KINETIK, Vol. 2, No. 1, Februari 2017, Hal. 37-42
ISSN : 2503-2259,
E-ISSN : 2503-2267

Pengunaan Teknik Keamanan Pada Jaringan Serat Optik dengan Metode Anti-Jamming dan Steganografi Menggunakan Modul Optisystem

Mia Rosmiati[*1], Arindra Rizky[2], Ian Pramana Depari[3]
[1,2,3]Universitas Telkom Bandung
mia@tass.telkomuniversity.ac.id[*1], ndrpurba@gmail.com[2], ianpramanadepari@gmail.com[3]

Abstrak

Serat optic merupakan media transmisi yang dapat menghantarkan informasi dalam bentuk cahaya. digunakannya cahaya sebagai media penghantar informasi membuat media ini dapat menghantarkan informasi dengan kapasitas besar dalam waktu yang sangat singkat. Sehingga saat ini serat optic banyak digunakan dalam Telekomunikasi. jaringan serat optic ini harus disertai dengan teknik keamanan yang andal dalam proses transmisi informasinya, karena jika terjadi penyerangan dalam jaringan yang serat optic maka data yang akan diterima oleh receiver akan jauh berbeda dengan data yang dikirim transmitter. Sehingga hal ini sangat fatal jika informasi yang dikirimkan memiliki tingkat kerahasiaan yang sangat tinggi seperti informasi keamanan Negara. Adapun metode yang dapat digunakan dalam pengamanan jaringan serat optic adalah metode Steganography dan metode Anti-jamming. Dari percobaan yang telah dilakukan terlihat bahwa teknik Steganography memiliki tingkat keandalan yang lebih baik jika dibandingkan dengan metode anti-jamming dengan nilai BER untuk metode steganography adalah 1.91219e-077.

Kata kunci: *Jaringan Serat Optic, Steganography, Anti-jamming, BER*

Abstract

Fiber optics is a transmission medium used to convert information into optical (light). As an transmission medium, light can deliver enormous information-carrying capacity in a very short time. Thus, make fiber optics commonly used in telecommunication. This fiber optics should be equipped with reliable protection during the transmission process because once it got attacked, the data received would be much different from the actual data sent by the transmitter. Therefore, it could be quite dangerous when the data being sent requires high level confidentiality, such as National information security. Anti-jamming and Steganography method can be used to protect the fiber optics. The experiment conducted shows that Steganography mehod has higher reliablity compared to anti-jamming method *with the BER values for steganography method is 1.91219e-077.*

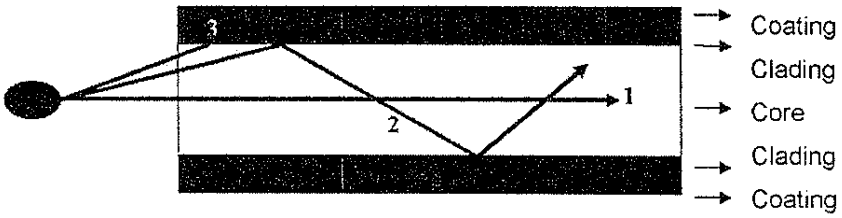
Keywords: *Fiber–Optic Network, Steganography, Anti-jamming, BER*

1. Pendahuluan

Serat *optic* adalah suatu kabel terbuat dari $SiCl_4$, berfungsi untuk menghantarkan cahaya yang mengandung informasi dengan kecepatan yang sangat tinggi ke *receiver*. Adapun untuk transmisi cahaya dalam fiber *optic* [1] bisa dilihat Gambar 1, terdapat tipe perambatan cahaya dalam fiber *optic*, yaitu:

1. Perambatan cahaya yang bergerak lurus di dalam fiber *optic*, sehingga cahaya mengalami transmisi jarak jauh.
2. Perambatan cahaya yang mengalami pemantulan (refleksi) di dalam fiber *optic*, hal ini dikarenakan diameter *core* lebih besar dibandingkan panjang gelombang cahaya, sehingga ada dua atau lebih cahaya yang dapat merambat pada media yang sama.
3. Cahaya mengalami pembiasan (refraksi), hal ini dikarenakan sudut cahaya datang lebih kecil dibandingkan sudut kritisnya, mengakibatkan cahaya tidak dapat merambat dalam fiber *optic*.

Makalah dikirim 30 Desember 2016; Revisi 30 Januari 2017; Diterima 1 Februari 2017



Gambar 1. Perambatan Cahaya di dalam Fiber Optik

Jika dilihat dari 3 fenomena diatas, maka ada dua hal yang harus dipenuhi agar cahaya dapat merambat dalam fiber *optic*, yaitu sudut datang harus lebih besar dari sudut kritis serta indeks bias *core* harus lebih besar dari indeks bias *cladding*.

Pada saat ini, jaringan kabel fiber *optic* sangat banyak digunakan untuk menunjang komunikasi dalam mengirim dan menerima data. Dengan menggunakan kabel fiber *optic* pengiriman data dapat lebih cepat tanpa perlu menunggu lama agar data sampai ke penerima. Pada saat mengirim data harus diperhatikan juga keamanan data yang dikirim agar data sampai ke tujuan yang diinginkan tanpa adanya gangguan dari pihak ketiga.

Meskipun kemungkinan data yang dikirim aman tetapi terkadang ada pihak ketiga yang ingin mengetahu data yang dikirim tersebut sehingga data yang dikirim tidak aman. Dalam hal ini sudah terjadi ancaman untuk pengirim, karena data yang dikirim tersebut dapat diketahui oleh pihak ketiga sehingga data tersebut tidak aman. Proses penyerangan dalam jaringan serat *optic* banyak dilakukan dengan cara melakukan *bending* (pembelokan pada serat *optic* utama), sehingga terdapat sebagian sinyal yang keluar dari *core*. Sinyal yang keluar dari *core* ini dapat di *tapping* oleh serat *optic* penyadap sehingga pihak ketiga dapat mengetahui informasi yang ditransmisikan oleh *transmitter* ke *receiver*. Oleh sebab itu, metode Steganography dan Anti-jamming dapat digunakan untuk meningkatkan keamanan dalam jaringan serat *optic*.

Metode Optical Steganography [2] bertujuan untuk meningkatkan privasi komunikasi dengan menyembunyikan sinyal dalam publik *channel*, sehingga tidak ada yang mengetahui keberadaan sinyal tersebut. Prinsip dasar dari Optical Steganoggrafi adalah merenggangkan pulsa data *stealth* secara temporal menggunakan dispersi tinggi dan Amplitudo dari pulsa yang cepat menurun setelah terjadi perenggangan sinyal sehingga sinyal dapat disembunyikan di publik *channel*.

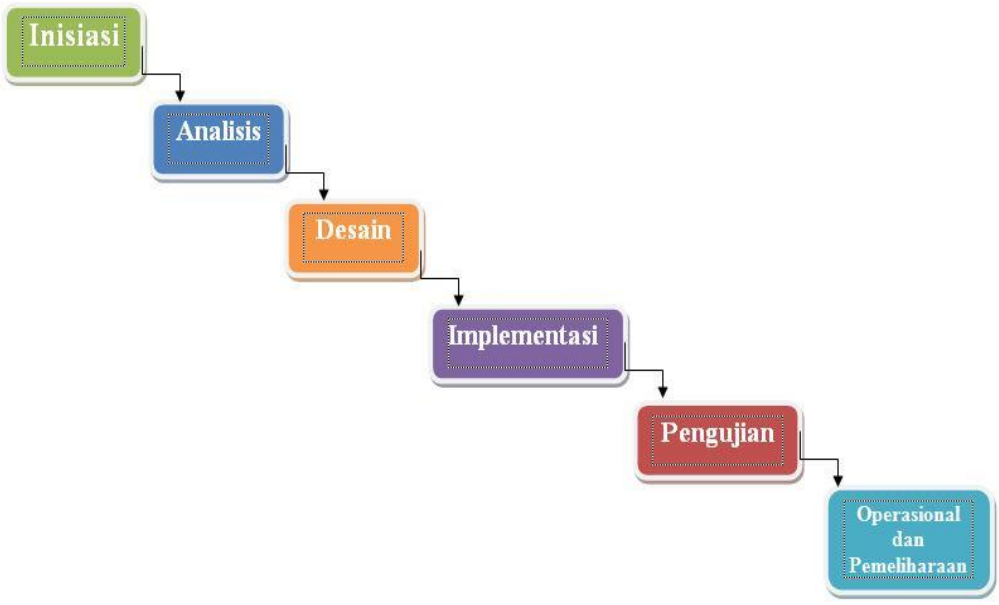
Anti-jamming merupakan teknik keamanan yang bertindak untuk mencegah tabrakan data dalam *system* mekanik dan perangkat komunikasi. Jaringan sering mendapat gangguan pada *channel* sinyal dengan *strong, noise*, dan Anti-jamming memiliki peran keamanan yang kuat serta mempunyai kecepatan pada proses. Adanya Anti-jamming, data tidak ada yang akan bertabrakan dan akan secara utuh didapat oleh penerima, lalu penyadap tidak dapat *recovery* data. Sehingga data yang didapat lebih cepat dan utuh [3].

Teknik keamanan yang digunakan ini berfungsi untuk mengamankan lapisan fisik serat *optic*, hal ini dikarenakan lapisan fisik serat *optic* sangat berperan penting dalam pengiriman informasi dengan menggunakan media serat *optic,* karena informasi yang dilewatkan berupa cahaya bertransmisi menggunakan prinsip gelombang cahaya dan berdasarkan indeks bias media. Sehingga jika media transmisi mengalami kerusakan, maka informasi dapat mengalami kerusakan dalam jumlah yang cukup besar.

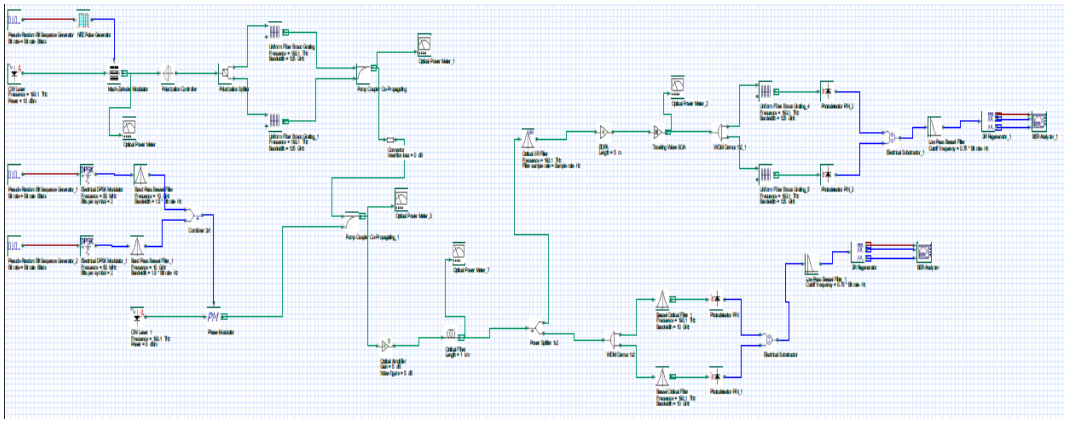
2. Metode Penelitian

Metode penelitian yang digunakan melalui simulasi *optisystem* untuk penggunaan dua teknik keamanan yang berbeda pada jaringan serat *optic* adalah metode Waterfall, seperti terlihat pada Gambar 2.

Proses inisiasi merupakan sebuah tahapan untuk menentukan teknik keamanan yang dibutuhkan jaringan serat optik, proses desain, dan implementasi pengujian dilakukan melalui aplikasi *optical system*. Proses desain keamanan yang digunakan adalah teknik Steganography dan Anti-jamming, sedangkan proses pengujian dilakukan dengan cara melihat nilai *bit error rate* (BER) terhadap data yang diterima oleh *receiver* setelah dilakukan proses penyerangan selama bertransmisi menggunakan media fiber optik, dengan cara membandingkan nilai BER untuk setiap teknik keamanan yang digunakan. Maka dapat ditentukan metode yang terbaik dalam mengirimkan data dengan menggunakan media fiber optik. Adapun desain jaringan serat optik dengan menggunakan teknik keamanan Steganography ditunjukkan oleh Gambar 3.



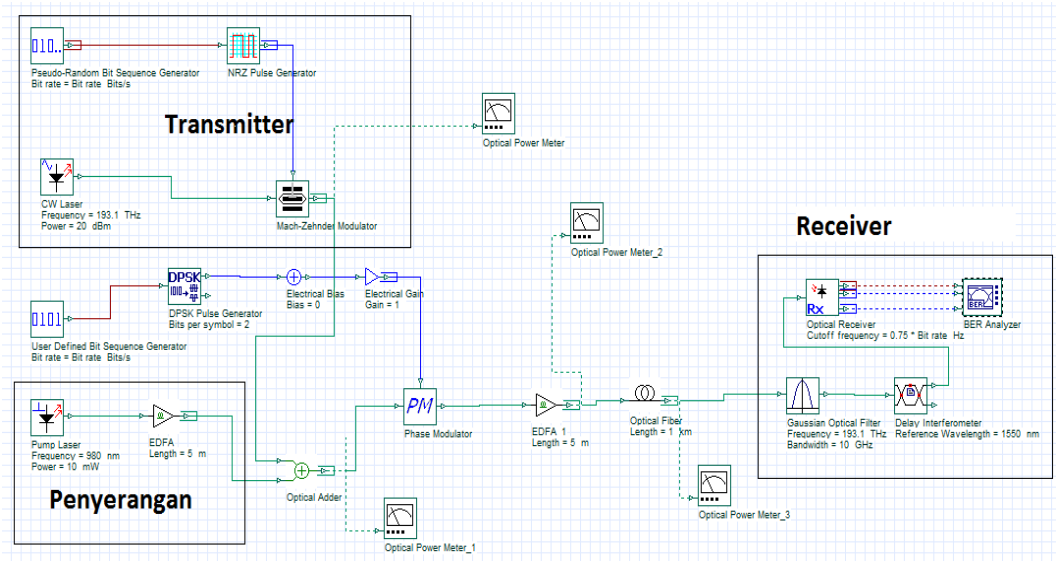
Gambar 2. Metode Waterfall



Gambar 3. Desain Jaringan Serat Optik dengan Menggunakan Optical Steganography.

Pada Gambar 3 terlihat bahwa jaringan serat *optic* terbagi menjadi dua, yaitu *stealth channel* dan *public channel*, dimana *public channel* berfungsi sebagai jaringan yang diserang dan tanpa menggunakan teknik keamanan. Dalam jaringan *stealth channel* berfungsi untuk mengamankan data dengan menyelipkan jaringan *public channel* menggunakan *connector* dalam menghubungkan *stealth channel* dan *public channel*, kemudian data diteruskan melalui EDFA *(erbium-doped* fiber *amplifier),* serta *optical* fiber, lalu dipecah menggunakan *splitter,* pada bagian *receiver* data tanpa menggunakan keamanan dan bagian *splitter* kedua jaringan di filter ke EDFA *(erbium-doped* fiber *amplifier),* maka sinyal di *compressor* akan meningkatkan sinyal, kemudian masuk ke *spliter* dan data di *decoder*.

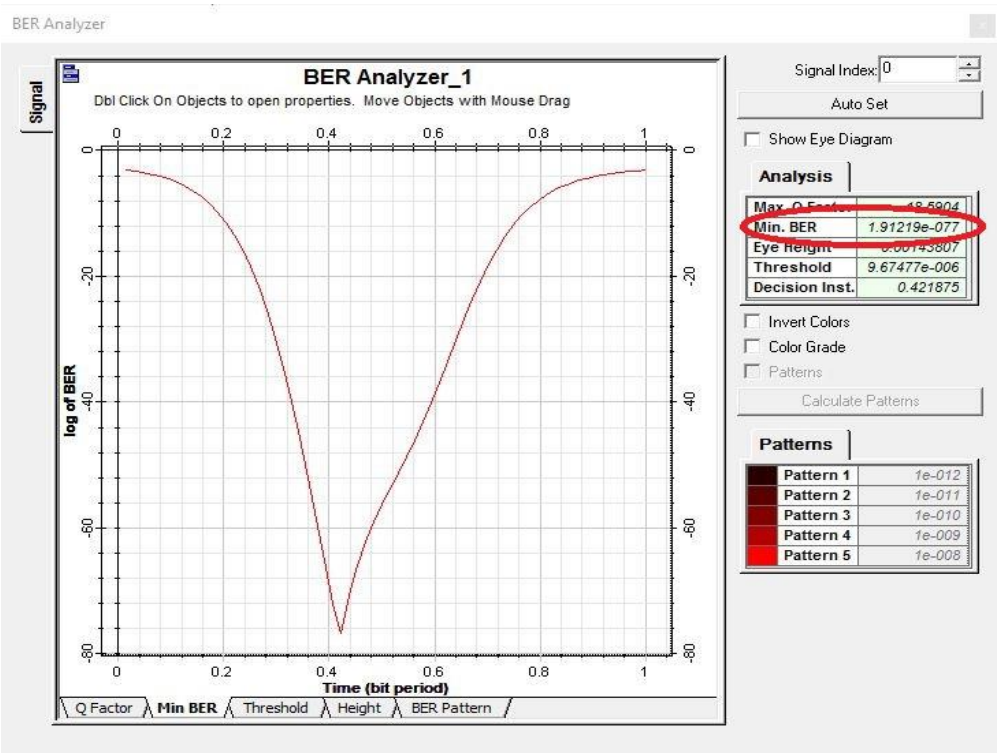
Gambar 4, jaringan serat *optic* menggunakan metode Anti-jamming, fungsi *pump* laser bertujuan untuk meningkatkan daya yang dikirimkan oleh *transmitter*, sehingga dengan adanya variasi daya yang digunakan pada *pump* laser maka data yang dilewatkan pada media serat *optic* dapat diamankan dari pihak ketiga.



Gambar 4. Jaringan Serat Optic dengan Menggunakan Metode Anti-jamming

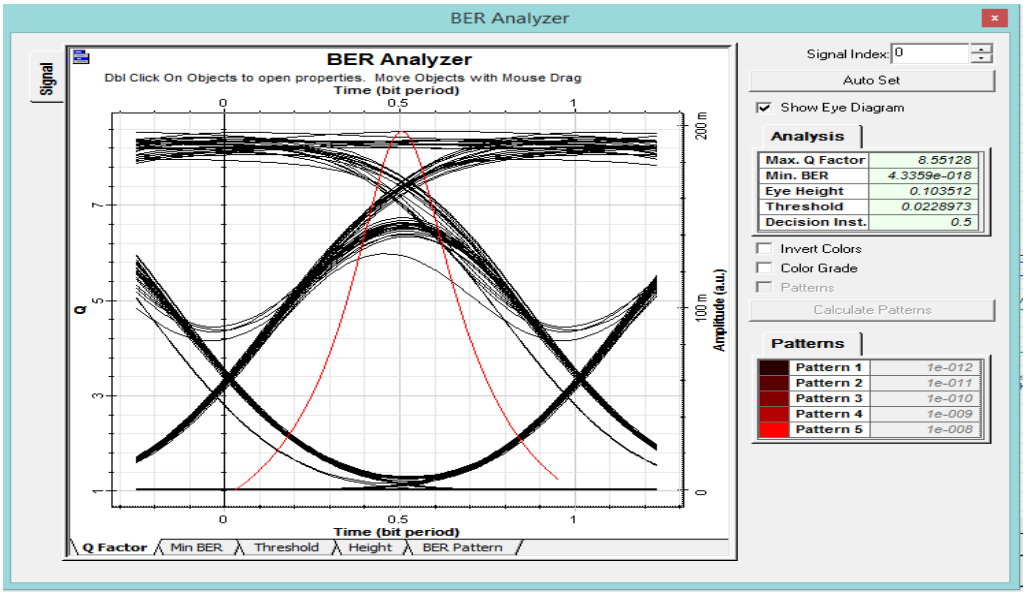
3. Hasil Penelitian dan Pembahasan

Proses pengujian keandalan *system* diukur berdasarkan nilai BER untuk jaringan serat *optic* menggunakan metode Steganography dan pengukuran BER dengan metode Anti-jamming. Percobaan teknik keamanan menerapkan metode Optical Steganography dengan *power* 10 dBm untuk *transmitter* serta 5 dBm pada Cw laser dan panjang kabel optik 1 Km.



Gambar 5. Nilai Bit Error Rate untuk Public Channel

Pada Gambar 5 menunjukkan nilai BER untuk jaringan fiber *optic* dengan Optical Steganografi di *stealth channel* adalah 1.91219e-077. Sedangkan besarnya nilai BER untuk jaringan serat *optic* menggunakan metode Anti-jamming. Berdasarkan Gambar 6 terlihat besarnya nilai BER untuk jaringan serat optik dengan teknik keamanan Anti-jamming adalah 4.33e-018.



Gambar 6. Pengukuran Bit Error Rate untuk Teknik Keamanan dengan Menggunakan Metode Anti-jamming

4. Kesimpulan

Berdasarkan pengujian yang dilakukan melalui penyerangan pada jaringan serat optik dengan menggunakan metode keamanan Steganography menunjukkan nilai BER yang lebih kecil dibandingkan dengan metode Anti-jamming, hal ini menunjukkan metode Steganography memiliki tingkat keandalan yang lebih baik jika dibandingkan dengan metode Anti-jamming dalam menghadapi penyerangan pada jaringan serat *optic.* Adapun penelitian yang dapat dilakukan untuk tahap berikutnya, yaitu dengan melakukan perbandingan pengukuran daya yang diterima oleh *receiver* setelah dilakukan penyerangan pada jaringan serat *optic*.

Referensi

[1] G. P. Agrawal. “Fiber-Optic Communication Systems.” Vol. 3. 2002.
[2] B. J. Ben Wu. “Optical Steganography, Secure Communicaation in Fiber-Optic Networks.” 2014.
[3] John Doe. “Internet Usage Within Nations.” Boston: Boston Publishing. 2000.
[4] Optisystem, "Optisystem," Optical Communication System Amplifier Design Software, 2009.
[5] Z.Wang. “Improving the Privacy of Optical Steganography with Temporal Phase Masks.” Opt. Express. Vol. 18. 2010.
[6] OptiSystem. OptiSystem Tutorials-Volume 1 and volume 2. 2014.
[7] Pramana, Ian Depari, “Pembangunan Teknik Keamanan Pada Jaringan Serat Optik dengan Metode Optical Steganography Melalui Modul Optisystem”, Buku Proyek Akhir Universitas Tekom, 2016.
[8] Rizki, Arindra S. Purba, “Pembangunan Teknik Keamanan pada Jaringan Serat Optik dengan Metode Anti-Jamming Melalui Modul Optisystem” Buku Proyek Akhir Universitas Tekom, 2016.