Proceedings of the South Asian Network Operators Group

Srijeyanthan Kuganesan
KTH Royal Institute of Technology

Proceedings of the South Asian Network Operators Group

A Wireless Network Performance and Security Case Study

Thusyanthan Arulsodhy*, Kuganesan Srijeyanthan, Nihanth Joseph and Chandana Gamage

Department of Computer Science and Engineering, University of Moratuwa, Sri Lanka

E-Mails: {athusy, srijeyanthan, nikkey}@gmail.com; chandag@uom.lk

* Author to whom correspondence should be addressed; Tel.: +94-114-216-066; Fax: +94-112-650-912

Abstract: The ease of setting up a wireless network and the low cost of wireless networking equipments have made such networks ubiquitous in universities, company office complexes, public facilities, etc. While setting up a wireless network consisting of multiple access points is easy and cheap, ensuring a secure and performance tuned network is not straightforward. In order to study the security and performance aspects of wireless networks and evaluate the tools available for network engineers to assess the wireless networks, the authors have selected a medium sized wireless network with several hundred users as a case study. In this study, data were collected about AP their locations, effectiveness based on that situated AP locations, utilization of network bandwidth and effectiveness of security. This paper presents results based on analysis of this data and suggestions based on this study. Since the target network includes more than 6 wireless networks, it can be confidently said, these data and the analysis can be generalized for WiFi networks found in many organizations.

Keywords: WiFi networks; AP locations; network performance.

1. Introduction

In this age of digital information, networks have become one of the most important infrastructure facilities and the Internet has become an essential technology and service for everyone. Along with the need for networking, the need for mobility of network nodes and flexibility in setting up networks have resulted in an extraordinary growth in wireless

Internetworking. The growth patterns of networks, applications and technologies clearly show mobile computing and wireless networking to be the main stay in future internetworks.

2. Methods

In this case study of WiFi network performance and security analysis, the Access Point (AP) location suitability was studies for a medium sized wireless network belonging to an engineering department of a university (referred to as the target network) with six sub networks. The study first analyzed sub network A (referred to as CSE-RESEARCH), which has a frequently high usage in terms of number of users of over 100 nodes and large bandwidth requirements. Secondly, the study focused on the target network as a whole. The usual approach to building WiFi networks is to place APs at locations that give the widest possible coverage. However, distance from potential nodes to the AP, obstructions in the wireless transmission paths and transmission interferences are also significant factors affecting the connectivity and bandwidth availability. To achieve an optimal network connectivity from a user point of view, the APs should also be placed allowing for optimal network performance and not merely the coverage area.

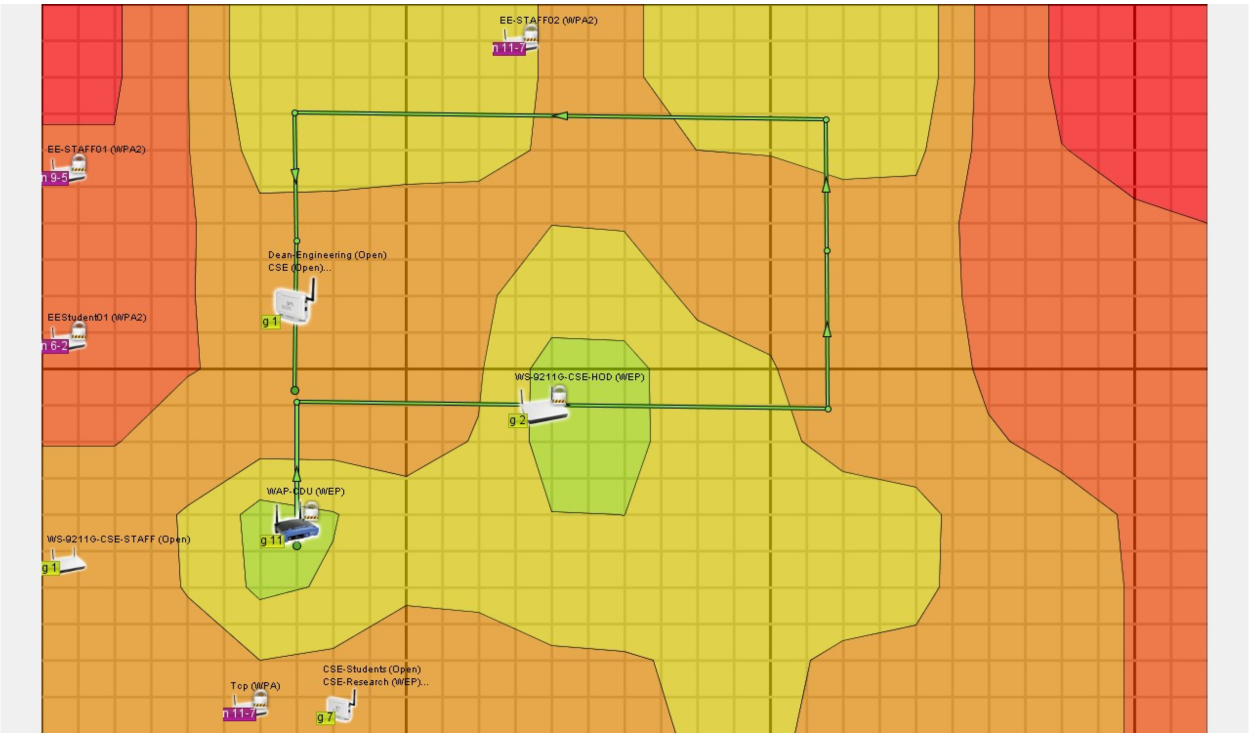


Figure 1. Coverage map considering the entire target network.

In this wireless network performance case study, to plot the coverage and the AP map, we have used the Ekahau HeatMapper [1], which provides heat-map type color coded coverage mapping of WiFi networks. This is an easy tool that locates all access points and the signal strength by distance. While there are many other wireless network mapping tools available, such as VisiWave [2], NetStumbler [3], we choose Ekahau Heat Mapper as it provides a real-time view to all APs and their configurations. The software that uses the built-in wireless network adapter of a laptop computer is designed to support 802.11n as well as a/b/g type networks.

To take measurements, the study team members activate the HeatMapper on the wireless laptop and walked within the physical locality of the target network as shown in figure 1. The green lines indicate the direction of the movement of the wireless device and the figure provides all the relevant information with respect to the target network physical area shown as a grid. The strength of the radio signal is the most basic measure that affects the quality of WiFi connectivity and the figure shows the signal strength in decreasing order as green, yellow, orange and red. In this color code, green indicates higher coverage and red indicates lower coverage. The signal strength is measured in dBm according to specifications of HeatMapper system and a higher signal strength is indicated by a lower negative number in dBm. The observed data in one of the sample tests is shown in table1.

Table 1. Color coding scheme for signal strength.

Color	*Signal Strength (dBm)*
Dark green	48 - 40
Light green	56 - 48
Lighter green	64 - 56

As indicated by the coverage map, it is relevant to note that the CSE-HOD wireless network has highest signal strength among wireless networks present in the target network physical locality. As the coverage map shows, the wireless radio signal strength is not uniformly distributed and a reconfiguration of the AP locations are required for improving the effective coverage area. However, it should also important to note the application-level scenario where available data shows that the WiFi networking capability is not used uniformly across the entire physical area of the target network.

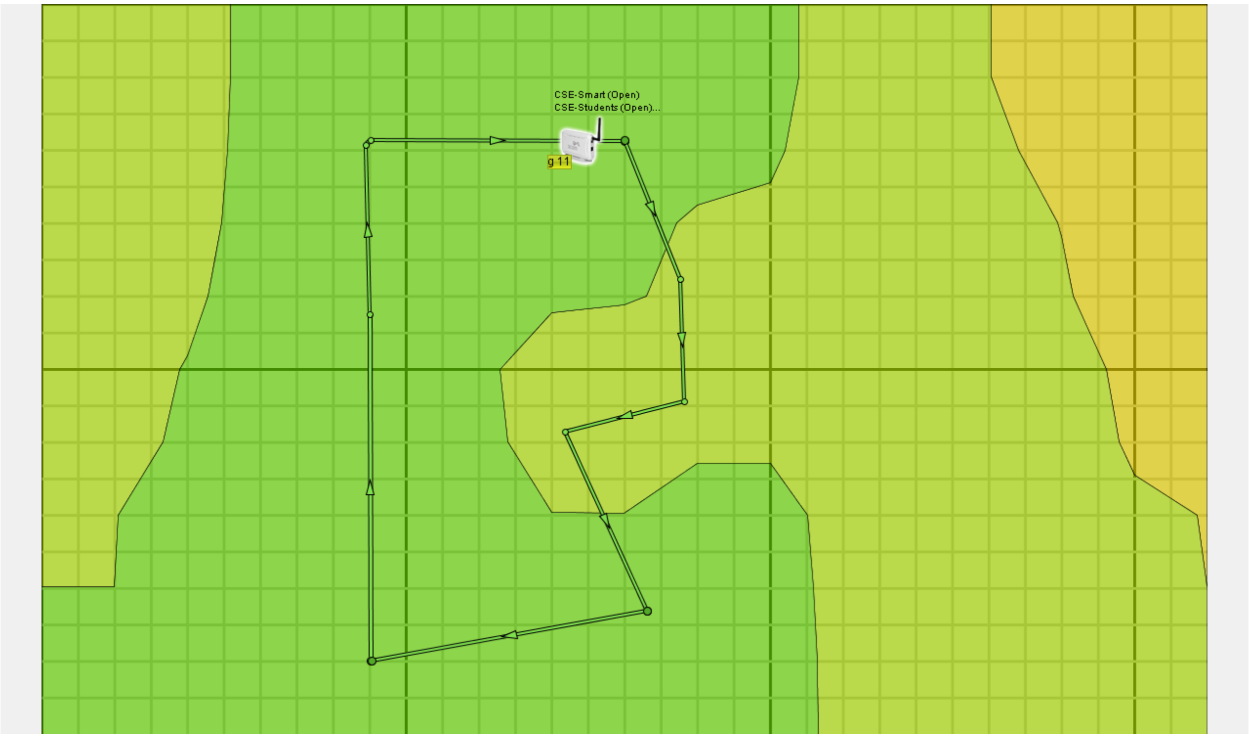


Figure 2. Coverage map considering the CSE-RESEARCH network.

The coverage map for the wireless sub network CSE-RESEARCH in the target network is shown in figure 2 and figure 3 and as can be seen approximately half the area is in green color. In the context of the entire target network, this sub network is considered to be a high bandwidth utilization network. Another factor of importance is that although the coverage map indicates the availability of several APs, many of these do not belong to the target network under study. There is significant wireless spectrum interference due to these outside APs.

3. Results

3.1. Wireless Network Connectivity

The efficient performance of a wireless network depends significantly on the signal strength of the wireless APs. If the wireless devices like laptop computers or hand-held WiFi devices fall out of the transmission range of the AP or fall in to a lower signal strength area, then the connections will drop. Initially, the wireless device should be within the range of the AP radio signal to get connected to the AP. The test results show the AP locations to give good radio coverage and signal strength. However, as the wirelesses APs of the target network are static, we cannot come to a conclusion that the existing positions are optimal for performance. A further study requires changing of the AP positions and checking the performance through a trial-and-error method.

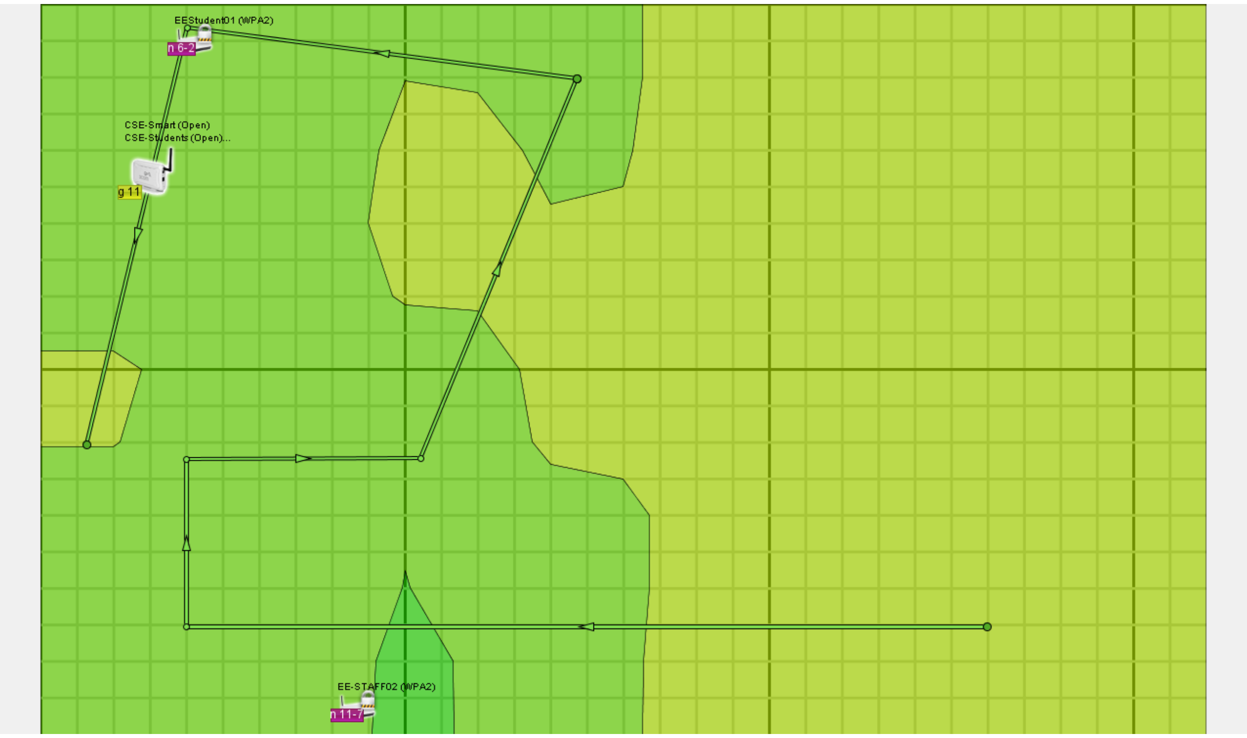


Figure 3. Expanded coverage map considering the CSE-RESEARCH network.

The network resources usage patterns and number of users are other important factors in determining AP positioning. The existing wireless network deployment provides good signal strength in some areas of high usage such as the CSE-RESEARCH sub network as shown in figures 2 and 3.

The presence of physical obstructions in the radio propagation paths degrade the WiFi signals and any barriers along the line-of-sight between the AP and the client device will have a negative impact. The artifacts such as walls, doors, furniture, etc present in an indoor environment weakens the signal due to scattering and absorption. In the target network, most of the APs are located inside buildings, where many of them are large open-plan style spaces. This configuration corresponds with the test data showing a higher bandwidth availability inside the labs than the outside when the survey was carried out by walking along corridors in the building. The omni-directional WiFi antennas used in the target network APs radiate the signal equally in all directions. Therefore, placing the APs in the center of the open-plan spaces has given a higher radio signal strength.

3.2. Wireless Network Security

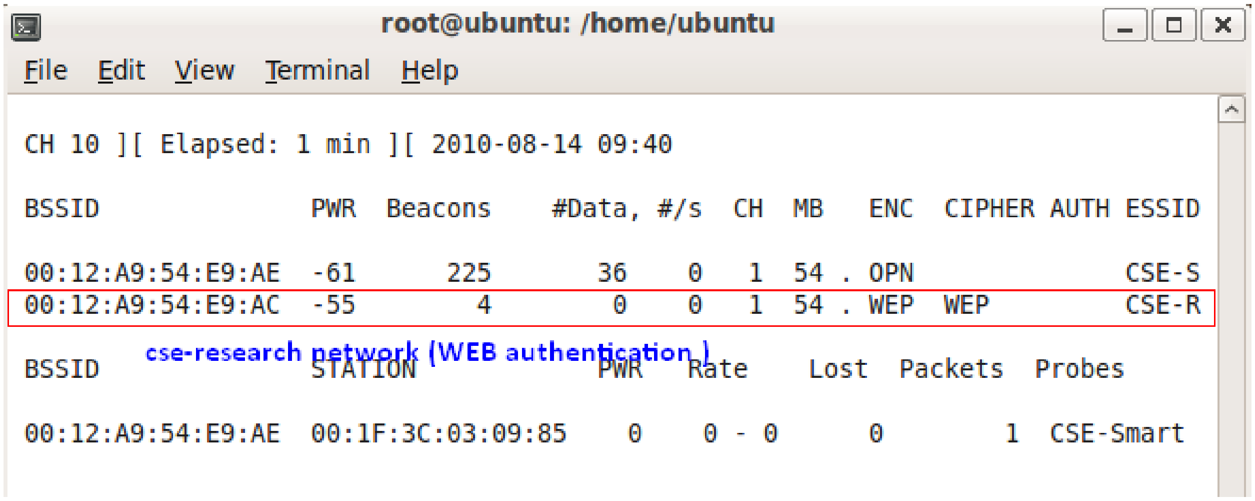
Unlike wired networks where connectivity requires physical contact with the infrastructure, wireless networks are accessible to anyone within the area of signal reception. In this context, network security is a major concern in WiFi networks to prevent unauthorized access or damage to systems and data. As both wireless networks and wireless-enabled laptop computers and hand held devices are becoming common place, potential to breach network security is very high. While wireless networks are designed and built with many security features and capabilities [4,5], attackers routinely compromise wireless network security and use it as a stepping stone to the fixed network infrastructure.

The target network that was studied had several APs that were unsecured thus allowing anyone to connect to the network without identification, authentication and authorization. The secured APs of the target network require the use of a security key to access the wireless network. Our tests have shown that all secured APs to use the same WEP encryption method. In the WEP standard, there are two authentication modes:

1. Open-System Authentication: This is the default mode in which all clients are accepted and association is granted by the AP and the key is never checked. However if a station key is incorrect, that station will not be able to send or receive packets as decryption will fail causing DHCP, ping, etc. to time-out.
2. Shared-Key Authentication: In this mode, the client has to encrypt a challenge before association is granted by the AP. However, as this mode is flawed and leads to key-stream recovery, it is never enabled by default.

As all the secured sub networks in the target network was using open-system authentication, we have chosen one wireless network (CSE-RESEARCH) network to demonstrate the compromise of the WEP authentication key.

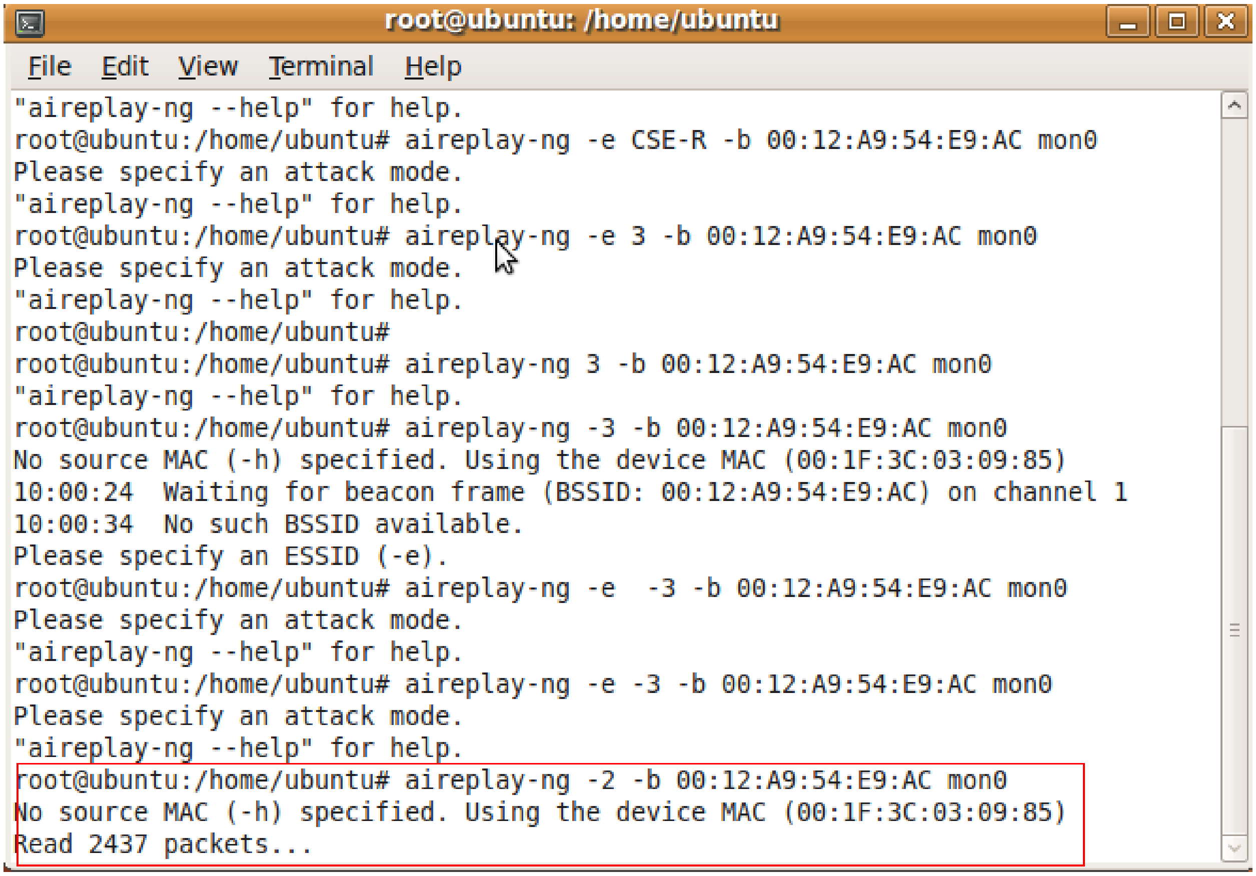
In the attack on CSE-RESEARCH network wireless AP, which uses a WEP 40/128 bit key with open-system authentication, we used the aircrack-ng 1.0 [6] tool in the Ubuntu OS environment. The aircrack tool has three major components: (1) the airomon for monitoring the wireless network, (2) aireplay for generating packets and capturing packets to target wireless network, and (3) aircrack for decrypting the captured packets.



```
CH 10 ][ Elapsed: 1 min ][ 2010-08-14 09:40

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:12:A9:54:E9:AE  -61      225       36    0   1  54 . OPN              CSE-S
00:12:A9:54:E9:AC  -55        4        0    0   1  54 . WEP  WEP         CSE-R

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:12:A9:54:E9:AE  00:1F:3C:03:09:85    0    0 - 0     0        1  CSE-Smart
```

cse-research network (WEB authentication)

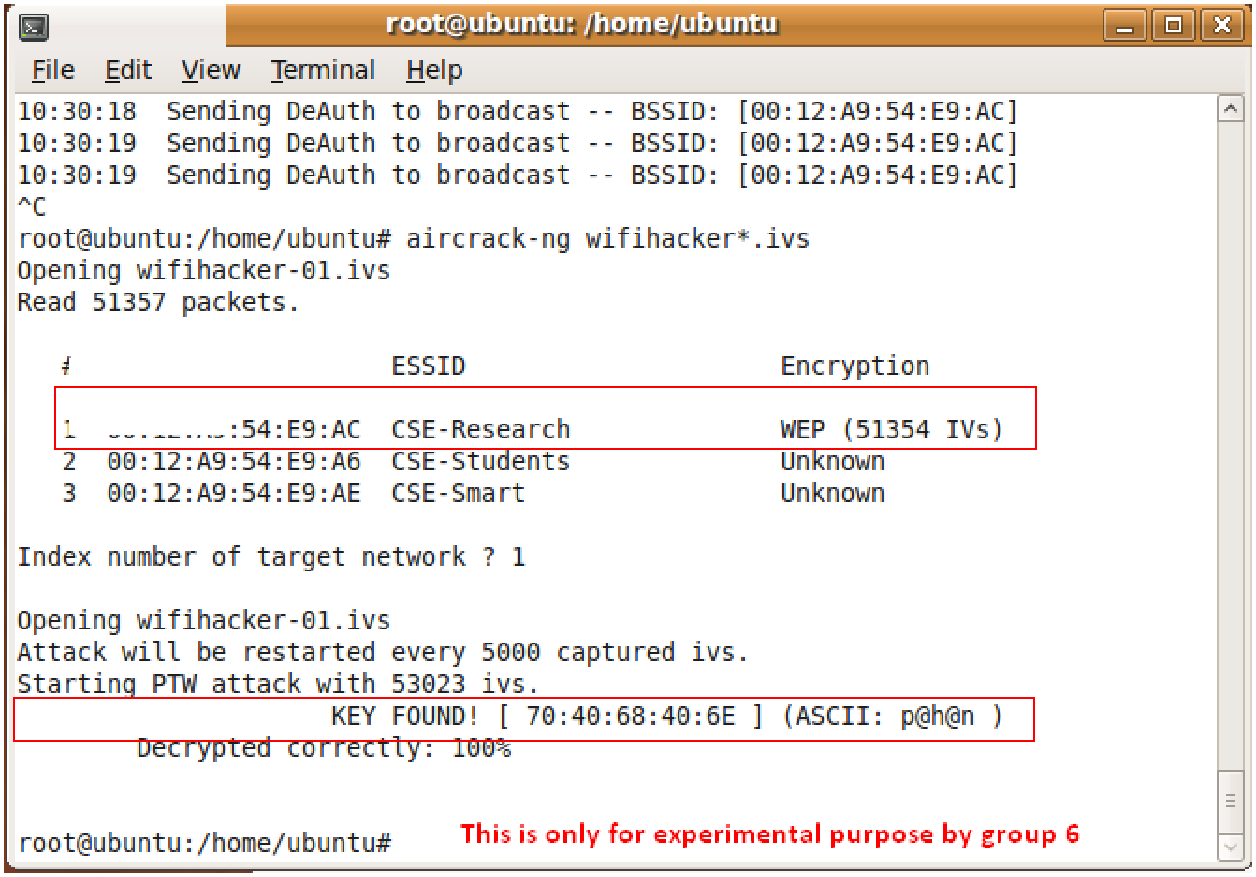
Figure 4. Packets captured by Airplay tool from target network.



```
"aireplay-ng --help" for help.
root@ubuntu:/home/ubuntu# aireplay-ng -e CSE-R -b 00:12:A9:54:E9:AC mon0
Please specify an attack mode.
"aireplay-ng --help" for help.
root@ubuntu:/home/ubuntu# aireplay-ng -e 3 -b 00:12:A9:54:E9:AC mon0
Please specify an attack mode.
"aireplay-ng --help" for help.
root@ubuntu:/home/ubuntu#
root@ubuntu:/home/ubuntu# aireplay-ng 3 -b 00:12:A9:54:E9:AC mon0
"aireplay-ng --help" for help.
root@ubuntu:/home/ubuntu# aireplay-ng -3 -b 00:12:A9:54:E9:AC mon0
No source MAC (-h) specified. Using the device MAC (00:1F:3C:03:09:85)
10:00:24  Waiting for beacon frame (BSSID: 00:12:A9:54:E9:AC) on channel 1
10:00:34  No such BSSID available.
Please specify an ESSID (-e).
root@ubuntu:/home/ubuntu# aireplay-ng -e  -3 -b 00:12:A9:54:E9:AC mon0
Please specify an attack mode.
"aireplay-ng --help" for help.
root@ubuntu:/home/ubuntu# aireplay-ng -e -3 -b 00:12:A9:54:E9:AC mon0
Please specify an attack mode.
"aireplay-ng --help" for help.
root@ubuntu:/home/ubuntu# aireplay-ng -2 -b 00:12:A9:54:E9:AC mon0
No source MAC (-h) specified. Using the device MAC (00:1F:3C:03:09:85)
Read 2437 packets...
```

Figure 5. Send and Receive requests from target network.

The attack followed the steps of extracting the SSID and channel information for the CSE-RESEARCH network and launching the aireplay tool with corresponding parameters with a path set to store the capturing files as shown in figure 4. In the next phase a large number of sent and received packets were captured and stored in to file with the traffic generation to the targeted network shown in figure 5. Finally, the captured trace file was used to crack the WEP key using the aircrack tool as shown in figure 6.



```
10:30:18  Sending DeAuth to broadcast -- BSSID: [00:12:A9:54:E9:AC]
10:30:19  Sending DeAuth to broadcast -- BSSID: [00:12:A9:54:E9:AC]
10:30:19  Sending DeAuth to broadcast -- BSSID: [00:12:A9:54:E9:AC]
^C
root@ubuntu:/home/ubuntu# aircrack-ng wifihacker*.ivs
Opening wifihacker-01.ivs
Read 51357 packets.

   #                     ESSID                         Encryption

   1  00:12:A9:54:E9:AC  CSE-Research                  WEP (51354 IVs)
   2  00:12:A9:54:E9:A6  CSE-Students                  Unknown
   3  00:12:A9:54:E9:AE  CSE-Smart                     Unknown

Index number of target network ? 1

Opening wifihacker-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 53023 ivs.
                     KEY FOUND! [ 70:40:68:40:6E ] (ASCII: p@h@n )
        Decrypted correctly: 100%


root@ubuntu:/home/ubuntu#
```

This is only for experimental purpose by group 6

Figure 6. Cracked WEP key for target network.

As shown in this case study, the wireless security in the target network is extremely weak. The solution would be to use WPA, which is the advanced encryption scheme superseding WEP. The wired equivalency privacy encryption has well-known weaknesses that make it relatively easy for a determined user with the right equipment to crack the encryption and access the wireless network. Each WEP data packet has an associated 3-byte Initialization Vector (IV) and after a sufficient number of data packets have been collected, aircrack can be run on the resulting capture file. The aircrack tool then performs a set of statistical attacks and recover the key. WPA resolves the issue of insecurity in WEP headers with their weak IVs and provides a way of insuring the integrity of the messages passed through message integrity check (MIC) using a scheme called the Temporal Key Integrity Protocol (TKIP) to enhance data encryption.

4. Conclusions

In this case study of a wireless network, we have studied the WiFi AP placement for performance and AP configuration for security. Our tests show that the APs in the target network should be repositioned to optimize effective signal strength and to improve coverage. The security tests showed the network to be completely vulnerable to attacks using off-the-shelf tools and the use of WEP to be the main reason for security compromises.

Acknowledgements

The authors gratefully acknowledge the infrastructure and technical support provided by the Department of Computer Science & Engineering, University of Moratuwa and the LK Domain Registry in Sri Lanka for conducting the network study described in this paper.

References

1. *Ekahau HeatMapper*, 2010. [Online]. Available: http://www.ekahau.com/ products/ heatmapper/ overview.html. [Accessed: Nov. 2, 2010].
2. AZO Technologies, "*VisiWave*", 2010. [Online]. Available: http://www.visiwave.com/. [Accessed: Aug. 19, 2010].
3. Marius Milner, "*NetStumbler*", 2002 - 2004. [Online]. Available: http://www.stumbler.net/. [Accessed: Nov. 28, 2010].
4. Linksys, "*Network Security Tips*". [Online]. Available: http://www.linksys.com/. [Accessed: Jun. 02, 2010].
5. "*How to: Define Wireless Network Security Policies*". [Online]. Available: http://www.wireless-nets.com/. [Accessed: Oct. 09, 2010].
6. "*Aircrack-ng*". [Online]. Available: http://www.aircrack-ng.org/ [Accessed: Nov. 22, 2010].