BAB II
LANDASAN TEORI

2.1 Computer Network

Menurut Sharam Hekmat di dalam bukunya yang berjudul "*Communication Networks*", dikatakan bahwa "*A computer network is the infrastructure that allows two or more computers (called hosts) to communicate with each other. The network achieves this by providing a set of rules for communication, called protocols, which should be observed by all participating hosts*." (Hekmat, 2005)

Atau dapat diartikan bahwa *Computer Network* atau dalam bahasa Indonesia adalah Jaringan Komputer merupakan sebuah infrastruktur jaringan yang membantu dua komputer atau lebih (disebut juga *host*) untuk dapat saling berkomunikasi satu dengan yang lainnya, dengan adanya berbagai aturan jaringan yang harus diikuti oleh seluruh *host*, yang disebut sebagai protokol.

Dalam bukunya Hermat mengatakan bahwa *The International Standards Organization (ISO)* telah membuat sebuah referensi jaringan yang disebut dengan *Open Systems Interconnection (OSI)* yang terdiri dari 7 lapisan yang masing – masing lapisan memiliki peran yang berbeda, yaitu :

1. *Application Layer*

   Berfungsi sebagai antarmuka aplikasi dengan jaringan, mengatur bagaimana aplikasi mengakses jaringan dan membuat *error message* (pesan kesalahan).

2. *Presentation Layer*

Berfungsi untuk mengubah data yang diinginkan aplikasi ke dalam bentuk yang dapat ditransmisikan oleh jaringan.

3. *Session Layer*

Berfungsi untuk mendefinisikan suatu koneksi jaringan dibuat, dijaga, ataupun dirusak.

4. *Transport Layer*

Berfungsi untuk memecah data menjadi banyak paket yang diurutkan dengan tujuan agar dapat diurutkan kembali setelah data sampai ke penerima.

5. *Network Layer*

Berfungsi untuk mendefinisikan *Internet Protocol (IP) Address* dari tiap *host* (deretan angka biner dari 32 sampai dengan 128 bit untuk mendefinisikan tiap *host* dalam jaringan), membuat *header* pada paket – paket, serta menyiarkan paket melintasi beberapa jaringan melalui *router.*

6. *Data – Link Layer*

Berfungsi menentukan bagaimana paket data tersebut dikelompokkan menjadi sebuah format yang disebut sebagai *frame*, memperbaiki kesalahan yang ada, pengendalian, dan pengalamatan pada perangkat keras.

7. *Physical Layer*

Berfungsi mendefinisikan sebuah media transmisi dari sebuah jaringan, sinkronisasi bit, topologi jaringan, pengabelan, arsitektur jaringan atau metode pensinyalan. Lapisan ini juga mendefinisikan bagaimana *Network Interface Card (NIC)*, perangkat yang menjembatani komputer dengan jaringan dapat berinteraksi dengan media radio atau kabel.

2.2 Wi-Fi

Menurut *Digi International Inc* di dalam bukunya yang berjudul "*An Introduction to Wi-Fi*", dikatakan bahwa "*Wi-Fi is the name given by the Wi-Fi Alliance to the IEEE 802.11 suite of standards. 802.11 defined the initial standard for wireless local area networks (WLANs).*" (*Digi International Inc*, 2008)

Atau dapat diartikan bahwa *Wi-Fi* merupakan istilah yang diberikan oleh *Wi-Fi Alliance* kepada jaringan lokal nirkabel sesuai dengan aturan IEEE 802.11 yang merupakan standar dari sebuah jaringan lokal nirkabel (WLAN).

Wi-Fi biasanya berada pada jangkauan sinyal 2,4 *gigahertz* UHF dan 5 *gigahertz* SHF.

Saat ini perangkat yang sudah dapat menggunakan *Wi-Fi* adalah *personal computer (PC), smartphone, tablet*, kamera digital, *smart TV, digital audio player*

dan *modern printer* yang terhubung dengan *wireless access point*, yaitu sumber akses jaringan nirkabel yang berjarak minimal 20 meter di dalam ruangan.

- **IEEE 802.11 (a / b / g / n)**

Merupakan aturan standar dari sebuah jaringan lokal nirkabel (WLAN) yang digunakan untuk mendefinisikan suatu *medium access control* (MAC) dan beberapa *physical layer* (PHY) untuk sebuah koneksi nirkabel *(fixed, portable,* dan *moving station*) di sebuah area (STA) dengan tujuan menyediakan konektivitas nirkabel pada mesin – mesin otomatis, perlengkapan, atau STA lain yang perkembangannya sangat pesat. (*IEEE Computer Society*. 2007)

- **802.11 *Deauthentication Frame***

Merupakan paket data berisi *error message* yang dikirim dari sebuah *station* (STA), disebut juga *Reason Code* yang harus diterima oleh si penerima (komunikasi satu arah) yang dimana koneksi langsung diputuskan dari STA pengirim. (*Cisco Support Community*, 2015)

2.2 *WPA* dan *WPA2*

WPA (Wireless Protected Access) merupakan metode pengamanan jaringan nirkabel yang menggunakan *Temporal Key Integrity Protocol (TKIP)* untuk enkripsi dan penggunaan Otentikasi *802.1X* dengan standar *Extensible Authentication Protocol (EAP)* yang menggantikan pendahulunya *WEP (Wired Equivalent Privacy)* untuk solusi keamanan yang lebih baik. (Wi-Fi Alliance, 2003)

WPA2 (Wireless Protected Access 2) memiliki kesamaan dengan *WPA,* tetapi mendapat penambahan metode enkripsi yaitu *Advanced Encryption Standard (AES)*. *AES* menggunakan algoritma *mathematical ciphering* yang menggunakan *key variable* dengan ukuran 128 - , 192 - , atau 256 bit. (Wi-Fi Alliance, 2003)

2.3 Beacon Flooding Attack

Beacon Flooding Attack merupakan jenis serangan ke jaringan nirkabel dengan mengirimkan banyak *Access Point* palsu yang dapat membuat scanner menjadi *crash* atau bahkan rusak. (Mark, 2015)

Terdapat 2 jenis *beacon flooding attack*, yaitu dalam bentuk *clone* dan dalam bentuk *list. Beacon flood* dalam bentuk *clone* merupakan pengiriman *Access Point* palsu yang nama SSIDnya disamakan dengan *Access Point* yang sudah ada, sedangkan *beacon flood* dalam bentuk *list* merupakan pengiriman *Access Point* palsu yang nama SSIDnya dibuat sendiri.

2.4 Jamming

Jamming di dalam jaringan nirkabel didefinisikan sebagai gangguan komunikasi nirkabel yang dikarenakan dengan menurunkan rasio *signal-to-noise* pada sisi *receiver* melalui transmisi yang mengganggu sinyal *wireless*. (K. Grover, A.L, 2014)

Biasanya suatu perangkat yang terhubung dengan *Internet* akan diserang pada bagian *Physical Layer* sehingga pihak luar tidak mendapatkan sinyal, kemudian sinyal itu pun mengembalikan beberapa paket data yang sudah sedikit dimodifikasi.

Menurut Kanika Grover, ada beberapa jenis jammer, yaitu :

1. *Proactive Jammer*

   Merupakan tipe *jammer* yang mentransmisi sinyal baik ada atau tidaknya komunikais data di jaringan tersebut. *Proactive Jammer* sendiri terdiri dari 3 macam :

- *Constant Jammer*

  Jammer ini akan memancarkan bit acak secara terus menerus tanpa mengikuti protokol *CSMA*. *Constant Jammer* mencegah perangkat yang tersambung dengan internet untuk berkomunikasi satu sama lain dengan membuat media wireless secara terus menerus dibuat menjadi sibuk.

- *Deceptive Jammer*

  Sama dengan *Constant Jammer*, tetapi yang dipancarkannya adalah paket reguler.

- *Random Jammer*

  Memancarkan bit acak dan paker reguler ke dalam jaringan. Dibandingkan dengan 2 *jammer* di atas, *jammer* ini lebih hemat energi. *Jammer* ini memiliki 2 fase, yaitu fase tidur dan fase

jamming. *Jammer* ini akan "tidur" untuk beberapa saat dan aktif untuk melakukan *jamming* sampai kembali ke waktu fase tidurnya.

2. *Reactive Jammer*

   Merupakan *jammer* yang bekerja hanya ketika ada aktivitas di jaringan tertentu. *Reactive Jammer* terdiri dari 2 macam :

- *Reactive RTS/CTS Jammer*

  Jammer ini baru bekerja ketika adanya aktivitas *RTS (Request To Send)* yang dikirimkan dari sender. *Jammer* ini akan menghilangkan aktivitas *RTS* tersebut sehingga tidak akan sampai ke *receiver*.

- *Reactive Data/ACK Jammer*

  Jammer ini bekerja dengan merusak paket *ACK*. *Jammer* ini akan membiarkan data sampai ke *receiver*, baru kemudian merusak paket *ACK* tersebut.

3. *Function-specific Jammer*

   Jammer yang dibuat hanya untuk fungsi tertentu. Selain bisa seperti *Proactive dan Reactive Jammer*, *Jammer* ini dapat bekerja pada satu saluran untuk menghemat daya ataupun langsung menyerang beberapa saluran sekaligus untuk bekerja secara maksimum tergantung daya yang dipakai. *Function-specific Jammer* memiliki 3 jenis yaitu :

- *Follow-on Jammer*

Jammer ini melewati seluruh saluran yang ada dalam jangka waktu yang sangat singkat (ribuan kali per detik) dan akan menyerang tiap saluran dalam waktu yang singkat.

- *Channel-hopping Jammer*

  Jammer ini melewati beberapi saluran yang berbeda secara proaktif. *Jammer* ini memiliki akses langsung ke saluran dengan mengutamakan algoritma *CSMA* yang disediakan *MAC layer*.

- *Pulsed-noise Jammer*

  Jammer ini dapat bertukar saluran dan melakukan *jamming* pada *bandwidth* yang berbeda dan periode waktu yang berbeda. Mirip dengan *Random Jammer*, *Jammer* ini juga dapat menyimpan daya dan melakukan jamming pada waktu tertentu. *Pulsed-noise Jammer* ini pun juga dapat menyerang banyak saluran, tak seperti pada *Random Jammer* yang hanya dapat menyerang 1 saluran saja.

4. *Smart-hybrid Jammer*

   Jammer ini dikatakan "*Smart*" karena dapat melakukan *jamming* secara efisien. Tujuannya adalah untuk memperbesar efek *jamming* yang telah dilakukan pada jaringan yang telah menjadi target. *Jamming* tipe ini pun juga terdiri dari 3 macam, yaitu :

- *Control Channel Jammers*

  Jammer ini bekerja pada *multi-channel network* dengan menarget saluran yang menjadi pusat kontrolnya (*Control Channel*) atau

jaringan yang biasanya digunakan untuk koordinasi aktivitas jaringan.

- *Implicit Jamming Attacks*

  Jamming dengan fitur tambahan yaitu dengan mematikan fungsionalitas dari target, yang dapat menyebabkan *Denial of Services (DoS)* yang tidak hanya berdampak pada target, tetapi juga pada perangkat lain yang berada dalam satu jaringan dengan target. Serangan ini dilakukan dengan mengeksploitasi algoritma yang terdapat di dalam jaringan nirkabel, dimana *AP (Access Point)* memberikan akses pada perangkat yang menjadi target tersebut dengan mengurangi kecepatannya. *Jamming* pun dilakukan dengan menyerang perangkat target yang berkomunikasi dengan *AP*.

- *Flow-jamming Attacks*

  Jamming ini melibatkan banyak jammer yang menyerang paket data yang terdapat di dalam suatu jaringan untuk mengurangi traffic flow. Serangan ini dilakukan dengan menggunakan informasi yang terdapat pada network layer.

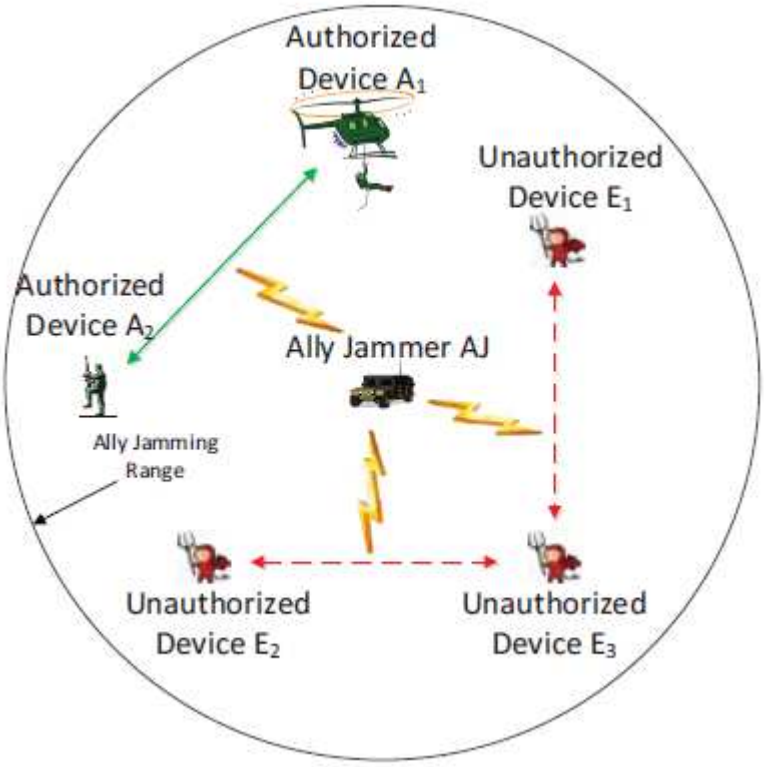
Lokasi peletakan *jammer* juga berperan penting dalam membuat suatu jammer dapat bekerja dengan lebih efektif. *Jammer* dapat diletakkan dimana saja tetapi alangkah baiknya diletakkan pada tempat yang dapat menjangkau semua perangkat yang terkoneksi dalam jaringan yang akan dijadikan target.

2.5 Contoh Penelitian Terdahulu

- *Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time (Wenbo Shen, Peng Ning, Xiaofan He, Huaiyu Dai)*

Penelitian ini bertujuan untuk membuat suatu *jammer* yang dapat memaksa putus koneksi terhadap perangkat yang tidak memiliki akses atas jaringan tersebut, yang berguna untuk memutuskan koneksi perangkat yang seharusnya tidak memiliki akses terhadapt suatu jaringan dengan sandi khusus sehingga tidak dapat diprediksi oleh perangkat tersebut, tetapi perangkat tersebut dapat kembali memiliki akses yaitu dengan perangkat yang memiliki akses terhadap jaringan tersebut dan juga memiliki sandi khusus tersebut.

Pertama sekali, jaringan harus dikonfigurasi agar dapat diakses oleh perangkat yang tidak memiliki akses. Kedua, perangkat yang memiliki akses harus terkoneksi dengan jammer, untuk memperkirakan jangkauan sinyal, memutuskan koneksi, dan mengembalikan koneksi yang terputus sebelumnya. Ketiga, jika dalam jangkauan terdapat banyak jammer, perangkat yang memiliki akses harus mengkonfigurasi jammer mana yang tersambung dengan dia, kemudian memancarkan ulang sinyal untuk mengembalikan transmisi sebelumnya.



Gambar 2. 1. Skenario *Ally Friendly Jamming*

Gambar 2.1 menunjukkan skenario *Ally Friendly Jamming*, dimana kita akan menggunakan 1 jammer. Perangkat yang memiliki akses dengan kode "A1" dan "A2", serta jammer dengan kode "AJ" memiliki sandi yang mereka gunakan untuk melakukan jamming pada jaringan, dengan kode "K". AJ menggunakan *Pseudo Random Number Generator (PRNG)* untuk memancarkan sinyal jamming XJ.

Ketika perangkat yang tidak memiliki akses (E1) mengirimkan sinyal XE1 ke perangkat lai yang juga tidak memiliki akses (E3), maka sinyal yang akan diterima oleh E3 adalah sinyal yang dikirimkan oleh e1, yaitu XE1 dan XJ yang berasal dari jammer. Jika daya yang dimiliki jammer sudah mencukupi, maka XJ

akan dapat merusak sinyal XE1 ketika sudah sampai di E3 yang membuat E1 dan E3 kehilangan akses atas jaringan tersebut.

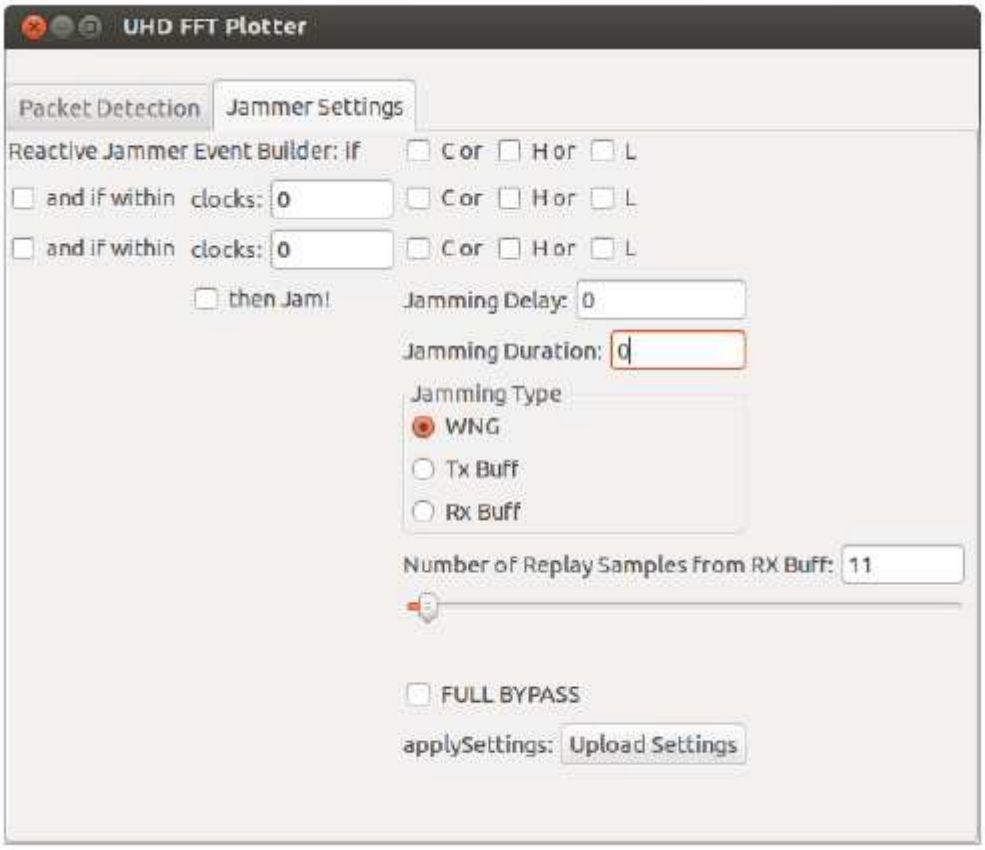
Ketika A1 mengirmkan sinyal XA1 ke A2, maka XJ juga ikut terkirim bersamaan dengan sinyal yang diterima oleh A2. Tetapi karena A2 memiliki sandi "K" yang sama dengan AJ, maka A2 juga dapat membuat ulang sinyal XJ dengan menggunakan sandi "K".

- *Real-Time, Channel-Aware Reactive Jamming in 802.11 Networks (Danh Nguyen, Boris Shishkin, Cem Sahin, David Dorsey, Nagarajan Kandasamy, and Kapil R. Dandekar)*

Penelitian ini bertujuan untuk melihat akibat dari Reactive Jammer yang digunakan pada protokol wireless. Reactive Jammer sendiri adalah jammer yang bekerja hanya ketika ada aktivitas di jaringan tertentu, yang dibuat dengan menggunakan GNU Radio dan USRP N210 *software-defined radio* (SDR) *platform.* Pemilihan *platform* ini didasarkan pada faktor hemat biaya dan *open source*. *Platform* ini dapat melakukan transmisi full duplex (komunikasi dua arah) dan juga mendukung SBX radio card. *Universal Hardware Driver* (UHD) untuk USRP N210 mengijinkan kustomisasi pada operasi yang dilakukan Digital Signal Processor (DSP) di banyak lokasi kritis yang ada pada *Digital Downcorversion Chain* (DDC). USRP N210 juga bertindak sebagai *Custom Packet Detector* dan sebagai jamming controller.

Mereka juga membuat suatu GUI berbasis Python untuk melakukan konfigurasi pada jammer, dengan menggunakan GNU Radio Companion dengan

beberapa implementasi kode tambahan. GUI ini digunakan untuk mengontrol deteksi dan memilih sinyal yang akan dijadikan sebagai target.



Gambar 2. 2. *Custom GUI* berbasis Python sebagai alat kontrol bagi *jammer*