Abstrak

Jaringan *Wi-Fi* saat ini sudah tersebar secara luas berkat penggunaannya yang sangat mudah, hal ini juga menjadi ancaman tersendiri bagi penyedia dan pengguna *Wi-Fi* tersebut, sekalipun sudah dilakukan pengamanan menggunakan protocol *Wi-Fi Protected Access (WPA)* bukan berarti jaringan Wi-Fi tersebut bebas gangguan. Hacker bisa tetap memanfaatkan kelemahan manajemen frame dari *IEEE 802.11* sebagai standard *Wi-Fi*, yaitu dengan melakukan *Deauthentication attack*, baik terhadap *Wireless Access Point (AP)* maupun terhadap stasiun sebagai tindakan jamming, akan tetapi kita tidak bisa mengetahui siapa yang melakukan *Deauthentication attack* tersebut. Dalam tesis ini penulis menganalisa cara menemukan lokasi dari sumber *Deauthentication attack* terhadap AP dengan membandingkan 3 metode, yaitu metode *wardrive*, metode *absorption* dan metode *trilateration* dibantu dengan penggunaan *Chanalyzer + adapter wi-spy 2.4x* sebagai tools untuk membaca sinyal *Received Signal Strength (RSS)* dari *attacker*. Serangan *deauthentication* yang dilakukan secara continue akan lebih mudah di analisa posisinya dari pada serangan yang dilakukan secara acak, dengan propagasi sinyal bisa memberikan perbandingan antar kekuatan sinyal dan jarak, dengan demikian posisi dari *attack*er bisa lebih mudah di tentukan. Hasilnya diperlihatkan dari pola grafik yang dihasilkan dari Received Signal Strength Indicator (RSS) dan bisa dibuktikan bahwa ketiga metode ini bisa digunakan untuk melokalisasi posisi dari *attacker*.

Keywords: Chanalyzer, RSS, Deauthentication attack, War-drive, Wi-Fi absorption, Trilateration

Abstract

Wi-Fi network is now widely used due to its very easy use. However, this condition also poses a threat for providers and users of Wi-Fi. Although security has been performed using the Wi-Fi Protected Access (WPA) protocol, it does not mean that the Wi-Fi network is free of interference. It is still possible for hackers to take advantage of the weakness of the management frame of the IEEE 802.11 as a standard of Wi-Fi by doing a deauthentication attack, either against the Wireless Access Point (AP) or to the station as an act of jamming, but we are not able to know the person doing such deauthentication attack. In this master's thesis, the author analyzes the ways of finding the location of the source of deauthentication attacks against AP by comparing three methods, namely wardriving, absorption and trilateration methods supported by the use of Chanalyzer + Wi-Spy 2.4x adapter as tools for reading the signal of the Received Signal Strength (RSS) from the attacker. The three methods are wardriving, absorption, and trilateration. The position of constant deauthentication attacks is more easily analyzed compared to that of random attacks. Signal propagation may provide a comparison between signal strength and distance which makes the position of attackers more easily located. The results are shown on the chart patterns generated from the Received Signal Strength Indicator (RSS), and it is proven that these three methods can be used to localize the position of attackers.

Keywords: *Chanalyzer, RSS, deauthentication attacks, Wi-Fi, wardriving, absorption, trilateration*

KATA PENGANTAR

Segala puji syukur saya panjatkan kepada Tuhan Yesus Kristus, karena berkat Dia sajalah tesis dengan judul "**Perbandingan Metode Lokalisasi Terhadap Sumber *Deauthentication attack* Pada AP 802.11n Menggunakan *Chanalyzer* dan Adapter Wi-Spy 2.4x**" ini dapat diselesaikan.

Tesis ini disusun untuk memenuhi salah satu persyaratan demi memperoleh gelar Magister Teknik (M.T.) dalam bidang keahlian Teknik Elektro pada program studi Manajemen Teknik Telekomunikasi di Universitas Mercubuana.

Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa hormat dan ucapan terima kasih yang sebesar besarnya kepada:

1. Bapak Prof. Dr. –Ing. Mudrik Alaydrus atas arahan dan waktu yang telah diluangkan kepada penulis untuk berdiskusi selama menjadi dosen wali, dosen pembimbing, dan perkuliahan.
2. Bapak Rizal Bahaweres, M.Kom. atas arahan dan waktu yang telah diberikan kepada penulis untuk berdiskusi selama menjadi dosen wali, dosen pembimbing, dan perkuliahan.
3. Semua dosen program Pascasarja Teknik Elektro di Universitas Mercubuana.
4. Kepada Mama Terkasih ibu Elsje Wongkar yang selama ini memberikan dukungan yang luar biasa tidak tergantikan.
5. Kepada kakak-kakak terkasih Sonny Mokoginta & Desyke Mantur, Feybe Mokoginta dan Robert yang selalu memberikan dukungan dan inspirasi.
6. Rekan-rekan program S2 Teknik Elektro angkatan 2012
7. Om Robby, tante Gerda, Marcel, Mario yang juga selalu memberikan Support yang luar biasa
8. Teman-teman Glow Club kamis thamres Dian, Rika, Siska, Kevin, Sasha, Devita, Stefie, The Grace, Mike, liza, Rudolf, Jena, billy, chika, natalie, k lina,

Florida, Jently Joels, jur-v, Kristi, sandi, Rizky, yang selalu mendoakan dan memberikan dukungan serta inspirasi

9. K Femmy, K Ebhy, Emen, Alex, Ika, Philips, Efraim, Thomas, k nona, via, Agnes, Lena, Jernih, Fitri, Syanet, Elsar dan Nia yang selalu mendoakan, menguatkan dan memberikan semangat untuk terus maju.
10. Vio Loveny sahabat terkasih yang selalu memberikan dukungan dan semangat sehingga Tulisan ini bisa selesai.
11. Affandi, Nunu, Raymond, Radian, Om Gandi, Rendy, Berly, Kores yang juga memberikan support untuk menyelesaikan tesis ini.
12. Kepada semua pihak yang telah membantu, yang namanya tidak dapat penulis sebutkan satu persatu.

Dengan keterbatasan pengalaman, pengetahuan maupun pustaka yang ditinjau, penulis menyadari bahwa tesis ini masih banyak kekurangan dan perlu pengembangan lebih lanjut agar benar-benar bermanfaat. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran agar tesis ini lebih sempurna, dan dapat penulis gunakan dalam penelitian dan penulisan karya ilmiah di masa yang akan datang.

Akhir kata, penulis berharap agar tesis ini memberikan manfaat bagi kita semua, terutama untuk pengembangan ilmu pengetahuan di bidang jaringan komputer

Jakarta, November 2015

Stenly Mokoginta

PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam tesis ini:

Judul	:	PERBANDINGAN METODE LOKALISASI TERHADAP SUMBER *DEAUTHENTICATION ATTACK* PADA AP 802.11N MENGGUNAKAN *CHANALYZER* DAN ADAPTER WI-SPY 2.4X
NAMA	:	STENLY MOKOGINTA
NIM	:	55412120018
PROGRAM	:	PASCASARJANA PROGRAM MAGISTER TEKNIK ELEKTRO
KONSENTRASI	:	MANAJEMEN TELEKOMUNIKASI
TANGGAL	:	21 NOVEMBER 2015

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan pembimbing yang ditetapkan sesuai dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana November 2015

Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, 21 November 2015

PENGESAHAN TESIS

Judul	:	PERBANDINGAN METODE LOKALISASI TERHADAP SUMBER *DEAUTHENTICATION ATTACK* PADA AP 802.11N MENGGUNAKAN *CHANALYZER* DAN ADAPTER WI-SPY 2.4X
NAMA	:	STENLY MOKOGINTA
NIM	:	55412120018
PROGRAM	:	PASCASARJANA PROGRAM MAGISTER TEKNIK ELEKTRO
KONSENTRASI	:	MANAJEMEN TELEKOMUNIKASI
TANGGAL	:	21 NOVEMBER 2015

Mengesahkan

Pembimbing Utama	Pembimbing Kedua
Prof. Dr. Ing. Mudrik Alaydrus	Rizal Bahaweres, M.Kom

Direktur Pascasarjana	Ketua Program Studi Magister Teknik Elektro
Prof. Dr. Didik J. Rachbini	Prof. Dr. Ing. Mudrik Alaydrus

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

AP : *Wireless Access Point*

ACK : *Acknowledgement*

CTS : *Clear to Send*

dBm : *Decibel Meter*

dB : *Decibel*

DoS : *Denial of Service*

FMS Attack : *The Fluhrer, Mantin and Shamir attack*

GHz : *Giga Hertz*

IEEE : *Institute of Electrical and Electronics Engineers*

LOS : *Line Of Sight*

LAN : *Local Area Network*

LLC : *Logical Link Control*

Log : *Logarithms*

mW : *miliWatts*

Mbps : *Megabits per second*

MSE : *Mean Square Error*

MAC : *Media Access Control*

MHz : *Mega Hertz*

NIC : *Network Interface Card*

OSI : *Open System Interconnection*

PS-Poll : *Power save Poll*

PTW attack : *Pychkine-Tews-Weinmann attack*

RF : *Radio Frequency*

RTS : *Request to Send*

RSS : *Received Sinal Strength*

Wi-Fi : *Wireless Fidelity*

WPA : *Wi-Fi Protected Access*

WPA2 : *Wi-Fi Protected Access 2*

WEP : *Wired Equivalent Privacy*

WLAN : *Wireless Local Area Network*

DAFTAR LAMPIRAN

DAFTAR ISI