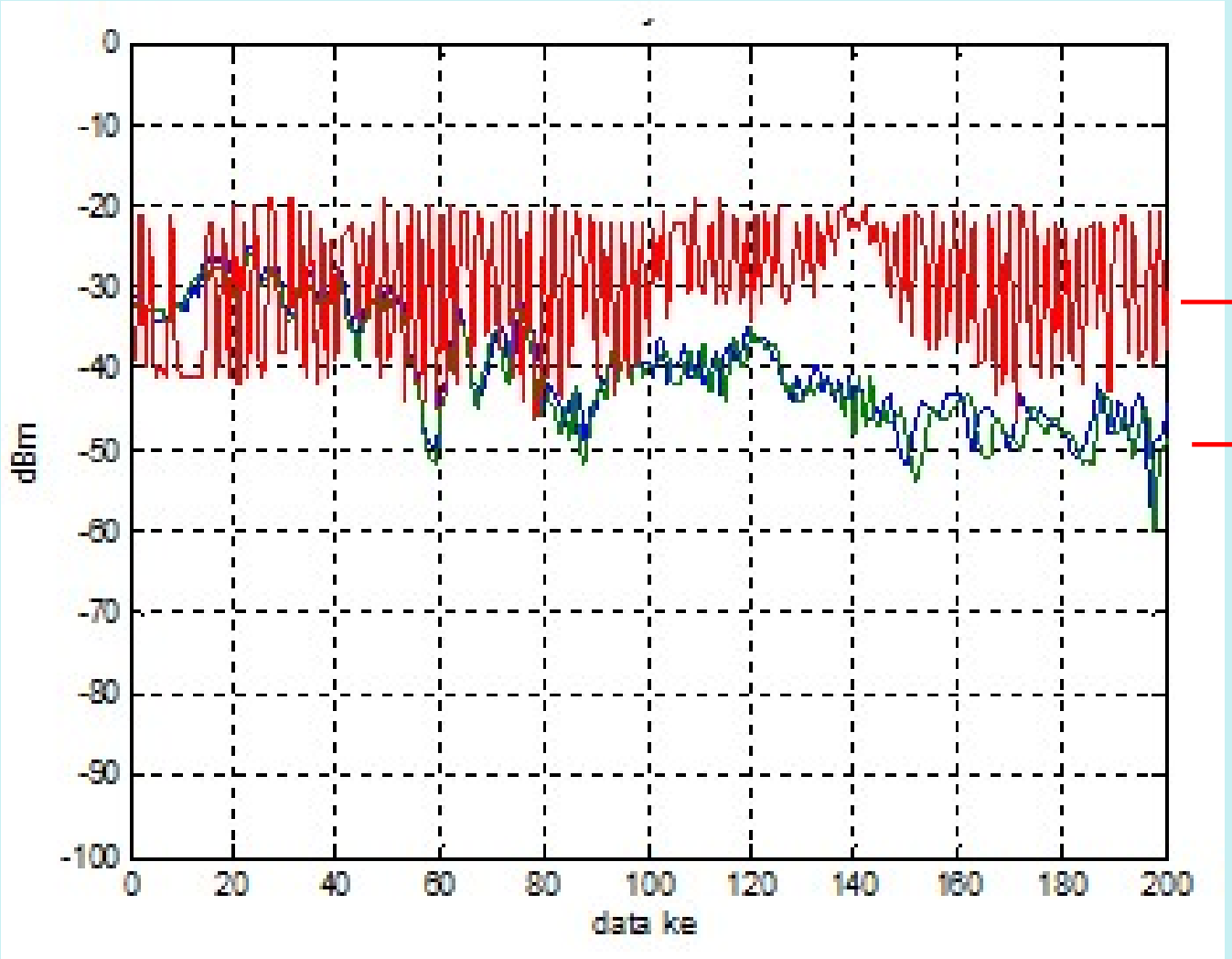
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
26309	101.865952	QuantaMi_b0:66:87	IPv6mcast_01	802.11	164	-81 dBm
26310	101.866361	QuantaMi_b0:66:87	IPv6mcast_01	802.11	164	-80 dBm
26311	101.866376	192.168.100.3	192.168.100.2	ICMP	131	
26312	101.866533		Tp-LinkT_0f:7e:b6 (…	802.11	50	-49 dBm
26313	101.867036	192.168.100.2	192.168.100.3	ICMP	158	-49 dBm
26314	101.877630	Cisco_0a:cd:91	Broadcast	802.11	312	-74 dBm
26315	101.877643		Azurewav_7a:31:3b (…	802.11	50	-86 dBm
26316	101.886471	Cisco_94:ff:b0 (f0:…	Azurewav_7a:31:3b (…	802.11	68	-85 dBm
26317	101.893531		SamsungE_8b:67:4c (…	802.11	50	-73 dBm
26318	101.893536	Cisco_0a:cd:90 (fc:…	SamsungE_8b:67:4c (…	802.11	68	-73 dBm
26319	101.902560	Cisco_0a:cd:93	Broadcast	802.11	303	-74 dBm
26321	101.912887	Cisco_94:ff:b1	Broadcast	802.11	309	-81 dBm
26322	101.915632	192.168.100.3	192.168.100.2	ICMP	131	
26323	101.915741		Tp-LinkT_0f:7e:b6 (…	802.11	50	-52 dBm
26324	101.916266	192.168.100.2	192.168.100.3	ICMP	158	-52 dBm
26325	101.919552		HonHaiPr_1a:4d:87 (…	802.11	50	-81 dBm
26327	101.921222		HonHaiPr_1a:4d:87 (…	802.11	50	-80 dBm
26328	101.921227	Cisco_94:ff:b0 (f0:…	HonHaiPr_1a:4d:87 (…	802.11	68	-81 dBm
26329	101.923261		HonHaiPr_1a:4d:87 (…	802.11	50	-80 dBm
26330	101.923266	Cisco_94:ff:b0 (f0:…	HonHaiPr_1a:4d:87 (…	802.11	68	-81 dBm
26331	101.928596		HonHaiPr_1a:4d:87 (…	802.11	50	-82 dBm
26332	101.934497	Cisco_94:ff:b3	Broadcast	802.11	300	-90 dBm

No.	Time	Source	Destination	Protocol	Length	Info
25982	100.756528	192.168.100.2	192.168.100.3	ICMP	158	-48 dBm
25993	100.806985	192.168.100.2	192.168.100.3	ICMP	158	-49 dBm
26005	100.858213	192.168.100.2	192.168.100.3	ICMP	158	-49 dBm
26015	100.907422	192.168.100.2	192.168.100.3	ICMP	158	-53 dBm
26025	100.957658	192.168.100.2	192.168.100.3	ICMP	158	-47 dBm
26050	101.007881	192.168.100.2	192.168.100.3	ICMP	158	-46 dBm
26062	101.060344	192.168.100.2	192.168.100.3	ICMP	158	-46 dBm
26081	101.111792	192.168.100.2	192.168.100.3	ICMP	158	-44 dBm
26099	101.158812	192.168.100.2	192.168.100.3	ICMP	158	-46 dBm
26115	101.211207	192.168.100.2	192.168.100.3	ICMP	158	-49 dBm
26129	101.261438	192.168.100.2	192.168.100.3	ICMP	158	-52 dBm
26142	101.316061	192.168.100.2	192.168.100.3	ICMP	158	-52 dBm

Kanal Wireless (4)



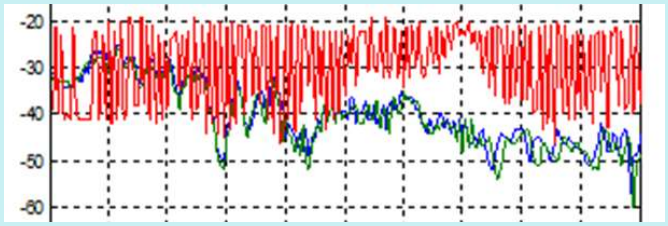
Data RSS Penyadap

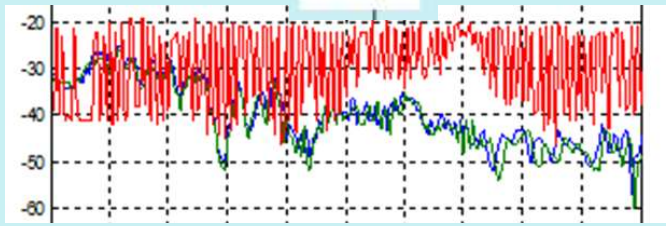
Data RSS kedua pengguna

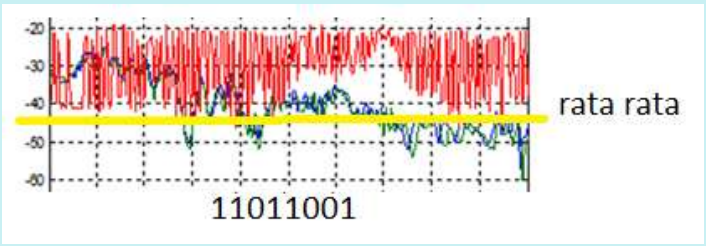
Tahapan Key Generation (1)

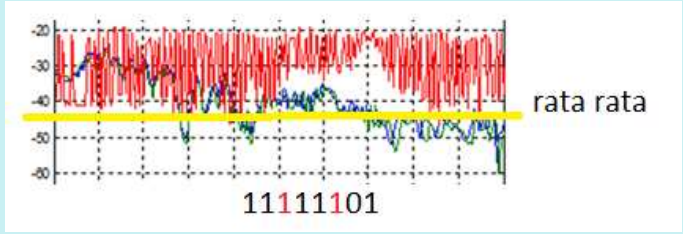
Alice

Bob









Capture RSS

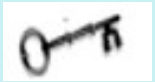
Kuantisasi

Koreksi error

Privacy amplification

11011001

11011001



Tahapan Key Generation (2)

Permasalahan di Masing-masing tahapan

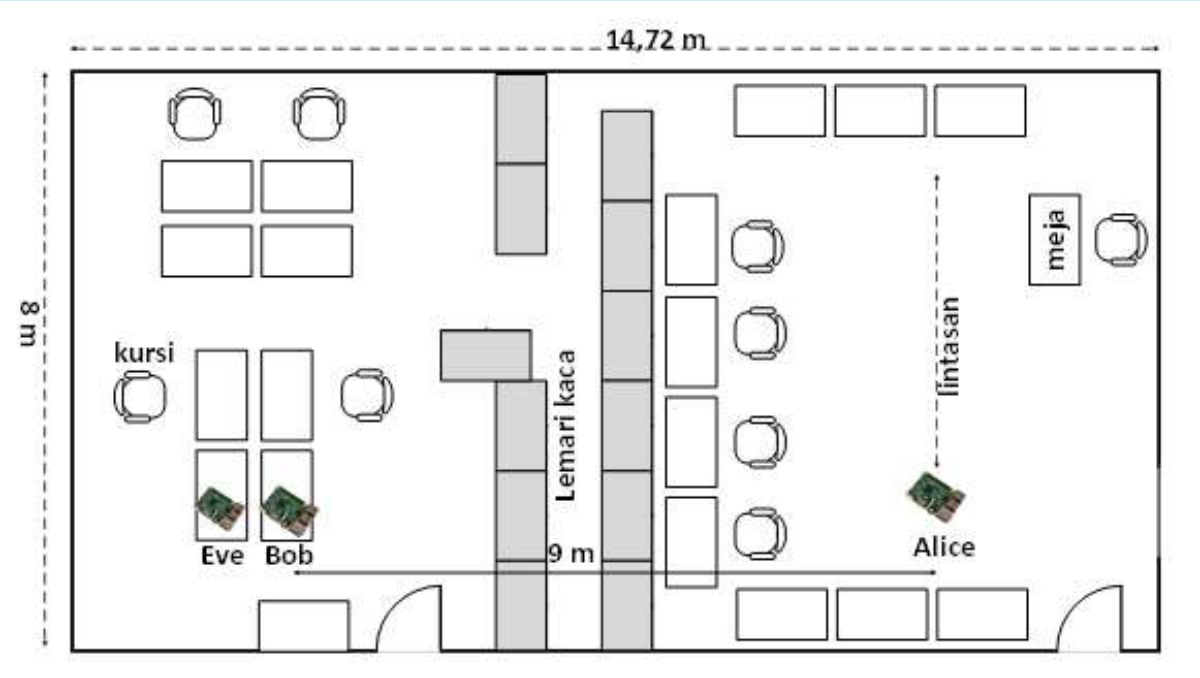
Tahapan Key Generation	Tujuan	Permasalahan
Capture RSS	Pengukuran kuat sinyal (RSS)	Adanya variasi RSS yang berbeda antara pengguna yang berkomunikasi karena: -noise -kondisi lingkungan -jenis perangkat wireless yang digunakan
Kuantisasi	Konversi RSS ke bit	Adanya hasil bit yang berbeda antara pengguna yang berkomunikasi karena: -tidak tepatnya level/threshold yang digunakan
Koreksi Error	Koreksi bit yang berbeda antar pengguna	Keterbatasan kemampuan koreksi dari metode yang digunakan serta lamanya proses koreksi
Privacy Amplification	Peningkatan keacakan serta verifikasi	

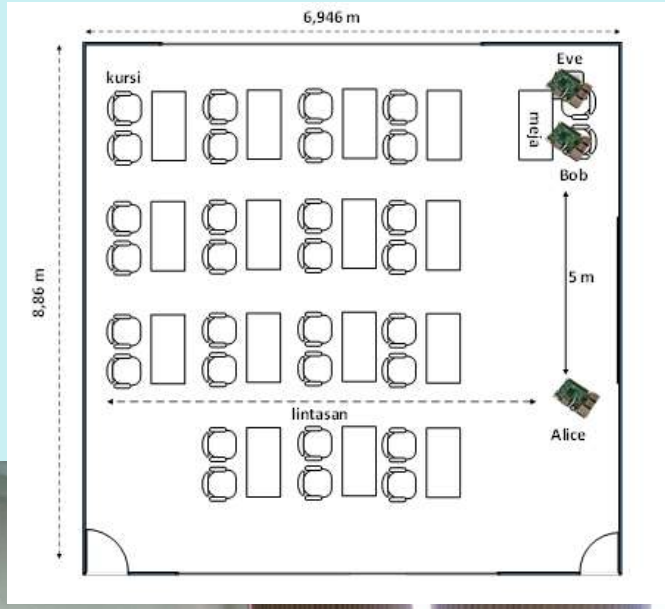
Skenario Aplikasi Key Generation (1)

Wireless Local Area Network (WLAN)

Sumber : M. Yuliana et.al, 2019

Koneksi WLAN → Laptop, PC, Handphone, Raspberry Pi (perangkat dengan sumber daya terbatas)
Standarisasi WLAN yang digunakan → IEEE 802.11 a/b/g/n yang beroperasi di 2.4 GHz dan 5 GHz



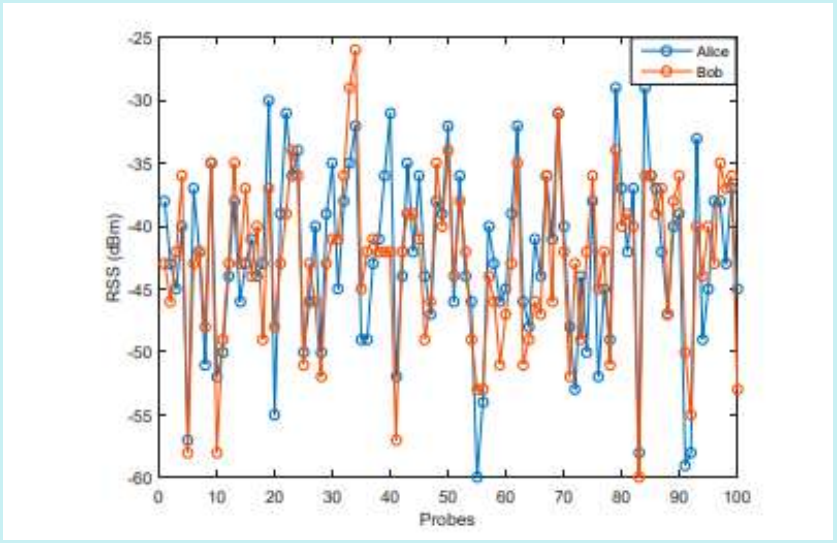


Skenario Aplikasi Key Generation (2)

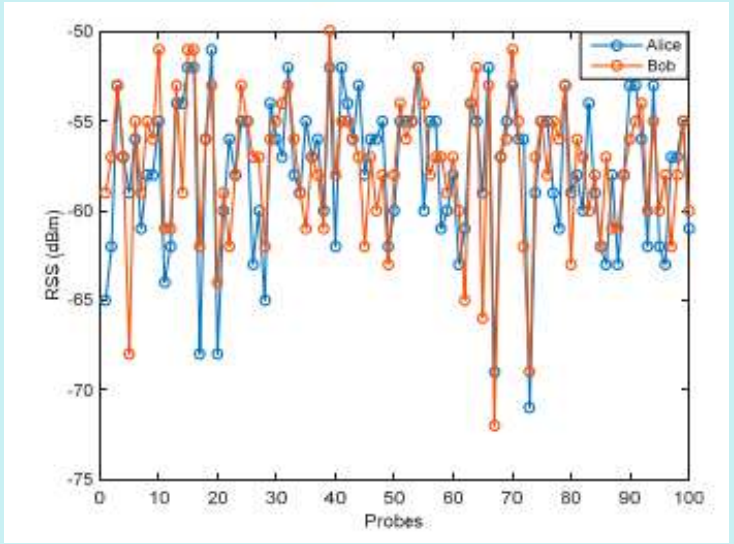
Sumber : M. Yuliana et.al, 2019

Wireless Local Area Network (WLAN)

- Kemiripan sinyal RSS yang diperoleh kedua pengguna lebih tinggi di lingkungan yang tanpa halangan



Tanpa halangan



Dengan halangan

Koefisien korelasi

Pengguna	Koefisien korelasi
Alice- Bob	0,7573
Alice-Eve	0.0216
Bob-Eve	0.0153
Alice-Bob	0,6988
Alice-Eve	0.0100
Bob-Eve	0.0282

Riset yang dilakukan :

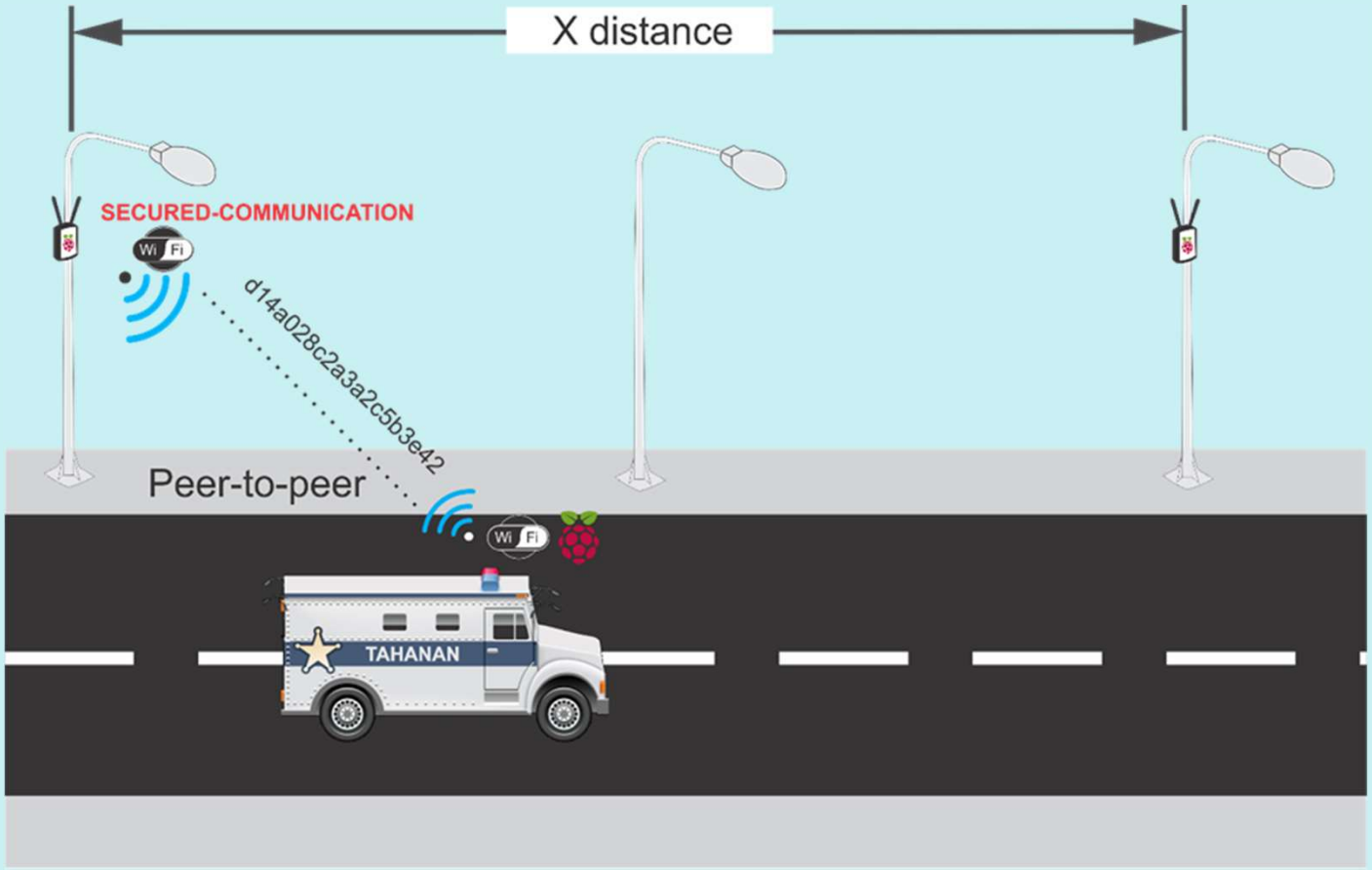
1. Meningkatkan kemiripan sinyal dengan melakukan modifikasi Kalman Filter
2. Mengusulkan metode kuantisasi baru → CMQ (menggunakan modifikasi mean dan variance)

Skenario Aplikasi Key Generation (3)

Vehicular Communication

Sumber : A. Visoka et al, 2019

- Beberapa riset juga menggunakan perangkat wireless IEEE 802.11



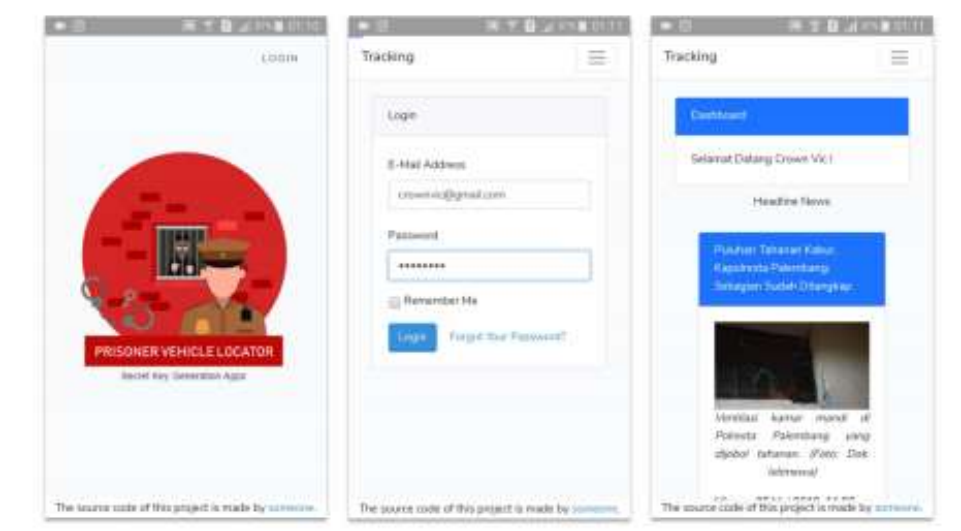
Sistem Keamanan Tracking posisi kendaraan tahanan

Skenario Aplikasi Key Generation (4)

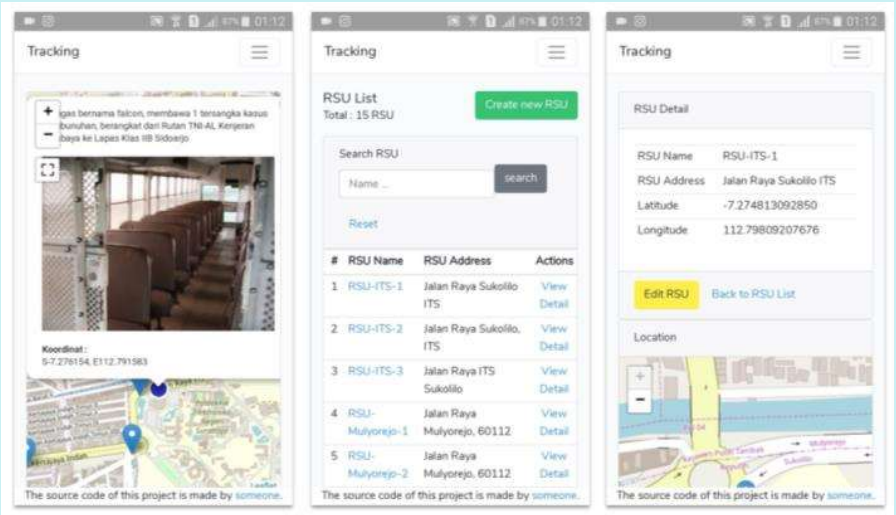
Vehicular Communication

Sumber : A. Visoka et al, 2019

Detil ilustrasi cara kerja sistem



Login



Tracking Interface

Skenario Aplikasi Key Generation (5)

Vehicular Communication

Sumber : A. Visoka et al, 2019

Aplikasi tracking

Video

Sumber : A. Visoka et al, 2019

Skenario Aplikasi Key Generation (6)

Vehicular Communication

Sumber : A. Visoka et al, 2019

a. 20 KM/H Non-Traffic Scenario

Device	Before Kalman	After Kalman
Vehicle – RSU1	0.423	0.911
Vehicle – RSU2	0.791	0.962

b. 30 KM/H Non-Traffic Scenario

Device	Before Kalman	After Kalman
Vehicle – RSU1	0.863	0.971
Vehicle – RSU2	0.125	0.830

c. 40 KM/H Non-Traffic Scenario

Device	Before Kalman	After Kalman
Vehicle – RSU1	0.109	0.815
Vehicle – RSU2	0.365	0.903

d. 20 KM/H Max-Traffic Scenario

Device	Before Kalman	After Kalman
Vehicle – RSU1	0.734	0.950
Vehicle – RSU2	0.724	0.909

e. 30 KM/H Max-Traffic Scenario

Device	Before Kalman	After Kalman
Vehicle – RSU1	0.898	0.983
Vehicle – RSU2	0.724	0.983

f. 40 KM/H Max-Traffic Scenario

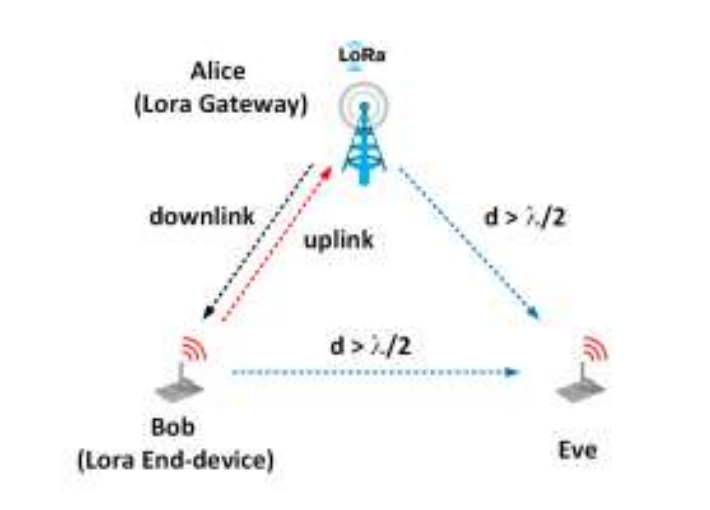
Device	Before Kalman	After Kalman
Vehicle – RSU1	0.039	0.872
Vehicle – RSU2	0.872	0.917

Riset yang dilakukan :

1. Meningkatkan kemiripan sinyal dengan menambahkan Kalman Filter sebelum kuantisasi
2. Memberikan kombinasi metode kuantisasi dan Kalman Filter

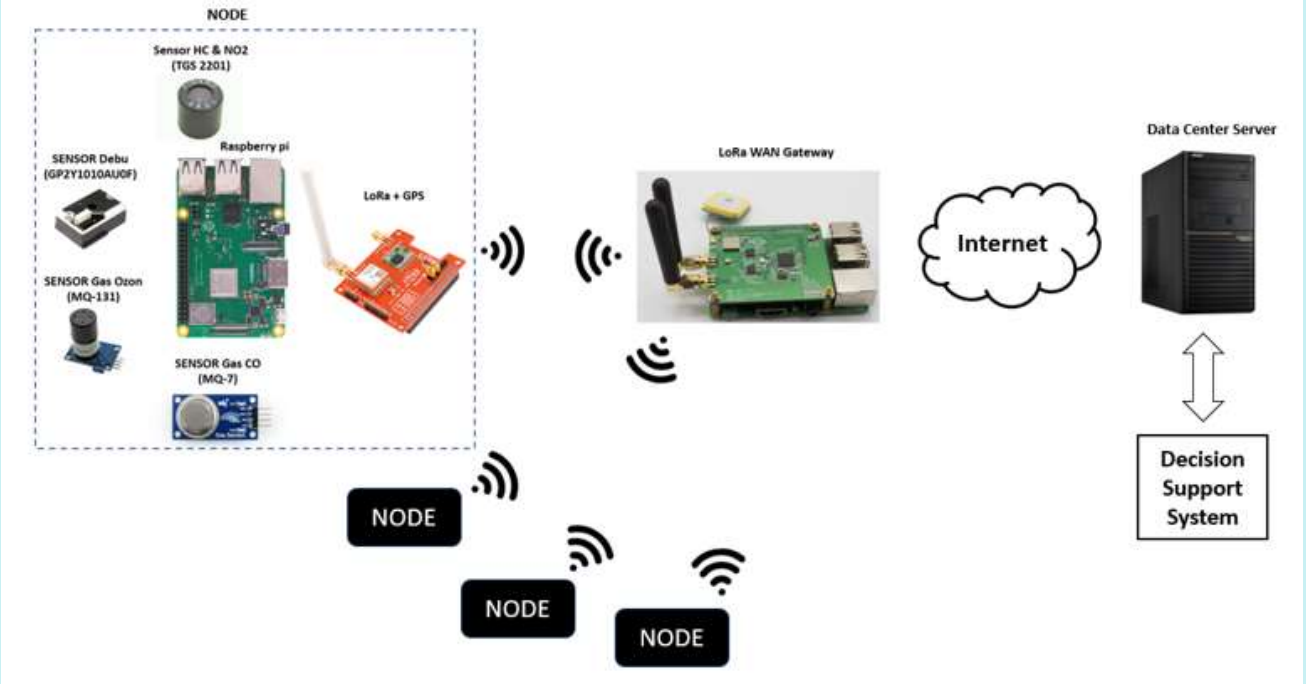
Skenario Aplikasi Key Generation (7)

Lora



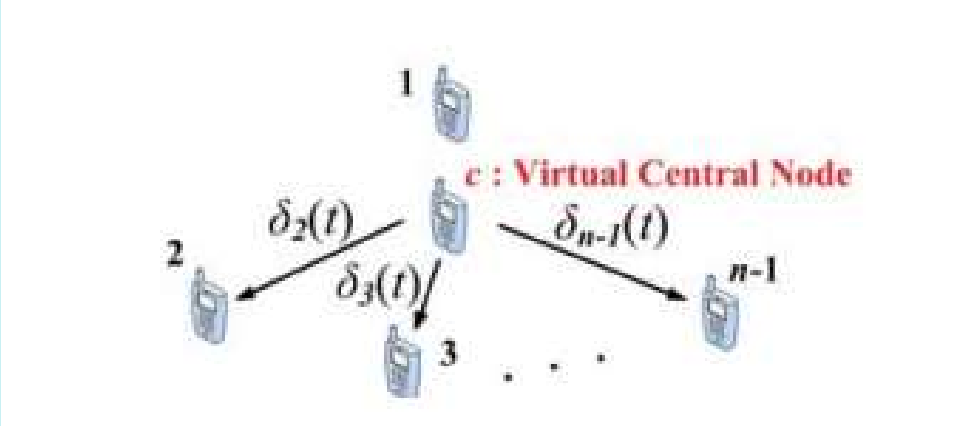
Sistem Model

Sumber : W. Xu et al, 2018



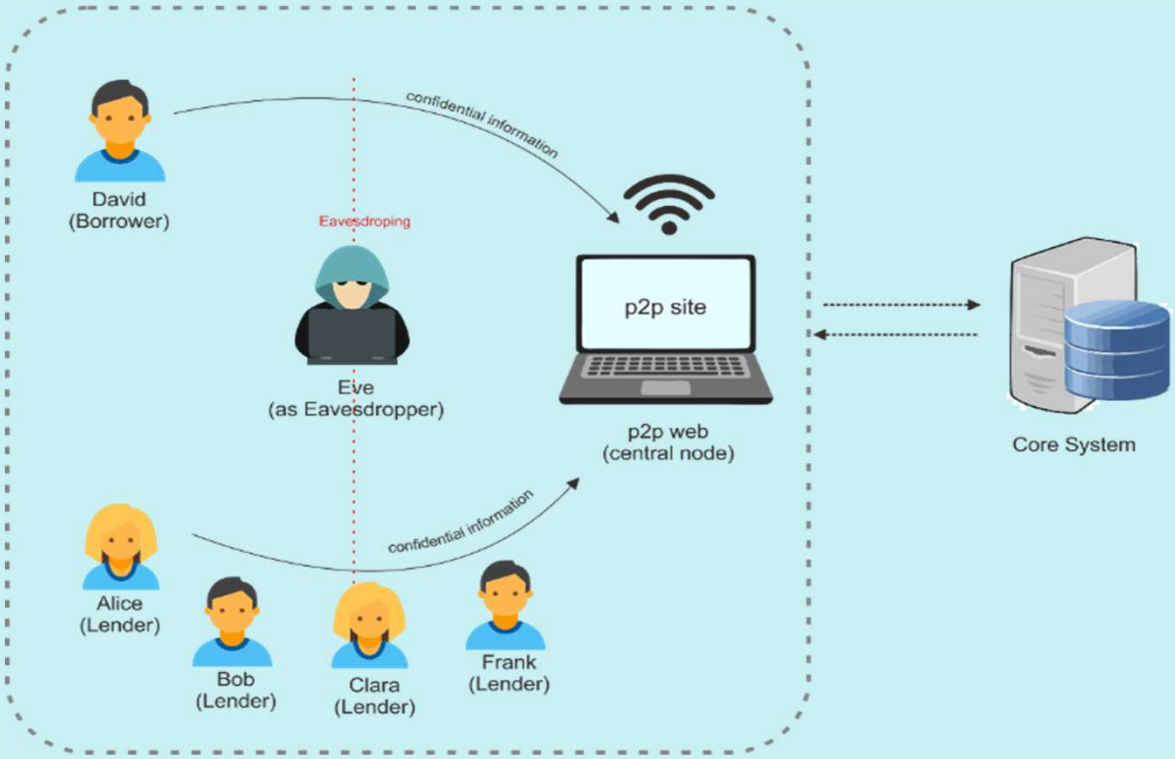
Skenario Aplikasi Key Generation (8)

Group key generation



Sistem Model

Sumber : H. Liu et al, 2014



Referensi

1. M. Yuliana, Wirawan. Suwadi, “A Simple Secret Key Generation by Using a Combination of Pre-Processing Method “, *Entropy*, 21(2), 192, 2019
2. A. Visoka *et.al*, “Analisa Keamanan Skema SKG Pada Analisa Tracking Posisi Mobil Tahanan”, Proyek Akhir PENS, 2019.
3. W. Xu *et al,* “LoRa-Key: Secure Key Generation System for LoRa-based Network”, J. *IEEE Int. of Things*, 2018
4. H. Liu *et al, “*Group Secret Key Generation via Received Signal Strength: Protocols, Achievable Rates, and Implementation”, *J. IEEE. Trans. On Mobile Comm*, 2014