This paper was presented at : **International Conference on Emerging of Networking, Communication and Computing Technologies (ICENCCT 2014)** Co-jointed with **International Conference on Emerging Trends of Computer Science with Educational Technology (ICETCSET 2014)** – Zurich, Switzerland on Feb 22-23, 2014 : Organized by : **Institute of Information System and Research Center (IISRC)**

An Efficient Monitoring Method of Wireless Network

GAO Shang
Information Science and Engineering College
Southeast University, Nanjing, China
goldensaintgao@qq.com
HU Aiqun
Information Science and Engineering College
Southeast University, Nanjing, China
aqhu@seu.edu.cn
SONG Yubo
Information Science and Engineering College
Southeast University, Nanjing, China
songyubo@seu.edu.cn
LI Tao
Information Science and Engineering College
Southeast University, Nanjing, China
lit@seu.edu.cn

Abstract ***:***

Wireless network monitoring can be used to the areas like network monitoring and information forensics. However, the great packet loss rate has always been its biggest bottleneck. This paper presents an efficient method of wireless network monitoring to reduce the packet loss. This method firstly forges a pseudo wireless access point with the information of original wireless access point, and builds up an extended service set together with the original access point. Then the stations are induced to the pseudo wireless access point with deauthentication flood attack without notice. Finally, packets of stations on pseudo wireless access point are captured with almost zero packet loss. Compared with the traditional method, this method has high efficiency and a very low rate of packet loss. It improves the existing wireless network monitoring methods.

Keywords : *wireless network monitoring, pseudo wireless access point, deauthentication flood attacks, data capture*

I. INTRODUCTION

As wireless network has become an important part of our daily life, monitoring technology is becoming more and more popular. We can use monitoring technology to collect network node information, analyze users' behaviors and even use on information forensics. However, the signal attenuation and data transmission conflicts in wireless environment make the great packet loss while monitoring. Besides, the packet loss will increase dramatically with the increase of transmission rate and station numbers, and is has become the bottleneck of wireless network monitoring.

Most solutions have been put forward to reduce the packet loss. Reference [1] designed a wireless network monitoring system, analyzed its workflow and completed the system. But it didn't test the packet loss rate. Besides, after analyzing its workflow, we can conclude that this system has not solved the packet loss problem. Reference [2] summarized the advantages of wireless network monitoring, and designed a network monitoring system based on network anomalies. However, because it's designed for testing network anomalies, its functions are very restrictive. To monitor multiple channels of wireless network environment, reference [3] made a system with several monitoring server. Yet the cost and the job of operators will rise at the same time. Though reference [4] used libcap asynchronous monitoring method, and improved the efficiency, it didn't essentially solve the problem of signal attenuation and data transmission conflicts in wireless environment. As the result, the improvement is extremely limited, the packet loss rate will increase drastically as the network environment becomes complex.

In this article, a new idea of efficient monitoring method is put forward, which can monitor the stations efficiently and without their notice. The structure is as follows: chapter two introduces the basic knowledge of efficient monitoring method; chapter three shows the principle and the design of this system; chapter four compared the efficiency through experiment, analyzes the result and concludes the whole system.

II. WIRELESS NETWORK MONITORING

A. Structure of WLAN

Wireless local area network (WLAN) consists of wireless network interface card (WNIC), wireless access point (AP), stations (STA) and related equipment. STA refers to a computer equipped with WNIC, such as a laptop, a tablet or a phone. AP is the key component to connect the WLAN and LAN, and is responsible for the management of STAs, similar to the HUB in wired network.

Basic Service Set (BSS) is an essential component of 802.11 networks, mainly two types: Infrastructure BSS, which consists of one AP and several STAs; independent BSS, which is built by several STAs. In Infrastructure BSS, STA should be associated with AP to build up the network. The association must be unique to STAs. As a result, each BSS has a basic service set identifier (BSSID) as its unique identity. BSSID is the second layer address of emitter (Normally MAC address).

802.11 allow several BSSs constitute an extended service set (ESS) to extend the coverage of the network area. All Aps in the same ESS should use the same extended service set identifier (ESSID). ESSID is the so called "name" of the network for users. The topology of WLAN is shown in figure 1.

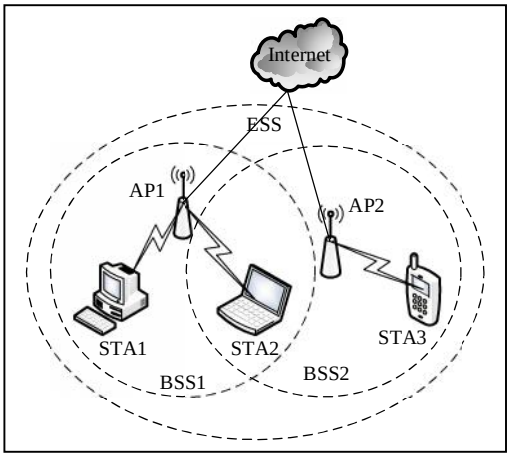

Figure 1. *Topology of WLAN*

In Figure 1, BSS1 consists of STA1 and STA2, and its BSSID is the MAC address of AP1. BSS2 consists of STA2 and STA3, and its BSSID is the MAC address of AP2. ESSID can be configured by users.

As STA2 moving from BSS1 to BSS2, the signal of AP1 will gradually weaken, and the signal of AP2 will gradually increase. When the signal of AP1 is less than the threshold value, STA2 will select the AP with the strongest signal in the same ESS (in this case, AP2), disassociate with AP1, and associate with AP2. The disassociation and association cannot be noticed by users.

B. The Principle of Wireless Network Monitoring

The current monitoring topology of WLAN is shown in Figure 2.

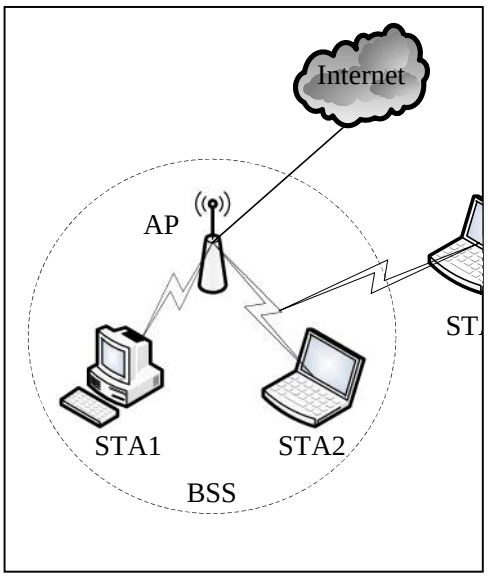

Figure 2. *Current Monitoring Topology of WLAN*

When STA3 wants to monitor STA2, the packets which STA3 capture is the packets between STA2 and AP. There will be a high packet loss rate due to the signal attenuation and data transmission conflicts of other STAs. However, if we can monitor and filter the packets on AP directly, there will be no problem of signal attenuation and data transmission conflicts. In this way we can capture the packets with almost zero packet loss. The method of this article is based on this idea.

III. THE PRINCIPAL AND DESIGN OF EFFICIENT MONITORING METHOD

A. The Principle of Efficient Monitoring Method

Based on the idea above, the efficient monitoring method forges a pseudo AP with the information of ESS, and builds up an ESS with previous BSS. The pseudo AP will use an amplifier so as its signal will be stronger than the previous AP. Then we use deauthentication attack to force the STA to disassociate with previous AP. After this, STA will find our pseudo AP and associate with it. Then, we can capture the packets on pseudo AP interface to get the packets of STA with almost zero packet loss. The topology of this system is shown in figure 3.

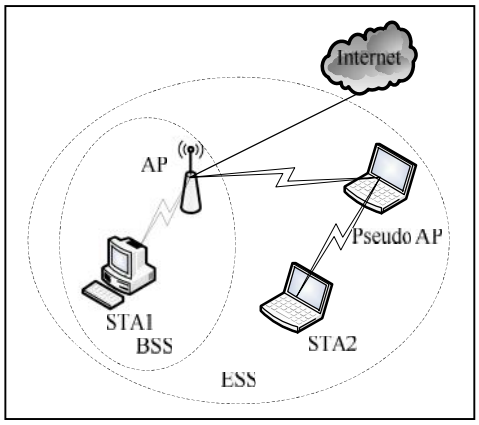

Figure 3. *Topology of Efficient Monitoring Method*

In this structure, there is no data loss between STA and pseudo AP. When packets lost between STA and pseudo AP, or between pseudo AP and AP, STA will resend the packets. As figure 4 shows, assuming STA2 will send packet 1 and 2 to AP, packet 1 is sent successfully, and packet 2 is lost between STA2 and pseudo AP, or between pseudo AP and AP, STA2 will resend packet 2 till success. Therefore, the theoretical packet loss rate is zero. But in the real test, its efficiency is limited by the CPU performance, and causes packets loss.

In current monitoring method, there will be no resend packets when monitor lost the packets which are successfully send from STA to AP. Therefore, the packet loss rate can be huge.

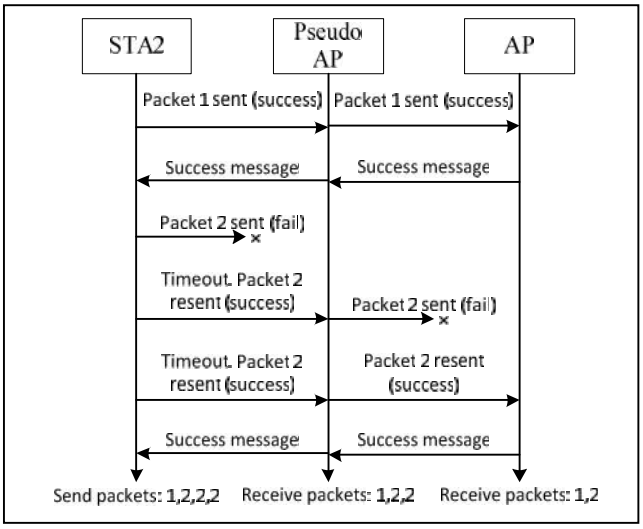

Figure 4. *Analysis of Efficient Monitoring Method*

B. The Design of Efficient Monitoring Method

To achieve the design above, we use five modules to complete different function.

Scan Module: Scan the current network environment with aircrack-ng, display APs' and STAs' information. Operator can select the STA which he wants to monitor based on the scan result. This module will also check the attack result with the current network information, and send re-attack message when attack fail, stop attack message when attack success.

Connect module: Connect to the selected AP with wpa_supplicant. The selected AP can be either one of them: the AP associated with the STA we want to monitor (real AP), other APs.

Soft AP module: Build up a pseudo AP with hostapd. The pseudo AP's BSS has the same ESSID, encrypt type and key with the real AP's. As a result, the pseudo AP is in the same ESS with real AP. Then we configure routing table, ARP proxy, NAT gateway and DHCP server to achieve forward function, so as the STAs can switch BSS without notice.

Attack module: Send massive deauthentication packets between STA and real AP with aircrack-ng. This deauthentication flood attack can break down the association between STA and real AP. After deauthenticated from real AP, STA will scan the network, select an AP with the strongest signal in the same ESS and try to associate again. After attack, this module will send check message to scan module, asking it return the attack result. Attacking will continue until the attack success message received.

Analyze module: Capture the packets of STA on pseudo AP with libcap. Show the result to the operator for further analysis.

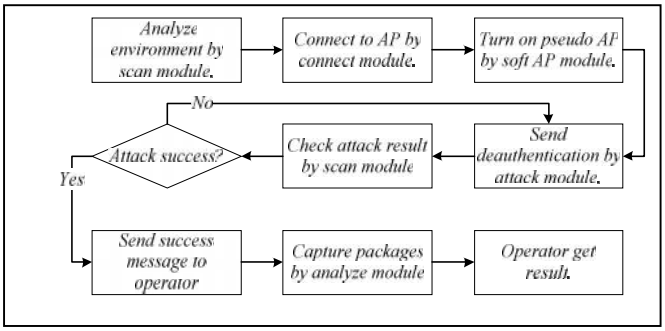

Figure 5. *Process of Delete Operation Filtration*

Efficient wireless network monitoring uses four WNIC to achieve scan, connect, soft AP and attack functions, and the WNIC in soft AP module has an amplifier to boost its signal. Its topology is shown in figure 6.

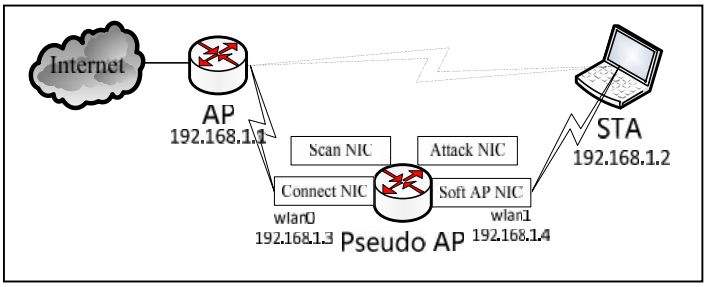

Figure 6. *Hardware topology of Efficient Monitoring Method*

During forward process, ARP proxy of wlan1 is required. Because there is no direct connection between STA and real AP, there will be no response to the ARP request of STA (request MAC address of 192.168.1.1). To avoid this situation, wlan1 should response to this ARP request, and send its MAC address to STA. As a result, ARP proxy should be used.

Besides, we need to configure the NAT gateway function on wlan0. STA is in the same LAN with real AP, but there is no direct connection between STA and real AP, so the packets will not be received by STA. NAT gateway is to avoid AP sending packets to STA directly, all the packets to STA should be sent to wlan0 first. And then routing table can forward the packets.

Finally, configure routing table and DHCP server. Routing table should be like table 1 to ensure the connection when STA switch BSS. DHCP server is to make sure STA can renewal its IP address when it expires.

TABLE I. ROUTING TABLE OF EFFICIENT MONITORING METHOD

Destination	Gateway	Netmask	Iface
192.168.1.1	*	255.255.255.255	wlan0

192.168.1.0	*	255.255.255.0	wlan1
default	192.168.1.1	0.0.0.0	wlan1

IV. PERFORMANCE ANALYSIS

In this chapter, we will analyze the performance of efficient monitoring method, and compare it with the traditional method. The test environment is shown in table 2.

TABLE II. MONITORING TEST ENVIRONMENT

	OS	**CPU**	**NIC chip**	**ROM**
Monitoring device	Ubuntu 12.04	Inter(R) Core(TM) i5-3210M 2.5GHz	RT2501USB Wireless Adapter	4GB
STA	Windows7	Inter(R) Core(TM) i3-2130M 3.4GHz	RT73USB Wireless Adapter	4GB
	Vendor	**Software Version**	**Hardware Version**	**Encrypt type**
AP	TP-Link	1.1.2 Build 20130109 Rel.59651s	TL-WVR300 v1.0	WPA2-CCMP

In this test, we captured the packets of STA on monitoring device, and got the packets on AP to calculate the packet loss rate. Besides, we increased the transmission rate to see the changes of packet loss rate. The result is shown in figure 7.

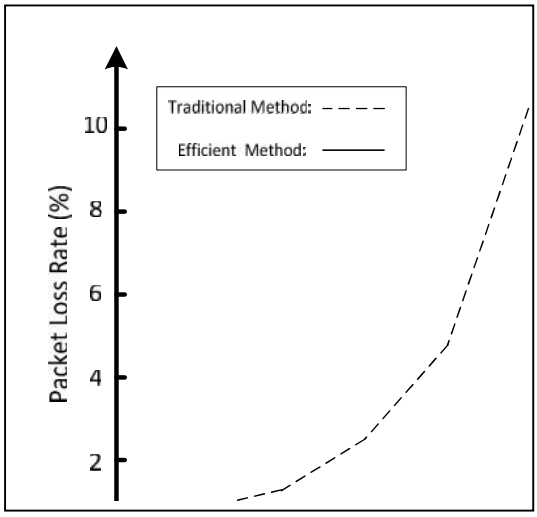

Figure 7. *Comparison of Efficient Monitoring Method and Traditional Monitoring Method*

Because of the signal attenuation and data transmission conflicts in traditional monitoring method, the packet loss rate increased dramatically with the data transmission rate, reached over 10% in 50Mbps. In contract, the

packet loss rate remained steady in efficient monitoring method, with 0 packet loss below 30Mbps. Because of the performance of CPU, there was about 0.002% packet loss rate in 50Mbps.

The test result shows that as long as the hardware processing ability is strong enough, there is almost no packet loss in the efficient monitoring method even in the case of high data transmission rate.

V. CONCLUSION

In this efficient monitoring method, there is almost no packet loss even in the case of high data transmission rate. This method breaks the bottleneck of traditional method, and greatly improves the efficiency and accuracy of the monitoring. However, when monitoring multiple STAs, the bandwidth of each STA will decrease, which lead to slow Internet access. The problem of how to allocate bandwidth rationally should be further studied.

VI. REFERENCES

[1] Jiantao Gu, Qun Wei, Wei Li. Design and Implementation of WLAN Monitoring and Management System [C] ICICA 2011, Part I, CCIS 243, 2011:496-C502

[2] Jihwang Yeo, Moustafa Youssef, Ashok Agrawala. A framework for wireless LAN monitoring and its applications [C] Proceedings of the 3rd ACM workshop on Wireless security. ACM, 2004: 70-79

[3] Deshpande U, Kotz D, McDonald C. Coordinated sampling to improve the efficiency of wireless network monitoring [C] Networks, 2007. ICON 2007. 15th IEEE International Conference on. IEEE, 2007: 353-358

[4] LIU Min, ZHU Zhixiang. An monitoring technique of wireless network based on Linux[J]. Journal of Xi'an University of Post and Telecommunications, 2011, 16(3): 65-68

[5] Fischer M J, Kern W F. System and method for monitoring performance of wireless LAN and dynamically adjusting its operating parameters: U.S. Patent 5,889,772 [P]. 1999-3-30

[6] Gast Matthew. 802.11 wireless networks: The definitive guide[M]. Southeast University Press, 2006

[7] Lynch J P, Wang Y, Loh K J, et al. Performance monitoring of the Geumdang Bridge using a dense network of high-resolution wireless sensors[J]. Smart Materials and Structures, 2006, 15(6): 1561.

[8] Straser E G and Kiremidjian A S 1998 A modular, wireless damage monitoring system for structures Technical Report no 128 (The John A. Blume Earthquake Engineering Center, Stanford, CA)

[9] Lynch J P and Loh K J 2006 A summary review of wireless sensors and sensor networks for structural health monitoring Shock Vib. Digest 38 91-12

[10] Spencer B F, Ruiz-Sandoval M E and Kurata N 2004 Smart sensing technology: opportunities and challenges J. Struct. Control Health Monitor. 11 349-68