Measuring Accuracy in Identifying and Detecting Unauthorized Access Point using Proactive Intrusion Detection Approach in Wireless Networks

Muhammad Salman[†], **Bagio Budiardjo**[††], **Kalamullah Ramli**[†††]

Electrical Engineering Department, Faculty of Engineering, Universitas Indonesia
Kampus Baru UI Depok 16424, INDONESIA

Summary
Currently, one of the major security issues in wireless environment is the intrusion coming from an unknown and unauthorized wireless access points. This access points could expose any sensitive information transmitted over the network. Until now the Intrusion Detection System (IDS) on Wireless network environment is still being developed because the necessary of its architectural design and IDS detection techniques need high levels of optimization in accommodating unique characteristics. IDS on Wireless network must have an adaptive nature and meet the scalability aspects in a distributed wireless network, as well as having a high accuracy detection with low false positive rate by taking into account the resource constraints on wireless networks. Furthermore, the convenience of the user in accessing network wirelessly could face the security risks against the intrusion of the possible Unauthorized Access Point, which is not legitimized and registered on a network. A more proactive detection system to protect this kind of intrusion has become an important part in the development of Intrusion Detection System. In this research, the mechanism of detecting the presence of Unauthorized Access Point is developed and the accuracy rate for identifying and detecting the presence of this kind of Access Point is also analyzed. During the test, it is showed that the accuracy of detection system reaches about 100% on idle traffic conditions, then declined to around 90%-70% in medium to low traffic conditions.

Keywords
wireless networks, unauthorized access point, proactive protection, intrusion detection system

1. INTRODUCTION

Today there are many solutions to reduce the risk of attack or threat on computer networks. Intrusion Detection System (IDS) is just one of many examples of the handling of the intrusion. Intrusion is defined as any activity that is disturbing the integrity, confidentiality, and availability of resources on the network. Basically, IDS is an application that can detect suspicious activity in a network. IDS can inspect traffic in a data communication system or network, perform analysis and look for evidence of infiltration experiments (including the category of intrusion or not) and sometimes provide treatment to disruption. IDS detection performed in order to prevent the occurrence of disturbances and acts as a deterrent (to prevent interference with the efforts / intrusion), and collect information in a log form to further enhance system security.

Along with the development of wireless network technology, security aspects become very important especially with the special characteristics of the wireless networks which have limited resources, and dynamic configuration changes due to mobility of its nodes. So it needs to develop a model of intrusion detection infrastructure model which can take steps to proactively prevent the intrusion of the potential presence and infiltration of a device that is not known (unknown devices) who infiltrated the network-based wireless. Actually the IEEE standard for IEEE 802.11 is not fully able to handle this kind of security issue.

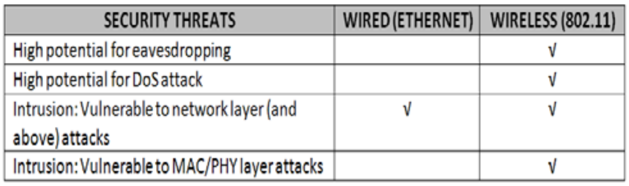
This research aim is to develop a model of proactive intrusion detection system to cover the weaknesses that exist in conventional IDS, especially in terms of protecting from the presence of illegal access point device. In general, conventional IDS is a passive system, since its function is more focused to detect intrusions and alert message is transmitted to the network administrator to indicate that there is an interferences or attacks against the network. Better IDS needs to be developed with more proactive in protecting against an intrusion, especially in wireless network environment which has a dynamic change of configuration. Moreover, this research also aims to help users, especially novice user to determine the presence of unauthorized access point, so that security and privacy of user information can be protected. The system developed also possible to detect any unauthorized access point without involving the network administrator by using the algorithm of Roundtrip Time (RTT) measurement method.

2. Threat to Wireless Network

Wireless networks have a number of potential risks which targeting to compromise the major aspect of security issue

Manuscript received June 5, 2014
Manuscript revised June 20, 2014

such as: confidentiality, availability, integrity, and non-repudiation [14]. Eavesdropping, DoS Attack, and Intrusion are some of the common attack on wireless network. Table 1 shows that wireless network is having more security risk than wired networks:



SECURITY THREATS	WIRED (ETHERNET)	WIRELESS (802.11)
High potential for eavesdropping		√
High potential for DoS attack		√
Intrusion: Vulnerable to network layer (and above) attacks	√	√
Intrusion: Vulnerable to MAC/PHY layer attacks		√

Table 1: Potential Security Attack between Wired and Wireless [17]

Actually, the encryption is not always secure. Past research on encryption method, it is found that there is a major weakness with common wireless authentication encryption called WEP. One of the major weakness is because of drawback in the implementation of RC-4 algorithm. This flaw becomes a serious vulnerability which allow attacker to scan and capture wireless network traffic and analyse the key used in WEP. Surprisingly the key can be cracked in a short time by using some common tools such as Airsnort and WEPCrack [9]. The process of cracking become trivial. Any intruder have an opportunity to access the wireless access point after taking over a WEP key.

Media Access Control (MAC) address is also on eof the most target of wireless attack. The address can be spoofed and masqueraded. During the attack, the intruder captures the wireless traffic to identify which MAC Addresses are permitted to have access to the wireless network. Most wireless access points implement this kind of authentication. Once the intruder found the list of registered MAC address, the access can be granted by changing the MAC address to become as the legitimate user. This kind of attack can be very trivial since there are also some common tools that is easy to used such as Airsnort, one of the famous wireless sniffer tool. It is not recommended to use MAC-based authentication to secure the wireless access point..

Another threat which is also the most serious attack called as “man-in-the-middle” (MITM) attack. One of the method is by spoofing or masquerading the wireless access point. During the attack, an attacker becomes an (unauthorized) access point and let the other users to authenticate to this spoofed access point which act as if the legitimate (authorized) access point. Then the attacker will have a complete control to take over the communications and also the authentication information to access to authorized Access Points. There are some tools which can be used to masquerade the legitimate APs, changing the signal strength and also MAC addresses to create numerous unauthorized Access Points.

3. Detection Mechanism and Principle

An intrusion caused by unknown or unauthorized access point could be detected with a timing-based algorithms using traffic analysis approach. RTT (roundtrip time) is implemented as the basis for timing-based algorithms, this is due to two things: first when the user connected to the network via the unauthorized access point, then all the packets will be passed through two hops, one hop between the user with the unathorized AP (UAP), one more hop between UAP to the legitimate AP. This is different if the user is connected directly to the AP because there is only one hop, so that the extra hop in the UAP had resulted in increasing the latency time for data transmission.

In this approach the DNS lookup and DHCP Request/Renew is used for probing, as it can address all three problems. DNS lookup service is handled by a node of a DNS server. A computer in a network typically will have a local DNS server to speed up the response from the DNS lookup. There are two types of DNS lookup, the first is recursive query and the second is a non recursive query. Recursive query will forward the query to the DNS server above it. If there are queries from users which could not resolved, there will be a notice of "no such hostname" as a response. RTT is calculated based on the time required to perform DNS lookup queries until no response from the DNS server which is received by the host. While DHCP Request/Renew in network is used to update the IP address, it is provided by the DHCP server when connected to a network host on the first time. The problem will occur when the UAP also serves as a DHCP server for hosts connected to its network. This is due to the UAP can control the IP addresses used by the host. Both services of DNS lookup and DHCP Request/Renew is also has no problems associated with restrictions by security devices such as firewalls and IPS, as those services should be opened on any network.

This detection algorithms timing is divided into two phases: in the first phase, the host sends DHCP Request/Renew and DNS lookup is repeated a number of n times, then RTTDHCP and RTTDNS record each RTT duration. Tdata is the time required to transmit packets which have DHCP and DNS packet with different sizes and transmission rates. The number of repetitions n play a role in the detection of accuracy while also increase the overhead. In the second phase, the average value and standard deviation of RTTDHCP and RTTDNS is also calculated.

4. System Design and Implementation

As a result from this development, there is a web based interface to detect whether an Access Point used by the users is an unauthorized access point (UAP) or not. This interface is very easy to be operated compare to the existing mechanism in which the user must install a specific software-tools designed specifically to detect the existence of UAP. In this interface, the UAP detection process begins when users get Internet access from a particular Access Point. Once the user connected to the website, then a process request for UAP detection on the server will be carried out, which then provide a response by sending the script to the user's computer and then executed.

The script of the interface has two tasks, at first it runs commands on a user's computer to send DHCP Request/Renew to the Access Point being used and then send DNS lookups to the DNS server used by the computer user, the process is repeated until a certain amount according to the desired level of accuracy of detection. The second task is to record the time of the duration of the DHCP Request/Renew as well as DNS lookup process which will then be sent to RAP detection applications that exist on the server. The next process occurs on the server side, which records the results DHCP Request/Renew and DNS lookup received and then stored in the database application. Finally the calculation is carried out to detect UAP using timing-based algorithms. Once the analysis is complete, the results indicating the AP status will be sent to a user via the web.

The UAP Detector developed in this research has the block diagram as shown in the following figure:

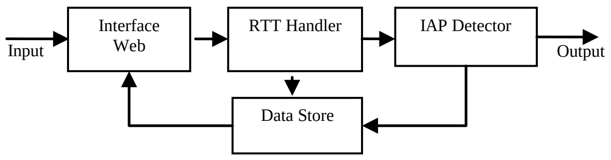


Figure 2: Block Diagram of UAP Detector

The UAP Detector consists of several modules which have different functions in accordance with their respective roles. The modules are as follows:

- Web Interface Module**:** The system interacts with the user using the web as a Graphical User Interface (GUI). This module is responsible for taking input from the user and displays output to the user.
- RTT Handler Module**:** This module is responsible for receiving and recording data of RTT$_{DNS}$ and RTT$_{DHCP}$ sent by the user's computer via a web interface. This data is temporarily stored in a data buffer for later process to obtain statistical data, and then new statistical data is forwarded to the RAP Detector Module to be analyzed using Time RTT measurement algorithm.
- **UAP** Detector Module**:** Data output from the module is already in the form of RTT data and statistics from RTT$_{DHCP}$ and RTT$_{DNS}$ to be analyzed by this module and determine whether AP status is an unauthorized Access Point (UAP) or legitimate AP. The UAP detection analysis is performed according to the following pseudo code on figure 3:

```
Start_time
For i = $ip_first to $ip_last Do
Switch on System Ping.exe AND Paket ARP
execute ping.exe
Get RTT, status online/offline
execute Paket ARP
Get MAC Address
Compare to Database (IP,MAC Address and RTT)
If (ip!=data_ip) OR (mac!=data_mac)
    then "alarm=Problem!" else "alarm=no problem!"
If (rtt>=200%)
    then "RTT tidak normal" else "RTT Normal"
Show IP,MAC Address, RTT and Alarm
End For
End_time
```

Fig. 3. Algorithm for Unauthorized AP Detection

- Module Data Store**:** Data Store module is responsible for storing the data entered by the user through a Web interface and also the results of data processed by RTT Handler module and UAP detector module. The database is handled by this module consists of several tables that store data input and output of the detection system as shown in figure 4.

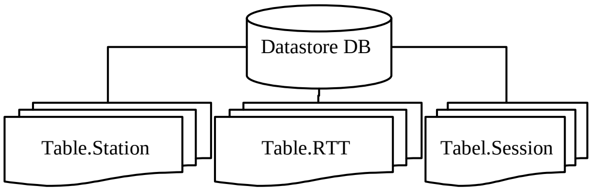


Figure 4: Database Table Structure for Datastore Module

5. Testing and Analysis

During testing stage, the testbed is configured with three networks connected to each other: (1) Wireless Network between Station, UAP and AP Server, (2) LAN that connects Legitimate AP with the DNS Server and Web Server, and (3) Internet gateway.

Basically all the scripts will be perform the execution based on the command of nslookup.exe (DNS lookup) and ipconfig.exe (DHCP Request/Renew) then this script to calculate and record the time duration between the start execution with the current command from the received command response. This is carried out repeatedly n times (iterations = n), and the duration of time will be analyzed as the Round Trip Time (RTT). When the Station is connected to the AP or UAP and get internet connection then the execution of scripts from a website interface will be carried out to calculate the RTT (DNS and DHCP) n times, this script then sends the statistics of the RTT data to the webserver for further processing. The network topology can be seen in Figure 5 as follow:

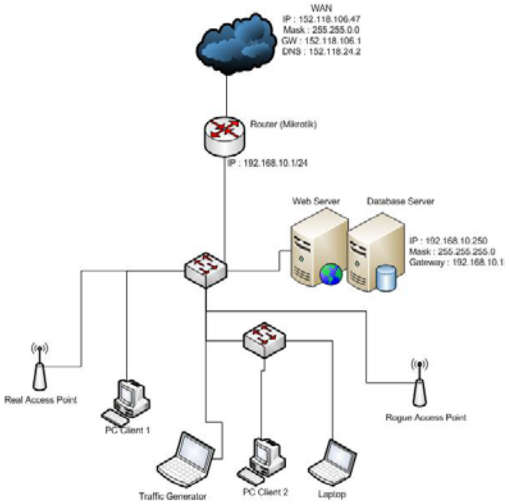


Figure 5: Network Topology for Unauthorized AP Detection

Prior to testing of the system, it must be determined all the parameters-parameters used. The settings and parameters on the system during the testing are shown in Table 3 as follow.

No	Protokol	802.11b	802.11g
1	BW WiFi	11 Mbps	54 Mbps
2	BW Ethernet	100 Mbps	100 Mbps
3	T_Process_DHCP	0,308365 s	0,308365 s
4	T_Process_DNS	0,074226 s	0,074226 s
5	T_Data_DHCP	0,089 ms	0,089 ms
6	T_Data_DNS	0,131 ms	0,131 ms

Table 3. Setting and Parameter for System Testing

T_Process_DHCP is the average time required by the script to do a DHCP request to DHCP server and receives its response. T_Process_DHCP value obtained by performing the DHCP requests to DHCP servers as much as n times and measure the packet arrival times at each node. T_Process_DNS value obtained by performing DNS lookup requests to DNS servers as much as n times and measure the arrival time of each packet in the network to get the average value.

The testing of the system is carried out by using several scenarios of different parameters, in order to obtain the test results that correspond to the real conditions:

a. Speed Data Transmission: RTT is inversely proportional to the speed of data transmission, if the data transmission speed of the RTT obtained will usually small, and vice versa.

	Average RTT after filtering					UAP
DHCP	0,001658	0,001837	0,00212	0,001764	0,00185	
DNS	0,008495	0,006881	0,007182	0,006815	0,008392	Rate
Δt	0,006836	0,005044	0,005062	0,005051	0,006542	auto
DHCP	0,001733	0,001749	0,002174	0,001954	0,002164	Rate
DNS	0,007175	0,009018	0,008067	0,008018	0,008715	54Mbps
Δt	0,005443	0,007269	0,005893	0,006064	0,006552	

Table 4. The effect on the Δt Transmission Speed

b. Wireless Traffic: RTT is also influenced by the wireless traffic that occurs between the Station to Station with UAP and AP. Detection of UAP will be more difficult if the network traffic condition is causing many packet queuing in the network. During testing the clustering is created based on the the utilization of traffic channel on the wireless network. If the traffic utilization is 00-10% so it is classified as idle, 15-50% is classified as medium traffic, and 60-100% is classified as traffic saturation.

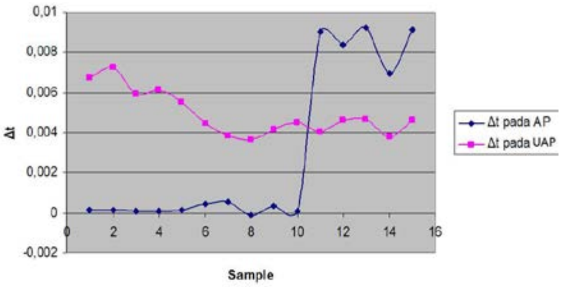


Figure 6. Comparison between AP and UAP Δt at various Traffic Conditions

Figure 6 shows that that the possibility to detect UAP in idle traffic conditions are the most effective way, while at saturation traffic conditions it is more likely to be in error detection whether it could lead to be false positive or false negative.

c. Access Point Workload: AP with a high workload in general also takes time to process the packets in and out, so the greater the workload of the AP will cause the increase in RTT. This test aims to determine the effect of workload on the AP to Δt. It is carried out at the expense of the AP by using a Traffic Generator and continuously transfer its data via the AP, with a light load (1 <Mbps), medium and heavyload (5 Mbps) (> 14 Mbps) respectively.

d.

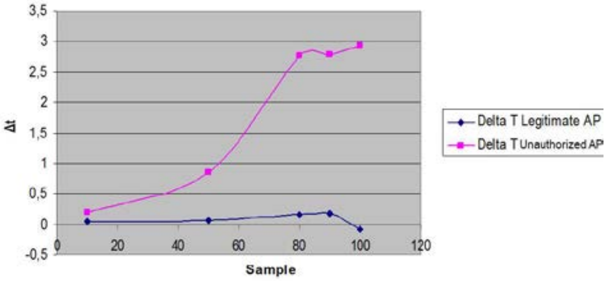
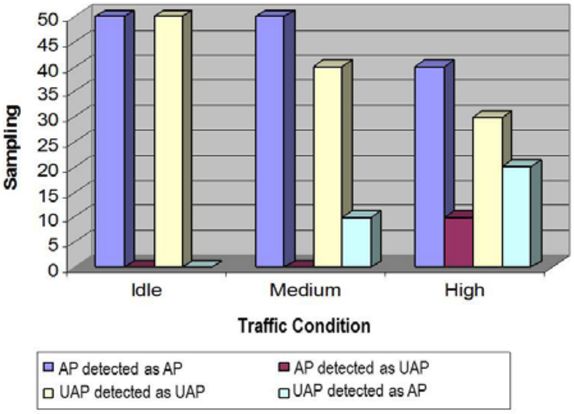


Figure 7: Load Effect on the AP to Δt

As shown in Figure 7, the test results turned out to show that there are significant variations in AP of given Δt at varying load. At heavy loads the Δt generated by UAP experienced a significant increase where Δt reaches nearly 3 seconds, and finally at a light load condition Δt approaches 0, 1 sec. In contrast to the AP Server testing it shows that the effect of load on the AP had only small influence on the variation of Δt. This is because the AP Server of DNS and DHCP packet transmission only occurs in one hop which is between Station to the AP. So that the AP result in DNS packets and DHCP are both experiencing the same delay variations.

In term of accuracy, the test is conducted on three existing traffic conditions which are: idle, medium, and high traffic. The testing is performed using 100 times sampling. Figure 8 shows a graph of test results of the system. During idle traffic conditions, it shows 100% accuracy rate which has never get error detection for both AP and UAP . Whereas in medium traffic conditions there are some errors detection occurred with 10% false negatives thus the overall accuracy of the system reaches 90%.

In high traffic conditions there is an increase in false negatives rate. UAP is detected as a legitimate AP is increased to 20% and an error occurs at the target AP detect is 10% or 10% false positive, so that the system reaches 70% accuracy. This occurs because at high traffic occurs considerable causing a lot of packet delay and retransmision.



Fi

gFigure 8. Accuracy Rate at Various Traffic Conditions

Conclusion

Wireless network security still has weaknesses which must be overcome especially in identifying the unauthorized access point. On the other hand, there are still many users who do not know how to detect this kind of threat. The system which has been developed is expected to easily detect the presence of UAP without involving a network administrator. From the test results and analysis of data obtained can be summed up that the speed of data transmission on the wireless network does not significantly affect the detection process of UAP ; the accuracy level of detection is affected by the traffic condition on a wireless network, the greater the traffic will diminished the accuracy of the system to detect UAP . The accuracy of the detection system reached 100% at idle traffic conditions, then declined to 90% in medium traffic conditions, and end up to 70% in high traffic conditions.

References

[1] Alvaro A.Cardenas, “A Framework for the Evaluation of Intrusion Detection Systems”, IEEE Symposium on Security and Privacy, 2006

[2] Gunter Schafer, “Security in Fixed and Wireless Networks: an Introduction to Securing Data Communications”, Wiley, 2003

[3] Guanlin Chen1, Hui Yao, Zebing Wang, “An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition”, Second International Conference on Future Networks, 2010

[4] Guanlin Chen, Hui Yao, Zebing Wang, "Research of Wireless Intrusion Prevention Systems based on Plan Recognition and Honeypot", In Proceedings of the

International Conference on Wireless Communications & Signal Processing, IEEE Computer Society, Nov. 2009

[5] H. Yin, G Chen, and J. Wang, ―Detecting Protected Layer-3 Rogue APs, Proc. Fourth IEEE International Conference Broadband Comm, Network, and System (BROADNETS '07), 2007.

[6] Hao Han, Bo Shen, Chiu C. Tan, Qun Li., Sanglu Lu., "A Measurement Based Rogue AP Detection Scheme", IEEE INFOCOM, Rio de Janeiro, 19-25 April 2009.

[7] Hao Han, Bo Sheng, Chiu C.Tan, Qun Li, Sanglu Lu, ―A Timing-Based Scheme for Rogue AP Detection, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Vol 22, No.11 November 2011

[8] Jack TIMOFTE, "Wireless Intrusion Prevention System", Revista Informatica Economica, vol. 47, March 2008

[9] L.Ma, A.Y. Teymorian and X. Cheng "A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks," Proc. IEEE INFOCOM, 2008.

[10] Lane, Heater D.. Securities Vulnerabilities and Wireless LAN Technology. SANS Institute, Virginia Beach 2006.

[11] Manivannan, N. dan Neelameham, P., 2006, "Wireless Security Techniques", Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2006 No.2(9)

[12] S.Shetty, M.Song, and L. Ma, ―Rogue Access Point Detection by Analyzing Network Traffic Characteristics, Proc. IEEE Military Comm. Conf (MILCOM '07), 2007.

[13] Songrit Srilasak, Kitti Wongthavarawat and Anan Phonphoem, "Integrated Wireless Rogue Access Point Detection and Counterattack System ", International Conference on Information Security and Assurance, Hanwha Resort Haeundae, Busan, Korea, 24 – 26 April 2008.

[14] Timothy R.Schmoyer, "Wireless Intrusion Detection and Response: A Case Study using the Classic Man-in-the-Middle-Attack", IEEE Communication Society, 2004

[15] Tung, S.S, Ahmad, N.N., Geok, T.K., 2006, "Wireless LAN Security: Securing Your Access point", IJCSNS International Journal of Computer Science and Network Security", VOL.6 No.5B, May 2006

[16] Watkins, Lanier, Beyah, Raheem, and Corbett, Cherita. ―A Passive Approach to Rogue Access Point Detection‖, IEEE GLOBECOM 2007 Proceedings.

[17] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs, Proc. Seventh ACM SIGCOMM Conference. Internet Measurement (IMC), 2007.

[18] Wu Junqi, "Study of Intrusion Detection System (IDSs) in Network Security", IEEE Wireless Communication, 2008

[19] Yujia Zhang, Guanlin Chen*, Wenyong Weng, Zebing Wang, "An Overview of Wireless Intrusion Prevention Systems", 2010 Second International Conference on Communication Systems, Networks and Applications

[20] Yaqing Zhang, Srinivas Sampalli, "Networking and Communications Client-based Intrusion Prevention System for 802.11 Wireless LANs", 2010 IEEE 6th Intemational Conference on Wireless and Mobile Computing.

Muhammad Salman received B.Eng from University of Indonesia and M.Sc. degrees, from Monash University, Australia. Now he is a PhD candidate from University of Indonesia. He is also working as a Head of Network Computing Laboratory. His research interest includes multimedia network, information security, wireless computing and web based application. He is a member of IEEE, ISACA, ISOC, ISSA and IACSIT.

Bagio Budiardjo received B.Eng from University of Indonesia., M.Sc from Ohio State University and PhD. degree from University of Indonesia. Now he has been a full professor at University of Indonesia since 2002. His research interest includes wireless networks, paralel computing, and traffic performance analysis. He is a member of IEEE Computer Society

Kalamullah Ramli received B.Eng. degree from Univerity of Indonesia, M.Eng from Wollongong University and Dr-ing from Universitat Duisburg-Essen, Germany. He has been a full professor at University of Indonesia since 2009. His research interest includes network computing, embedded system, and wireless network. He is a member of IEEE Computer Society.