Network Sniffing Tools for WLANs: Merits and Limitations

Nguyen The Anh
Department of Computer Science
The National University of Singapore
3 Science Drive 2 Singapore 117543
Email: nguyenth@comp.nus.edu.sg

Rajeev Shorey
Research Staff Member
IBM India Research Laboratory
Indian Institute of Technology, Delhi 110016
Email: srajeev@in.ibm.com

Abstract— **This paper presents an overview of several popular sniffers that are available in the Internet, from simple and compact tools to more complex and multi-functional ones. We describe important wireless sniffing tools such as Wellenreiter, Kismet, Ethereal, AirTraf and AirSnort. We discuss their functions along with their strengths and weaknesses. We describe how they can be used for different purposes such as hacking, exploiting security holes, and their usage characterization of wireless networks. Through a detailed experimental study conducted at the National University of Singapore during a four months period in 2004, we observe several interesting**

I. Introduction

This paper presents the results of our study on free and open source wireless sniffers. We explore their features in a real wireless environment - the WLAN of the National University of Singapore (NUS).

There are two types of wireless utilities on the Internet - Active and Passive scanners [1], [8], [9], [10]. Active scanners are those which send out probes and watch responses. Measurements are done through analyzing these responses. The advantages of these tools are they are very handy and provide many useful link monitoring features. However the drawback is that they can not monitor "closed" networks as they are configured not to broadcast their SSIDs. Active sniffers can only work when the network card has been associated with the network to be monitored. Therefore it is not difficult to detect these types of sniffers. Passive scanners are those which turn their network cards into the RF-MON mode. In this mode, sniffers can easily eavesdrop traffic. It is very hard to detect this type of sniffer as it secretly captures packets passing by the wireless interface.

By switching wireless network adapter into radio frequency monitoring (RF-MON) mode, a sniffer can easily sniff packets, hence, passively monitors all network traffic rather than just the traffic destined for its network adapter. In wireless networks, one adapter can eavesdrop on a single channel at a time to monitor all traffic that goes from client to access point and back. Access points can use any of the available channels, and in larger environments, they are usually set up in a way that prevents channel overlapping so that adjacent access points don't interfere with one another. However, recent sniffers can switch very fast back and fort between channels to monitor traffic from all channels.

WLAN are exposed to many security threats, especially eavesdropping [1]. Wireless eavesdropping presents the same danger in networks as wired eavesdropping. One could use this technique to gather user login credentials, networking information (IP addresses and MAC addresses), email, or potentially anything else that traverses the segment. Some security mechanism like WEP (Wired Equivalent Privacy) encryption makes eavesdropping more difficult, but not impossible for wireless sniffers available on the Internet. Many academic papers have discussed WEP weaknesses [2].

In this paper, we present an overview of the available open-source wireless sniffing tools. We identify their functions as well as their different applications. We analyse the sniffers through a comprehensive study of the WLAN traffic at the National University of Singapore [4].

The paper is organized as follows. In Section II, we present an overview of some of the popular wireless sniffers. In Section III, we discuss the WLAN analysis using sniffers. Our methodology is presented in Section IV followed by the results in Section V. Section VI has the conclusions.

II. Wireless Network Monitoring Tools

In this section, we present an overview of some of the popular wireless sniffers.

1) Wellenreiter: Wellenreiter is a very compact and handy tool with user friendly interface. Some basic features of Wellenreiter are:

- discover networks (BSS/IBSS), and detect ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer,
- display decoded DHCP and ARP traffic that gives further information about the networks,
- save Ethereal/TCPDUMP-compatible dumpfile,
- track the location of the discovered networks using a supported GPS device and the gpsd,
- display level of networking activity at channels,
- and display MAC and IP address of detected wireless clients.

2) Kismet: Kismet [5] has all the features that Wellenreiter has. Moreover, it can report a significant amount of information about the networks such as the number of packets captured, the number of encrypted packets so far, the instant

0-7803-8964-6/05/$20.00 ©2005 IEEE

packet rates. Besides, it can sniff into and decode (according to IEEE standards) the captured traffic in real time. This is an ideal utility for hackers. While driving around a building, they can see the information flows and capture information interesting to them. However, Kismet can only decode simple traffic such as FTP, HTTP, etc.

Interestingly, Kismet is not just a hacking tool. It has a feature that helps us detect network intrusion effectively. By sniffing into the traffic, Kismet detects those clients who send out probes but never join the network and alert user.

Kismet can run on Linux PCs and handhelds.

3) AirTraf: Kismet and Wellenreiter offer pretty detailed information about APs and clients, however some real time performance analysis features need to be added, for example, the throughput, bandwidth, and latency of TCP connections at a particular wireless client; the number of internal and external packets. Those kinds of information are very useful to analyze and characterize usage behavior of a particular wireless network.

AirTraf [6] is another passive scanner that covers Kismet's limitations in analyzing performance of wireless network. AirTraf can tell a lot of information such as the internal and external traffic together with the current bandwidth of the AP.

AirTraf can also give a complete report on protocols analysis. From that report we can figure out what protocols are dominant, what is their performance in the network. This should be very helpful to characterize the usage behaviors of wireless networks such that one can adjust accordingly to maximize the performance.

The most interesting feature of AirTraf is that it can analyze every aspect of TCP connections at a particular wireless client. There are four modes in the "TCP Performance Analysis": (i) *Connections*: This mode keeps track of Open/Closed connections, total packets, total bytes, (ii) *Statistics*: This mode keeps track of number of Incoming/Outgoing and Retransmission packets, (iii) *Latency*: This mode keeps track of Incoming/Outgoing time and Round-trip time, (iv) *Bandwidth*: This mode keeps track of Incoming/Outgoing and total bandwidth.

4) Ethereal: Kismet or AirTraf alone give an outside view of the wireless networks. If we want to sniff into the traffic to see what is going on and who is doing what, i.e., what do the packets captured contain, then Ethereal is what we need. Ethereal is probably the best traffic analyzer over the Internet. It works by decoding each field of the packet according to the IEEE standards and specifications. There are more than 500 application protocols that Ethereal can decode. For WEP encrypted network, Ethereal can also decode packets if the WEP key is given.

Like Wellenreiter and Kismet, Ethereal is also a passive scanner. It can capture the packet live or write to dumpfiles. The power of Ethereal lies in the ability to analyze dumpfiles. Ethereal can filter out interesting packets or data stream. It can also gives out statistics of some protocols such as TCP, HTTP. The most interesting feature is that Ethereal can analyze the dump file and show the protocol hierarchy.

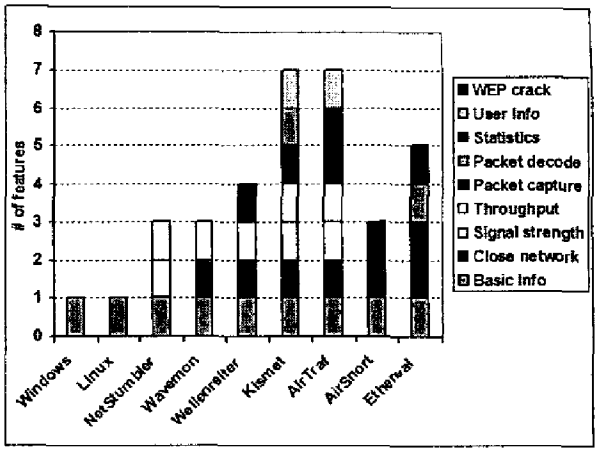

Fig. 1. Summary of features of some wireless sniffers

5) AirSnort: AirSnort [7] is a WLAN tool which decrypt encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

Let us see how AirSnort works [7]. AirSnort attacks the WEP's weakness as described in [2]. AirSnort cracks WEP keys by collecting encrypted packets with weak IV keys (about 5-10 million packets). Then they are sorted according to which key byte that helps to expose. When a sufficient number of weak IVs have been gathered for a particular key byte, statistical analysis will show a tendency towards a particular value for that key byte. Then AirSnort will make a key guess based on the highest ranking values in the statistical analysis phase. The number of guesses that AirSnort will make for each key byte is governed by the "breadth" parameter in the preferences section of AirSnort. Some key bytes may take a few packets to be revealed, while others may require a very large amount of packets and time.

We summarize the features of each tool in Figure 1.

III. WLAN Analysis Using Sniffers

WLANs are becoming more and more popular due to their low cost and ease of deployment. Researchers have studied and proposed methodologies to characterize the usage of these networks [8]–[10]. Their methods share a common way of collecting data: collecting tcpdump trace at the router, collecting SNMP trace by querying access points and collecting authentication log. This method is suitable for the analysis of very large scale WLANs.

However, for a very small scale network such as a study area of a library, such method appears to be too expensive and not practical. Moreover, analyzing the data takes a long time. In this paper we would like to propose a simpler method of analyzing small scale WLAN traffic by using open-source wireless sniffers. The description of our method is as follows:

- *Collecting data:* We use a wireless sniffer having the wireless packet capturing feature (e.g., Ethereal) to capture the wireless traffic.

- *Analyzing data:* We use a network analyzer (e.g., Ethereal) to obtain statistical information. We also use Ethereal to filter out interesting packets such as authentication packets to derive more interesting information. Tcpstat is also used to calculate statistics. AirSnort and Kismet will help us to understand the security issues in our analysis.

In the next section, we demonstrate a short analysis of the WLAN at the National University of Singapore (NUS). The idea of this analysis is on the same lines as that in [8]. We used wireless sniffers to extract as much information as possible to characterize network performance, user behaviour at the central area of Central Library in NUS. Our analysis should help answer the following questions: (i) What is the user behaviour?, (ii) How is the wireless traffic?, (iii) How is the network distribution across APs?, and, (iv) What are the key design principles?

IV. Methodology

A. Network Environment

The WLAN in NUS is an IEEE 802.11b network and APs are set up to provide network access to students everywhere to enhance the studying capabilities. We are interested how the students make use of the facilities at the central part of the Central Library. This is the biggest library in NUS.

We carried out our analysis at the central part of the library building, the level 4, 5 and 6. The central part of level 5 includes a study area and a laptop charging area. They are covered by two APs called Ctr-1 (BSSID: 00:0E:83:12:B1:90) and Ctr-2 (BSSID: 00:0E:83:19:1E:40). Level 6 is a reference area of the Chinese Library which has 1 AP called ChLib (BSSID: 00:0E:38:C4:E6:30). The central part of level 4 is a composition of 3 areas, the lounge, the information area and the two seminar rooms. The lounge is covered by the AP called Lounge (BSSID: 00:0F:84:A3:DC:70) and the one that covers the information area and the two seminar rooms is called Info (BSSID: 00:0E:83:19:1E:70). The information area is equipped with several PCs for the students to browse the library catalogue and provide the wireless access to the two small seminar rooms. Our analysis will characterize the network usage in different areas through studying the packets captured from these five APs.

B. Trace Collection & Analysis

We placed a sniffer at the level 5. The sniffer comprises of a Pentium III 900 MHz laptop running Linux Kernel 2.4, and an PCMCIA Cisco Aironet 350 series card. The coverage of an AP and the wireless adapter is 60 m, therefore, we could capture the packets from APs in level 4 and level 6 also. We used Ethereal to capture packets in promiscuous mode and dumped in to *libpcap* dump files for later analysis.

The trace collection started on Monday (September 27, 2004) to Friday (October 1, 2004). Each day, we collected trace from 9:00 AM to 9:00 PM. During the weekend, the library is close earlier, therefore, we did not want to include in our analysis. We summarize the information we captured from the dump files. The total traffic collected is 15.228 GB over a period of 60 hours. The average traffic rate is 0.557 Mbps, the maximum rate is 4.790 Mbps and the minimum rate is 0.019 Mbps.

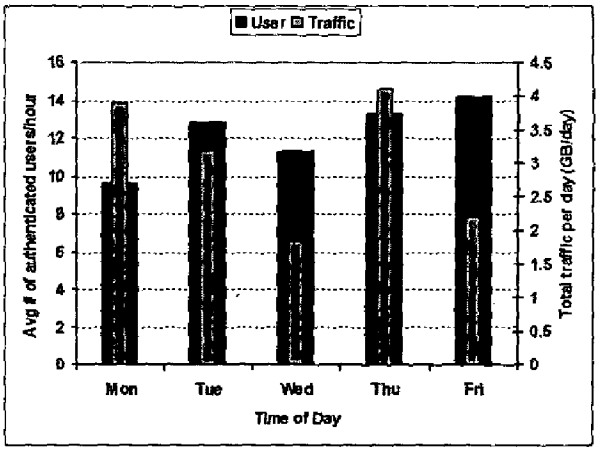

Fig. 2. Average Number of Authenticated Users per hour vs. Total Traffic

The dump files were analyzed with the help of Ethereal and Tcpstat. Ethereal is very powerful that it can help us calculate statistics from the dump files. We also made use of the filtering function of Ethereal to filter out interesting packets such as authentication packets for further analysis. We included some information obtained from AirSnort to calculate the load traffic an the level of data encryption at each APs.

V. Results

A. Daily Traffic vs Number of Users

By using Ethereal we sorted the the packets captured according to source and destination IP address. By this way we could filter out the authenticated wireless users because the NUS WLAN is in a different subnet from the wired LAN and has the private network ID equal to 172.18. Then we examined the MAC addresses to identify unique users.

In Figure 2, we compare the average number of authenticated users per hour to the total traffic captured on the same day. We see that although Wednesday has the least traffic however the average number of authenticated users per hour is fairly high with more than 3 GB of data. Comparing the statistics from Monday and Friday, we also see the contrast between these two days: Monday has more traffic with less users whereas Friday has more users and less traffic.

From this observation, we see that the traffic is not directly proportional to the number of authenticated users. The total traffic and the number of authenticated users are the two independent variables. Therefore, the number of users alone does not precisely characterize the load on the network. We need to look at the real traffic to see the real network load.

1) Traffic Characterization: We used Ethereal to calculate the number of packets belonging to different types of frames and protocols. The protocol mix is presented in Figure 3. TCP is the most dominant protocol, it occupies 43% of the traffic,

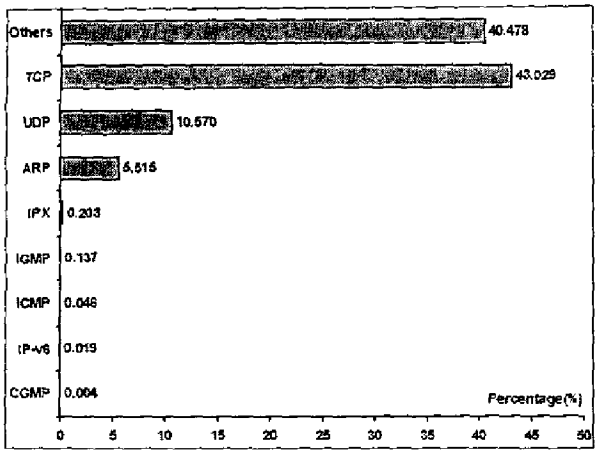

Fig. 3. **Protocol Mix of Wireless Traffic**

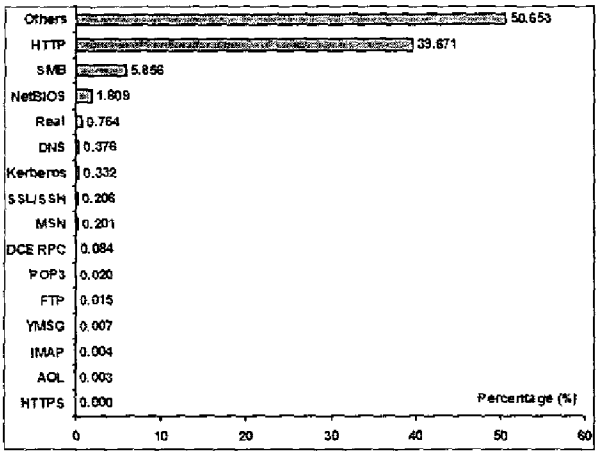

Fig. 4. **Application Mix of Wireless Traffic**

this is followed by UDP and ARP which account for 10.5% and 5.5% respectively. We also see some traffic from IPv6. The *Others* packets (40.7%) are undecoded frames (because of WEP encryption), and IEEE 802.11 management frames.

In Figure 4, we can see that web browsing (i.e., HTTP traffic) is the most popular application contributing to 39% of the total number of packets, followed by SMB, NetBIOS. We can also see some Real Time Streaming Protocol. We also observe the unpopularity of long-live protocols such as FTP. As expected, we also see small traffic generated by popular Instant Messenger (IM) programs such as Yahoo Messenger, AOL of MSN. This explains that IM is very popular among students. The rest (50%) accounts for IEEE 802.11 managment packets and undecoded packets.

We conclude that the traffic comprises of mostly short-lives protocol such as HTTP. Therefore we can conclude that the network is not used to the maximum capacity.

2) User Distribution: By filtering authentication packets and examining the MAC address we were able to count the number of authenticated users in an interval of time. The result

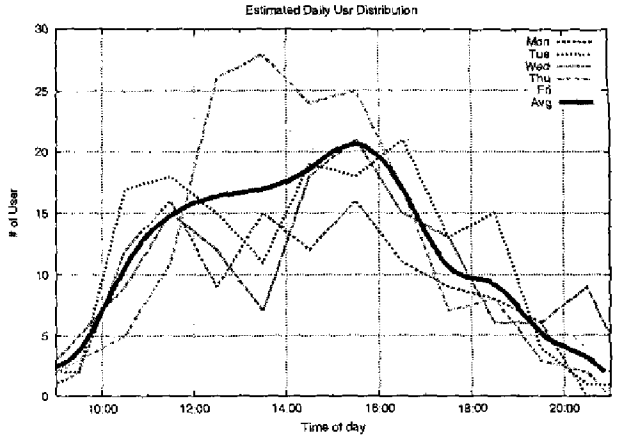

Fig. 5. **The authenticated user distribution of the network**

is presented in Figure 5.

As expected the authenticated user distribution is pretty the same as the network throughput distribution. The shape of the distribution is close to a bell-shaped curve. The number of wireless users increases from 9 AM to 12 PM for all the days. However from this point of time, each day expresses different behaviour. From 12 noon to 2 PM this is the lunch time and the number of users is expected to decrease. We can observe this phenomena from Monday, Tuesday and Wednesday. However on Thursday and Friday, the number of users increases during this period of time.

We also see that the user distribution is centralized at the center of the day from 11 AM to 6 PM. This result agrees with the network throughput distribution as seen from the daily traffic patterns. throughput distribution in as seen from the Daily Traffic Patterns.

3) Network Load Distribution Across APs: In previous sections we described the whole network. We now want see how the traffic load is distributed among the APs. We use AirSnort to count the packets from these APs. Figure 6 shows the network load distribution among the APs. The APs Ctr-1 and Ctr-2 accounts for the most packets, 26% and 41% respectively. This result is expected as these two APs are located at the study area. However Ctr-2 has the number packets nearly twice as much as Ctr-1. The reason can be that the study area covered by Ctr-2 has 120 seats for students while Ctr-1 covers only 64 seats including 24 seats from the Laptop Charging area. Therefore, it may be the case that Ctr-2 bears the heavier load than Ctr-1.

The rest traffic is accounted for the Info (14%), ChLib(12%) and Lounge (7%). Interestingly, despite being located in the reference area of the Chinese Library, ChLib bear less traffic than Ctr-1 and Ctr-2. This may be because there is not much material on Chinese online. Student rather study the offline materials provided by the libarary. Therefore, we see less traffic in this AP. The Info is placed at the open space at the information area and provides the wireless access to the 2 small seminar rooms, so it bears higher traffic than the other

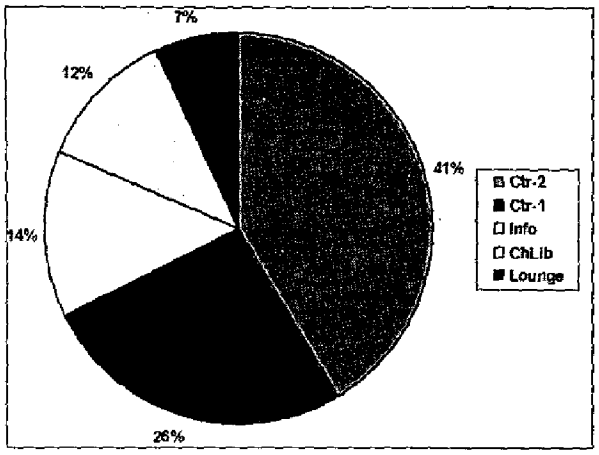

Fig. 6. **Distribution of network load on APs**

two. The Lounge is placed in the lounge where students have a nap, relax after studying; therefore we expect to see very little traffic in here.

B. Summary of Our Analysis

Through our analysis, we have been able to answer some of the important questions. These are explained below.

- *What is the user behaviour?* The wireless user distribution is like a bell shape curve. The number of users increases from the beginning of the day and decreases at the end of the day. By investigating the protocol mix we see that web browsing is the dominant application. We also see the presence of Real Time Streaming Protocol and popular Instant Messenger programs such as MSN, AOL and Yahoo Messenger. We do not observe much persistent applications such as FTP.
- *How is the wireless traffic?* Throughout the trace, we observe that the network never reaches its capacity. The average throughput is only 0.557 Mbps while the maximum recorded is 4.79 Mbps. Like the number of authenticated users, the traffic curve is also bell shape. Traffic gets higher at the beginning of the day and drops down gradually near the end of the day.
- *How is the distribution across APs?* The network load is uneven across APs. We observe that APs located at the study area bear the most traffic especially APs near to the power sockets. However, we also notice that study area in which the offline materials are more resourceful (the Chinese Library we mentioned) bears much lower traffic than the general study area. APs in the relaxing area and area with available PCs connected to Internet bear lower traffic.
- *What is the level of security of the network?* The network employs LEAP authentication and WEP encryption. However these security features were not configured properly at the AP side or user's side that there is a certain number of packets are not properly encrypted. This presents a big threat to our network.

From the statistics that we have collected so far, we arrive at some useful design principles.

- We are in agreement with the previous papers that when designing WLAN, we should focus on location rather than movement. Popular areas such as study area, class rooms or labs should be paid more attention as these places are visited by students most. Installing wireless resource in these areas helps increase the productivity of students.
- We observed that the network is under-utilized. The network never reaches its maximum capacity. We should utilize the resources by putting more material online. This will increase the demand of using wireless resources in the campus.
- Providing more power sockets can increase the number of wireless users. This enables users to have longer study sessions.
- APs should be examined regularly to ensure the security of the network. If there is a low level of packets encryption at an AP, there must be some misconfiguration.

VI. Conclusions

In this paper, we have presented an overview of the available open-source wireless sniffing tools. We have identified their functions as well as their applications in hacking, war driving and especially in analyzing a small WLANs through a comprehensive study at the National University of Singapore. There are some disadvantages of the methods described in the paper. It is implicitly assumed that wireless sniffers capture the complete wireless traffic. This not always true as the radio channel is highly lossy. In addition, in networks that employ WEP encryption, decoding the packets is hard and it is easy to miss out on important traffic. In our analysis, there are nearly 50% of the packets that were not decoded by Ethereal.

References

[1] N. S. Willam A. Arbaugh and Y. J. Wan, "Your 802.11 Wireless Network has No Clothes," http://www.cs.umd.edu/~waa/wireless.pdf, March 30 2001.

[2] I. M. Scott Fluhrer and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," http://www.crypto.com/papers/others/rc4_ksaproc.ps, July 25 2001.

[3] "Netstumbler's home page," http://www.netstumbler.com.

[4] "National University of Singapore home page", http://www.nus.edu.sg

[5] "Kismet's home page and documentation," http://www.kismetwireless.net.

[6] "Airtraf's home page and documentation," http://www.airtraf.sourceforge.net.

[7] "Frequently Asked Questions About AirSnort," http://airsnort.shmoo.com/faq.html.

[8] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan, "Characterizing user behavior and network performance in a public wireless lan," in *Proceedings of the 2002 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*. ACM Press, 2002, pp. 195–205.

[9] D. Tang and M. Baker, "Analysis of a local-area wireless network," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM Press, 2000, pp. 1–10.

[10] D. Kotz and K. Essien, "Analysis of a campus-wide wireless network," in *Proceedings of the 8th annual international conference on Mobile computing and networking*. ACM Press, 2002, pp. 107–118.