JURNAL INFOTEL
Informatika - Telekomunikasi - Elektronika

Website Jurnal : http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN : 2085-3688; e-ISSN : 2460-0997

Kajian Aspek *Security* Pada Jaringan Informasi dan Komunikasi Berbasis *Visible Light Communication*

Syifaul Fuada
Pusat Penelitian Mikroelektronika, Institut Teknologi Bandung
Jln. Ganesha No. 10, Kampus ITB, Kota Bandung (40116), Jawa Barat, Indonesia
Email korespondensi : syifaulfuada@pme.itb.ac.id

Dikirim 15 Januari 2017, Direvisi 08 Februari 2017, Diterima 15 Februari 2017

Abstrak – Penerapan *visible light communication* (VLC) berlandaskan pada pedoman IEEE 802.15.17 yang mana aturan tersebut baru dirancang dalam waktu 5 tahun belakangan ini (sejak tahun 2009), didalamnya meliputi standar layer fisik (*physical layer*) dan layer MAC (*medium access control*). Sebagaimana teknologi komunikasi pada umumnya, VLC juga menyediakan akses *security* yang dibahas pada bagian layer MAC. Namun pada praktiknya masih belum begitu masif dilakukan oleh para peneliti. Hal ini sangat wajar karena mengingat VLC merupakan teknologi yang sedang dalam tahap pengembangan, yang menjadikan penelitian VLC umumnya berfokus pada 'bagaimana meningkatkan *speed* dari keterbatasan komponen-komponen pembangun (IC, photodiode, LED, transistor) yang tersedia saat ini. Tantangan teknologi VLC selain target peningkatan kecepatan *bit-rate, mobility communication,* mengurangi *interference noise,* menyediakan layanan *multi-acces* juga salah satunya adalah isu *security*. Makalah ini merupakan studi *literature* (*review paper*) yang didapatkan dari dokumen-dokumen hasil peneltian baik di jurnal dan *conference* terkait dengan praktik-praktik *security* VLC yang pernah dilakukan dengan skema *indoor* maupun *outdoor*.

Kata kunci – VLC, *Security*, Komunikasi dan Informasi, *Review*

Abstract - Implementing VLC system is based on IEEE 802.15.17 standard where this guideline was designed within the past 5 years ago (since 2009), this guideline covers standard of *physical layer* (PHY) and *medium access control* layer (MAC). As communication technology in general, VLC provide security acces which discuss in MAC layer part. However in real practice, we found that they haven't been massively conducted by researchers in the world. The reality is very reasonable due to this technology is under development, it can make VLC studies commonly are focus on "how to increase the speed of VLC with limitations components which are available at this time (such as ICs, photodiodes, LEDs, transistors, etc.)". VLC technology challenges, not only 1) to increase the speed of bit-rate, 2) serve mobility communication, 3) reduce noise interference, 4) providing multi-service acces, but also how to implement security issues in VLC. This paper is a study of literature (review paper) which are obtained from the scientific documents from journals and conferences related to security practices VLC both for indoor and outdoor schemes.

Keywords – VLC, Security, Information and Communication, Review

I. PENDAHULUAN

Teknologi *wireless* berkembang pesat dan mengalami peningkatan akses kecepatan [1]. Komunikasi berbasis cahaya tampak atau lazimnya disebut *visible light communication* (VLC) merupakan salah satu teknologi nirkabel yang sedang menjadi *trend* didunia dalam kurun waktu 5 tahun terakhir ini. Bermula dari demonstrasi sistem VLC Prof. Harald Haas di tahun 2011 tentang *Light Fidelity* (Li-Fi) pada forum TEDx menujukkan bahwa terobosan teknologi ini dapat dijadikan alternatif komunikasi masa depan yang mana memiliki kelebihan dibandingkan teknologi komunikasi *wireless* lain seperti *infra-red, fiber-optic* dan *radio frequency*, yakni bebas regulasi, cakupan *bandwidth* yang lebih besar, aman untuk kesehatan dan masih banyak yang lainnya. Sifat dari *visible light* adalah tidak dapat menembus objek padat seperti

tembok, sehingga menjadikan teknologi komunikasi ini terbatas pada arah dan area tertentu. Namun justru VLC dianggap sebagai sebuah media komunikasi nirkabel yang lebih aman dari pada radio. Pedoman standar komunikasi VLC adalah 802.15.17 yang diluncurkan beberapa tahun yang lalu.

Dalam aplikasinya, penerapan VLC dibagi menjadi dua bagian yakni *outdoor* dan *indoor application*. Komunikasi *vehicle to vehicle* termasuk dalam jenis *outdoor*, sedangkan *indoor* dipergunakan pada perkantoran, rumah, bangunan bertingkat (gedung), *conference ballroom* dan lain-lain. Prinsip kerjanya adalah komputer sebagai sumber data mengirimkan sinyal informasi berupa data-data dalam bentuk digital, kemudian diubah menjadi analog melalui *Digital to Analog Converter* (DAC) selanjutnya ditransmisikan menggunakan LED. Pada bagian penerima, photodetektor menerjemahkan sinyal yang linier terhadap sinyal terkirim, kemudian diproses menggunakan *Analog to Digital converter* (ADC) dan selanjutnya ditampilkan dalam komputer kembali. Ilustrasi aplikasi komunikasi dan *sharing* informasi melalui pemanfaatan cahaya tampak (devais LED) secara umum ditunjukkan pada Gambar 1, dimana sistem dapat difungsikan secara *broadcast, sensing information* (*information-based*) dan dua arah atau *bidirectional* (*communication-based*).

Gambar 1. Aplikasi VLC Pada *Indoor* Untuk Komunikasi Sekaligus *Sharing* Informasi [2]

Slogan umum untuk VLC adalah "*What you see is what you send*" [3], yang bermakna bahwa data-data yang dikirimkan dari devais ke devais atau komputer ke komputer sebenarnya dapat dilihat melalui cahaya tampak tersebut, namun diperlukan alat khusus untuk menerjemahkan data yang dikirimkan. Maka dari itu walaupun VLC disinyalir lebih *secure* karena area sebaran sumber cahaya terbatas, bukan mustahil teknologi ini dapat di *attack* atau di *jamming* dengan berbagai skenario tertentu. Hal ini didasari dengan prinsip VLC itu sendiri bahwa cahaya tampak sebagai sumber informasi tersebut dapat dilihat sinyal terpancarnya dengan menggunakan *photodiode* dan rangkaian pengolah sinyal kemudian diterjemahkan serta diolah datanya ke dalam *microcontroller*.

Beberapa peneliti di dunia telah memikirkan jauh akan hal ini meskipun teknologi VLC sendiri sedang berkembang, yakni bagaimana menyediakan akses yang benar-benar *secure*. Pada aplikasi komunikasi VLC untuk kepentingan militer dalam skema *vehicle to vehicle*, diperlukan skema komunikasi khusus seperti yang telah dijelaskan di atas. Lebih jauh lagi, nantinya VLC juga dimanfaatkan untuk aplikasi akses internet super cepat. Dengan demikian apabila diterapkan pada tempat umum seperti bandara, *conference ballroom*, dan lain sebagainya, maka *security* diperlukan untuk membatasi akses.

Tujuan penulisan ini adalah untuk mengkaji beberapa skema *communication security* berbasis VLC yang pernah dilakukan oleh beberapa peneliti yang dimaksud. Makalah ini terbagi menjadi beberapa bagian. Pertama memaparkan tentang latar belakang penulisan dan tujuan utama. Bagian kedua menerangkan teknologi VLC yang terdiri atas: kelebihan VLC, aplikasinya, sistem utama dan layer-layer VLC. Bagian ketiga menerangkan kanal VLC dan zona aman untuk komunikasi. Bagian keempat mendiskusikan tentang beberapa skema keamanan komunikasi VLC yang pernah diteliti sebelumnya, yang mencakup *indoor* dan *outdoor*. Bagian akhir merupakan kesimpulan dan pustaka.

II. TEKNOLOGI VLC

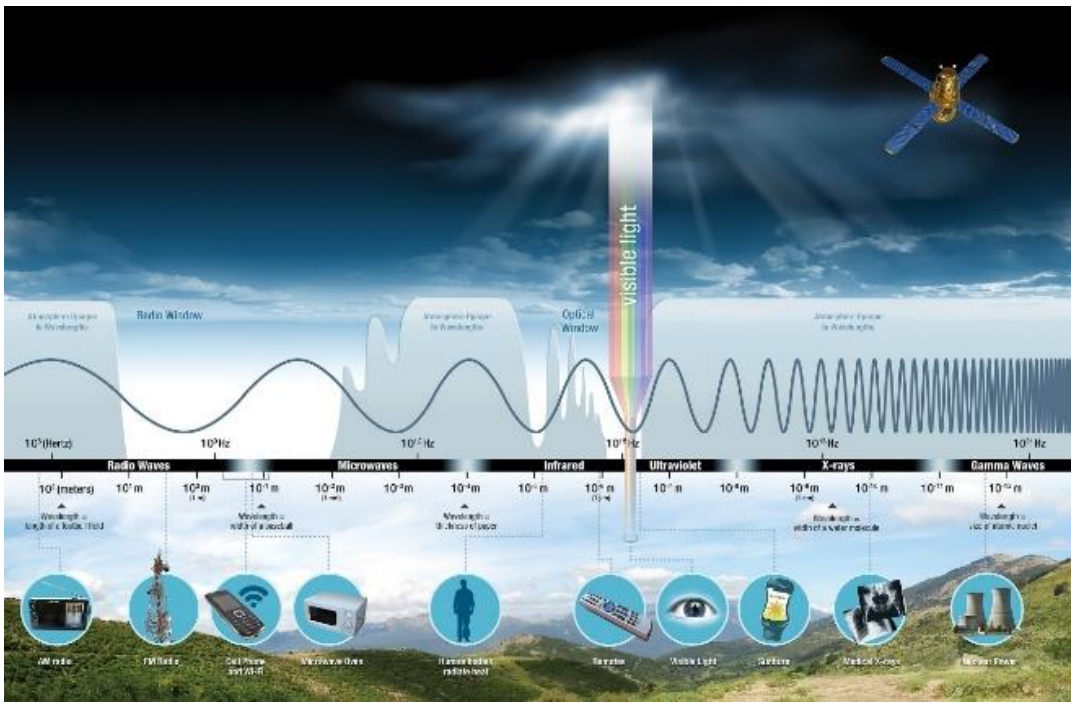
A. VLC vs Teknologi Wireless lainnya

Secara teori, cahaya tampak menyediakan *bandwidth* frekuensi sekitar 400 THz, yang bersifat *non-lisenced* atau tak berlisensi sehingga bebas dipergunakan. *Bandwidth* sebesar ini kira-kira 1000 kali lebih lebar dibandingkan kapasitas frekuensi radio yang selama ini digunakan untuk sarana komunikasi [4]. Spektrum cahaya tampak terletak antara panjang gelombang 380 hingga 780 nanometer yang dapat digunakan sebagai media VLC. Gambar 2 menunjukkan spektrum cahaya tampak dalam keseluruhan spektrum elektromagnetik dan beberapa aplikasi pemanfaatannya.

Komunikasi VLC memiliki beberapa keuntungan dibandingkan frekuensi radio tradisional dan infra merah, yakni konsumsi daya yang lebih rendah dan implementasi yang lebih murah dan mudah ketika memanfaatkan infrastruktur lampu penerangan untuk VLC [6].

Sementara komunikasi RF dan IR memerlukan *base station* khusus sehingga menambah konsumsi energi. Ketika membandingkan dengan resiko

kesehatan, RF memiliki potensi risiko kesehatan yang lebih besar daripada IR dan VLC yang kini sudah banyak dilihat pada berita-berita yang beredar bahwa salah satu yang akan diakibatkan adalah penyakit kanker.



Gambar 2. Spektrum Cahaya Tampak Dalam Band Gelombang Elektromagnetik [5]

Tabel 1. Perbandingan Komunikasi RF, IR, Dan VLC

Parameter	VLC	RF	IR
Bandwidth (teori)	bebas lisensi ~400 THz	teregulasi, terbatas, < 300 GHz	~ 400 THz
Interferensi Elektromagnetik	tidak	ya	tidak
Konsumsi Daya	rendah	medium	rendah
Standar	802.15.7 (terus berkembang)	banyak, sudah sangat matang	802.11
Resiko kesehatan	Kesehatan mata	Kanker	Kanker kulit dan mata
Harga	rendah	rendah-medium	medium

Sementara resiko kesehatan dari IR dihasilkan dari efek pemanasan radiasi tak tampak yang diserap oleh kulit dan mata manusia [7]. VLC memancarkan cahaya tampak yang apabila level iluminansinya sangat tinggi dapat membuat silau mata manusia. Namun hal ini bukan menjadi sebuah problem yang begitu berarti. Perbandingan ketiga teknologi komunikasi *wireless* ini apabila ditinjau dari aspek *bandwidth*, interferensi elektromagnetik, konsumsi daya, standar, resiko kesehatan, dan harga disajikan dalam Tabel 1 [8]. Sedangkan perbedaan berdasarkan aplikasi real (*range*, *data-rate*, dan cakupan atau *mobility*) disajikan dalam Tabel 2 [9].

Tabel 2. Perbandingan Teknologi Wireless

Jenis	Teknologi	*Range*	*Data-rate*	Mobilitas
RF	Wi-Fi 2.4 GHz	*Indoor:* 70m *Outdoor*: 35mm	65 Mbps	Rendah
	Wi-Fi 5 GHz	*Indoor*: 35mm	780 Mbps	Rendah
	3G HSPA	Tergantung jenis *cell* yang dipergunakan (dari *picocell* sampai *macrocell*), jangkauan sampai 100 km	42 Mbps sampai 1 Gbps	Tinggi
	4G		sampai 100 Mbps	Tinggi
	MM-Wave (60 GHz)	Beberapa ratus meter	7 Gbps	Rendah
Optik	Infra-red (IR)	1 meter	1 Gbps	Tidak ada
	VLC	Sampai 10 meter	Sampai 3 Gbps	Rendah

Standar sistem VLC baru dirancang dalam 5 tahun terakhir, yakni dimulai dari tahun 2009 dimana IEEE 802.15.17 membentuk *task group* yang bekerja untuk membuat standar VLC yang meliputi *physical layer* dan *medium access control* (MAC) berdasarkan pendekatan *clean slate*. Selanjutnya *draft* standar IEEE 802.15.7 tersebut dipublikasikan pada Tahun 2010 yang mengajukan penggunaan beberapa teknik modulasi antara lain *On-Off Keying* (OOK), *Variable*

Pulse-Position Modulation (VPPM), dan *Color-Shift Keying* (CSK). Meskipun juga mengakomodasi sistem komunikasi dengan aspek *security*. Pada praktiknya belum tentu dapat diaplikasikan pada suatu devais tertentu. Belum adanya standar baku tersebut membuat para peneliti dari seluruh dunia melakukan eksperimen tentang *security* VLC dengan berbagai skenario dalam satu dekade terakhir ini.

B. Aplikasi VLC

Ditinjau dari aspek aplikasi VLC terbagi dalam tiga hal, yakni aplikasi dalam ruang (*indoor*) seperti perkantoran, laboratorium, perhotelan, *conference hall*, kampus, tempat-tempat umum tertutup (bandara, stasiun, terminal), mini-market, kamar pribadi, rumah sakit dan masih banyak lagi. Selanjutnya adalah aplikasi *outdoor*, seperti penerapan VLC pada sistem penerangan jalan umum (PJU), *traffic light, vehicle to vehicle*. Dan yang ketiga adalah aplikasi bawah air (*under-water communication*). Dalam perancangannya, masing-masing terkendala oleh berbagai masalah eksternal, yakni pada aplikasi luar ruang berupa pengaruh dari cahaya matahari secara langsung dan gejala alam seperti kabut, hujan badai. Pada aplikasi *indoor*, seperti efek tertutup oleh objek atau istilahnya *shadowing* baik dari peralatan rumah tangga (lemari, meja, kursi, tembok penghalang), pelemahan cahaya atau istilahnya *fading*. Sedangkan ditinjau dari aspek area penelitian, riset VLC terbagi menjadi 3 bagian utama yakni digital [10-11], analog [12] dan *channel*.

Sebagaimana yang diketahui bahwa sifat sebaran cahaya adalah merata ke semua arah, maka semakin jauh dari sumber cahaya maka level iluminasi akan melemah [13]. Selanjutnya adalah gangguan dari *ambient light*, baik dari cahaya matahari yang menerobos masuk ke dalam ruang ataupun dari *artificial light* (*incandescent light, fluorescent light, DC lamp* atau lampu senter). Masalah *roaming, inter-cell interference*, efek *multi-path*, kemampuan mobilitas VLC juga menjadi masalah utama pada aplikasi VLC dalam ruang. Sedangkan pada aplikasi *under-water*, masalah umum adalah terletak pada medium penghantar informasi. Di mana karakteristik air sangat berbeda dengan karakteristik udara yang menjadikan cahaya informasi yang dipancarkan oleh LED transmitter mengalami beberapa perubahan sifat (efek *absorbing* dan *scattering*) [14]. Selain itu, faktor internal juga menjadi problem utama yang berasal dari komponen-komponen elektronik sistem VLC itu sendiri, seperti *optical excess noise, shot noise, thermal noise, flicker noise* dan lain-lain [15]. Dan yang tidak kalah penting adalah tentang kemananan (*security*) pada VLC yang baru-baru ini sedang hangat didiskusikan.

C. Sistem Utama VLC

Ditinjau menurut sistem utama, VLC terbagi menjadi tiga bagian, yakni: pemancar (*transmitter*), penerima (*receiver*) dan kanal (*channels*). Pada bagian pemancar dipergunakan devais *Light Emitting Diode* (LED). Salah satu tantangan dalam perancangan LED *driver* untuk VLC adalah bagaimana agar fungsi utama LED sebagai media penerangan (*illumination*) tidak terdegradasi apabila sekaligus digunakan untuk media komunikasi dan informasi. LED putih umumnya dipilih sebagai *transmitter* VLC karena warna putih ini juga cocok digunakan sebagai sarana penerangan ruangan dibandingkan dengan warna biru, merah, dan hijau. Sedangkan pada sisi *receiver* dapat berupa *photodetector* (*photodiode, phototransistor*, LDR, atau *imaging sensor* atau kamera sensor).

a) LED sebagai *transmitter*

Keunggulan LED dibandingkan sumber penerangan konvensional seperti *incandescent* dan *fluorescent*, yaitu mampu di-*switch on* dan *off* dalam kecepatan tinggi dan memungkinkan untuk mengontrol level iluminasi pada frekuensi tinggi [16]. LED merupakan perangkat semikonduktor yang memiliki kemampuan mengubah energi listrik secara langsung menjadi energi cahaya. Sama halnya diode, struktur utama dalam LED adalah sebuah chip semikonduktor yang menciptakan *p-n junction*. Ketika dibias maju, Elektron dan *hole* mengalir dari *junction* ke elektroda dengan tegangan yang berbeda-beda. Foton terbentuk dan terpancar menjadi cahaya tampak. Efek ini disebut *electroluminescence* [17]. Perbandingan berbagai jenis LED yang terdapat dipasaran disajikan pada Tabel 2 [8]. Berdasarkan informasi dapat dilihat bahwa setiap jenis LED memiliki karakteristik sendiri-sendiri. Karakteristik-karakteristik tersebut dapat dijadikan referensi untuk memilih jenis LED yang sesuai dengan persyaratan tertentu dalam perancangan sistem atau sesuai kebutuhan. Untuk aplikasi *indoor*, level ilumninansi mengacu pada IEEE 802.15 di mana untuk ruangan biasa adalah 150lm sampai 400lm dan untuk laboratorium 400lm sampai 600lm.

Tabel 3. Perbandingan Jenis-Jenis LED

Parameter	pc-LED	RGB LED	*u*LED	OLED
Bandwidth	3-5 MHz	10-20 MHz	>300 MHz	<1 MHz
Disipasi daya	130 lm/W	65 lm/W	N/A	45 lm/w
Harga	rendah	tinggi	rendah	Sangat terjangkau

Parameter	pc-LED	RGB LED	*u*LED	OLED
Kompleksitas	rendah	medium	Sangat tinggi	Tinggi
Aplikasi khusus	Iluminasi		802.11	*Display*

b) *Channels*.

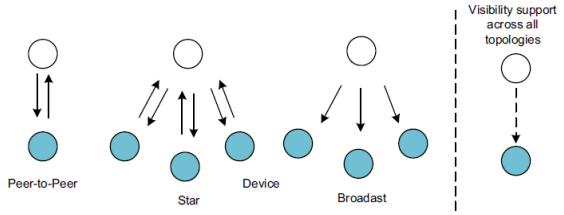
Kanal VLC adalah berupa ruangan bebas, bagian ini akan dijelaskan secara detail pada *section* III.

c) *Photodiode* (PD) sebagai *receiver*.

Dibandingkan devices lainnya *seperti light dependent resistor (LDR), photo*-IC, sel surya dan *phototransistor*, PD memiliki banyak keunggulan pada sisi stabilitas, presisi dan respon. PD yang komersil memiliki bermacam-macam tipikal, diantaranya: *precision* yang lebih tepat dipergunakan untuk *light measurement, high speed* umumnya berkarakteristik *high cut-off frequency* yang sesuai untuk aplikasi optik, dan *integrated photodiode* seperti jenis S8745 dan S9295 produksi HAMAMATSU® dimana PD terintegrasi dengan *pre-amp* dalam satu *chip* [18]. Masing-masing tipikal tersebut memiliki keunggulan dan kelemahan tersendiri. Kemampuan ideal PD dapat dilihat pada *datasheet* dari masing-masing *manufacturer* dimana spesifikasinya dapat dianalisa melalui hubungan antara daya LED pada VLC dengan daya yang diterima PD (akan dibahas pada Bab III).

D. Layer-layer VLC

Berdasarkan layer, sistem VLC dibagi menjadi tiga bagian utama yakni layer fisik (*physical layer*), layer *Medium Acces Control* (MAC layer) dan layer aplikasi. Kajian ketiga hal ini disajikan dalam IEEE 802.15.7.



Gambar 3. Topologi MAC Layer Berdasarkan IEEE 802.12.7 [19]

Topologi MAC *layer* ditampilkan pada Gambar 3 yang terbagi menjadi tiga link, ialah: 1) *peer-to-peer*, dimana pada topologi ini terdiri dari satu devais sebagai koordinator atau *master* dan satu sebagai *client* dimana keduanya dapat berkomunikasi secara dua arah yakni *downlink* (dari koordinator ke *client*) dan *uplink* (dari *client* ke koordinator). Impelementasinya dapat dilakukan secara *half-duplex* yakni bergantian antara *downlink* dan *uplink* (prinsip ini seperti HT) maupun *full-duplex*, yakni berkomunikasi secara bersamaan (prinsip ini seperti telefon genggam modern). Tipikal topologi *peer-to-peer* ini sesuai apabila diterapkan untuk aplikasi komunikasi nirkabel lainnya seperti NFC (*Near Field Communication*). Opsi untuk *uplink* dapat berupa *IR, Near UV* atau bahkan lampu LED (*visible light*). Selanjutnya K. Cui, dkk [20] melakukan eksperimen teknologi untuk *uplink* dan membandingkannya (Tabel 4).

Berdasarkan hasil eksperimen tersebut dapat disimpulkan bahwa *near UV* lebih baik pada kanal LOS dibanding kedua devais, artinya pengaruh *background interference* (dalam kasus tertutup oleh objek padat) terhadap performa jaringan komunikasi lebih sedikit. Sedangkan untuk kanal NLOS, *infra-red* memiliki performa yang lebih baik. Kelemahan keduanya adalah *low-rate*, sehingga untuk keperluan *high speed uplink* dapat memanfaatkan LED namun hal ini dapat menganggu pengguna karena cahaya tampak yang dipancarkan berada di dekat mata, selain itu juga kurang baik pada kanal LOS maupun NLOS dibandingkan *near UV* dan *infra-red*.

Tabel 4. Perbandingan Devais Untuk *Uplink*

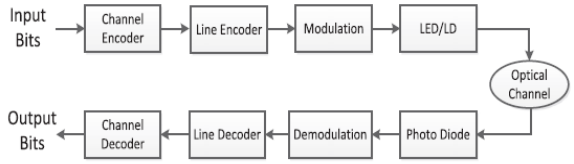
Devais untuk *Uplink*	Jarak (m)	LOS path loss (dB)	NLOS path loss (dB)
IR (850 nm)	1.8	32	38.5
Near UV (375 nm)	1.7	30.4	49
Visible (470 nm)	1.8	34.1	47.2

Selanjutnya adalah topologi *star* yang mirip dengan *peer-to-peer* (Gambar 3), namun pada sisi *client* lebih dari satu devais yang terkoneksi secara langsung dengan *master*. Tipikal topologi ini dapat diterapkan pada aplikasi "VLC *Wireless acces network*". Sampai saat ini, banyak berbagai tantangan untuk membangun MAC layer dengan topologi *star* karena dari masing-masing devais *client* tersebut berkomunikasi secara dua arah (*bi-direcional*) bahkan dengan waktu yang bersamaan.

Terakhir adalah topologi *broadcast*, topologi mirip dengan *star* namun hanya satu arah yakni dari *master* ke banyak *client.* Cocok dipergunakan untuk komunikasi VLC dengan skema *broadcasting information.*

Layer VLC selanjutnya adalah layer fisik (*physical layer*), yang berhubungan dengan komponen-komponen pembangun VLC dan hubungan antara devais dengan medium (kanal). Dalam hal ini mencakup tentang rangkaian *analog front end* (AFE), *digital signal processing* (DSP), dan desain modulasi. Blok diagram umum layer fisik ditunjukkan pada Gambar 4. Pada awalnya sinyal informasi masuk (dari komputer), selanjutnya diolah oleh *channel encoder, line encoder.* Sinyal termodulasi tersebut diproses oleh LED driver (*Analog-front end transmitter*) dan

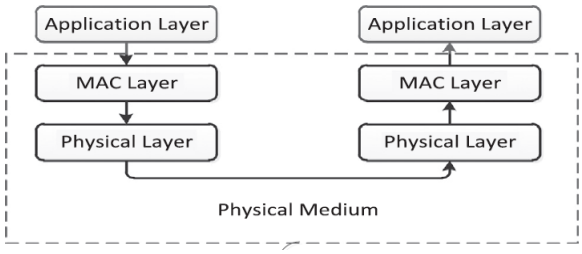
ditransmisikan melalui medium cahaya. Selanjutnya *photodiode* menerima sinyal dan kemudian diolah pada bagian *decoder*. Output data diterima kembali oleh komputer yang mana sinyal input harus linier dengan sinyal output.



Gambar 4. Topologi PHY Layer Berdasarkan IEEE 802.12.7 [19]

Menurut IEEE 802.15.7, layer fisik (PHY layer) terbagi menjadi tiga divisi yakni PHY I yang beroperasi pada *range* kecepatan transfer data mulai dari 11.67 sampai 266.6 Kbps, PHY II dengan rate kecepatan mulai 1.25 sampai 96 Mbps dan PHY III mulai dari 12 sampai 96 Mbps. Hubungan antara PHY layer dengan MAC layer ditunjukkan pada Gambar 5.

Layer aplikasi merupakan keluaran akhir dari sistem, contohnya adalah implementasi sistem VLC untuk *vehicle to vehicle communication*, *Light-Fidelity*, rumah sakit, *real-time audio & video transmission*, *underwater communication*, *space communication*, *localization based movable devices (*berbasis *mobile robot* atau *autonomous robot)*, WLANs, *visible light ID system* dan masih banyak lagi.

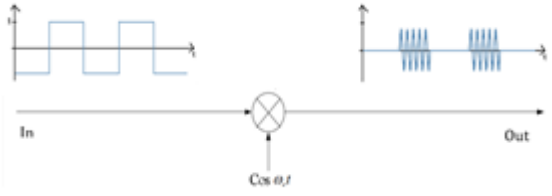


Gambar 5. Arsitektur VLC [21]

E. *Modulasi*

Modulasi termasuk bagian dari PHY layer yang memiliki peran penting sebagai penumpang data-data informasi via amplitudo, frekuensi atau gabungan keduanya. Dari berbagai jenis teknik modulasi untuk VLC yang diajukan oleh para peneliti sebelumnya, setidaknya jenis-jenis teknik modulasi tersebut dapat dibedakan menjadi dua kategori besar yaitu modulasi digital yakni: *On-Off Keying* (OOK), *Pulse Width Modulation* (PWM), dan *Pulse Position Modulation* (PPM) dan modulasi analog terdiri dari modulasi *single-carrier* (*Amplitude Modulation* dan *Frequency Modulation*) dan *multi-carrier* (*Orthogonal Frequency Division Duplexing* atau OFDM).

On of Keyying (OOK) adalah teknik modulasi yang paling banyak digunakan untuk pada VLC. Hal ini dikarenakan oleh kesederhanaan dari OOK yang mana Bit '1' disimbolkan dengan satu pulsa dengan lebar baik itu satu periode pulsa penuh atau hanya setengahnya. Sedangkan bit '0' disimbolkan dengan tidak adanya pulsa. Ilustrasi ditunjukkan pada Gambar 6.



Gambar 6. Diagram Blok OOK

Persamaan gelombang pembawa (*carrier*) adalah,

$$C_t = A_c * cos\omega_c t \quad (1)$$

Sehingga persamaan sinyal OOK adalah,

$$s(t) = \begin{Bmatrix} A_C, & 0 < t \le T, \log ika(1) \\ 0, & 0 < t \le T, \log ika(0) \end{Bmatrix} \quad (2)$$

Sinyal pembawa (*carrier signal*) tersebut dapat berupa Sin $\omega_c t$ atau Cos $\omega_c t$, karena tidak terpengaruh pada besar fasanya. Dengan demikian, hasil sinyal output dari modulasi OOK adalah terdapat sinyal pembawa pada *high level* (representasi logika 1) dan pada *low level* tidak dihasilkan sinyal pembawa (representasi logika 0).

III. KANAL VLC DAN ZONA AMAN KOMUNIKASI

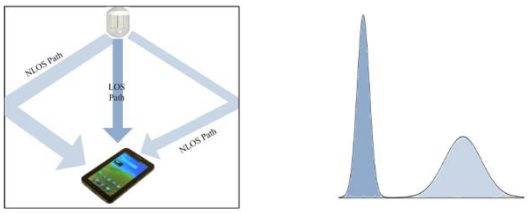
A. *Kanal VLC*

Kanal pada VLC berupa *free space* yang dalam implementasinya terbagi menjadi dua jenis link, yakni *Line-of-Sight (LOS) link* dan *Non-LOS link* yang masing-masing memiliki keunggulan dan kelemahan. Perbedaan kedua jenis kanal ini ditunjukkan pada Gambar 7 [22]. Kanal LOS adalah devais penerima (*client*) dihadapkan langsung (*direct*) dengan *master* atau *source* untuk menerima data. Sedangkan NLOS, respon data yang diterima setelah cahaya terpantul objek padat (dalam hal ini adalah tembok).

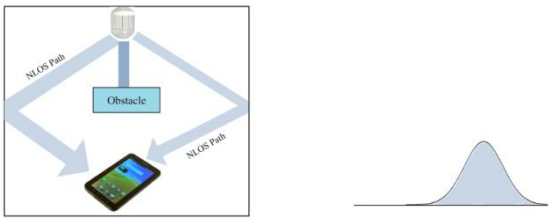
Pada Gambar 7 dapat disimpulkan bahwa LOS link kelemahan utamanya adalah efek *shadowing* yang diakibatkan oleh penghalang (*obstacle*) yakni tertutup oleh objek benda mati (peralatan rumah tangga atau penghalang seperti tembok dan pantulan kaca) ataupun bergerak seperti aktivitas manusia. Sinyal yang diterima *photodetector* berasal dari sumber cahaya dan juga pantulan, apabila tertutup objek maka informasi akan terblok, artinya yang diterima hanyalah impuls sinyal dari pantulan.

Kekurangan selanjutnya adalah cakupan yang sempit sehingga tidak mendukung *mobile user*, karena konfigurasi ini mengharuskan *transmitter* dan *receiver* disejajarkan dalam garis lurus. Solusi masalah ini adalah dengan cara pemilihan *photodiode* dengan FOV

yang luas. Kelebihannya adalah konfigurasi ini menawarkan laju data berkecepatan tinggi dalam jarak yang jauh. Kemudian, tidak rentan terhadap distorsi yang berasal dari induksi sinyal *multipath* dan *ambient light noise*. Ilustrasi LOS link ditunjukkan pada Gambar 8 [23].



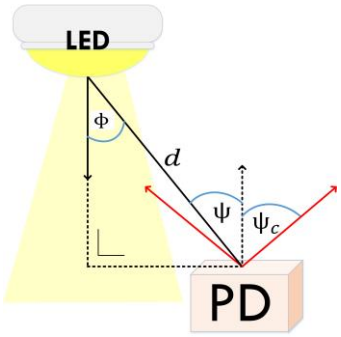
(a) Kanal LOS



(b) Kanal NLOS

Gambar 7. Respon Impuls dari Kanal LOS maupun NLOS

Untuk skema *security*, umumnya kanal LOS dipergunakan sebagai acuan utama, maka dari itu, pada makalah ini hanya dibahas tentang pemodelan matematika dari kanal LOS dan simulasi (distribusi angular cahaya) ditunjukkan pada Gambar 9 yang mengacu pada Tabel 5.



Gambar 8. Geometri Kanal LOS

Distribusi angular dari pola intensitas radiasi LED dalam suatu ruangan dimodelkan dengan intensitas cahaya Lambertian [23]. Persamaan matematisnya ditunjukkan pada persamaan (3).

$$R_0(\theta) = \begin{cases} \frac{(m_1+1)}{2\pi} \cos^{m1}(\theta) & untuk\ \theta \in [-\pi/2, \pi/2] \\ 0 & untuk\ \theta \geq \pi/2 \end{cases} \quad (3)$$

Dimana m_1 adalah indeks Lambert yang menunjukkan derajat pengarahan sumber cahaya, sedangkan sudut θ = 0 adalah sudut pancaran daya maksimum. Maka intensitas pancaran cahaya sesuai dengan persamaan (4).

$$S(\theta) = P_t\, R_0(\theta) \quad (4)$$

Photodiode dimodelkan sebagai area aktif A_r yang menangkap pancaran cahaya datang pada sudut Ψ yang nilainya lebih kecil dari FOV *photodiode* tersebut. Area pengumpulan cahaya efektif dari *photodiode* tersebut adalah.

$$A_{eff}(\Psi) = \begin{cases} A_r \cos\Psi & 0 \leq \Psi \leq \pi/2 \\ 0 & \Psi > \pi/2 \end{cases} \quad (5)$$

DC gain untuk *receiver photodiode* yang terletak pada jarak *d* dan sudut penerimaan θ terhadap *transmitter* seperti ditunjukkan pada Gambar 7, adalah:

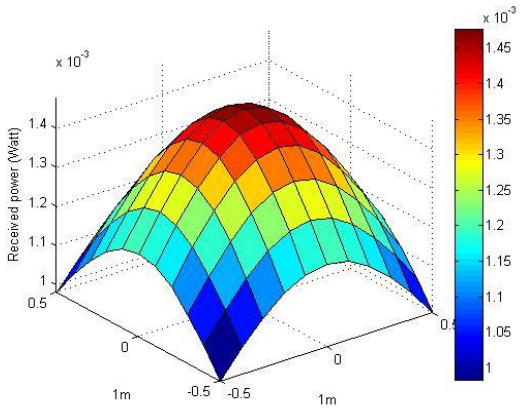
$$H_{los}(0) = \begin{cases} \frac{A_r(m_1+1)}{2\pi} \cos^{m1}(\theta) \cos\Psi & untuk\ 0 \leq \Psi \leq \Psi_c \\ 0 & lainnya \end{cases} \quad (6)$$

Maka daya yang diterima *photodiode* adalah sebesar.

$$P_{r-loss} = H_{los}(0) P_t \quad (7)$$

Simulasi pada Gambar 9 menunjukkan bahwa sebaran intensitas cahaya informasi yang dipancarkan ke dalam suatu ruangan tidak merata baik pada titik-titik tertentu, sudut ruang ataupun jarak. Hal ini ditunjukkan dengan gradasi warna yang berbeda-beda dalam beberapa area.

Daya maksimum yang diterima oleh *photodiode* pada jarak kurang dari 250 cm adalah 1.4 hingga 1.2 dBm. Sementara itu pada jarak lebih dari 500 cm, daya yang diterima *photodiode* berkisar 1 dBm.



Gambar 9. Distribusi Sebaran Cahaya Inforamsi

Tabel 5. Parameter-Parameter untuk Simulasi

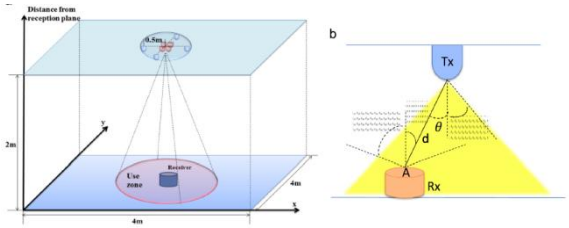
Parameter-parameter	Nilai
Area fisik photo-detector (*Ar*)	7.02 mm² (datasheet)
PD concentrator refreactive index	*Ignored*
Receiver's field of view (FOV) angle	*50º (datasheet)*
Daya LED	8 Watt
Reflectivity of wall	*Ignored*
Transmitter's semi-angle at half power	*60°*
Dimensi ruangan (W x L x H)	1m x 1m x 1m

Parameter-parameter	Nilai
Koordinat *transmitter*	0,0
Receiver plane	*0.85m (above the ground)*
Jarak *(d)*	1 meter
Jumlah LED yang digunakan	1 buah

LED akan mengalami pelemahan (*fading*) selama merambat di ruang bebas, artinya semakin jauh jarak *receiver* maka sinyal yang diterima akan semakin kecil dan bahkan tidak diterima sama sekali [24]. Untuk itu, solusi dari permasalahan umum ini adalah meningkatkan daya dari LED atau menambah jumlah LED. Namun hal ini bukan solusi pilihan karena akan menyebabkan pemborosan energi apabila daya LED semakin besar padahal hemat energi adalah anjuran utama. Dan penambahan jumlah LED dapat menimbulkan masalah *roaming*. Solusi ideal adalah dengan optimasi filter *photodiode* dan ketepatan *photodiode*.

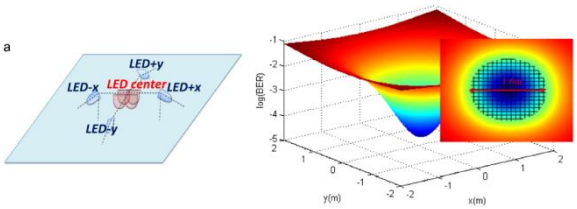
B. *Zona aman VLC*

Eksperimen dan demonstrasi tentang area cakupan komunikasi VLC dilakukan oleh C.W. Chow, dkk [25] dengan menggunakan kanal LOS, persamaan matematis mengacu pada *section* III poin 3.1. Tujuan investigasi ini adalah untuk mengetahui distribusi iluminansi sumber cahaya informasi dalam satu ruang berukuran panjang, lebar, tinggi = 4m x 4m x 4m, dimana mula-mula LED 10 Watt 4 buah ditempatkan di tengah-tengah (Gambar 11). Pada skenario tersebut juga digunakan 4 buah LED yang dipasang mengelilingi *center* LED (5 Watt dan 15 Watt). *Transmitter* diatur berjarak 2 m ke penerima. Parameter-parameter tersebut dikalkulasi menggunakan matlab dan hasilnya ditunjukkan pada Gambar 11.

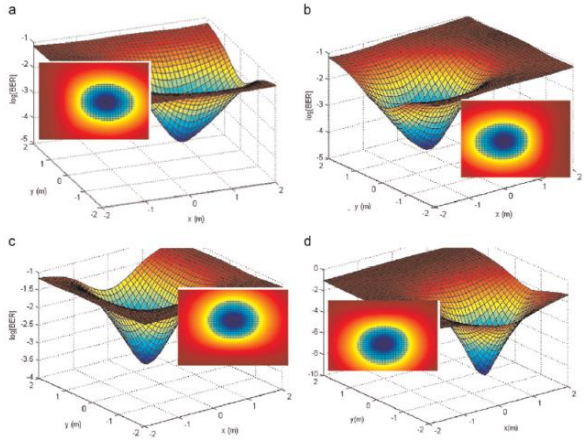


Gambar 10. Skema *Security* Pada Aplikasi *Indoor* Dengan *Setting* Ruangan 4m X 4m X 3m Menggunakan 4 Buah LED (Ditunjukkan Warna Merah), 4 *Intrussion* LED (Ditunjukkan Warna Biru) Dan Pemodelan Kanal LOS [25]

Selanjutnya diubah skenario sebagai berikut: LED+x, LED-x, LED-y, LED+y (Gambar 12). Berdasarkan simulasi dapat disimpulkan bahwa dengan metode superposisi dari LED, distribusi cahaya dapat diatur. Dengan demikian data-data yang dipancarkan dari LED dapat diproteksi berdasarkan skema pengubahan posisi *transmitter* tersebut dengan tanpa mengubah fungsi utama sebagai penerangan. Sistem ini diimplementasikan pada *PHY layer*, maka untuk *enkripsi* data perlu diimplementasikan pada *MAC layer*.



Gambar 11. Detail Posisi LED Pada *Indoor* dan Hasil Simulasi Mula-Mula [25]



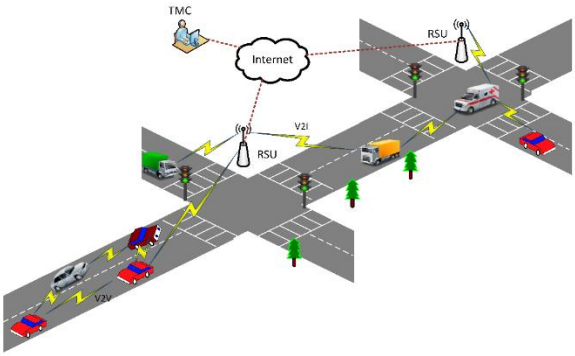
Gambar 12. Distribusi Cahaya Saat (a) LED-x 5W dan LED - x 15W, (b) LED-x 15W dan LED - x 5W, (c) LED-y 15W dan LED - y 5W, (d) LED-y 5W dan LED - y 15W [25]

IV. PRAKTIK-PRAKTIK *SECURITY* VLC

A. *Skema Security pada Aplikasi Outdoor*

Salah satu contoh pemanfaatan VLC pada aplikasi luar ruang adalah pada kendaraan (*vehicle*), hal ini tidak dapat dipungkiri bahwa beberapa bagian kendaraan menggunakan sistem pencahayaan seperti lampu depan dan belakang. Sejalan dengan itu, pengembangan kendaraan cerdas juga merupakan salah satu topik yang menarik pada bidang elektro-otomotif (*autotronics*), contoh aplikasi untuk *monitoring system* pada kondisi baterai ataupun ban, *auto-brake*, *intelligent steering* dan termasuk pula teknologi komunikasi antar kendaraan atau istilanya *vehicle to vehicle communication* (V2V) seperti yang diilustrasikan pada Gambar 12 [26].

Skema V2V ini mengacu pada IEEE 802.11p (atau dalam penamaan lain adalah DSRC) yang merupakan standar *Wireless Acces for Vehicular Environment* (WAVE) yang berbasiskan pada RF. Telah dijelaskan di Bab sebelumnya bahwa salah satu alternatif komunikasi nirkabel selain RF adalah media *optic* berbasis cahaya tampak/ VLC. Selain bebas lisensi, konsumsi daya relatif rendah termasuk masalah *cost*. Namun kelemahan utama adalah tidak tahan terhadap gejala alam dan gangguan cahaya lain. Kelemahan lain adalah pada *range* dan *area* terbatas sehingga mobilitas kurang. Namun justru ini menjadikan VLC lebih *secure*. Perbandingan antara DSRC dan VLC disajikan dalam Tabel 6.



Gambar 12. Struktur Jaringan Ad Hoc Pada Aplikasi Otomotif

Secara PHY layer, pemanfaatan teknologi VLC pada aplikasi *vehicle to vehicle communication* (V2V) dapat diterapkan langsung pada perangkat kendaraan tanpa menambah lampu khusus, yaitu pada *headlamp* seperti yang dilakukan oleh H-H. Yoo, dkk [27], selanjutnya *backlamp* dikembangkan oleh W. Viriyasitavat, dkk [28], ataupun lampu sirine [29] yang dikhususkan untuk mobil ambulans.

Dengan keterbatasan jangkauan VLC, sangat potensial untuk dikembangkan pada kendaraan perang saat sedang konvoi dan terjadi komunikasi (*packet data share*) antara satu dengan yang lainnya. Meninjau *rule* strategi perang, struktur konvoi ini dilakukan dengan kendaraan berjajar secara searah antara satu dengan yang lainnya dan berdekatan, kondisi nyata ditunjukkan pada Gambar 13. Selama dalam perjalanan, komando-komando taktik bersumber pada kendaaran paling depan kemudian diteruskan informasi ke kendaraan dibelakangnya. Atau dapat dilakukan sebaliknya. Teknologi komunikasi harus mendukung kecepatan dan ketepatan dalam rangka mempercepat informasi yang disampaikan. Dalam hal ini VLC sangat potensial karena cepat rambat cahaya jauh lebih cepat dari gelombang radio sehingga *delay* atau waktu tunda pengiriman paket data relatif tidak ada.

Tabel 6. Perbandingan Antara VLC dengan IEEE 802.11p (DSRC) Pada Aplikasi V2V

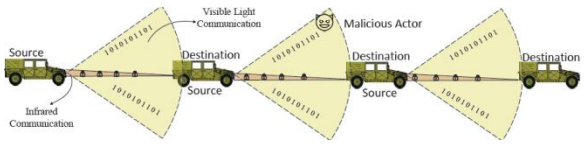
Properti	VLC	DSRC
Skenario komunikasi	Tipikal LOS	LOS ataupun NLOS
Transmission Range	*Short Range*	*Long Range*
Data Rate	*Up to 400Mb/s*	*Up to 54Mb/s*
Frequency Band	*400 - 790 THz*	*5.8 - 5.9 GHz*
Power Consumption	*Relatively Low*	*Medium*
Spatial Reuse Efficiency	*High*	*Low*
Electromagnetic Interference	*No*	*Yes*
Licensing	*Free*	*Required*
Coverage	*Narrow*	*Wide*
Cost	*Low*	*High*
Mobility	*Medium*	*Not Affected*
Weather Condition	*Sensitive*	*Robust*
Ambient Light	*Sensitive*	*Not Affected*
Delay	*Relatively none*	*Relatively low*

Untuk aplikasi V2V dengan pemanfaatan VLC pada *military networks*, diperlukan skema khusus. Artinya tidak cukup sampai level PHY, namun juga pada level MAC. Cahaya tampak yang dipancarkan oleh LED bukan jaminan aman meskipun area terbatas seperti yang ditunjukkan pada Gambar 14.

S. Ucar, dkk [30] mendemonstrasikan *protocol* komunikasi yang didesain khusus untuk skenario V2V pada aplikasi militer (*MAC layer level*). Sedangkan pada PHY layer, setiap kendaraan dipasang masing-masing 1 buah lampu untuk memancarkan cahaya tampak, dalam hal ini LED dan perangkat infra merah. Fitur-fitur *protocol* yang telah didesain seperti yang ditunjukkan pada Gambar 16 adalah sebagai berikut: 1) dapat secara langsung mengirimkan data ke target yang berpartisipasi dalam tukar menukar informasi, artinya tidak semua perangkat dapat menerima. 2) Komunikasi berbasis *full-duplex* sehingga dapat dipergunakan untuk pengiriman maupun penerimaan dalam satu waktu, VLC mengirimkan data-data terenkripsi sedangkan infra merah dipergunakan untuk mengirimkan kunci (*key*). Dan juga 3) dilengkapi dengan sistem *key generator* untuk setiap paket data yang dikirim sehingga data-data terenkripsi tidak dapat didekripsi tanpa *generator keys*. Hasil penelitian tersebut menunjukkan pada data terenkripsi, pesan yang diterima lebih lamban, hal ini karena faktor proses *keys generator*. Selain itu tidak dapat dipergunakan apabila jarak antar mobil tidak sejajar. Namun, hasil penelitian ini sangat positif sebagai alternatif komunikasi yang aman.

(a) (b)

Gambar 13. Ilustrasi Konvoi Kendaraan-Kendaraan Militer (Google) yang Berjajar Secara Tegak Lurus Dari Depan Ke Belakang

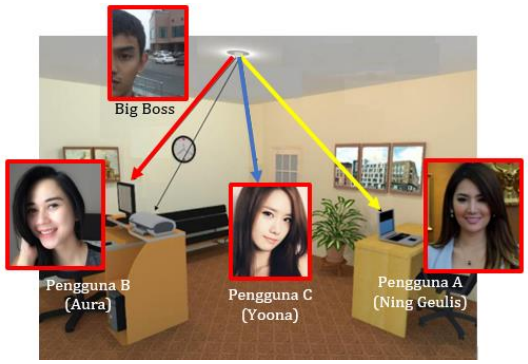


Gambar 14. Skema *Security* V2V Pada Kendaraan Militer [30]

B. *Skema Security pada Aplikasi Indoor*

Pemanfaatan VLC sebagai *sharing* informasi dan komunikasi sangat ideal diterapkan pada area dalam ruang. Cahaya informasi yang dipancarkan oleh LED tidak dapat menembus penghalang (seperti hasil

simulasi pada Gambar 9 dan 12) sehingga disinyalir lebih *secure* dan terbatas pada area-area tertentu. Selain untuk komunikasi *one by one*. VLC juga berpotensi untuk aplikasi *multi-user* atau *multi-client* dan *multi-master*. Dalam hal ini dapat berupa *platform* untuk *chatting* antar *user* atau *broadcast* informasi dari *server* pusat berbasis VLC dalam skema *indoor*. Ilustrasi ditunjukkan pada Gambar 15 dimana terdapat contoh tiga *user*: pengguna A, B, C dan *server* dengan *nickname* "Bigboss". Selain itu, *server* dapat mengendalikan semua perangkat elektronik (*printer*, TV, AC, dan lain-lain) dengan perintah via cahaya tampak.



Gambar 15. *Security* Pada Layer Fisik/ PHY Layer Pada Jaringan VLC, (Skenario Komunikasi Diadopsi dari [31])

Beberapa bentuk *attacking* yang kemungkinan akan terjadi pada jaringan komunikasi dan informasi berbasis VLC pada aplikasi *indoor* menurut tinjauan [32] adalah: *jamming, snooping* dan *data modification.*

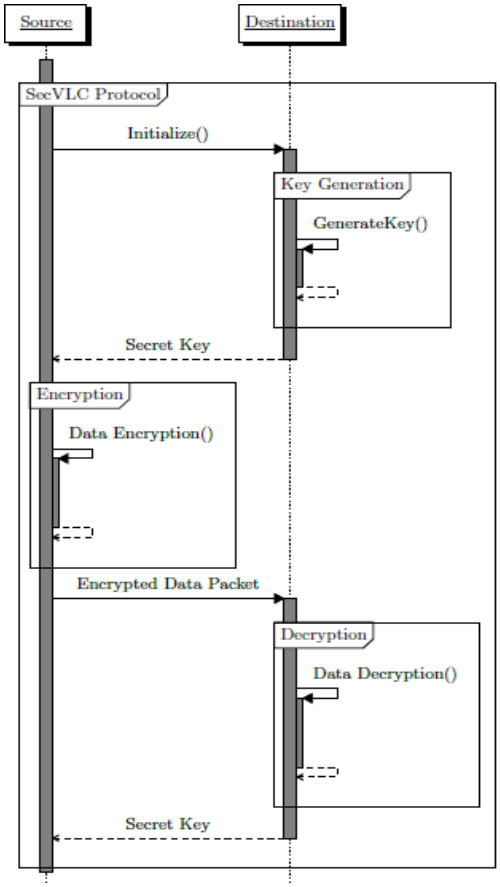
C. Friendly Jamming

Skema ini adalah pengganggu informasi yang dikirimkan atau di *broadcast* dari *master* ke *user* atau sebaliknya. Untuk lebih menyederhanakan kasus ini, dapat mengacu pada Gambar 15. Dalam suatu ruang terdapat dua *user* yakni Aura, Yoona dan pada *server* terdapat 1 LED *transmitter* yakni *big boss* dan ditambahkan 1 LED lagi sebagai *jammer* (LEDj) dimana penempatan tidak harus diletakkan ditengah ruang.

Selanjutnya data-data *pseudo* atau *dummy* secara acak dikirim dengan melalui LEDj tersebut. Ilustrasi ditampilkan pada Gambar 17, dimana area komunikasi ditunjukkan pada warna biru, jangkauan cahaya informasi warna kuning, informasi sebenarnya ditunjukkan dari LED yang dalam hal ini berwarna putih. LEDj atau *jammer* berwarna merah. Gambar 17 merupakan skenario *friendly jamming* yang diadopsi dari J. Classen, dkk [33].

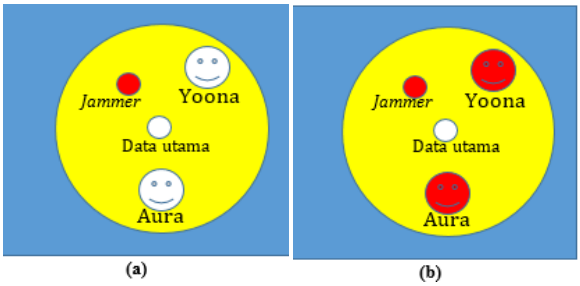
Meskipun LEDj diletakkan beberapa meter dari LED sumber, skenario *jamming* akan sukses apabila jarak LEDj dengan *user* dekat. Hal ini dapat dibuktikan dengan mengadopsi skenario pada Gambar 11, dimana pengubahan posisi LED pada LED-x, LED-y, LED+y, LED+x (diibaratkan sebagai LEDj) juga dapat mengubah area jangkauan cahaya informasi. Sehingga dapat disimpulkan bahwa Yoona dan Aura tidak akan tahu bahwa data-data yang diterimanya berasal dari Bigboss atau tidak.

Akan tetapi apabila jarak LEDj terlalu jauh dengan *user*, maka level intensitas dari LEDj tersebut melemah sehingga tidak terlalu berpengaruh pada LED utama.



Gambar 16. Langkah Kerja *Protocol* Komunikasi yang Diajukan Oleh Ucar, Dkk [30] Pada MAC Layer VLC Untuk Keperluan Komunikasi Kendaraan Militer

Untuk keperluan *jamming*, intensitas yang dipancarkan harus kuat. Hal ini juga sesuai dengan pendapat [32] yang menyatakan bahwa *"jamming is directly proportional to range to the longer range, this feature being inversely proportional to the transmission power"*, dapat disederhanakan menjadi persamaan berikut: $J = \frac{R}{P}$, dimana J adalah *jamming*, R menyatakan jarak dan P merupakan daya LEDj.



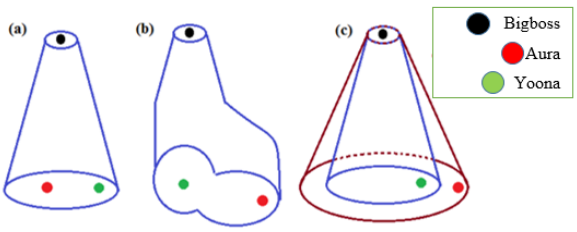
Gambar 17. (a) Skenario *Friendly Jamming*; (b) *Jamming* Sukses

D. Data Snooping

Berbeda dengan *jammer* yang menggunakan perangkat LED untuk mentransmisikan data-data palsu atau pengganggu, *Snoopers* hanya mengintip data-data yang diterima oleh para *user* lainnya. Skenario ini telah banyak dipraktekkan pada komunikasi RF, karena area jangkauan luas sehingga mobilitas tinggi maka *attacker* RF dikategorikan sebagai *active snoopers.* Sedangkan pada *indoor* VLC, *attacker* hanya perlu mendapatkan sinyal yang dipancarkan oleh LED. Hal ini dapat dilakukan dengan berdiam diri sehingga dikategorikan sebagai *passive snoopers.*

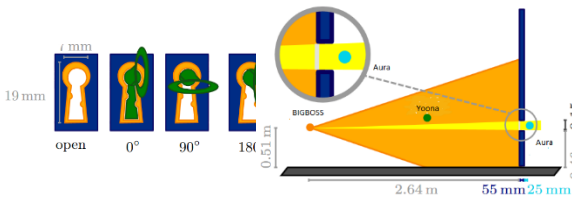
Sebagai gambaran, pada makalah ini diberikan contoh yang mengacu pada Gambar 15 dimana pada ruangan tersebut terdapat tiga *user.* Yoona sebagai penerima data dan Bigboss sebagai *emitter*, di sini Aura berperan sebagai *snoopers.* Data-data yang berisi informasi pribadi atau penting dikirimkan oleh *Bigboss* kepada Yona via *visible light.* Di area yang sama, cahaya tampak juga menjangkau beberapa *user* yang lain (dalam posisi antara LED dan *user* secara LOS). Dengan demikian Aura berpotensi mengetahui data-data tersebut.

Sebagai ilustrasi ditunjukkan pada Gambar 17, dimana warna hitam adalah *emitter* dari Bigboos, titik merah adalah Aura dan titik hijau sebagai representasi Yoona. Seorang *attacker* dalam hal ini Aura berlokasi di area yang tercakup oleh *emitter* LED secara langsung (Gambar 17a). Kemudian pada area yang tidak jauh dari posisi semula, Aura tetap mendapatkan informasi karena pantulan-pantulan berkas cahaya dari objek lain, dalam hal ini adalah kaca atau cermin, namun sinyal yang diterima lemah. Hal ini dapat terjadi karena sesuai dengan pemaparan sebelumnya tentang *channels*, bahwa ada dua jenis LOS yakni berhadapan langsung dengan *emitter* dan NLOS dimana sinyal diterima berasal dari pantulan objek. Apabila Aura terlalu jauh, maka informasi tidak akan diterima sama sekali.



Gambar 18. *Attack* Jaringan Komunikasi VLC Yang Standar Dengan Cara *Snooping/Sniffing* Diadopsi Dari Skenario Pada Skenario I.M. Gracia, dkk [34]

Potensi resiko dari *data sniffing* didefinisikan oleh [32], "*Snooping is directly proportional to the transmission power and the radiation angle*". Dapat disederhanakan menjadi persamaan berikut: $S = P * A$, dimana S adalah *snooping,* A menyatakan *angle* atau sudut dan P merupakan daya LED utama (*main emitter*). Pada skenario ini, keterbatasan *attacking* terletak pada faktor fisik dan tentu saja lebih sulit dari pada *snooping* pada jaringan Wi-fi. Namun hal ini tidak menutup kemungkinan bahwa permasalahan ini akan terjadi karena eksperimen yang dilakukan oleh J. Classen, dkk [35] membuktikan bahwa sinyal dapat ditangkap meskipun melalui celah kecil melalui lubang kunci pintu rumah. Skenario ditunjukkan pada Gambar 19.



(a) (b)

Gambar 19 (a),(b). *Sniffing* dari Lubang Kunci Diadopsi dari Skenario J. Classen, dkk [35]

E. Modifikasi Data

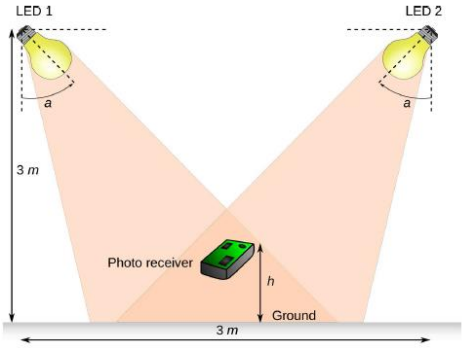
Resiko *data modification* diestimasikan sebagai hasil penjumlahan antara resiko *jamming* dan *snooping* [32]. Dapat direpresentasikan dengan $M = J * S = R * A$. Dimana M merupakan *modification,* S adalah *snooping, J* adalah *jamming,* R representasi dari jarak kanal antara LED dan *receiver,* kemudian A adalah sudut pancaran dari LED terhadap *receiver*. Kemungkinan resiko ini sangat kecil karena dipengaruhi oleh beberapa faktor, namun memungkinkan terjadi apabila dalam jaringan VLC tanpa *security.*

F. Penggunaan Kriptografi Untuk Mengamankan Data

Dengan mengetahui potensi-potensi resiko *attack* pada jaringan VLC tersebut, pengamanan data (*security*) komunikasi mutlak diperlukan baik pada aplikasi *outdoor* maupun *indoor*. Pemilihan jenis modulasi juga mempengaruhi keamananan sistem VLC itu sendiri, dalam hal ini modulasi OOK dapat dengan mudah dideteksi karena representasi '0' dan '1' hanya ditunjukkan oleh level amplitudo. Dengan metode *wiretap* keadaan sinyal digital dapat terbaca. Akan tetapi, dengan menerapkan sistem enkripsi dan dekripsi data menjadikan akses komunikasi lebih lamban karena faktor *delay* seperti yang telah dipraktikkan oleh A. Mukerjee [36]. Untuk menjawab tantangan itu dapat diterapkan teknik *security* untuk komunikasi VLC dua arah, dimana pada bagian *master* terdiri dari dua LED yakni untuk *broadcast* informasi ke publik dan LED satunya lagi untuk transfer komunikasi pribadi antara *master* dengan *user/client*. Metode yang seperti ini diajukan oleh A. Hilmia, dkk [37].

Problem lainnya adalah ketika jumlah LED pada ruangan lebih dari satu dan kesemuanya memanfaatkan enkripsi data sehingga daerah antar LED atau *interseption area* tidak dapat perform dengan baik, ilustrasi ditunjukkan pada Gambar 20. A. Mustafa &

L. Lampe [31] melakukan eksperimen dengan dua buah LED dan satu transmitter diletakkan di antara area iluminasi, masing-masing LED menggunakan kriptografi untuk mengirimkan data namun secara parsial dengan penerapan algoritma *Shamir's Secret Sharing.* Hasil penelitian menunjukkan bahwa *receiver* tetap dapat menerima data terenkripsi dan berhasil didekripsikan meskipun pada posisi intersep ataupun sudut dan jarak LED ke *receiver* dirubah-ubah.



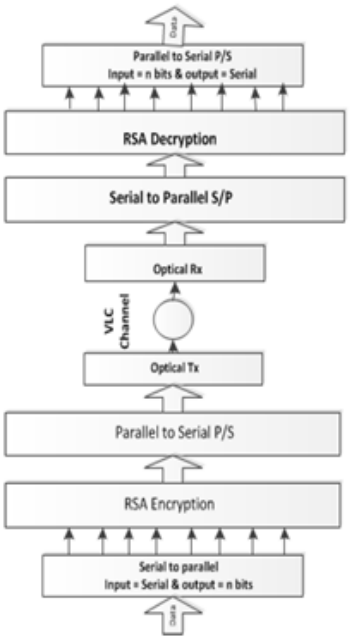
Gambar 20. Daerah Intersepsi Antara Dua Buah Transmitter [31]

Berikutnya Y. Liu, dkk [38] melakukan penelitian dengan skema LED ke *mobile device* dengan memanfaatkan kamera pada ponsel, pada skema tersebut diatur bagaimana agar data-data informasi hanya dapat diterima oleh *user* yang memiliki *key*. Data yang dikirim adalah berupa *image* dengan metode pemisahan *pixel* dan *grayscale level*. Semakin tinggi level iluminansi maka level *grayscale* akan menurun dan *image* dapat terlihat dengan lebih jelas.

Kemudian F. Mousal [39] melakukan investigasi pengaruh kriptografi terhadap performansi VLC ditinjau dari *Bit error ratio* (BER). Algoritma RSA diterapkan pada MAC layer dan set up ruangan 5 m x 5 m x 5 m dengan jarak antara LED ke *receiver* adalah 2.15 m. Blok algoritma yang diterapkan ke sistem VLC ditunjukkan pada Gambar 21. Data dikirim 2 Mb/s dan 12 Mb/s dengan panjang key 8 bit dan 16 bit. Hasil menunjukkan bahwa SNR dengan *key* 16 bit lebih besar dari pada data 8 bit, artinya semakin panjang *key* maka potensi *error* semakin besar. Potensi kesalahan data diterima akan semakin besar apabila *bit-rate* VLC semakin tinggi (>12Mb/s).

Sebagai *overview*, langkah-langkah untuk membuat pasangan kunci *public key* dan *private key* pada algoritma RSA adalah sebagai berikut.

a) Pilih dua bilangan prima yang berbeda secara acak, bilangan p dan q. Sebaiknya ($p \neq q$) karena apabila $p = q$ maka nilai n akan bernilai kuadrat [40].
b) Hitung $n = p * q$
c) Hitung $\varphi = (p\text{-}1)*(q\text{-}1)$.
d) Pilih kunci publik e, dimana $1 < e < \varphi(n)$, gcd $(e, \varphi(n)) = 1$
e) Bangkitkan kunci privat dengan menggunakan persamaan $d = e^{-1} \bmod \varphi(n)$.
f) Hasil dari algoritma adalah kunci publik = [e, n], kunci privat = [d, n]
g) Untuk enkripsi menggunakan persamaan: $C = m_t^e \bmod n$, dimana m_t merupakan *transmitted message* dan e adalah kunci penerima pesan
h) Untuk deskripsi menggunakan persamaan: $m_r = C^d \bmod n$, dimana m_r merupakan *received message* dan d adalah kunci pengirim pesan.



Gambar 21. Blok diagram algoritma RSA pada kriptograsi sistem VLC pada penelitian F. Mousal, dkk **[39]**

V. PENUTUP

A. *Kesimpulan*

VLC merupakan salah satu alternatif komunikasi yang menawarkan laju kecepatan mencapai *Giga bit per secon* (Gbps). Kemudian cakupan *bandwidth* yang lebih lebar, kecepatan akses data yang tinggi, serta bebas lisensi. VLC juga disinyalir lebih aman dari RF baik untuk keperluan *sharing* informasi maupun akses komunikasi searah/dua arah. Teknologi VLC berpedoman pada standar IEEE 802.15.7 yang mencakup tentang *PHY layer*, *MAC layer* dan *application layer*. Aspek-aspek *security* ini dibahas dalam MAC layer. Berbeda dengan RF yang praktik-praktik skema keamanan telah banyak dilakukan, *security* pada VLC masih jarang dilakukan sehingga menjadikan area riset ini sangat potensial untuk dikembangkan kedepannya.

Meskipun VLC terbatas pada area tertentu, bukan berarti aman dari serangan-serangan (*attack*) dari peretas. Resiko kerentanan jaringan komunikasi VLC yakni serangan secara *jamming* yakni dengan menggunakan *transmitter* untuk mengirim data-data *dummy*. Serangan dengan cara *snooping* yakni

mengintip komunikasi antara *master* dengan *client* yang lain secara illegal. Dan mengubah data asli juga menjadi potensi utama namun porsi keberhasilannya relatif kecil. Pada makalah ini juga telah dibahas beberapa contoh skema *secure* VLC pada *outdoor* maupun *indoor*. Pada aplikasi *outdoor*, sistem *security* dapat dimanfaatkan di kendaraan militer dengan protokol baru. Namun, sebagai akibat dapat meningkatkan *delay* komunikasi karena pengaruh *key* yang saling dikirimkan oleh kendaraan tersebut sangat memakan waktu (dalam hitungan detik). Selanjutnya pada aplikasi *indoor* sistem *security* tersebut dapat dimanfaatkan untuk membangun struktur *secure chatting.*

Algoritma yang dicoba pada skenario *security* ini juga bermacam-macam, yakni berupa *shamir's secret,* RSA, *Morse code*, *grayscale level* dan masih banyak lagi. Tentunya bidang pengembangan kriptografi juga menjadi area riset VLC yang bersifat terbuka.

DAFTAR PUSTAKA

[1] A A. Hikmaturokhman, W. Pamungkas, P.I. Setyawan, "Analisis Perhitungan Cakupan Sinyal Sistem Wcdma Pada Area Kampus Akademi Teknik Telekomunikasi Sandhy Putra Purwokerto," JURNAL INFOTEL, Vol. 5(1), pp. 21-29, Mei 2013.

[2] C-C. Chen, W-C. Wang, J-T. Wu, H-Y. Chen, K. Liang, "Visible light communications for the implementation of internet-of-things", *Opt. Eng.* 55(6), 060501, June, 2016.

[3] J.P. Conti, "What you see is what you send", *Engineering & Technology*, pp 66-68, November 2008, article available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4783247.

[4] H. Parikh, J. Chokshi, N. Gala, and T. Biradar, "Wirelessly transmitting a grayscale image using visible light," in *Proc. ICATE*, pp. 1–6, 2013.

[5] National Aeronautics and Space Administration, Science Mission Directorate. Introduction to the Electromagnetic Spectrum. Retrieved *[insert date - e.g. August 10, 2016]*, from NASA Science website: http://science.nasa.gov/ems/01_intro, 2010.

[6] S. Zhao, J. Xu, and O. Trescases, "A dimmable LED driver for Visible Light Communication (VLC) based on LLC resonant DC-DC converter operating in burst mode," in *Proc. 28th Annu. IEEE APEC Expo*, pp. 2144–2150, 2013.

[7] E. Schubert, *Light-Emitting Diodes*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[8] D. Karunatilaka, F. Zafar, V. Kalavally, "LED Based Indoor Visible Light Communications: State of the Art*," IEEE Communication Surveys & Tutorials*, Vol. 17(3), pp. 1649-1678, 2015.

[9] O. Ergul, E. Dinc, O.B. Akan, "Communicate to illuminate: State-of-the-art and research challenges for visible light communications," *Physical Communication*, Vol. 17, pp. 72 – 85, 2015.

[10] A. P. Putra, S. Fuada, Y. Aska, T. Adiono, "System-on-Chip Architecture for High-Speed Data Acquisition in Visible Light Communication System," *Proc. of the IEEE Int. Symposium on Electronics and Smart Devices* (ISESD), October 2016.

[11] T. Adiono, Yulian Y. Aska, A.A. Purwita, S. Fuada, A.P. Putra, "Modeling OFDM system with Viterbi Decoder Based Visible Light Communication," *Proc. of the Int. Conf. on Electronic, Information and Communication* (ICEIC), January 2017.

[12] S. Fuada, T. Adiono, A. P. Putra, Y. Aska, "A Low-cost Analog Front-End (AFE) Transmitter Designs for OFDM Visible Light Communications," *Proc. of the IEEE Int. Symposium on Electronics and Smart Devices* (ISESD), October 2016.

[13] S. Fuada, A.P. Putra, Y. Aska, T. Adiono, "A First Approach to Design Mobility Function and Noise Filter in VLC System Utilizing Low-cost Analog Circuits,"*accepted in i-JES IAOE.*

[14] D. Wen, W. Cai, Y. Pan, "Design of Underwater Optical Communication System," *Proc. of OCEANS*, pp. 1-4, June 2016.

[15] K. Sindhubala and B. Vijayalakshmi, "Review On Impact Of Ambient Light Noise Sources and Applications In Optical Wireless Communication Using LED," *Int. J. of Applied Engineering Research*, Vol. 10(12), pp. 31115 – 31130, 2015.

[16] T. Adiono, S. Fuada, A.P. Putra, Y. Aska, "Desain Awal *Analog Front-End Optical Transceiver* untuk aplikasi *Visible Light Communication*," *J. Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, Vol. 5(4), pp. 319-327, November 2016.

[17] Y.Gu, N. Narendran, T. Dong, and H. Wu, "Spectral and luminous efficacy change of high-power LEDs under different dimming methods," in *Proc. 6th Int. Conf. Solid State Lighting*, Vol. 6337, 2006.

[18] S. Fuada, A.P. Putra, T. Adiono, "Analysis of Received Power Characteristics of Commercial Photodiodes in Indoor LOS Channel Visible Light Communication". *Unpublished*.

[19] L.U. Khan, "Visible light communication: Applications, architecture, standardization and research challenges," *Digital Communications and Networks*, 2016. DOI: http://dx.doi.org/10.1016/j.dcan.2016.07.004i.

[20] K. Cui, G. Chen, Q. He, and Z. Xu, "Indoor optical wireless communication by ultraviolet and visible light," *Proc. SPIE Free-Space Laser Communications IX*, 74640D, August 2009.

[21] IEEE, P802.15.7 – Standard for Short-Range Wireless Optical Communication, 2011.

[22] M. Noshad and M. Brandt-Pearce, "Can visible light communications provide Gb/s service?" Aug. 2013, arXiv: 1308.3217.

[23] A. Pradana, "Rancang Bangun Layer Fisik Komunikasi Cahaya Tampak Berbasis DC-OFDM dan PWM," Master Thesis, ITB, Indonesia, 2016.

[24] S. Fuada, T. Adiono, A. P. Putra, Y. Aska, "LED Driver Design for Indoor Lighting and Low-rate Data Transmission Purpose," *Unpublished.*

[25] C-W. Chow, Y. Liu, C-H. Yeh, C-Y Chen, C-N. Lin, D-Z. Hsu, "Secure communication zone for white-light LED visible light communication," *Optics Communications*, Vol. 344, pp. 81–85, 2015.

[26] U.H. Jayo, A.S.K. Mammu and I.D. Iglesia, "Reliable Communication in Cooperative Ad hoc Networks," [Online] available at http://www.intechopen.com/books/contemporary-

issues-in-wireless-communications/reliable-communication-in-cooperative-ad-hoc-networks.

[27] J-H. Yoo, J-S. Jang, J. K. Kwon, H-C. Kim, D-W. Song and S-Y. Jung, "Demonstration of Vehicular Visible Light Communication Based on LED Headlamp," Int. J. of Automotive Technology, Vol. 17(2), pp. 347−352, 2016.

[28] W. Viriyasitavat, S-H Yu and H-M Tsai, "Short Paper: Channel Model for Visible Light Communications Using Off-the-shelf Scooter Taillight," *Proc. of 2013 IEEE Vehicular Networking Conference* (VNC), pp. 170-173, 2013.

[29] Visible Light Communication, [Online] Available at: https://www.disneyresearch.com/project/visible-light-communication/

[30] S. Ucar, S.C. Ergen, O. Ozkasap, D. Tsonev, H. Burchardt, "SecVLC: Secure Visible Light Communication for Military Vehicular Networks," *Proc. of the 14th ACM Int. Symposium on Mobility Management and Wireless Access (MobiWac)*, pp. 123-129, November 2016.

[31] A. Mostafa, L. Lampe, "Physical-Layer Security for Indoor Visible Light Communications," *Proc. of IEEE ICC Optical Networks and Systems*, pp. 3342-3347, 2014.

[32] G.J. Blinowski, "Practical Aspects of Physical and MAC Layer Security in Visible Light Communications Systems," Int. J. of Electronics and Telecomunications, Vol. 62(1), pp. 7-13, 2016.

[33] J. Classen, D. Steinmetzer, M. Hollick, "Opportunities and pitfalls in securing visible light communication on the physical layer," *Proc. of the 3rd Workshop on Visible Light Communication Systems* (VLCS), pp. 19-24, October 2016.

[34] I.M. Gracia, A.M.R. Aguilera, V. Guerra, J. Rabadan, "Data Sniffing Over an Open VLC Channel," *Proc. of the 10th Int. Symposium on Communication Systems, Networks and Digital Signal Processing* (CSNDSP), 2016

[35] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, E. Knightly, "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications," *Proc. of the 2nd Int. Workshop on Visible Light Communications Systems* (VLCS), pp. 9 -14, 2015.

[36] A. Mukherjee, "Secret-Key Agreement for Security in Multi-Emitter Visible Light Communication Systems," *IEEE Communications Letters*, Vol. 20(7), pp. 1361 - 1364, July 2016.

[37] A. Hilmia, K. Hewage, A. Varshney, C. Rohner, T. Voigt, "Poster Abstract: BouKey: Location-Based Key Sharing Using Visible Light Communication," *Proc. of the 15th ACM/IEEE Int. Conf. on Information Processing in Sensor Networks (IPSN)*, April 2016.

[38] Y. Liu *et. al*, "Light Encryption Scheme Using Light-Emitting Diode and Camera Image Sensor," *IEEE Photonics J.*, Vol. 8(1), February 2016.

[39] F. Mousa1 *et. al*, "Investigation of Data Encryption Impact on Broadcasting Visible Light Communications,"*Proc. of the 9th Int. Symposium on Communication Systems, Networks & Digital Signal Processing* (CSNDSP), Oktober 2016.

[40] R. Munir, "Algoritma RSA dan ElGamal, [Online], Available at "http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Algoritma%20RSA.pdf," 2004.