JISKa, Vol. 4, No. 3, JANUARI, 2020, Pp. 156 – 164
ISSN : 2527 – 5836 (print) | 2528 – 0074 (online)

Deteksi Serangan *Distributed Denial of Services* (DDOS) Berbasis HTTP Menggunakan Metode *Fuzzy* Sugeno

Nadila Sugianti [(1)], Yayang Galuh [(2)], Salma Fatia [(3)], Khadijah Fahmi Hayati Holle [(4)]
[(1,2,3,4)]Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang
Jl. Gajayana No.50, Dinoyo, Kec. Lowokwaru, Kota Malang, Jawa Timur 65144
*Email: nadilasgnti@gmail.com[(1)], yayanggaluh1198@gmail.com[(2)], salmafatia7@gmail.com[(3)], khadijah.holle@uin-malang.ac.id[(4)]

Abstract

Distributed Denial of Services (DDOS) is a type of attack that exploits the web. This attack causes the server to go down and a system error. Thus, early detection of DDOS attacks is fundamental. The purpose of this paper is to develop applications that are capable of detecting HTTP-based DDOS attacks. This paper uses the sugeno fuzzy method for a systematic approach. From several studies that have been conducted, the researchers identified that the optimal input variables included the number of users, number of packages, number of lengths / users, and length of packages. Data processing used MATLAB software. The validity of the test uses the formula for the level of accuracy as in equation (3), resulting in an application that is able to detect HTTP-based DDOS attacks using sugeno fuzzy method with an accuracy rate of up to 90%.

Keywords : DDOS, Fuzzy Logic, Fuzzy Sugeno, HTTP

Abstrak

Distributed Denial of Services (DDOS) merupakan salah satu jenis serangan yang mengeksploitasi web. Serangan ini mengakibatkan server menjadi down dan system error. Sehingga, deteksi dini serangan DDOS merupakan hal yang fundamental. Tujuan paper ini adalah membangun aplikasi yang mampu mendeteksi serangan DDOS berbasis HTTP. Paper ini menggunakan metode fuzzy sugeno untuk pendekatan sistematis. Dari beberapa penelitian yang sudah dilakukan, peneliti mengidentifikasi bahwa variabel input yang optimal meliputi jumlah user, jumlah paket, jumlah panjang/user, dan panjang paket. Pengolahan data digunakan software MATLAB. Validitas pengujian menggunakan rumus tingkat keakuratan seperti pada Pers.(3), menghasilkan sebuah aplikasi yang mampu mendeteksi serangan DDOS berbasis HTTP menggunakan metode fuzzy sugeno dengan tingkat keakuratan mencapai 90%.

Kata Kunci : ***DDOS, Logika Fuzzy, Fuzzy Sugeno, HTTP***

1. PENDAHULUAN

Website atau yang disingkat *web* merupakan sistem yang di dalamnya terdapat informasi berupa manuskrip, gambar ataupun suara yang umumnya ditulis memakai format HTML (Sugianto, 2003). Untuk dapat mengakses HTML, diperlukan sebuah protokol bernama *Hypertext Transfer Protocol* (HTTP). *Distributed Denial of Services* (DDOS) merupakan salah satu jenis eksploitasi kelemahan pada sebuah *web*. DDOS merupakan upaya serangan terhadap *server* di dalam jaringan internet dengan cara membanjiri banyak data pada lalu lintas jaringan untuk mengganggu jalannya lalu lintas normal pada *server*. Serangan ini dapat mengakibatkan *server* menjadi *down* dan mengakibatkan *system error* (Adrian & Isnianto, 2016). Oleh karena itu, deteksi dini serangan DDOS merupakan hal yang fundamental.

Serangan DDOS dapat dideteksi menggunakan teknik *soft computing*, salah satunya adalah *fuzzy logic*. Metode fuzzy sugeno diusulkan sebagai pendekatan sistematis karena mampu memberikan representasi yang lebih efisien secara komputasi jika dibandingkan mamdani. Dengan menggunakan pendekatan sugeno jumlah aturan jauh lebih kecil daripada metode *fuzzy* mamdani. Metode sugeno terlah berhasil diterapkan pada sejumlah masalah dunia nyata seperti perkiraan fungsi non-linear statis, seperti prediksi pasar saham (Kulkolj, 2002).

Beberapa penelitian terdahulu sudah membahas metode *fuzzy* sugeno untuk mendeteksi serangan DDOS, namun beberapa variabel tidak disertakan (Petkovic, Basicevic, Kukolj, & Popovic, 2015). Pada paper ini peneliti menentukan variabel *input* yang optimal untuk metode sugeno agar mencapai tingkat deteksi yang lebih baik dalam lingkungan yang dinamis (Petkovic, Basicevic, Kukolj, & Popovic, 2015). Paper ini diharapkan dapat menciptakan suatu aplikasi guna mendeteksi serangan DDOS berbasis HTTP dengan tingkat akurasi yang baik menggunakan metode *fuzzy* sugeno.

2. METODE PENELITIAN

Mekanisme penelitian ialah semua proses yang dibutuhkan mulai dari perencanaan hingga pelaksanaan penelitian. Mekanisme penelitian yang diimplementasikan terbagi ke dalam beberapa tahapan.

2.1 Pengambilan Data Awal

Informasi penelitian yang digunakan berupa data sekunder yang terdiri dari data variabel yaitu, jumlah user, jumlah paket, jumlah paket/user dan panjang paket. Setiap variabel terdiri dari status yang normal atau DDOS. Data ini di dapatkan dengan melakukan 10 kali percobaan pengambilan paket pada website menggunakan *Wireshark* selama delapan detik. Dari data yang sudah di dapatkan, kemudian dimasukkan ke dalam Microsoft Excel. Data hasil deteksi terdapat pada Tabel 1.

Tabel 1. Hasil Deteksi Website E-Learning UIN Malang.

No	User	Jumlah Paket	Panjang/User	Panjang Paket	Status
1	3	32	228.9583	686.875	Normal
2	3	287	291.2114	873.6341	Normal
3	3	319	270.0491	810.1473	Normal
4	3	377	275.2909	825.8727	Normal
5	3	364	281.2363	843.7088	Normal
6	3	13943	230.5874	691.7621	DDOS
7	3	19818	245.2742	735.8226	DDOS
8	3	20214	244.811	734.4329	DDOS
9	3	26193	251.1058	753.3173	DDOS
10	3	17748	246.7402	740.2205	DDOS

2.2 Penentuan Fungsi Keanggotaan Himpunan *Fuzzy*

Himpunan *fuzzy* (*fuzzy set*) merupakan sebuah pengelompokkan yang dinyatakan dalam fungsi keanggotaan (*membership function*). Definisi fungsi keanggotaan yaitu, grafik yang menunjukkan batas nilai input suatu variabel dengan interval nilai antara 0 sampai 1 (Kusumadewi & Purnomo, 2010).

Terdapat beberapa fungsi keanggotaan himpunan *fuzzy* seperti fungsi keanggotaan linear, fungsi keanggotaan segitiga, dan fungsi keanggotaan trapesium. Peneliti menggunakan fungsi keanggotaan segitiga seperti pada Pers.(1)

$$\mu(x) = \begin{cases} 0 & ; x \leq \text{a atau } x \geq \text{c} \\ \frac{(x-a)}{(b-a)} & ; \text{a} \leq x \leq \text{b} \\ \frac{(c-x)}{(c-b)} & ; \text{b} \leq x \leq \text{c} \end{cases} \quad (1)$$

2.2 Pengukuran Nilai Penegasan (Defuzzifikasi)

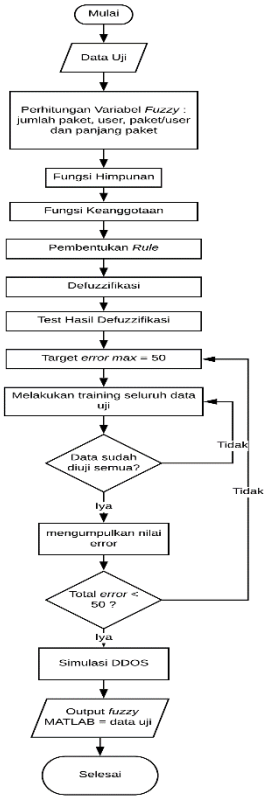
Nilai defuzzifikasi didapatkan dengan cara mencari nilai rata-ratanya. Rumus defuzzifikasi dituliskan sebagaimana pada Pers.(2) berikut.

$$Z = \frac{\sum_{i=1}^{n} a_i z_i}{\sum_{i=1}^{n} a_i} \qquad (2)$$

Nilai dimana α_i merupakan α predikat ke-*i*, sedangkan z_i merupakan hasil pada anteseden aturan ke-*i*.

2.2 Perancangan Aplikasi Pendeteksi DDOS

Aplikasi pendeteksi DDOS ini dibuat menggunakan pemrograman MATLAB R2017B dengan menggunakan *tools* pemrogramannya yang bernama *fuzzy toolbox.* Aplikasi dibangun menggunakan *interface* GUI MATLAB sehingga tampilan menjadi menarik dan lebih mudah untuk digunakan. Gambar 1 merupakan alur dari perancangan aplikasi DDOS.



Gambar 1. Alur Aplikasi DDOS.

3. HASIL DAN PEMBAHASAN

Dalam sistem pendeteksi serangan DDOS ini, terdapat empat variabel input, yaitu jumlah user, jumlah paket, panjang paket, dan jumlah panjang dibagi dengan user. Sedang, variabel output-nya adalah status. Penentuan variabel semesta pembicaraan terdapat pada Tabel 2.

Tabel 2. Semesta Pembicaraan Variabel Input dan Output.

Fungsi	Variabel	Semesta Pembicaraan

Input	Jumlah user	[0 - 7]
	Jumlah paket	[0 – 29.000]
	Jumlah panjang/user	[0 - 292]
	Panjang paket	[0 - 875]
Output	Status	[0 - 1]

Pada tabel 2, yang menjadi semesta pembicaraan merupakan data minimal dan data maksimal setiap variabel yang didapat dari fungsi keanggotaan himpunan *fuzzy*. Tahapan membuat fungsi keanggotaan sesuai pada Pers.(1) dilakukan untuk mencari nilai domain.

Fungsi keanggotaan himpunan fuzzy pada variabel Jumlah user terdiri dari SEDIKIT, SEDANG, dan BANYAK.

$$\mu\text{Sedikit} = \begin{cases} 0 & ; x \leq 0 \text{ atau } x \geq 3 \\ \frac{(x-1)}{(1{,}5-0)} & ; 0 \leq x \leq 1{,}5 \\ \frac{(1{,}5-x)}{(3-1{,}5)} & ; 1{,}5 \leq x \leq 3 \end{cases}$$

$$\mu\text{Sedang} = \begin{cases} 0 & ; x \leq 2 \text{ atau } x \geq 5 \\ \frac{(x-2)}{(3{,}5-2)} & ; 2 \leq x \leq 3{,}5 \\ \frac{(3{,}5-x)}{(5-3{,}5)} & ; 3{,}5 \leq x \leq 5 \end{cases}$$

$$\mu\text{Banyak} = \begin{cases} 0 & ; x \leq 4 \text{ atau } x \geq 7 \\ \frac{(x-4)}{(5{,}5-4)} & ; 4 \leq x \leq 5{,}5 \\ \frac{(5{,}5-x)}{(7-5{,}5)} & ; 5{,}5 \leq x \leq 7 \end{cases}$$

Fungsi keanggotaan himpunan fuzzy pada variabel Jumlah data terdiri dari SEDIKIT, SEDANG, dan BANYAK.

$$\mu\text{Sedikit} = \begin{cases} 0 & ; x \leq 0 \text{ atau } x \geq 1000 \\ \frac{(x-1)}{(500-0)} & ; 0 \leq x \leq 1000 \\ \frac{(500-x)}{(1000-500)} & ; 500 \leq x \leq 1000 \end{cases}$$

$$\mu\text{Sedang} = \begin{cases} 0 & ; x \leq 500 \text{ atau } x \geq 10.000 \\ \frac{(x-500)}{(5.000-500)} & ; 500 \leq x \leq 5.000 \\ \frac{(5.000-x)}{(10.000-5.000)} & ; 5.000 \leq x \leq 10.000 \end{cases}$$

$$\mu\text{Banyak} = \begin{cases} 0 & ; x \leq 5.000 \text{ atau } x \geq 29.000 \\ \frac{(x-5.000)}{(14.000-5.000)} & ; 5.000 \leq x \leq 14.000 \\ \frac{(14.000-x)}{(29.000-14.000)} & ; 14.000 \leq x \leq 29.000 \end{cases}$$

Fungsi keanggotaan himpunan fuzzy pada variabel Jumlah paket/user terdiri dari KECIL, dan BESAR.

$$\mu\text{Kecil} = \begin{cases} 0 & ; x \leq 0 \text{ atau } x \geq 200 \\ \frac{(x-0)}{(100-0)} & ; 0 \leq x \leq 100 \\ \frac{(100-x)}{(200-100)} & ; 100 \leq x \leq 200 \end{cases}$$

$$\mu\text{Besar} = \begin{cases} 0 & ; x \leq 100 \text{ atau } x \geq 196 \\ \frac{(x-100)}{(196-100)} & ; 100 \leq x \leq 196 \\ \frac{(196-x)}{(292-196)} & ; 196 \leq x \leq 292 \end{cases}$$

Fungsi keanggotaan himpunan fuzzy pada variabel Panjang data terdiri dari KECIL, dan BESAR.

$$\mu\text{Kecil} = \begin{cases} 0 & ; x \leq 0 \text{ atau } x \geq 610 \\ \frac{(x-0)}{(305-0)} & ; 0 \leq x \leq 305 \\ \frac{(305-x)}{(610-305)} & ; 305 \leq x \leq 610 \end{cases}$$

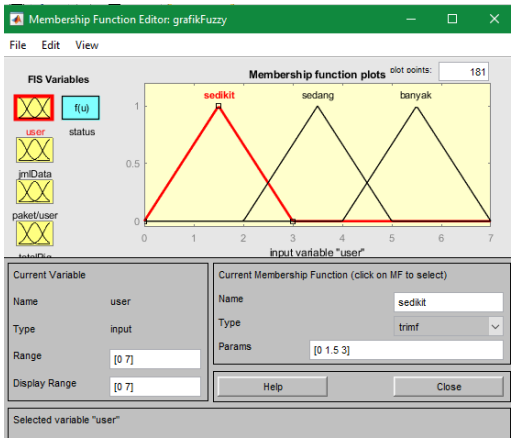
$$\mu\text{Besar} = \begin{cases} 0 & ; x \leq 305 \text{ atau } x \geq 875 \\ \frac{(x-305)}{(570-305)} & ; 305 \leq x \leq 570 \\ \frac{(570-x)}{(875-570)} & ; 570 \leq x \leq 875 \end{cases}$$

Berdasarkan fungsi keanggotaan dari setiap variabel *input* yang telah dijelaskan, maka diperoleh nilai domain untuk setiap himpunan *fuzzy*. Nilai domain terdapat pada Tabel 3.

Tabel 3. Nilai Domain pada Variabel

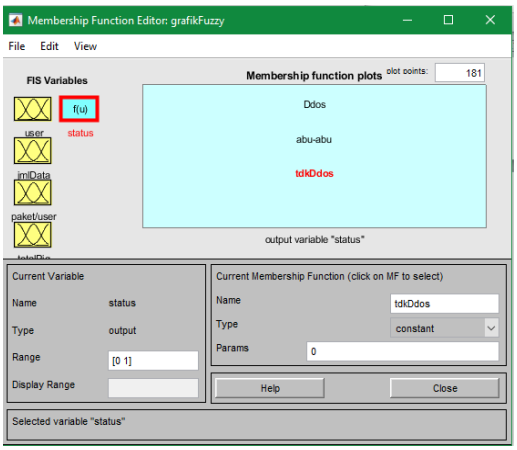
Fungsi	Variabel	Himpunan	Nilai Domain
Input	Jumlah user	Sedikit	[0 - 3]
		Sedang	[2 - 5]
		Banyak	[4 - 7]
	Jumlah paket	Sedikit	[0 – 1.000]
		Sedang	[500 –10.000]
		Banyak	[5.000 – 29.000]
	Jumlah panjang/user	Kecil	[0 - 200]
		Besar	[100 - 292]
	Panjang paket	Kecil	[0 - 610]
		Besar	[305 - 875]
Output	Status	Normal	[0]
		DDOS Ringan	[0.6]
		DDOS Berat	[0.9]

Selanjutnya melakukan implementasi menggunakan *software* bantuan berupa MATLAB. Gambar 2 merupakan bentuk dari fungsi keanggotaan himpunan *fuzzy* pada variabel input jumlah user dengan menggunakan *fuzzy toolbox* pada MATLAB.



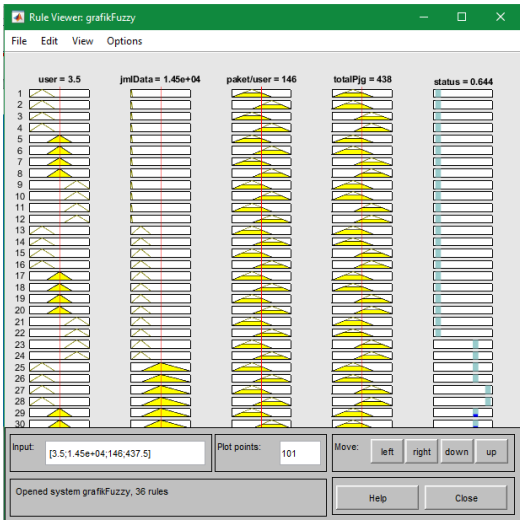
Gambar 2. Fungsi Keanggotaan Variabel *User* pada MATLAB.

Pembentukan himpunan *fuzzy* untuk variabel *output* terdapat pada Gambar 3 dengan tipe fungsi keanggotannya berupa *constant*.



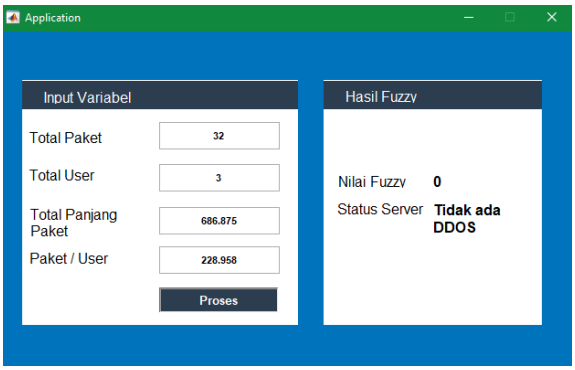
Gambar 3. Fungsi Keanggotaan Variabel *Output* Status.

Tahapan pembentukan aturan *fuzzy*. Terdapat 36 aturan *fuzzy* yang diimplementasikan ke dalam sistem pendeteksi DDOS ini. Pembentukan aturan *fuzzy* didapatkan dari empat variabel *input* dan satu variabel *output* yang sudah di definisikan sebelumnya dengan melakukan analisa batas tiap-tiap himpunan. Gambar 4 merupakan hasil pembentukan aturan *fuzzy* (*rule view*) berdasarkan variabel linguistik dan variabel numerik pada *fuzzy toolbox* MATLAB.



Gambar 4. Rule View (Hasil Optimasi/Defuzzifikasi).

Pembuatan model *fuzzy* untuk mendeteksi serangan DDOS berbasis HTTP akan dikatakan baik jika sudah dilakukan pengujian. Peneliti menggunakan 10 sampel untuk mengetahui keakuratan dan *error* pada aplikasi pendeteksi DDOS yang kami bangun berdasarkan hasil pengujian. Pada bagian ini dilakukan pengujian data berdasarkan paket data yang telah didapatkan pada Tabel 1.



Gambar 5. Tampilan Hasil Pengujian Data 1.

Gambar 5 merupakan tampilan dari aplikasi yang dibangun menggunakan GUI MATLAB. Aplikasi dijalankan untuk melakukan pengujian seluruh sampel. Tabel 4 merupakan hasil perolehan pengujian data yang dilakukan.

Tabel 4. Hasil Pengujian Sampel dengan MATLAB.

No	Data Uji	Matlab	Hasil
1	Normal	Normal	Sesuai
2	Normal	Normal	Sesuai
3	Normal	Normal	Sesuai
4	Normal	Normal	Sesuai
5	Normal	Normal	Sesuai
6	DDOS	Normal	Tidak Sesuai

7	DDOS	DDOS	Sesuai
8	DDOS	DDOS	Sesuai
9	DDOS	DDOS	Sesuai
10	DDOS	DDOS	Sesuai

Pada tabel 4, didapatkan perbandingan nilai logika *fuzzy* sugeno untuk mendeteksi serangan DDOS berbasis HTTP. Pengujian ini memakai rumus tingkat keakuratan.

$$\text{Tingkat Keakuratan} = \frac{Jumlah\ Data\ Benar}{Jumlah\ Data\ Keseluruhan}\ x\ 100\% \qquad (3)$$

Berdasarkan Tabel 4 diatas, dari 10 data yang digunakan sebagai sampel dalam penelitian ini 9 diantaranya dapat terdeteksi secara akurat. 10% dari data sampel tidak dapat dideteksi secara akurat karena pada data acuan yang dipakai memiliki konstanta yang telah ditentukan sebagai pembeda antara data normal, DDOS ringan, dan DDOS berat. Sedangkan, data tersebut masih termasuk ke dalam limit data yang normal. Sehingga tingkat ketepatan dari model fuzzy ini mencapai 90% dengan *error* 10%. Dengan demikian, logika fuzzy yang menggunakan metode sugeno telah memenuhi batasan dari paper ini yaitu untuk mendeteksi serangan DDOS berbasis HTTP.

4. KESIMPULAN

Berdasarkan pembahasan yang telah dijelaskan dan hasil pengujian yang telah dilakukan mengenai masalah mendeteksi serangan DDOS berbasis HTTP berdasarkan jumlah user, jumlah paket, jumlah paket/user dan panjang data yang ditangkap maka dapat diambil kesimpulan, yaitu :

1. Untuk mendeteksi suatu website terkena serangan atau tidak dapat memasukkan nilai pada kolom input yang terdapat pada Gambar 5 sesuai dengan data yang sudah di dapatkan.
2. Pada hasil pengujian, logika fuzzy menggunakan metode sugeno mampu digunakan sebagai pendeteksi dalam menentukan serangan DDOS berbasis HTTP dengan tingkat keakuratan mencapai 90%.

DAFTAR PUSTAKA

Adrian, R., & Isnianto, H. N. (2016). Analisa Pengaruh Variasi Serangan DDOS pada Performa Router. *Seminar Nasional Teknologi Terapan*.

Kulkolj, D. (2002). Design of Adaptive Takagi-Sugeno-Kang Fuzzy Model. *Applied Soft Computing*, 89-103.

Kusumadewi, S., & Purnomo, H. (2010). *Aplikasi Logika Fuzzy untuk Pendukung Keputusan.* Yogyakarta: Graha Ilmu.

Muhammad, A. W., & Alameka, F. (2017). Integrasi Normalized Relative Network Entropy dan Neural Network Backpropagation (BP). *JURTI*, 1-6.

Muhammad, A. W., Riadi, I., & Sunardi. (2016). Analisis Statistika Log Jaringan untuk Deteksi Serangan DDOS Berbasis Neural Network. *Jurnal Ilmiah ILKOM*.

Petkovic, M., Basicevic, I., Kukolj, D., & Popovic, M. (2015). Evaluation of Takagi-Sugeno-Kang Fuzzy Method in Entropy-based Detection of DDoS Attacks. *Computer Science and Information Systems*, 139-162.

Rahakbauw, D. L. (2015). Penerapan Logika Fuzzy Metode Sugeno untuk Menentukan Jumlah Produksi Roti Berdasarkan Data Persediaan dan Jumlah Pertanian. *Jurnal Ilmu Matematika dan Ilmu Terapan*, 121-134.

Rumare, R. R., Ciptaningtyas, H. T., & Santoso, B. J. (2017). Aplikasi Pendeteksi Serangan pada HTTP Menggunakan N-Gram. *Jurnal Teknik ITS*.

Sihombing, R. O., & Zulfin, M. (n.d.). Analisis Kinerja Trafik Web Browser dengan Wireshark Network Protocol Analyzer pada Sistem Client-Server.

Simanjuntak, P., Suharyanto, C. E., & Khairiyah, R. (2018). Fuzzy Sugeno untuk Menentukan Penilaian kompetensi Karyawan PT. Scheinder Batam. *Information Sytem Developtment*, 2.

Siregar, J. J. (n.d.). Analisis Exploitasi Keamanan Web Denial of Services Attack.

Sugianto, D. (2003). *LDL Membangun Website dengan PHP.* Jakarta: D@takom.

Wardhana, L., & Makodian, N. (2010). *Teknologi Wireless COmmunication dan Wireless Broadcast.* Jakarta: Andi Offset.