WIRELESS LOCAL AREA NETWORK SECURITY ANALYSIS:
A CASE STUDY OF ABU WIRELESS LOCAL AREA NETWORK

BY

SHEHU MUHAMMAD-TUKUR

DEPARTMENT OF MATHEMATICS

FACULTY OF SCIENCE

AHMADU BELLO UNIVERSITY, ZARIA-NIGERIA

MARCH, 2011.

WIRELESS LOCAL AREA NETWORK SECURITY ANALYSIS:
A CASE STUDY OF ABU WIRELESS LOCAL AREA NETWORK

BY

SHEHU MUHAMMAD-TUKUR
(B.Sc Mathematics with Computer Science, 2006)

M.SC/SCIEN/00142/2008-2009

AHMADU BELLO UNIVERSITY ZARIA, IN PARTIAL FULFILMENT A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL, OF THE REQUIREMENT FOR THE AWARD OF MASTER DEGREE OF SCIENCE IN COMPUTER SCIENCE DEPARTMENT OF MATHEMATICS, AHMADU BELLO UNIVERSITY, ZARIA-NIGERIA.

MARCH, 2011.

DECLARATION

I declare that the work in this thesis wo-rk entitled "Wireless Local Area Network Security Analysis: A Case study of the ABU Wireless LAN" has been performed by me in the Department of Mathematics under the supervision of Prof. S.B Junaidu, and Dr. M. I. Buhari. The information derived from the literatures has been duly acknowledged in the text and a list of references provided. No part of this research work was previously presented for another degree or diploma at any University.

SHEHU MUHAMMAD-TUKUR	_____	_____
Name of Student	**Signature**	**Date**

CERTIFICATION

This thesis entitled "Wireless Local Area Network Security Analysis: A Case study of the ABU Wireless Local Area Network" by **MUHAMMAD-TUKUR Shehu** meets the regulations governing the award of the degree of Master of Science in Computer Science of the Ahmadu Bello University, Zaria and is approved for its contribution to knowledge and literary presentation.

Prof. S.B Junaidu Major Supervisor	Date
Dr. M. I. S. Buhari Minor Supervisor	Date
External Examiner	Date
Dr A.A Tijjani Head of Department	Date
Prof. A. A. Joshua Dean, Postgraduate School	Date

ACKNOWLEDGEMENT

All praise is to Almighty Allah (alone) unto whom I turn to make a request and HE bestows the benefit asked for. Although I am closefisted and stingy but HE always lend me generous share in the bounties. May Allah's blessing and peace be upon Prophet Muhammad (SAW) and also, on to those his descendants who are pure.

My sincere appreciation goes to my supervisors, in person of Prof. S. B. Junaidu whose critical supervision and inputs made it possible for me to surmount the hurdles I encountered during the course of this study. May God who alone knows how best to reward every one, bless you and your family abundantly Sir. Dr. M.I Buhari my minor supervisor, thank you so much for your constructive criticisms and suggestions throughout my work may God rewards you.

To the Projects Implementation and Management Committee (PIMC) of Ahmadu Bello University MacAuthur Foundation Projects, I say thank you so much, this dissertation has been completed with support from the A.B.U MacAuthur Foundation Projects.

I will like to say thank you to my Head of Department in person of Dr. A.A Tijjani. To the entire staff and students of the Department of Mathematics, Ahmadu Bello University Zaria, I say thank you. To my beloved, wife Haj Aishat Ibrahim and daughter Amina S. Tukur, I say thank you for your support, love, encouragement and tolerance, for bearing with me when I had to leave you in pursuit of this degree and to my beloved mother, brothers, sisters and friends for their assistance and support, I appreciate you all.

My acknowledgement will be incomplete without mentioning my good and dedicating friend Engr. Yusuf ICT, thank you so much for your academic contribution towards achieving this goal. May God reward you abundantly ameen.

DEDICATION

I dedicate this work to my late father in person of Alh. Muhammad-Tukur Abubakar and My loving Mother Haj Amina Umar, whose encouragement and challenges serve as a source of inspiration to me right from my childhood.

ABSTRACT

This research thesis work studied the security settings of Wireless Local Area Network (WLAN), their vulnerability, and alternative solution (s), taken ABU wireless LAN as the case study. The research work present results from a comprehensive trace of wireless network security in a large wireless LAN which is the ABU wireless LAN using two software tools as CommView-for-WiFi for packet capture on the network, and Aircrack-ng for decrypting the encryption found in some Access Points (AP) within the network coverage range. This has been carried out using the campus-wide network of more than 100 access points (APs) spread over the buildings of the University. Potential problem(s) and appropriate solution(s) which is the use of WPA2 has also been discussed for the improvement of the wireless network in terms of security settings for effective and secure communication putting access control in to cognizance.

TABLE OF CONTENTS

CHAPTER FOUR: ANALYSIS AND DISCUSSION OF OUR PROPOSED SECURITY MECHANISM

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATION

LIST OF TABLES

LIST OF FIGURES

[1] Fig. 3.1, 3.2, 3.3 and 3.4 are courtesy of micros access company that gives a Picturial representation of the wireless deployment in the organization

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

1.2 Wireless Local Area Networks (WLANS)

A wireless LAN (WLAN) is analogous to a wired LAN with radio waves being the transport medium instead of traditional wired structures. This allows the users to move around in a limited area while being still connected to the network. Thus, WLANS combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs (WLAN Association, 1999). In other words, WLANS provide all the functionality of wired LANs, but without the physical constraints of the wire itself.

Generally a WLAN (in Infrastructure mode) consists of a central connection point called the Access Point (AP). It is analogous to a hub or a switch in traditional star topology based wired local area networks. The access point transmits the data between different nodes of a wireless local area network and in most cases serves as the only link between the wireless LAN and the wired LAN. A typical access point can handle some handsome amount of users within a radius of about 300 feet. The wireless nodes, also called clients of a WLAN usually consist of Desktop PCs, Laptops or PDAs equipped with wireless interface cards.

1.3 Types of Wireless Networks

The 1999 version of the 802.11 standard (John *et al.,* 2001) defines the following three types of wireless networks:

1.3.1 Independent Basic Service Set (IBSS)

IBSS commonly referred to as Ad Hoc network, is logically comparable to a Peer-to-Peer network in case of a wired LAN as shown in Fig. 1.1. In case of IBSS different end nodes communicate without any Access Point and thus without any connection to a wired network. It is used to quickly set up a wireless network (to avoid the hidden node problem[2]) such as for a group meeting or at a convention center or at an airport, etc.

Fig. 1.1 Ad-hoc Mode[3]

1.3.2 Basic Service Set (BSS)

BSS which is commonly referred to as an infrastructure network consists of a single Access Point as shown in Fig. 1.2. All the communication between any two nodes has to pass through the AP. The coverage area is greatly increased as compared to an IBSS.

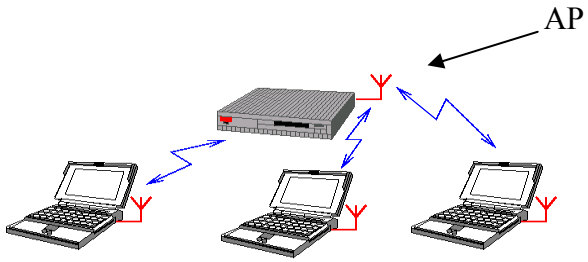

Fig. 1.2 Infrastructure Mode

[2] A hidden node problem occurs when a wireless node cannot hear one or more of the other nodes therefore media access protocol cannot function properly. Thus multiple nodes will attempt to transmit their data over the shared medium simultaneously causing signal interference with one another.

[3] Fig. 1.1, 1.2, and 1.3 are pictures courtesy of http://rnvs.informatik.tu-chemnitz.de.

1.3.3 Extended Service Set (ESS)

An ESS consists of multiple BSSs each having a single Access Point. Access Point in each BSS is connected to a distribution system that is usually a Wired Ethernet Network.

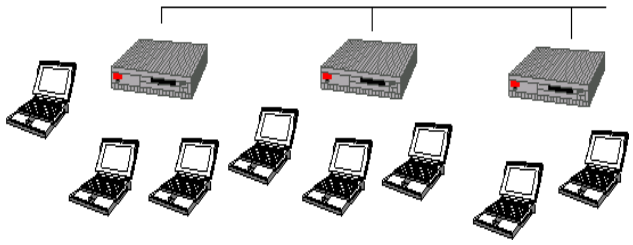

Fig. 1.3 Extended Service Set (ESS)

1.4 Wireless Networking Standards

Institute of Electrical and Electronics Engineers (IEEE) (WLAN Association, 2002) has specified various WLAN standards. Some important standards in the context of this thesis are summarized in Table 1.1.

Table 1.1 IEEE WLAN Standards

Standard	**Description**	**Approved**
IEEE 802.11	Data rates up to 2Mbps in 2.4-GHz ISM band	July 1997
IEEE 802.11a	Data rates up to 54Mbps in 5-GHz UNII band	Sept 1999. End user product began shipping in early 2002
IEEE 802.11b	Data rates up to 11Mbps in 2.4-GHz ISM band	Sept 1999. End user product began shipping in early 2000

Other standards are the following:

IEEE 802.11g:

In 2002 and 2003, WLAN products supporting a newer standard called 802.11g emerged in the market. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHZ frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

IEEE 802.11n:

The newest IEEE standard in the WiFi category is 802.11n. It was designed to improve on 802.11g in the amount of bandwidth supported by utilizing multiple wireless signals and antennas (called MIMO[4] technology) instead of one. When this standard is finalized, 802.11n connections should support data rates of over 100 Mbps. 802.11n also offers somewhat better range over earlier WiFi standards due to its increased signal intensity. 802.11n equipment will be backward compatible with 802.11g gear.

1.5 Problem Definition

Ubiquitous network access without wires is the main attraction underlying wireless network deployment. Although this seems as enough attraction, there exists other side of the picture.

[4] MIMO (Multiple Input, Multiple Output) is an antenna technology for wireless communications in which multiple antennas are used at both the transmitter and the destination receiver.

Before going all Wireless an organization should first understand how wireless networks could be vulnerable to several types of intrusion methods used by intruder[5] on a network.

The literatures studied do not offer an experimental evaluation of link-layer security in heavily utilized and congested wireless networks such as the ABU wireless network. We believed that gaining a deep understanding of the real-world security features at the link layer in congested networks is important. The insight can help in the design of robust protocols and implementations to handle attacks from intruders, and other related problems more effectively.

This thesis focused on one aspects of network security, which is the access control at link layer with respect to ABU wireless LAN. Potential problems and appropriate suggestions will be made. In this thesis we will focus on access control at the link layer, i.e., the procedure used by devices to convince the network that their packets should be forwarded.

Link-layer services may be vulnerable to a large class of denial-of-service attacks based on identity spoofing. This happens because some security services identify clients (users) using only their MAC addresses, which can be easily forged. For example, an attacker in an IEEE 802.11 network can disrupt service to well-behaved clients by spoofing their addresses or the addresses of their access points and requesting disconnection.

Our preliminary findings will be to propose that link-layer can be used to provide an effective security feature in a WLAN based on access control.

[5] Intruder (or hacker) is a person that use a computer mostly laptop to use network facility un-authorizingly.

1.6 Link-Layer Security in Local Area Networks

Local area networks (LANs) have become indispensable, the installed base for both wired and wireless LAN technologies has reached impressive numbers and it still grows at high yearly rates. Employees expect their companies to provide them with bandwidth-rich environments, mobile users expect wireless service to be available everywhere, and every new hardware generation is expected to provide faster and cheaper network devices. As with any other asset, local area networks need to be secured. In this work, we focus on access control aspects of network security.

To control access to their resources, networks need mechanisms that allow them to specify who their intended users are. Additionally, installations want their users to be accountable for their network traffic. This applies not only to enterprise installations but also to public networks such as those available in cafeterias, libraries, and airport lounges, which can also have their infrastructure used for malicious purposes.

Our work have identified a dichotomy between wired and wireless LANs with respect to these security aspects and proposes a solution that is compatible with current network architectures and consistent with current technology trends. In wired networks, proper access control can be achieved using a simple security model that leverages physical security measures. Inherent characteristics of wireless links break this simple model and that current mechanism that address this wireless security problem “incur considerable management

costs". In fact, studies suggest that security and privacy are still the main barriers to the adoption of wireless LANs (Lidl *et al.,* 1999).

1.7 Security in Wired LANS

Access control in wired networks is a less complicated problem because they are able to leverage physical security measures already deployed. Enterprises can lock their Ethernet ports inside buildings protected by keys, badges, and security personnel, physical security measures that are necessary for the protection of all company assets. Wired ports are just a subset of these assets, being reasonably protected without any additional mechanism and without increasing management costs. If a user or client has the credentials needed to walk into an office and connect his/her laptop to a wired port, most of the time there is nothing else he/she needs to do to use the network. In this case, network access control decisions are inherently based on the physical location of clients, and network security is directly related to the level of physical security implemented.

In fact, this base security level seems sufficient for most wired installations. I.e., for the purpose of access control at the link layer, most wired networks reach a level of protection considered acceptable by simply leveraging physical security measures. This way they can avoid the additional costs incurred by mechanisms such as PPPoE (Lidl *et al*., 1999).

Extra security is left to upper layers: for instance, applications can use protocols such as IPSec (Kent and Atkinson, 1998), SSL/TLS and SSH (Ylonen, and Lonvick, 2006) to create end-to-end secure tunnels and implement finer-grained access control. Once malicious

activity is detected, the network can identify the port being used and find the offending device, which may have its connection terminated or even be physically removed.

1.7.1 Challenges in Wireless Security

Enterprises see many advantages in deploying wireless LANs (WLANs), a technology that in the past few years has witnessed considerable market penetration. Compared to wired networks, WLANs incur lower installation costs per user given the reduced cabling and manual labor required. Moreover, connectivity is provided to mobile users at no extra cost, improving efficiency and productivity.

One major challenge regarding the deployment of wireless networks is dealing with the unpredictable nature of signal propagation (Ivan *et al*., 2008). While signal strength decreases with distance, the rate of decay inside a building depends on the construction materials used, floor layouts, the placement of furniture and other obstacles, as well as the number of people and their moving patterns. The resulting reflection, diffraction, and scattering of waves create environment-dependent oscillations in received signal strength, which challenge not only services such as network planning but also all others that rely on signal strength statistics.

Regarding security, one major disadvantage of wireless networks is that they violate the physical security model that is so effective in wired LANs, therefore requiring additional mechanisms to implement proper access control. Unlike the wired scenario, there is no inherent access control: wireless links extend connectivity beyond physical boundaries, making networks available in parking lots, across the street, and in nearby buildings, adjacent locations where coverage was not intended. When left unprotected, these wireless links make

networks vulnerable to misuse and attacks. It is also more difficult to make clients accountable for their acts, as misbehaving devices can move freely and be 50 meters from the access points they use. Moreover, malicious users can use directional antennas and amplifiers to produce higher signal strength levels and create many different signal strength patterns to further obfuscate their physical locations.

To make matters worse, current access control solutions are not suitable for all wireless installations: they either provide little security improvements or incur high management overhead. On one hand, there are mechanisms that are easy to deploy but that add little or no protection. For instance, installations may leave their wireless links open, hide network names (SSIDs in 802.11 jargon), or use MAC address lists. As these solutions can be easily broken by hackers, networks are still at risk of being compromised. On the other hand, there are several mechanisms that provide higher security levels and fine-grained access control capabilities, but at much higher costs to secure wireless LANS (LAN MAN Standards Committee of the IEEE Computer Society, 2004). The higher management costs come from adding and removing users, granting and revoking access rights, as well as protecting sensitive information (keys), which is vital for keeping systems uncompromised. These mechanisms also place a lot of responsibility on users, who have to choose proper passwords and keep them safeguarded. As a result of this trade-off between security and management costs, a large percentage of wireless networks still operate with insecure configurations and many of them are commonly victims of network abuse.

A world-wide wardriving effort performed in June 2004 detected over 200,000 access points, with more than 60% of them running without cryptographic protection (then using WEP) and

over 30% with the default SSID set by the manufacturer (The Official Worldwide Wardrive, 2004). In enterprise environments, insecure configurations are also common. A study performed by RSA and NetSurity in March 2005 revealed that over 30% of enterprise wireless LANs in London, Frankfurt, New York, and San Francisco lacked basic security measures (RSA Security Inc, 2005). While these configurations may be complemented by VLANs and firewalls to restrict the services available to wireless clients, networks are still left unprotected and vulnerable to misuse. Of 700 institutions that responded to the 2005 CSI/FBI Computer Crime and Security Survey, over 15% acknowledged that their wireless networks were victims of abuse during the previous year (David and Cliff, 2002). This number is clearly a lower bound, as these institutions need at least to be aware that such attacks took place and willing to share that information. Unfortunately, this situation is doomed to get worse because the number of deployed access points keeps rising at a considerable rate, allowing malicious users to find vulnerable networks with minimal efforts. According to the study by RSA, the number of access points detected in London and Frankfurt increased respectively by 62% and 66% between 2004 and 2005 (RSA Security Inc., 2005). Market research shows that WLAN unit shipments increased 39% between 2004 and 2005, with access points accounting for 81% of the wireless equipment revenue (Jorgen, *et al*., 1995). Finally, link-layer services may be vulnerable to a large class of denial-of-service attacks based on identity spoofing. This happens because despite the established session keys, these services identify clients using only their MAC addresses, which can be easily forged. For example, an attacker in an IEEE 802.11 network can disrupt service to well-behaved clients by spoofing their addresses or the addresses of their access points and requesting disconnection. Bellardo and Savage have shown that effective attacks can be easily implemented: a 10-second deauthentication attack can immediately knock a client off

the network and possibly incur minute-long outages given the interaction between 802.11 and TCP (Lidl *et al.*, 1999). These attacks can be currently implemented in 802.11 networks even if the security mechanisms proposed by the 802.11 standard are used, given that control and management frames are still transmitted without cryptographic protection such as WEP (Kent and Atkinson, 1998).

Another option would be for the attacker to use many different addresses to submit high rates of requests in order to overload the network.

In summary, if on one hand wireless LAN technology is compelling for many reasons on the other they introduce a new security paradigm that creates challenges for access control. It is clear that security problems will continue to exist unless cheaper yet effective solutions become available.

1.8 Research Motivations

For the past couple of years, increasing number of wireless local area networks (WLANs) based on the IEEE 802.11 protocols, have been deployed in various types of locations, including homes, schools, airports, business offices, government buildings, military facilities, coffee shops, book stores, as well as many other venues.

One of the primary advantages offered by WLAN is its ability to provide connectivity to portable devices, such as wireless laptops and PDAs. In some remote communities, WLANs are implemented as a viable last-mile technology (Interlink Networks, 2002), which link

homes and offices in isolated locations to the global Internet. The further widespread deployment of WLANs, however, depends on whether secure networking can be achieved.

In order for critical data and services to be delivered over WLANs, reasonable level of security must be guaranteed. The Wired Equivalent Privacy (WEP) protocol, originally proposed as the security mechanism of 802.11b WLANs, is known to be easily cracked by commonly available hacking software. Alternative security mechanisms, such as SSL, VPN, and the being-developed 802.11i protocols, provide mechanisms to enhance security in WLANs, but still not enough. In this research work we have studied the security aspects of the A.B.U WLAN, by starting with an overview of the WLAN technology and the respective vulnerabilities of various protocols, followed by a discussion of alternative security mechanisms that should be used to protect the ABU WLAN, which could also be use on other wireless LAN installation that follows thesame architectural deployment.

1.9 Objectives of the Study

a) To carry out an empirical study on wireless network security behaviour, taken ABU wireless network as the case study for appropriate data.

b) To analyze the data gotten from the study with respect to the security of the network

c) To suggest a better security mechanism and management techniques for a secured, effective and efficient communication, from the wireless network within the main

campus, and the entire University (ABU Zaria) at large putting access control in to cognizance.

1.10 Research Methodology

This research endeavor the use of an efficient, effective, and secure wireless communication in ABU Zaria by:

a) Using a laptop to which Vistumbler and CommView for WiFi is installed to access services at the APs within wireless coverage range.
b) Aircrack-ng software tool is used to analyze the data collected from the empirical study
c) A better up design and security mechanism have been suggested for enhancement of the wireless network security which suite other wireless installations.

This study requires the following processes:

a) The connecting and reading data from access points within the wireless coverage range across the entire campus, to the laptop using the CommView-for-WiFi software tool.
b) Using Aircrack-ng software tools to study the security setting for its strength or otherwise.
c) An Enhance encryption mechanism has been given with its simulated instance.

1.11 Contribution to Knowledge

The popularity of wireless LANs has exposed a significant security gap between wireless and wired networks, mainly due to how these two technologies security measures are. A current

solution that address the “wireless security” problem and that in fact provide satisfactory levels of protection incurs higher management costs.

The main achievement of our work has been to find out, and make appropriate suggestion on the approach that has a substantial increase in the costs of mounting attacks in the service area, simultaneously providing higher security than basic mechanisms and lower management costs.

1.12 Organization of the Thesis

The thesis work is structured as follows: in chapter one, we have given the general background of the study, problem definition, research motivations, objectives, research methodology, and finally contribution to knowledge.

In chapter two, we reviewed wireless LAN security of the IEEE 802.11 wireless standards and also some related literatures in the context of this work.

In the third chapter, we present an overview on the wireless LAN deployment in the campus, study the security settings and analyze it, and finally compromise the WLAN security.

In the fourth chapter, enhanced security feature/settings with relevant configuration are suggested for effective and secure communication.

In chapter five, conclusion, recommendations and future research direction has also been provided.

CHAPTER TWO: LITERATURE REVIEW

2.1 Definition of Terms

2.1.1 Base Station

It serves as service or signal provider to either client stations and/or clients (users) that are normally within the remote area (i.e. the network coverage area).

2.1.2 Client Stations

They are wireless devices that receive and transmit signal from the main-base station, to clients within the network coverage area.

2.1.3 Satellite (VSAT)

It means Very Small Aperture terminal. It is a device that provides Internet access to organizations.

2.1.4 Modem

It is a device that receives and transmit signal from the satellite to the clients and/or client stations and vice versa.

2.2 Review of Related Literature

Atheros Communication, 2004 describes security methods available today- from older protocols that have vulnerability such as the Temporal Key Integrity Protocol(TKIP), which is a modification on WEP to defend against currently known attacks (it is WEP + four patches for key mixing; message integrity; re-keying and initialization vector

protection). The paper discussed on this protocol (WEP), that provide the base line security customers demand on to the next generation security based on their research finding which they claimed it offers better performance (Atheros Communication, 2004) .

To sustain the fast deployment of IEEE 802.11 technology there is a need for protection against such low-cost, yet very effective attacks. In this work, they describe and evaluate DiscoSec, a solution against the most prominent vulnerabilities within present WLANs. A similar goal was also set within the IEEE 802.11 Task Group, which is still in proposal stages, and therefore, they implement the concept of DiscoSec as an open-source IEEE 802.11 device driver to serve as a benchmark and prototype for future developments. The rest of the paper is structured as follows. In Section 2, they discuss various security objectives influencing the design of DiscoSec. The key exchange and implementation related decisions are presented in Section 3, while Section 4 illustrates the impact of resource-depletion attacks and introduces a protection to mitigate them. In Section 5, DiscoSec was evaluated using three different hardware platforms and conduct real-world measurements to analyze the key exchange, the frame authentication, and the impact of DiscoSec on overall network throughput. Various design and implementation decisions were based on measurements using modern equipment (Ivan *et al*., 2008).

Concerning attacks based on unauthenticated management and data frames, the work demonstrate their devastating effect on IEEE 802.11 networks. Based on the same vulnerabilities, in various attacks are successfully mounted even against the new security standard IEEE 802.11. While the empirical demonstration is a frequently used method to illustrate the problem of link-layer security, protection against such attacks prevalently

remains conceptual. The authors employ two protocols, SIAP and SLAP, to establish a secure association utilizing public key infrastructure. While their solution offers encryption, it also modifies the IEEE 802.11 state machine and requires a SIAP server. In commercial products, Cisco offers a feature called Management Frame Protection (MFP), but there is regrettably no detailed information other than white papers. Interestingly, MFP does not seem to be a client-side supported feature, and thus only protects APs, while clients remain vulnerable to management frame attacks. The first solution with a design supporting the IEEE 802.11 state machine, extensively tested on performance limited hardware and available for use on present devices was introduced and it is less effective because access control is not considered (Ivan *et al*., 2007).

Wireless messaging is now a dynamic ingredient in the communication modes of our life. Many applications over the Internet now use wireless messages to contact with the end user. This paper describes the messaging infrastructure and the related protocols used in this scenario. It also presents many ways you can use the wireless networks to talk with your applications. There is also a growing concern over how much these services are secure and how they can be compromised, which are described briefly in this presentation (Mishra *et al*., 2004).

The literatures studied do not offer a real evaluation of security at the link layer taken access control in to cognizance which we have address in our work, and we finally provide an enhance security mechanism to be implemented to enhance the ABU wireless LAN security in terms of access control to the network.

2.3 The Challenge of Wireless LAN Security

Because of their flexibility, affordability, and ease of installation, the use of wireless local area networks (wireless LANS, WLANs, and WiFi) are increasing at a tremendous rate. According to In-Stat MDR estimates, there are currently more than 75 million wireless LANs in use worldwide, with 40 million more estimated to begin operation this year. META Group and In-Stat/MDR estimate that, 95% of corporate laptop computers that have been shipped in 2005 are equipped for wireless operation. An equal amount of wireless support devices, such as access points, routers, printers, scanners, and handhelds, are also being produced to meet the demand for wireless.

As wireless LAN deployments increase, so does the challenge to provide these networks with security. Wireless LANs face the same security challenges as their wired counterparts, and more. Because the medium for wireless is air, wireless LANs have the added issue of securing data that travels the airwaves. This has given momentum to a new generation of hackers who specialize in inventing and deploying innovative methods of hijacking wireless communications.

Some enterprises believe they do not have to concern themselves with wireless security if they run non-mission-critical systems with non-sensitive information on their wireless LANs. This can be a costly mistake, since most enterprise wireless LANs connect back to a wired network at some point. Hackers can use a user laptop as an entry point into the entire enterprise network!

2.4 Risks and Vulnerabilities of Wireless LANS

Along with the many conveniences and cost-saving advantages to wireless LANs, there are also some inherent risks and vulnerabilities.

2.4.1 The Nature of the Wireless Medium

Traditional wired networks use cables to transfer information, which are protected by the buildings that enclose them. To access a wired network, a hacker must bypass the physical security of the building or breach the firewall.

On the other hand, wireless networks use the air, which is an uncontrolled medium. Wireless LAN signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls.

Additionally, since the WLAN medium is airwaves, it is a shared medium that allows anyone in proximity to "sniff" the traffic. The risks of using a shared medium is increasing with the advent of readily-available "hacker's tools." A variety of specialized tools and tool kits enable hackers to "sniff" data and applications, and to break both the encryption and authentication of wireless data.

2.4.2 Insecure Wireless LAN Devices

Insecure wireless LAN devices, such as access points and user stations, can seriously compromise both the wireless network and the wired network, making them popular targets for hackers.

2.4.3 Insecure Access Points

Access points can be insecure, due to improper configurations and design flaws. Access points shipped with default configurations that are insecure. They are pre-configured with a default password; they broadcast service set identifiers (SSIDs); and they often require no encryption or authentication. If deployed with default settings, they become gateways that hackers use to access both the wireless and the wired network.

Intruders (hackers) can convert laptops into "soft" access points (APs) by either using a variety of software programs, such as HostAP, Hotspotter, or Airsnark, or, by simply using a USB wireless adapter. Using soft APs, a hacker can cause a legitimate user to connect to the hacker's own laptop, compromising that user's machine.

2.4.4 Insecure User Stations

Insecure wireless user stations such as laptops or bar code scanners pose even a greater risk to the security of the enterprise network than insecure access points. The default configuration of these devices offer little security and can be easily misconfigured. Intruders can use any insecure wireless station as a launch pad to breach the network. Below is a diagrammatical representation of some attacks usually done by a network hacker.

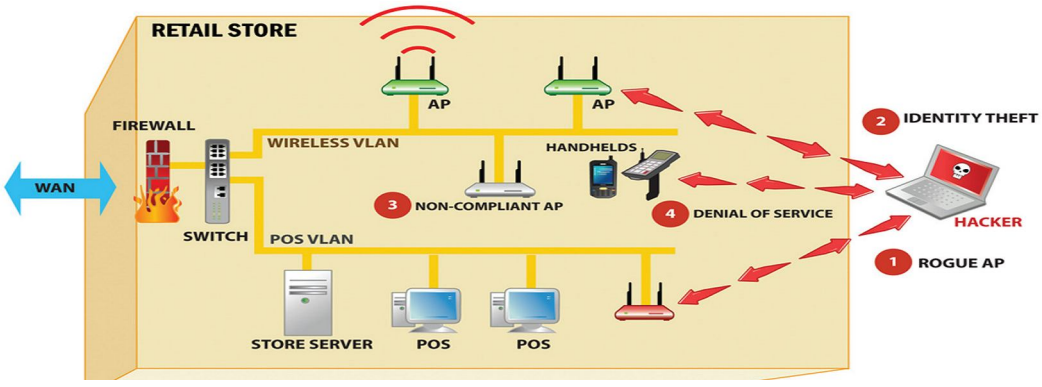

Fig. 2.1 A common wireless LAN security risks (Pierre, 2001)

2.5 IEEE 802.11 Security Features

The security features provided in 802.11 standards (John *et al*., 2001) are as follows:

2.5.1 Service Set Identifier (SSID)

SSID acts as a WLAN identifier. Thus all devices trying to connect to a particular WLAN must be configured with the same SSID. It is added to the header of each packet sent over the WLAN (i.e. a BSS) and verified by an Access Point. A client device cannot communicate with an Access Point unless it is configured with the same SSID as the Access Point.

2.5.2 Wired Equivalent Privacy (WEP)

According to the 802.11 standards, Wired Equivalent Privacy (WEP) was intended to provide "confidentiality[6] that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy" (Interlink Networks, 2002).

IEEE specifications for wired LANs do not include data encryption as a requirement. This is because approximately all of these LANs are secured by physical means such as walled structures and controlled entrance to building etc. However no such physical boundaries can be provided in case of WLANs thus justifying the need for an encryption mechanism.

WEP provides for Symmetric Encryption using the WEP key. Each node has to be manually configured with the same WEP key. The sending station encrypts the message using the WEP key while the receiving station decrypts the message using the same WEP key. WEP uses the RC4 stream cipher, which is an encryption algorithm based on modulo arithmetic.

[6] Confidentiality here means instead of port connection of a client in wired network, in wireless WEP enable channel assignment which in some extent leverage physical security.

2.5.3 MAC Address Filters

In this case, the Access Point is configured to accept association and connection requests from only those nodes whose MAC addresses are registered with the Access Point. This scheme provides an additional security layer.

2.6 Intrusion Methods Used By Hackers

2.6.1 Invasion & Resource Stealing

Resources of a network can be various devices like printers, Internet access and so on. First the attacker will try to determine the access parameters for that particular network. For example if network uses MAC Address based filtering of clients, all an intruder has to do is to determine MAC address and assigned IP address for a particular client. The intruder will wait till that valid client goes off the network and then he starts using the network and its resources while appearing as a valid user.

2.6.2 Traffic Redirection

An intruder can change the route of the traffic and thus packets destined for a particular computer can be redirected to the attacking station. For example ARP tables (which contain MAC Address to IP Address Mapping) in switches of a wired network can be manipulated in such a way that packets for a particular wired station can be re-routed to the attacking station.

2.6.3 Denial of Service (DOS)

Two types of DOS attacks against a WLAN can exist. In the first case, the intruder tries to bring the network to its knees by causing excessive interference. An example could be excessive radio interference caused by 2.4 GHz cordless phones or other wireless devices

operating at 2.4GHz frequency. A more focused DOS attack would be when an attacking station sends 802.11 dissociate message to the target station and effectively disconnects it.

2.6.4 Rouge Access Point (Fake AP)

A rogue Access Point is one that is installed by an attacker (usually in public areas like shared office space, airports, Universities and so on) to accept traffic from wireless clients to whom it appears as a valid Authenticator. Packets thus captured can be used to extract sensitive information or can be used for further attacks before finally being re-inserted into the proper network.

2.7 Security Concerns on IEEE 802.11 Network (Interlink Networks, 2002)

2.7.1 MAC Addresses Authentication

Such sort of authentication establishes the identity of the physical machine, not its human user. Thus an attacker who manages to steal a laptop with a registered MAC address will appear to the network as a legitimate user.

2.7.2 One-Way Authentication

WEP authentication is client centered or one-way only. This means that the client has to prove its identity to the Access Point but not vice versa. Thus a rogue Access Point will successfully authenticate the client station and then subsequently will be able to capture all the packets send by that station through it.

2.7.3 Static WEP-Keys

There is no concept of dynamic or per-session WEP keys in 802.11 network specification. Moreover the same WEP key has to be manually entered at all the stations in the WLAN.

2.7.4 Service Set Identifier (SSID)

Since SSID is usually provided in the message header and is transmitted in clear text format, it provides very little security. It is more of a network identifier than a security feature.

2.7.5 WEP Key Vulnerability

WEP key based encryption was included to provide same level of data confidentiality in wireless networks as exists in typical wired networks. However a lot of concerns were raised later regarding the usefulness of WEP. The IEEE 802.11 design community blames 40-bit RC4 keys for this and recommends using 104- or 128-bit RC4 keys instead. Although using larger key size does increase the work of an intruder, it does not provide completely secure solution. Many recent research results have proved this notion (Jesse, 2000). According to these research publications the vulnerability of WEP roots from its initialization vector and not from its smaller key size

CHAPTER THREE:

AN EMPERICAL STUDY OF ABUWIRELESS NETWORK

3.1 Introduction

The popularity of wireless LANs has exposed a significant security gap between wireless and wired networks, mainly due to how these two technologies leverage link layer security measures.

In order to have an effective study of the wireless security of the ABU wireless local area network we start with an over view of the WLAN technology and the respective vulnerabilities of various protocols, followed by a discussion of alternative security mechanisms that should be used to protect the ABU WLAN, which also suite other installations.

3.2 IEEE802.11 Standard Used By ABU WLAN

IEEE 802.11 standard used by ABU WLAN are as follows:

3.2.1 IEEE 802.11 a

It is used mainly for digital centers within some faculties in the university. We have 12 of them out of which 10 are deployed in the main campus and the remaining two in the Kongo campus of the university. It has frequency of 5.0 GHz and runs at 54 mbps.

3.2.2 IEEE 802.11 b | g

These two standards are used for the one backbone and the three base stations of the network. The same configuration has been used to configure the client stations within each base station of the network. They both have frequency of 2.4 GHz. The major distinction between IEEE 802.11 g and IEEE 802.11 b is that IEEE 802.11 g runs at 54 mbps while IEEE 802.11 b runs at 11 mbps.

3.2.3 IEEE 802.11 b | g versus IEEE 802.11a

IEEE 802.11 g is among the latest WLAN standard in the WiFi category It has a frequency of 2.4GHz as the IEEE 802.11b and it is also backward-compatible[7] with IEEE 802.11b, and not backward compatible with IEEE 802.11a. It covers far distance and it is effective and efficient, only that it has same data rate with IEEE 802.11a. The major distinction between IEEE 802.11g and IEEE 802.11a is the technology behind them.

Security feature used by these IEEE 802.11 a | b | g wireless standard are the same which are the following: Wired Equivalence Privacy (WEP), MAC address base filtering, Service Set Identifier (SSID), etc.

3.3 ABU Wireless LAN Deployment

The following are some features of the ABU wireless local area network:

a) There exist base station and client stations across the campus

b) All the client stations transmit signal across for Internet access

c) Client stations are normally connected to a switch within a building (department)

[7] Backward-compatible here means network devices configured with IEEE802.11b can be connected to a network configured with IEEE802.11g and vice versa.

d) Computers (clients) are connected to the switch using Ethernet cable for Internet access (wired connection). Or APs are connected to the switch for wireless signal transmission within the building.

e) There could be one or more access points within a building depending on the availability of signal for Internet access.

3.3.1 ABU-Zaria Wireless Network Layout

There is one backbone (main base station) and other 3 base stations for the University wireless LAN deployment, so as to provide effective signal transmission across the campus.

Samaru base station (at senate building) is the main backbone or base station via which all the other three base stations are connected. This station receives signal from the main service provider's satellite and channelized it appropriately.

It serves as signal transmitter to the other 3 base stations, which are the Senate WEST base station, Senate EAST base station, and Senate NORTH base station. These base stations connect a number of client stations across departments and other buildings, which in return connects clients to the network via AP wirelessly.

3.3.2 Senate West Base Station

This base station connects the following client stations in the campus, which are; Shika, Doctors resident, Mathematics Department, Electrical engineering, Mechanical engineering, IAR, BIOTECH, Wired connection to SAFE HOSTEL, Sickbay(UHS), Akenzua hall, Medicine, Suleiman hall, Amina hall.

Water resources engineering (new engine) is a newly installed client station that connects Metallurgical engineering and Textile science department using wired connection. The deployment of the Senate WEST base station and its client stations are as shown in Fig. 3.1.

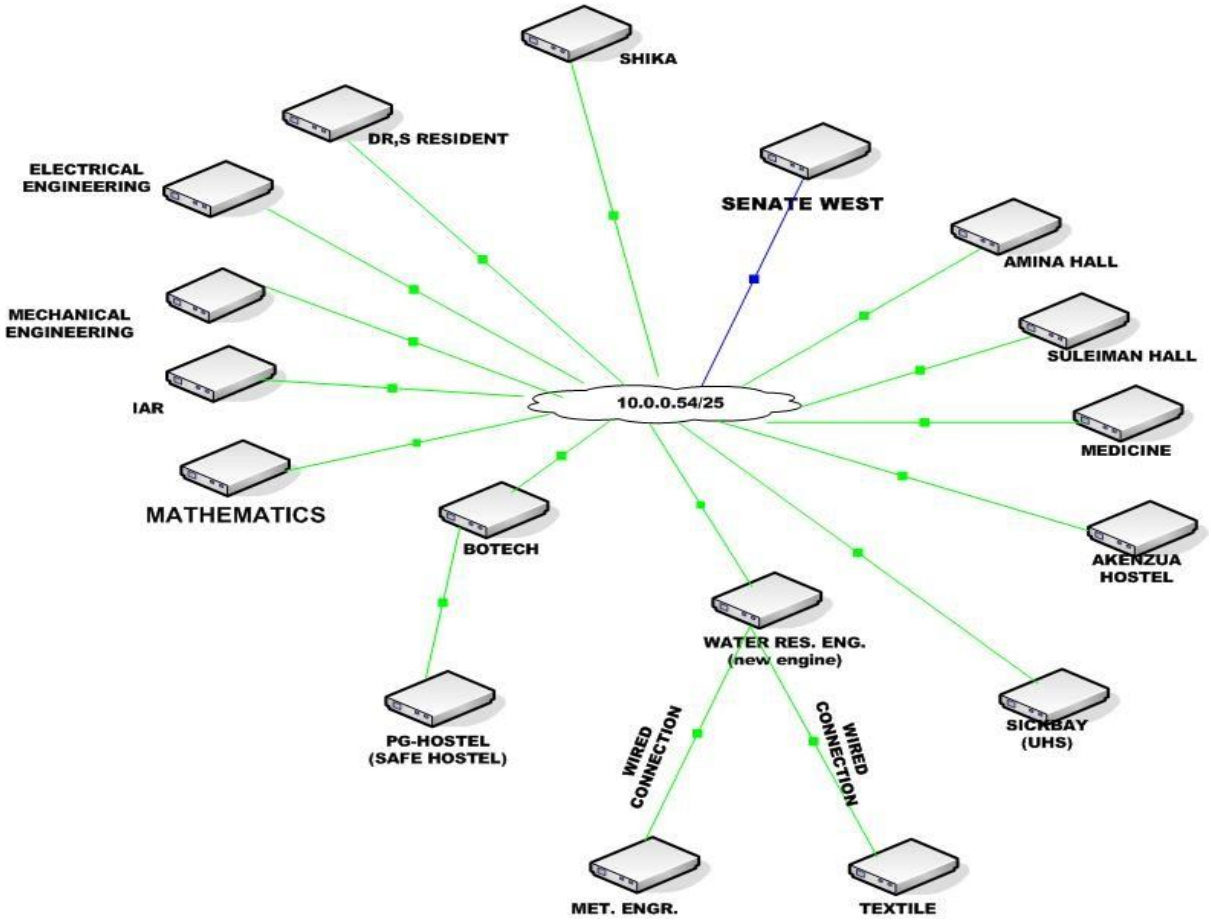

Fig. 3.1 Senate WEST base station

3.3.3 Senate East Base Station

This base station connects the following client stations in the campus, which are; IDR, ALEX hall, RIBADU hall, Pharmacy, CERT, Development Office, Abdullahi Smith, IACC, ICSA/RAMAT, Chemistry, Estate Department, and DAC.

Economics connects Political Science department using wired connection. The deployment of the Senate EAST base station and its client stations are as shown in Fig. 3.2.

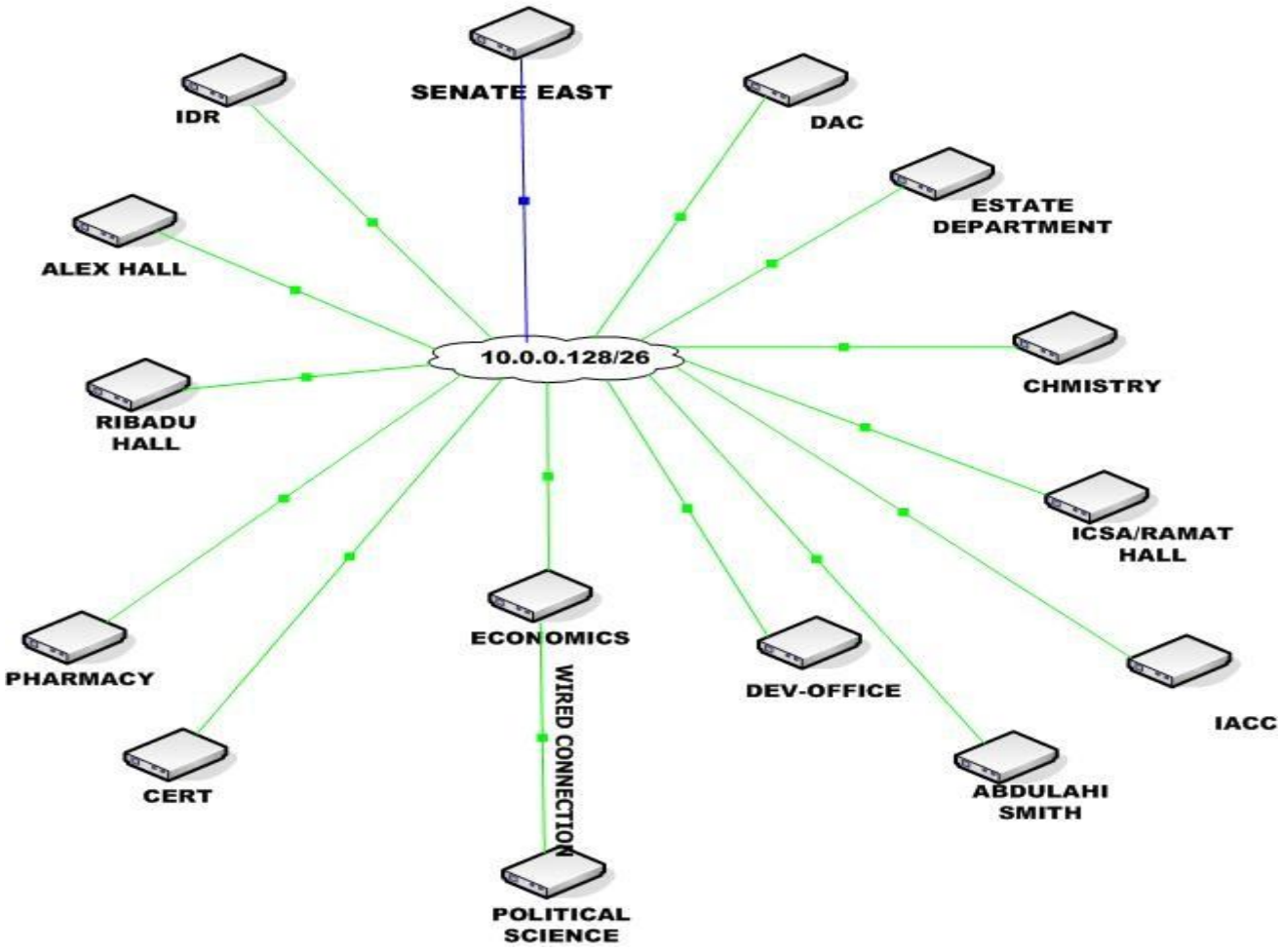

Fig. 3.2 Senate EAST base station

3.3.4 Senate North Base Station

This base station connects the following client stations in the campus, which are; BOOKSHOP, HNISS, and KONGO-BASE which this connects accounting, law, business, and hostels departments

Some Department have digital centers which are political science, biology and vet medicine**,** while some department are connected using wired connection from CISCO, which are geology, geography, and physics. The deployment of the Senate NORTH base station and its client stations are as shown in Fig 3.3.

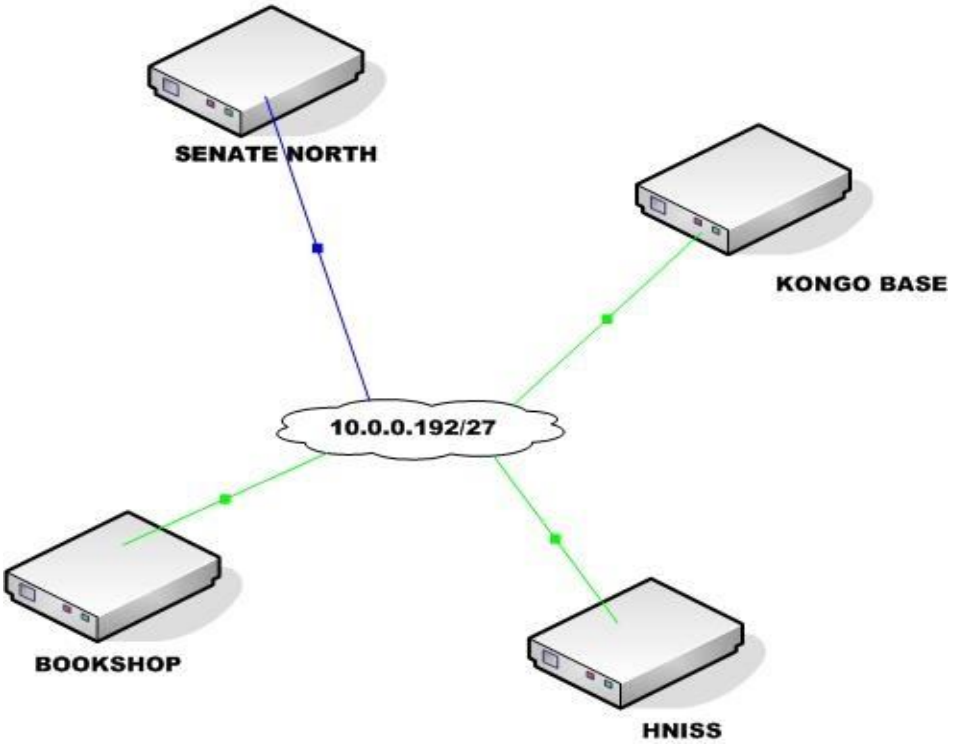

Fig. 3.3 Senate NORTH base station

3.4 Signal Flow across the Network for Internet Access

3.4.1 Main Base – Station

This base station serves as the backbone of Internet access in the University. It connects the core router which is a wireless router that receives and transmit signal from the satellite and modem at the senate and pass it to the core switch for Internet access.

The core switch receives and transmit signal to the three base stations from the router. It connects the three base stations as senate WEST, senate EAST and senate NORTH respectively.

3.4.2 General Over View of Signal Flow on the Network

Intel Sat 10

It is the service provider's satellite that transmit signal to the satellite and modem at senate.

Satellite and Modem at senate

Receive Signal from the main satellite and transmit it to CORE Router which in turns connects the core switch for signal flow to other devices on the network.

Core Switch

It connects all the 3 BASE stations to the main network via the core router. It receives signal from the router and transmit to the 3 base stations as senate EAST base-station, senate WEST base-station, and senate NORTH base-station. Client stations are linked or connected to all the 3 base stations. The client stations transmit signals to APs which are indoors within

departments which in return transmit wireless signal to clients (users) within a building for Internet access.

In summary, access of a signal from a user (client) point of view can be considered as a thing that happen on a sub-level which is as follows:

Client Station receive signal from the main base station at senate and transmit it to departmental access points which can be one or more within a department depending on signal strength within that building.

APs within the department(s) now transmit the signal they received from the client station to the clients (user) that are within that remote area of coverage.

Clients (user) now enjoy the signal for Internet access base on fulfilling the requirements or credentials for allowing access to the network.

The general signal flow on the network is as presented in the Fig. 3.4.

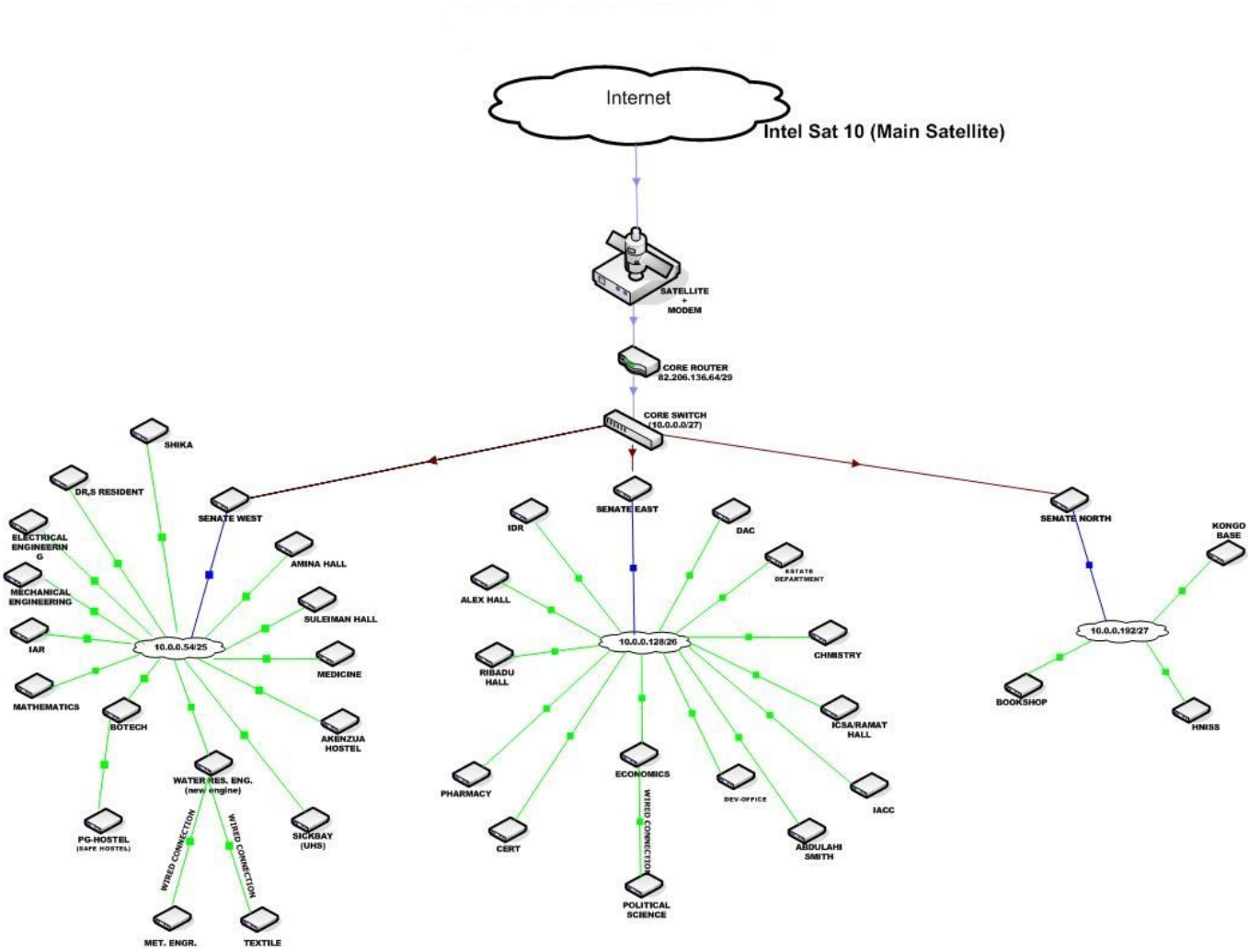

Fig. 3.4. General Overview of ABU Zaria Wireless LAN[8]

[8] Figure 3.1, 3.2, 3.3 and 3.4 are courtesy of micros access company that gives a Picturial representation of the wireless deployment in the organization

3.5 ABU WLAN Network Security

The network security comes in two forms as follows:

3.5.1 Security at Application Level

It is the one in which all the access points are not secured, but rather, the security is at the server level with the help of a software tool that grant or reject request from clients (users) wanting to connect to the network.

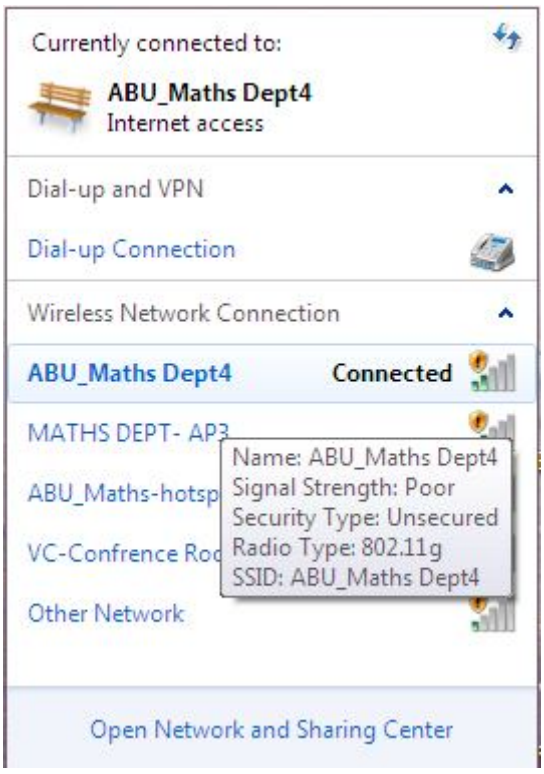

Fig. 3.5 Another way to know whether an access point is secured or not

The security at the application level is normally seen in form of web page when trying to access the network for Internet access or any other thing at all. It is called hotspot security as it only warrants clients to have IP address.

This kind of security is vulnerable to attack by web hackers, or could crash to generate high sense of denial of service attack on the network.

3.5.2 Security at the Network Level

Using a Vistumbler and CommView for WiFi we found that the secured access points for fiber-optics project are configured with WEP encryption which is the security at network level. As shown in the diagram below;

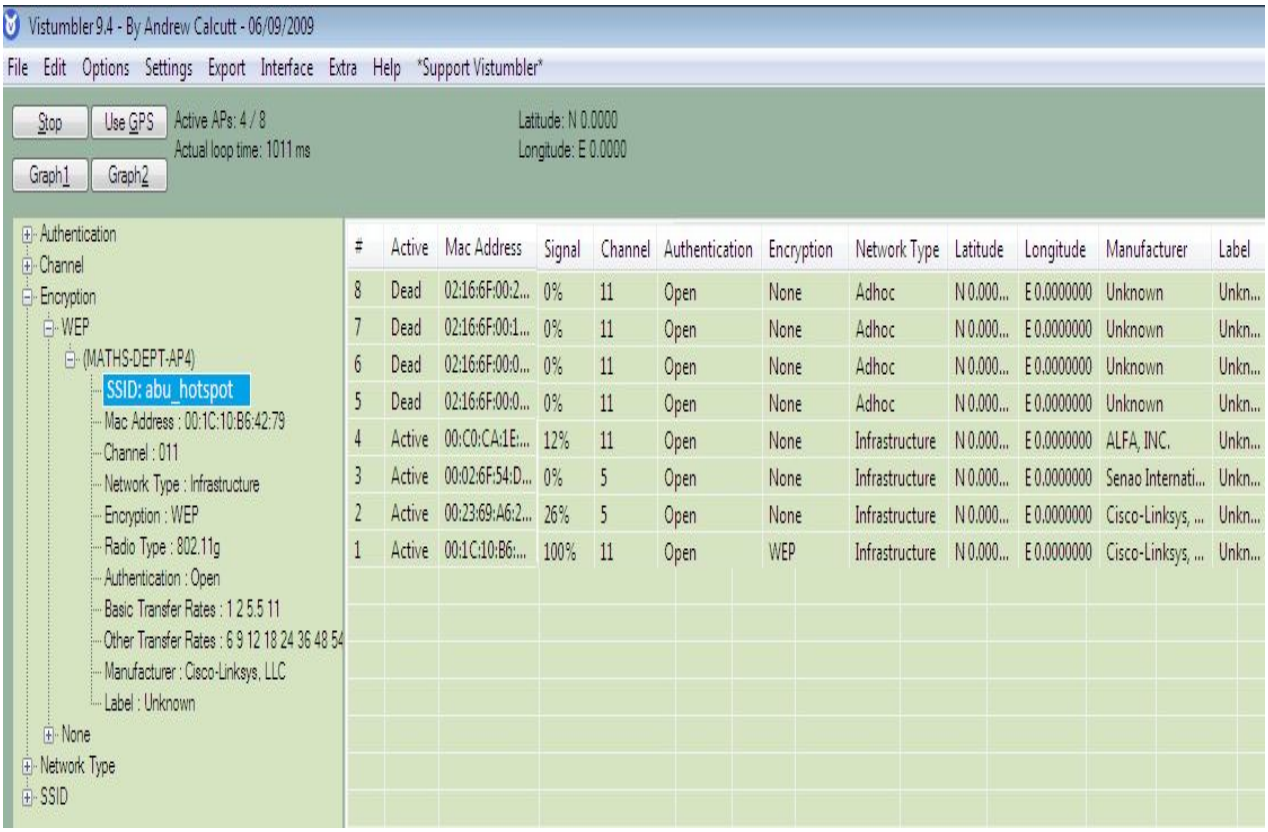

Fig. 3.6 Sample Capture (Scan) using Vistumbler

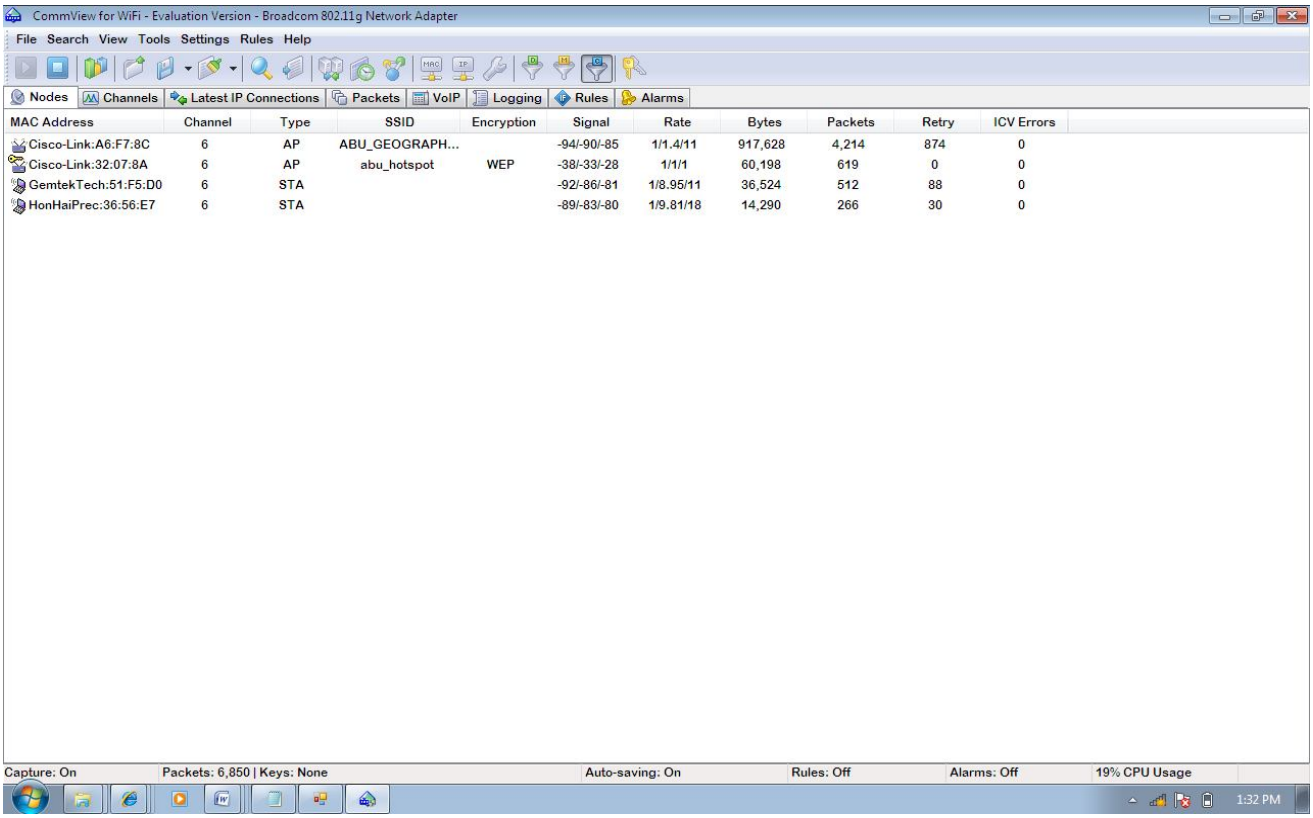

Fig. 3.7 Sample nodes during the scan using CommView for WiFi

Implementation problems with the WEP encryption scheme revolved around the initialization vector (IV) field of the scheme, a random number concatenated with the network key, used to provide some randomization to the scheme. WEP is based on the RC4 stream cipher algorithm, and as with any stream cipher, identical keys must not be used. The IVs change with each packet and eventually repeat, giving an attacker two packets with identical IVs. The counter used for IVs was 24 bits long, which on a fairly busy network meant that there was a good chance that after 5,000 packets, an IV would be repeated, yielding an IV collision where two packets were encrypted with the same key, thus providing a basis for cryptanalysis. If more collisions are encountered, this increases the chances of an attack (Interlink Networks, 2002).

3.6 Compromising the Network Security (Hacking)

It deals with overcoming the network security for further attacks and or actions on the network.

3.6.1 Software Tool for the Hacking

To hack the network for security threat, we use two software tools, namely CommView for WiFi and aircrack-ng.

3.6.2 Commview for Wi-Fi

CommView for WiFi is a special edition of CommView designed for capturing and analyzing network packets on wireless 802.11a/b/g networks. CommView for WiFi gathers information from the wireless adapter and decodes the analyzed data.

With CommView for WiFi you can see the list of network connections and vital IP statistics and examine individual packets. Packets can be decrypted utilizing user-defined WEP keys and are decoded down to the lowest layer, with full analysis of the most widespread protocols. Full access to raw data is also provided. Captured packets can be saved to log files for future analysis. A flexible system of filters makes it possible to drop unnecessary packets or capture the essential packets. Configurable alarms can notify the user about important events such as suspicious packets, high bandwidth utilization, or unknown addresses. CommView for WiFi includes a VoIP module for in-depth analysis, recording, and playback of SIP and H.323 voice communications. CommView for WiFi features full decoding of the following protocols: ARP, BCAST, BGP, BMP, CDP, DAYTIME, DDNS, DHCP, DIAG, DNS, EIGRP, FTP, G.723, GRE, H.225, H.261, H.263, H.323, HTTP, HTTPS, ICMP, ICQ, IGMP, IGRP, IMAP, IPsec, IPv4, IPv6,

IPX, HSRP, LDAP, MS SQL, NCP, NDS, NetBIOS, NFS, NLSP, NNTP, NTP, OSPF, POP3, PPP, PPPoE, RARP, RDP, RIP, RIPX, RMCP, RPC, RSVP, RTP, RTCP, RTSP, SAP, SER, SIP, SMB, SMTP, SNA, SNMP, SNTP, SOCKS, SPX, SSH, TCP, TELNET, TFTP, TIME, TLS, UDP, VTP, **WEP**,WDOG,YMSG,802.1Q.

CommView for WiFi is a helpful tool for WLAN administrators, security professionals, network programmers, or anyone who wants to see the full picture of their WLAN traffic.

3.6.3 Aircrack-ng

Aircrack-ng is an 802.11 WEP key cracking program aimed at revealing the secret word for a given wireless LAN configuration. It works hand in hand with the CommView for WiFi.

3.7 Steps for a Successful Hacking

To compromise the network security, we run CommView as shown below to scan for access points within the range.

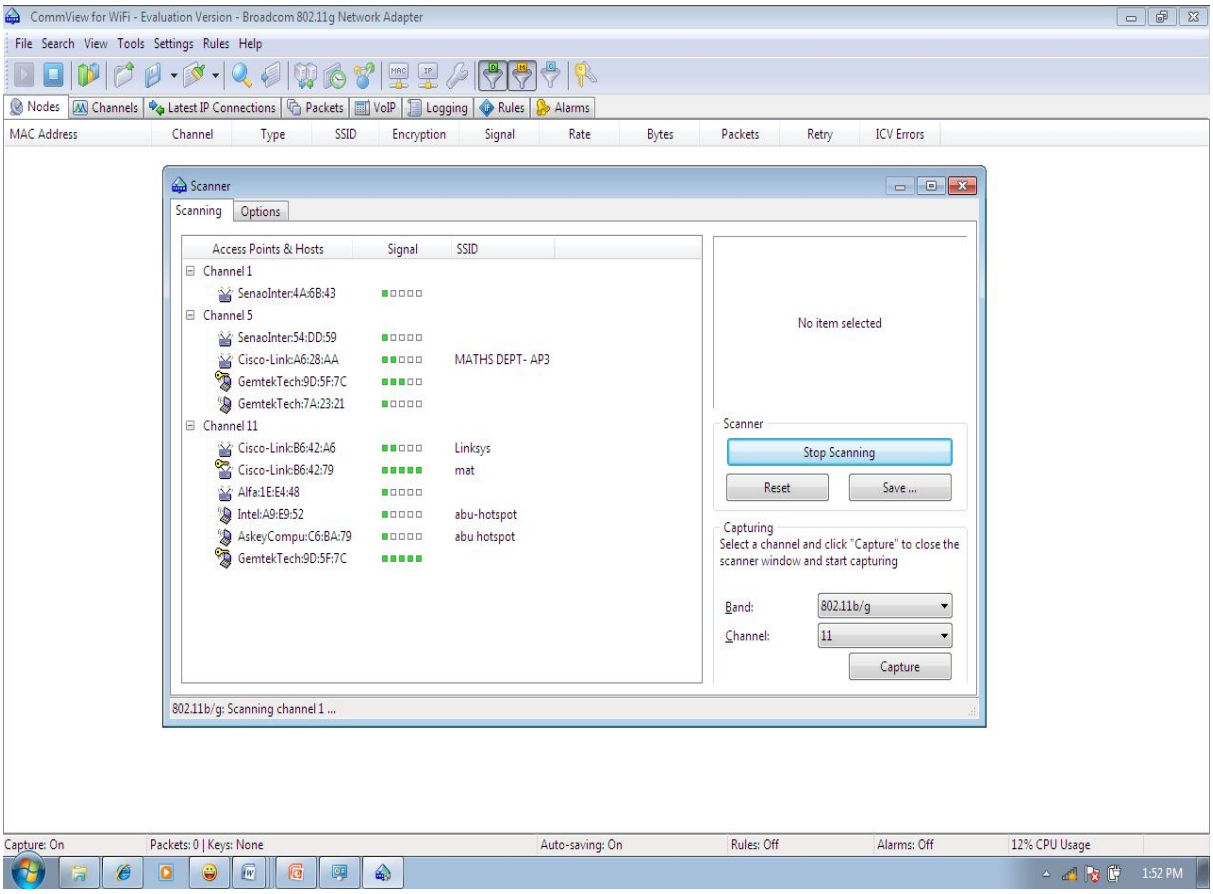

Fig. 3.8 Some APs scanned within the range, with some indicating key as their encryption form

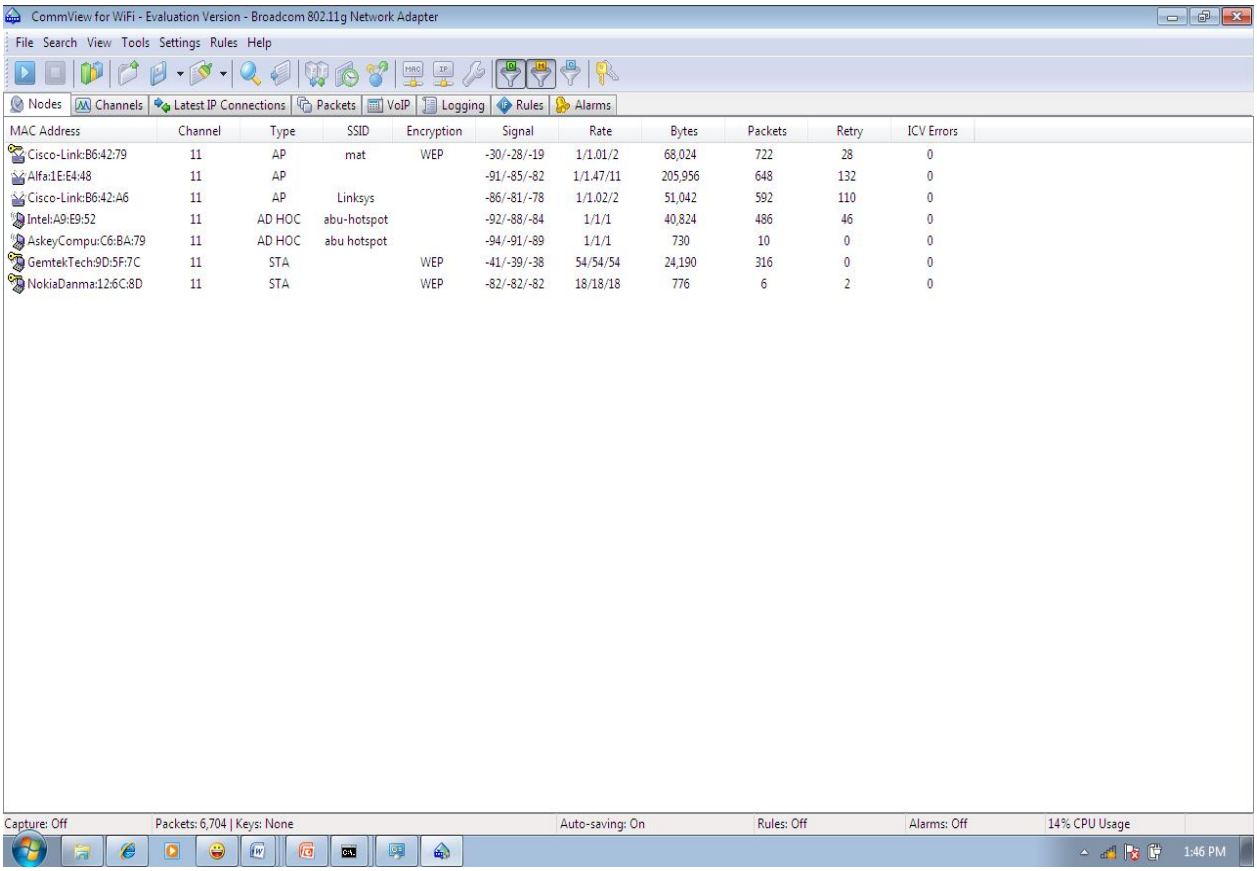

Fig. 3.9 Some nodes (APs) within the range indicating WEP encryption

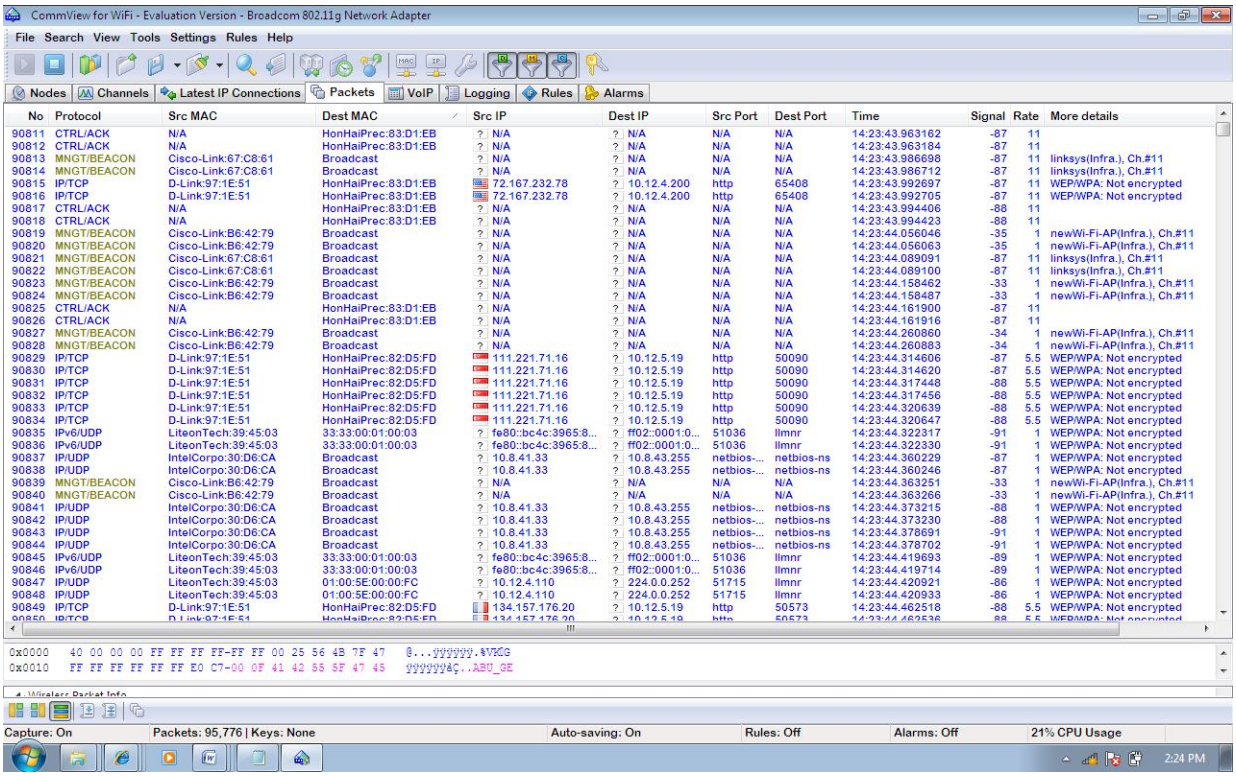

Fig. 3.10 Sample packets capture from the network for analysis

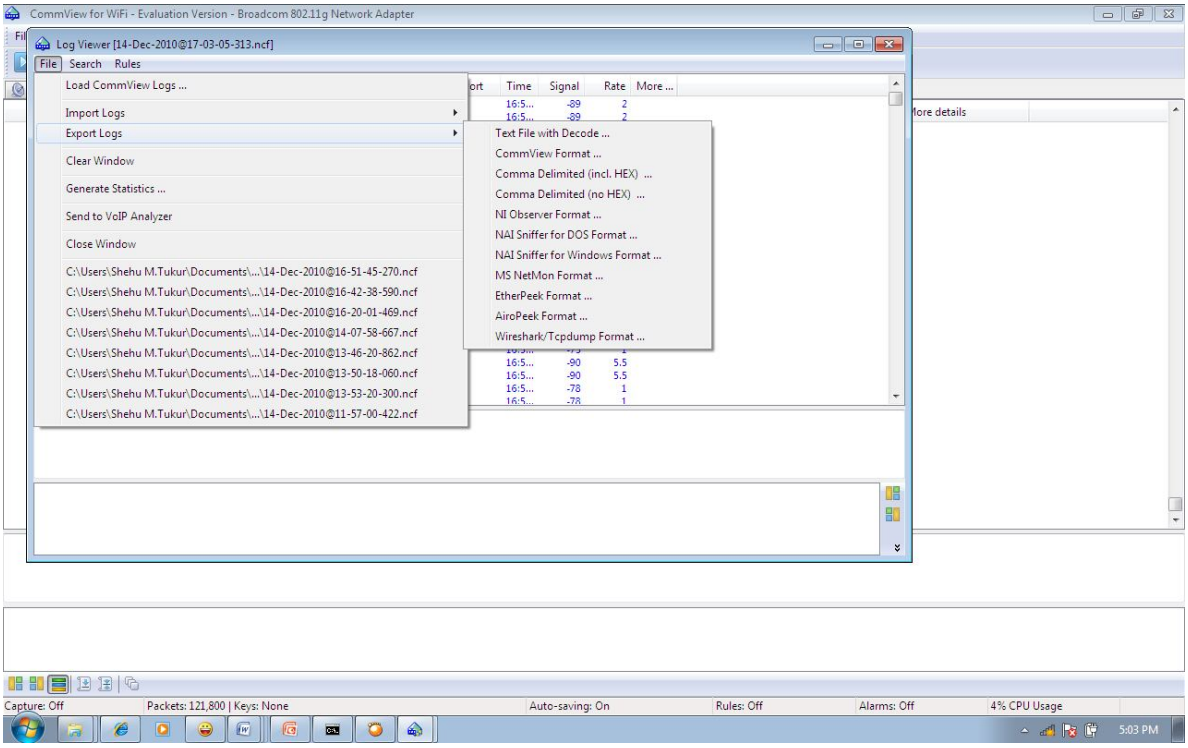

Fig.3.11 Converting sample capture (Log file) to "* .cap" format for WEP decryption

3.8 Resulting Hacking on the Network

To hack or compromise the network security we launch the aircrack-ng application with the *.cap file version of the log file resulting from the packet capture during the scan. After which we specify the key length as below for a successful decryption.

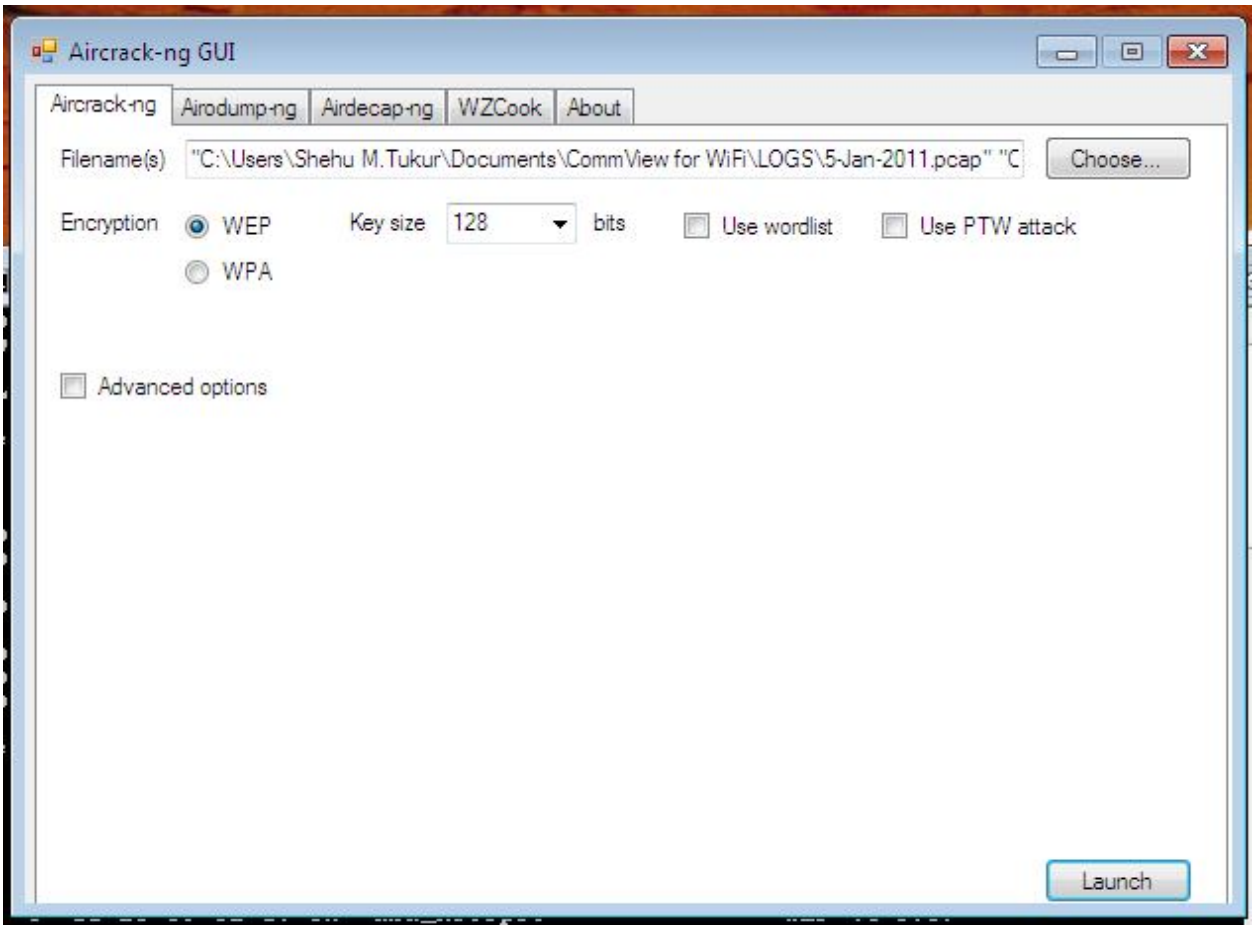

Fig.3.12 Lunching aircrack-ng and calling the .cap file from it for decryption.

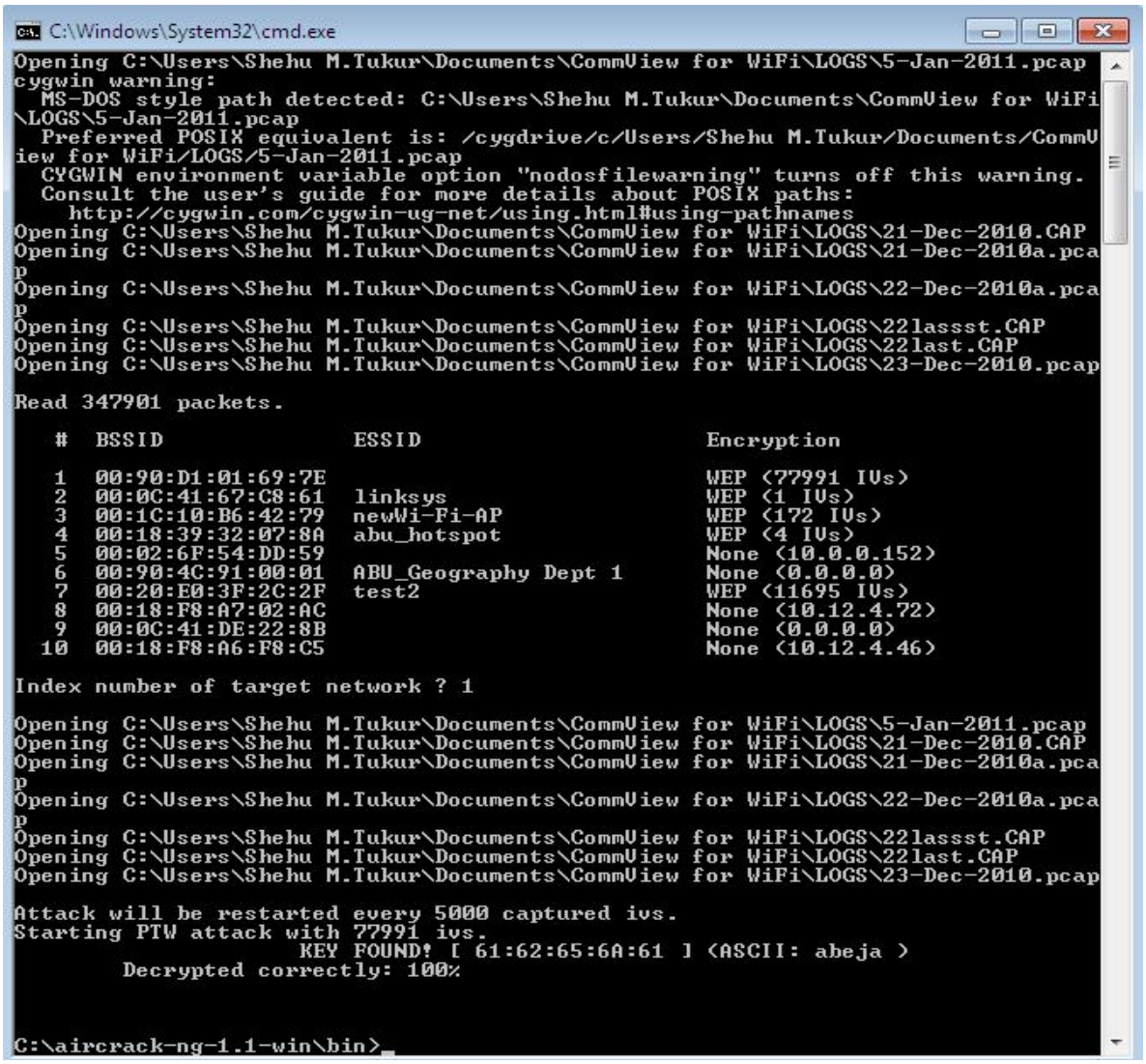

Fig. 3.13 successful decryption result from aircrack-ng software tool

Finally, the resulting attack reveals 61:62:65:6A:61 as the WEP key for one of the encrypted AP in the range. By exposing the encryption key of the network, an intruder could launch different types of attack on the network. This could be one of those attacks an intruder can lunch on an IEEE 802.11 wireless network as described in chapter 2 of this research work, which could either be setting of Fake AP for client to connect through for viewing client's data/message for bridging security or denial of service attack for insufficient Internet access.

CHAPTER FOUR: ANALYSIS AND DISCUSSION OF OUR PROPOSED SECURITY MECHANISM

4.1 Wi-Fi Protected Access 2 (WPA2)

4.2 Introduction

By 2001, a series of independent studies from various academic and commercial institutions had identified weaknesses in Wired Equivalent Privacy (WEP), the original native security mechanism for wireless local area networks (WLANs) in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification. These studies showed that, even with WEP enabled, an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to the wireless network via the WLAN (Wi-Fi Group, 2003).

This fact has further been proven by us in this our research work, simply via the use of two software tools as: CommView for Wi-Fi to capture encrypted packets for analysis, and aircrack-ng for cracking the WEP encryption found in some access points (APs) within the network environment in the campus. As a result, enterprises found it necessary to supplement WEP with third-party security solutions such as VPN, IEEE 802.1X authentication services servers, or add-on proprietary technologies (Paul, 2006).

To address this situation, Wi-Fi Alliance introduced 2 new interoperable Wi-Fi security specifications for both enterprise and home networks.

In 2003, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA) as a strong, standards-based interoperable Wi-Fi security specification. WPA provides assurance to enterprises, small businesses and home users that their data will remain protected and that only authorized users may access their networks. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption (Wi-Fi Alliance, 2003).

In 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), the second generation of WPA security. Like WPA, WPA2 provides enterprise and home Wi-Fi users with a high level of assurance that their data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance (Paul, 2006).

4.3 Components Overview for WPA and WPA2 Implementations

This section provides a general description and overview of Wi-Fi Protected Access 2 (WPA2), launched in September 2004. It describes its features and benefits, identifies the differences between Enterprise and Personal Wi-Fi certified products, and explains how WPA2 provide protection from network attacks. Special attention is given to the components needed to build a wireless environment in the enterprise. This section also discusses transitioning enterprises from WPA to WPA2. WPA2 are not automatically enabled in the default configuration of new wireless access points (APs) and client devices. They must be configured when the products are installed.

4.4 WPA2 Features and Benefits

4.4.1 WPA

WPA addresses all known vulnerabilities in WEP, the original, less secure 40 or 104-bit encryption scheme in the IEEE 802.11 standard. WPA also provides user authentication, since WEP lacks any means of authentication. Designed to secure present and future versions of IEEE 802.11 devices, WPA is a subset of the IEEE 802.11i specification.

WPA replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology.

WPA was designed and has been scrutinized by well-known cryptographers. It can be implemented immediately and inexpensively as a software or firmware upgrade to most existing Wi-Fi certified access points and client devices with minimal degradation in network performance. WPA offers standards-based, Wi-Fi certified security. It assures users that the Wi-Fi certified devices they buy will be cross-vendor compatible.

When properly installed, WPA provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1X authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

4.4.2 WPA2

WPA2 was launched in September 2004 by the Wi-Fi Alliance; WPA2 is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES).

AES satisfies U.S. government security requirements. It has been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). Organizations that require the AES encryption available in WPA2 should be aware that upgrading to it may require new hardware.

4.5 Enterprise and Personal Modes for WPA2

There are 2 modes of WPA2 certification—Enterprise and Personal as shown in the table 4.1, which provides an authentication and encryption solution. All Wi-Fi certified devices are certified as WPA-Personal by default. Vendors can request additional WPA2-Personal, WPA-Enterprise or WPA2-Enterprise certification (Paul, 2006).

Table 4.1 WPA2-Enterprise certification

	WPA2
Enterprise Mode (Business and Government)	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal Mode (SOHO/personal)	Authentication: PSK Encryption: AES-CCMP

4.5.1 WPA AND WPA2 Enterprise Mode

Enterprise mode operates in a managed mode to meet the rigorous requirements of enterprise security. It leverages the IEEE 802.1X authentication framework which uses an Extensible Authentication Protocol (EAP) type with an authentication server to provide strong mutual authentication between the client and authentication server via the access point.

In this mode, each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP encryption is used. TKIP employs an encryption cipher that issues encryption keys for each data packet communicated in each session of each user, making the encryption code extremely difficult to break. For WPA2, AES encryption is used. AES is stronger than TKIP, thus providing additional network protection.

4.5.2 WPA AND WPA2 Personal Mode

Personal Mode is designed for home and small office/home office (SOHO) users who do not have authentication servers available. It operates in an unmanaged mode that uses a pre-shared key (PSK) for authentication instead of IEEE 802.1X. This mode uses applied authentication in which a pass-phrase (the PSK) is manually entered on the access point to generate the encryption key. Consequently, it does not scale well in the enterprise. The PSK is typically shared among users. A PSK of sufficient strength—one that uses a mix of letters, numbers and non-alphanumeric characters—is recommended.

Personal Mode uses the same encryption methods as Enterprise Mode. It supports per-user, per-session, per-packet encryption via TKIP with WPA or AES with WPA2.

4.6 Protection from Network Attacks with WPA2

WPA2 protect the wireless network from a variety of threats, including lost or stolen devices (Resource stealing) and hacker attacks such as 'man-in-the-middle', authentication forging, replay, key collision, weak keys, packet forging, and 'brute-force/dictionary' attacks.

WPA2 addresses the weaknesses of original WEP security resulting from WEP's imperfect encryption key implementation and its lack of authentication. Using TKIP, it brings an enhanced encryption algorithm and with IEEE 802.1X/EAP authentication it brings standards-based mutual authentication to Wi-Fi networks. Together, TKIP encryption and mutual authentication insulate the Wi-Fi network from a variety of threats when WPA-Enterprise mode is used.

WPA2 offers advanced protection from wireless network attacks. Using AES, government grade encryption and IEEE 802.1X/EAP authentication WPA2 provides stronger standards-based mutual authentication and advanced encryption to protect the Wi-Fi network from a variety of threats and attacks.

4.7 Enterprise Mode Components for a Secure Environment

Enterprise authentication authorizes users' access to the network on a per-user basis. An authentication deployment confirms user identity and determines the rights for each user. There are 6 components to authentication in an enterprise deployment for either WPA2 as shown in Fig. 4.1.

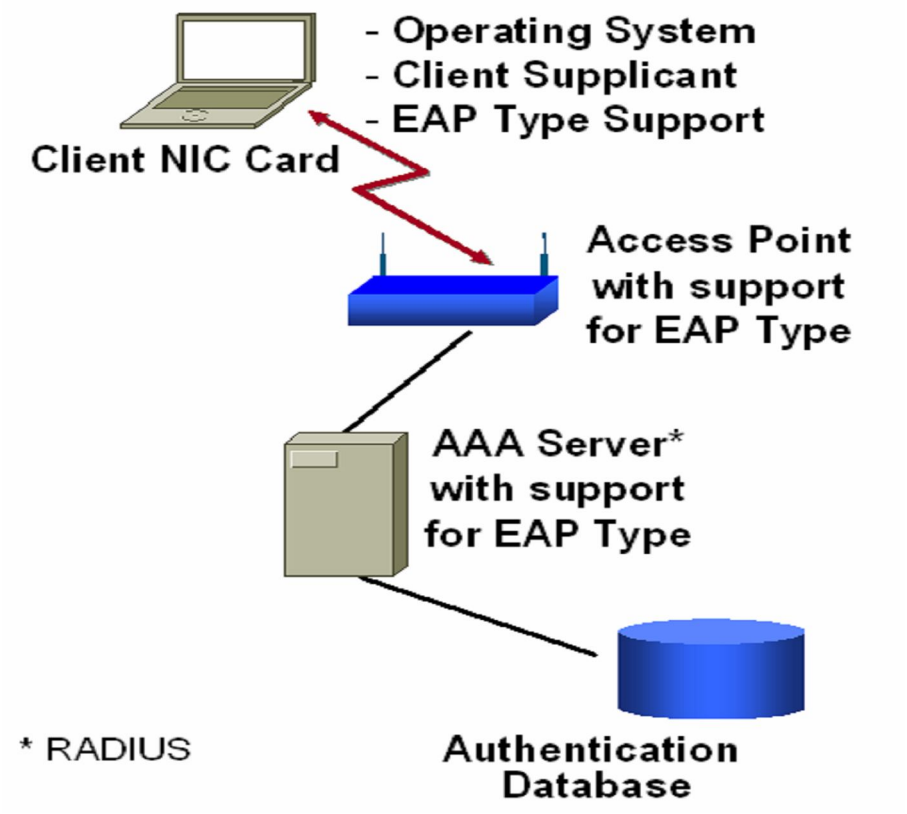

Fig. 4.1 WPA and WPA2 Components

They include the following:

a. Client devices that are WPA2-Enterprise Wi-Fi certified

b. Client supplicant

c. EAP type

d. APs that are WPA2-Enterprise Wi-Fi certified

e. Authentication server (AAA Server[9])

f. Authentication database

All of these components are required. The individual components are discussed below.

4.7.1 Client Adapter (NIC)

Client workstations will require the installation of new WPA2-Enterprise Wi-Fi certified client devices or software/hardware upgrades to the presently installed Wi-Fi certified devices.

As new equipment is added to the Wi-Fi network, new devices should be WPA2-Enterprise Wi-Fi certified as applicable. In many cases with Wi-Fi certified products, only a software or firmware upgrade is needed for WPA2; new hardware is not required. This is possible by managers asking their vendor what is required to upgrade a client adapter to WPA2.

4.7.2 Client Supplicant

An IEEE 802.1X supplicant is required on the client. A supplicant is software that is installed on the client to implement the IEEE 802.1X protocol framework and one or more EAP methods. When deploying WPA2, managers should make sure that all client devices possess the necessary supplicant for their operating system. If a supplicant is not present, network managers must obtain one.

Supplicants may be included in the client operating system, integrated into drivers, or installed as third-party standalone software. Some vendors of wireless client devices ship

[9] AAA Server means Authorization Authentication Accounting server.

the supplicant with their cards. Wi-Fi certified client devices are confirmed to work with Microsoft, Funk Software, or a vendor supplied WPA2-enabled supplicant. However, the device need not possess the supplicant to be WPA-Enterprise or WPA2-Enterprise Wi-Fi certified. Network managers should check with their vendor to confirm if supplicants are included with the client devices.

4.7.3 EAP Authentication Types

Extensible Authentication Protocol (EAP) types offer a range of options that can be used with different authentication mechanisms, operating systems, and back-end databases. Each maps to different types of user logins, credentials and databases used in authentication. The EAP type used in WPA2-Enterprise deployments should be selected to support the organization's security strategy in accordance with the client supplicants and the back-end database used to store client identity credentials.

The Wi-Fi Alliance certifies WPA2-Enterprise products in tests on an open architecture in which EAP-TLS is used. However, as WPA2 are open platforms that are designed to be extensible, other EAP types that are not tested by the WPA2 certification program should run in a WPA2 environment. Example EAP types include EAP-TLS, EAP-TTLS, PEAP v.0, PEAP v.1 and other open standard types. The Wi-Fi Alliance plans to add more EAP types to its interoperability testing in the future. Managers should ask their vendor about other EAP types.

4.7.4 Access Points

New APs to be deployed in an enterprise network using EAP authentication should be WPA2-Enterprise Wi-Fi certified. Currently installed Wi-Fi certified APs may be upgradeable to WPA2-Enterprise via a firmware or hardware upgrade; otherwise a new AP will be required.

4.7.5 Authentication Server/Database

WPA2-Enterprise employs IEEE 802.1X authentication with EAP types which provide mutual authentication on Wi-Fi networks. This helps to insure that only authorized users are granted access to the network and that users only access authorized areas within the network. The requirements for an authentication server in a wireless network are similar to those of a wired LAN; the authentication server stores the list of the names and credentials of authorized users against which the server verifies user authenticity. Typically, a Remote Authentication Dial-In User Service (RADIUS) server is used.

User credentials may also be stored in an external database, such as SQL, LDAP or Active Directory, that can be accessed by the authentication server. The configuration is not determined by standards and can be specific to implementation.

Organizations that have already deployed a proprietary solution with WEP and an authentication server will have these basic components in place. If these devices are Wi-Fi certified, only upgrades to WPA2-Enterprise for the APs and client devices should be required. Once deployed, new authentication protocols can usually be implemented without changes to the infrastructure.

If an authentication infrastructure has already been deployed for the wired LAN, it may be utilized for WPA2.

4.8 WLAN Authentication and Encryption Methods

4.8.1 Static WEP and Dynamic WEP with IEEE 802.1x

WEP is the original, static 40-bit or 104-bit encryption scheme in the IEEE 802.11 standard. It lacks any means of authentication. WEP has been proven to be insecure and vulnerable to network attacks as we have found out.

WEP with IEEE 802.1X is referred to as "dynamic WEP". Dynamic WEP is a non-standard interim technology that some vendors introduced after the weaknesses of static WEP were uncovered. It uses WEP encryption with IEEE 802.1X authentication. Because it still uses WEP encryption, dynamic WEP deployments are also insecure and vulnerable to network attacks.

The Wi-Fi Alliance does not recommend deploying a Wi-Fi network with static WEP or dynamic WEP. Both methods are insecure and should be transitioned to WPA2.

4.8.2 How WPA2 Authentication Works

WPA2-Enterprise mutual authentication is initiated when a user associates with an access point. The AP blocks access to the network until the user can be authenticated. The user provides credentials which are communicated to the authentication server. The authentication process is enabled by the IEEE 802.1X/EAP framework. With EAP, IEEE 802.1X creates a framework in which client workstations and the authentication server

mutually authenticate with one another via the AP. Mutual authentication helps to ensure that only authorized users access the network and confirms that the client is authenticating to an authorized server. It helps to protect users from accidentally connecting to unauthorized 'rogue' APs, and as such prevent DoS attack on the network.

If the authentication server accepts the user's credentials, the client joins the WLAN. If not, the client remains blocked. Once the user has been authenticated, the authentication server and the client simultaneously generate a Pairwise Master Key (PMK).

A 4-way handshake then takes place between the client and the AP, to complete the process of authenticating the AP with the client, establishing and installing the TKIP (WPA) or AES (WPA2) encryption keys. As the client begins communicating on the LAN, encryption protects the data exchanged between the client and the AP.

4.8.3 How WPA2 Encryption with AES Works

AES is a block cipher, a type of symmetric key cipher that uses groups of bits of a fixed length - called blocks. A symmetric key cipher is a cipher that uses the same key for both encryption and decryption. The word cipher is used in cryptography to describe the instructions or algorithm used for encrypting and decrypting information.

With AES, bits are encrypted in blocks of plaintext that are calculated independently, rather than a key stream acting across a plaintext data input stream. AES has a block size of 128 bits with 3 possible key lengths 128, 192 and 256 bits as specified in the AES standard. For the WPA2/802.11i implementation of AES, a 128 bit key length is used. AES encryption includes 4 stages that make up one round. Each round is then iterated 10, 12 or 14 times

depending upon the bit-key size. For the WPA2/802.11i implementation of AES, each round is iterated 10 times.

AES uses the Counter-Mode/CBC-Mac Protocol (CCMP). CCM is a new mode of operation for a block cipher that enables a single key to be used for both encryption and authentication. The 2 underlying modes employed in CCM include Counter mode (CTR) that achieves data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to provide data integrity.

CBC-MAC is used to generate an authentication component as a result of the encryption process. This is different from prior MIC implementations, in which a separate algorithm for integrity check is required. To further enhance its advanced encryption capabilities, AES uses a 48-bit Initialization Vector (IV). AES has no known attacks and the current analysis indicates that it takes 2^{120} operations to break an AES key—making it an extremely secure cryptographic algorithm (Paul, 2006).

4.9 WPA2 Security Advantage

When compared with the IEEE 802.11 security standard using 40-bit WEP with no dynamic keying, TKIP and AES make it far more difficult-if not impossible-for a would-be intruder to break into a Wi-Fi network. By greatly expanding the size of keys and number of keys in use, creating an integrity checking mechanism, using a strong encryption cipher; and imposing replay protection, AES and TKIP greatly increase the strength and complexity of wireless encryption. Together with the IEEE 802.1X/EAP mutual

authentication framework, TKIP and AES magnify the complexity and difficulty involved in decoding data on a Wi-Fi network—making the Wi-Fi network secure.

4.10 Steps and Tools for WPA2 Deployment

4.10.1 Introduction

The migration path in upgrading to WPA2 will depend upon the security environment and the user authentication policies in place. We are at this point presenting the 7 Steps to Prepare for a WPA2 deployment. These steps focus on the authentication portion of WPA2 (Paul, 2006).

4.10.2 Seven Steps to Prepare For WPA Or WPA2 Deployment

Each of the 7 steps listed below is required to determine the components of a WPA2 deployment, which will prepare network, network managers to deploy WPA2 including the implementation of IEEE 802.1X authentication and AES (WPA2) encryption for an enterprise environment.

After following all 7 steps, network managers will know the components needed for a WPA2 deployment and be prepared to implement IEEE 802.1X authentication policies and begin deployment. Enterprises that already have an IEEE 802.1X/EAP framework for wireless computing in place and intend to continue using it will have already addressed the first 6 steps and may begin at step 7.

These 7 steps address the requirements for any network using IEEE 802.1X authentication. The effort and investment made in following the 7 steps will serve for WPA2 deployments. The 7 steps are:

Step 1: Security Mechanism and Credentials

Step 2: User Authentication Database

Step 3: Client Operating Systems

Step 4: Supplicants

Step 5: EAP Types

Step 6: Authentication Server

Step 7: Access Points and Client NIC Cards

4.10.3 Step 1—Security Mechanism and Credentials

Many existing enterprise networks already have a network security policy in place. Security policies, credentials and user identity management mechanisms will impact WPA2 enterprise deployment. Typically, the database is stored on the server or, externally, in Microsoft Active Directory, Novell LDAP, iPlanet or Secure ID Token.

If already running IEEE 802.1X authentication, and an authentication system is in place, a manager can continue to use it to store security credentials if it supports the EAP type(s) selected for the Wi-Fi network.

If there is not already a security policy in place, a manager will have to select one, provide the necessary user credentials to support it, and confirm that the credentials chosen can be managed by the authentication server.

4.10.4 Step 2—User Authentication Database

A database is required for user authentication. If users are already being authenticated, network managers should consider the database already in house. In the absence of an existing user authentication database, network managers will have to select one.

Selection should be based on the following considerations:

a) The security policy and the management of user credentials
b) The credential type selected
c) How user identity information will be stored
d) Budget considerations
e) Server environment

The server environment (UNIX, Linux, or NT) will heavily influence what database is implemented. This is due to the technology in place with these different types of Operating System.

4.10.5 Step 3—Client Operating Systems

Determine which client operating systems (OS) will be supported — Windows XP, 2000, NT, 98, 95; Windows CE; Mac OS; Linux; Palm OS; DOS or a proprietary system. Network managers should make sure that EAP type, selected database, and supplicants will support the operating system that will be used with WPA or WPA2.

4.10.6 Step 4—Supplicants

This step and Step 3 (Client Operating Systems), Step 5 (EAP Types), and Step 6 (Authentication Server) should be considered in parallel as the selection of the supplicant should be based on the EAP types, as well as on the client operating systems and authentication database being used.

Network managers should determine if they already have a supplicant to support existing client operating systems. If not, one should be obtained. Some operating systems include free supplicants. Others require the purchase of an after-market supplicant. In some settings, aftermarket supplicants may offer more flexibility as they are not tied to a particular operating system. Features may vary between built-in supplicants and third party supplicants.

4.10.7 Step 5—EAP Types

In parallel with Step 4, decide which EAP-type will be used. The EAP type selected should support the selected database for user credentials and the network security strategy. It should match the user authentication policies, user management strategy, and client operating system.

Some examples of EAP types that match various databases include:

Windows Microsoft format NT or Active Directory—works with PEAP v0/-MSCHAP v2, EAP-TLS, and EAP-TTLS/ MSCHAP v2

Linux LDAP or Netscape Directory Service (NDS)—works with PEAP v1/ MD5, PEAP v1/ GTC, EAP-TLS, EAP-TTLS/CHAP

UNIX A token or one-time password (OTP) server—The server has a token card with a reference ID that works with PEAP v1/EAP-GTC, EAP-TTLS/GTC

Network managers should ask their vendor how other EAP types compare. Since the Wi-Fi Alliance certifies WPA-Enterprise and WPA2-Enterprise products in tests on an open architecture, a variety of open standard and other EAP types can be used. Additional information about EAP types is included in Section I of this whitepaper.

4.10.8 Step 6: Authentication Server

Select an authentication server that will work with the selected user credentials database and matching EAP types. Network managers may change EAP types to match the current server. Or, network managers may wish to purchase a new server to work with the EAP type that best supports their security policies. Typically, a RADIUS server is used. If selecting a new server, network managers must verify that it will work with the selected database and matching EAP-types.

4.10.9 Step 7: Access Points and Client NIC Cards

Confirm that all APs and client devices to be used in the deployment are WPA-Enterprise or WPA2-Enterprise Wi-Fi CERTIFIED as applicable. WPA-Personal and WPA2-Personal APs and clients are not recommended for enterprise deployments because they do not support IEEE 802.1X and EAP authentication. Typically, WPA and WPA2 are not

automatically implemented in the default configuration of new wireless client devices and APs. They must be configured when the products are installed.

Legacy devices may require WPA2 upgrades. Many vendors provide WPA firmware updates for legacy APs and client devices. A hardware upgrade may be needed for WPA2 devices. Network managers should contact their vendor for upgrade information regarding the devices already in place.

A list of product vendors with products that are WPA-Enterprise and WPA2-Enterprise Wi-Fi certified is available at www.wi-fi.org.

4.11 Examples of WPA2 Deployment Configurations

The example of WPA2-Enterprise deployment configurations shown below illustrate how the 7 Steps to Prepare for WPA2 Deployments might apply in a Windows environment.

4.11.1 Windows Deployment of WPA2 Wireless Encryption

a. Security Credentials: Digital Certificate X.509
b. Database: Microsoft Active Directory
c. Client OS: Windows XP
d. Supplicant: Built into Windows XP for EAP-TLS
e. Authentication EAP Type: EAP-TLS
f. Authentication Server: Cisco Secure Access Control Server (RADIUS server)
g. Access Points and Client Devices: WPA-Enterprise Wi-Fi CERTIFIED

4.12 Simulated Instance for the WPA2 Deployment

The simulation example of WPA2 deployment was carried out in this research work using Cisco Packet Tracer.

Cisco Packet Tracer is a powerful network simulation program that allows students to experiment with network behavior and ask "what if" questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts. Packet Tracer supplements physical equipment in the classroom by allowing students to create a network with an almost unlimited number of devices, encouraging practice, discovery, and troubleshooting. The simulation-based learning environment helps students develop 21st century skills such as decision making, creative and critical thinking, and problem solving.

Packet Tracer complements the Networking Academy curricula, allowing instructors to easily teach and demonstrate complex technical concepts and networking systems design. The software is available free of charge to all Networking.

Below is diagrammatical representation of the simulation result for packet tracer.

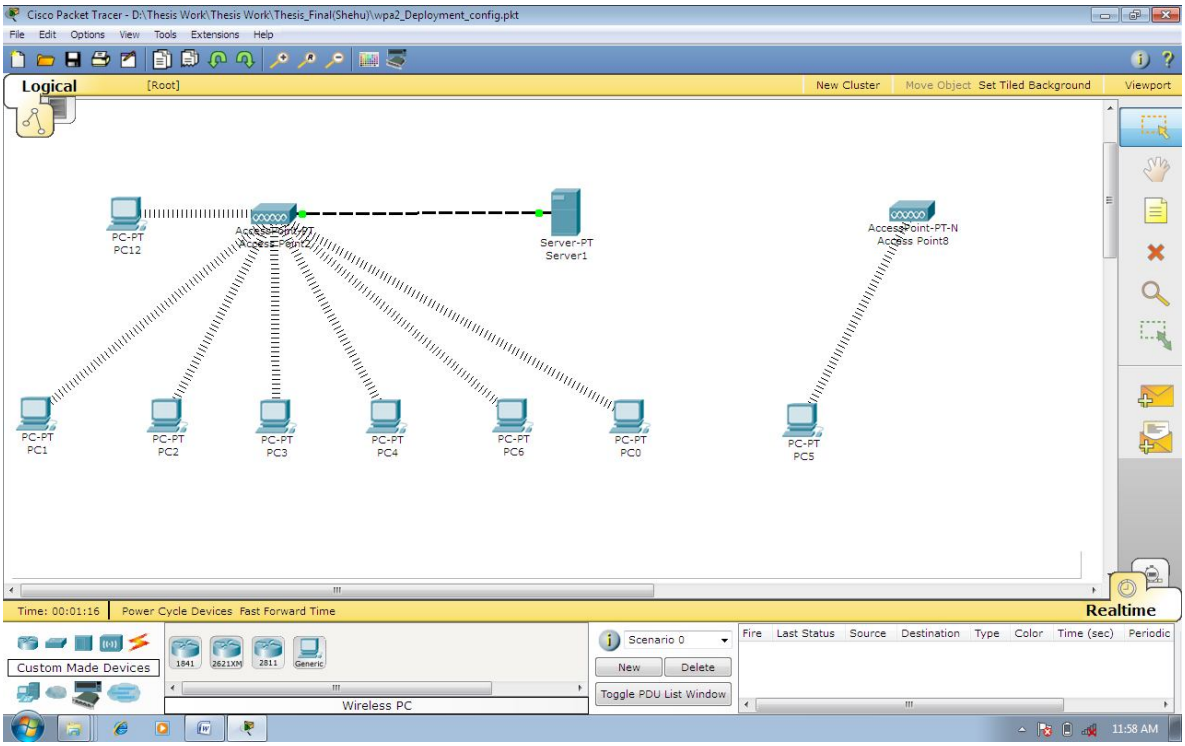

Fig. 4.2 Simulated Instance of a wireless network configured with WPA2 security

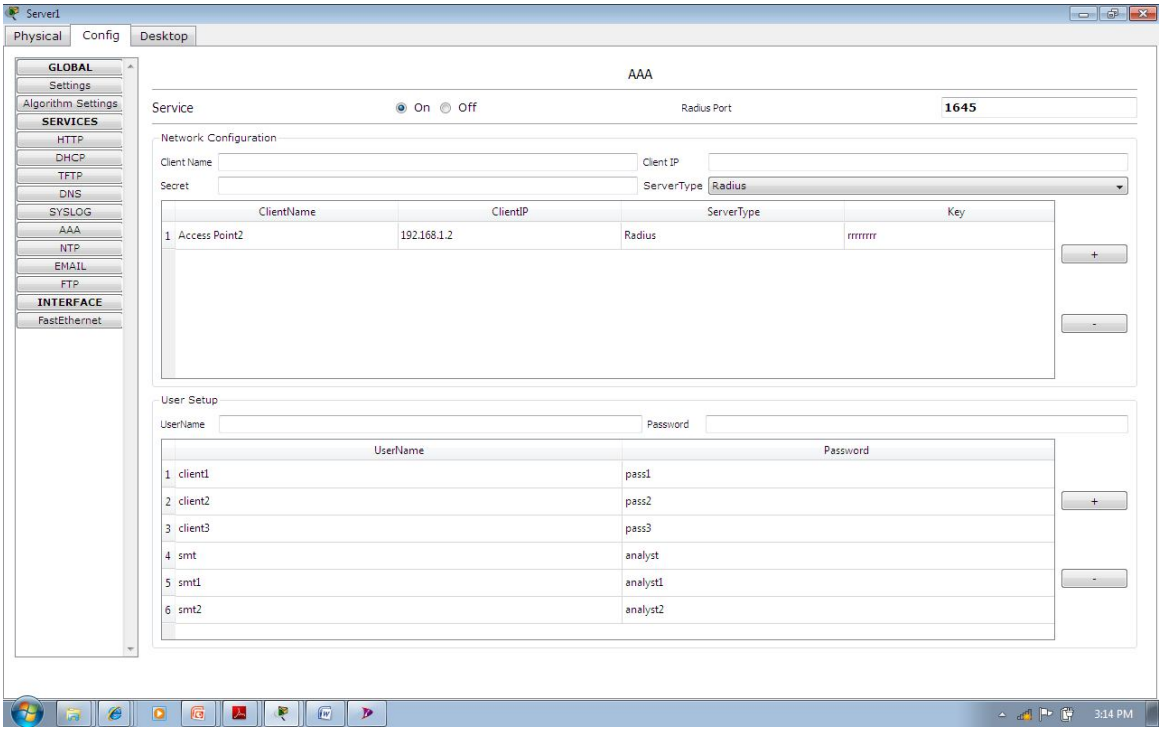

Fig. 4.3 Radius Server Configuration for List of devices to connect to the network

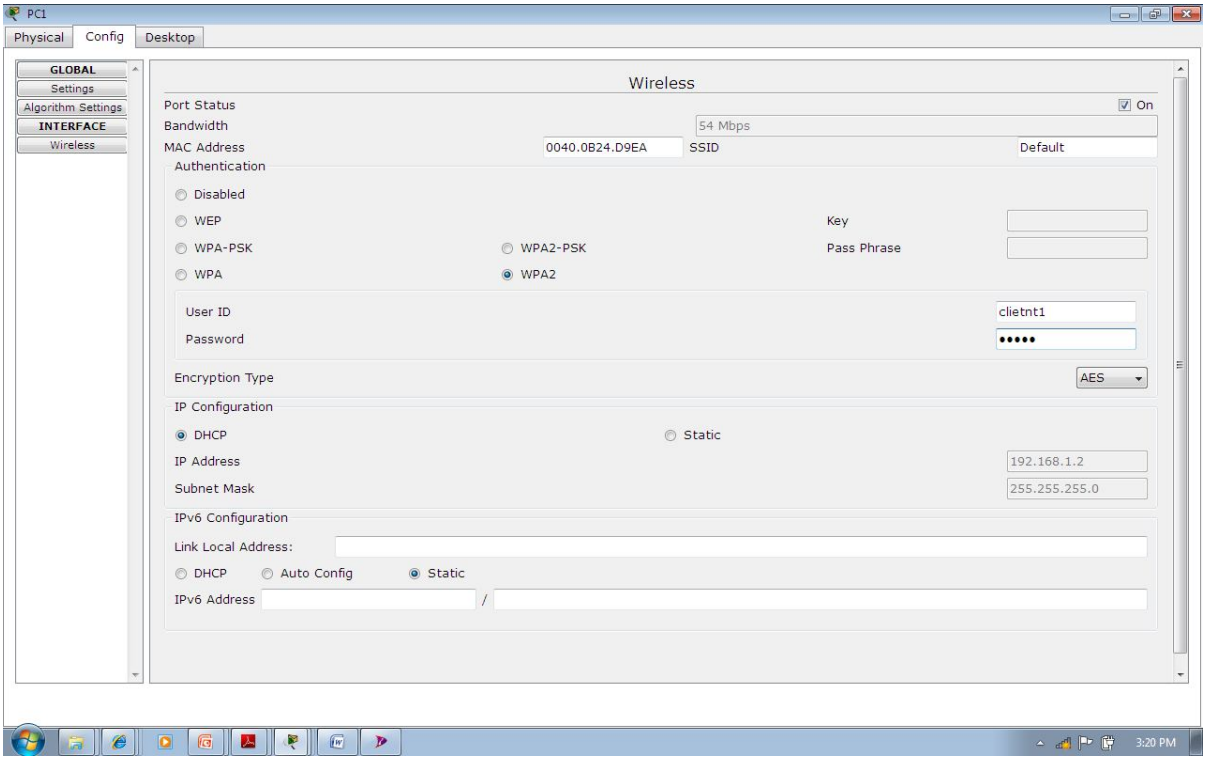

Fig.4.4 Client Configuration to connect to the RADIUS server for IP address

CHAPTER FIVE: SUMMARY, CONCLUSION, RECOMMENDATION AND FUTURE WORK

5.1 Summary

In this thesis work, we have shown that, the wireless LAN security provided by the IEEE802.11 wireless devices are not enough to guard against methods employed by network hackers to break the security. This happens by our ability to decrypt an encrypted AP(s) with WEP encryption to expose the secret word for the encryption which could lead to different types of attacks on the network such as setting of Fake-AP or rouge AP, denial of Service attack on a major web site and so on. This implies that most of the aforementioned security settings with the IEEE802.11 wireless devices lack proper access control mainly at the link layer. Nowadays, wireless networks are forced to rely on mechanisms based on some security mechanism to achieve satisfactory security levels. Statistics suggest that the costs associated with creating, revoking, and securely managing of credentials are too high for a large percentage of wireless installations, which are ultimately forced to use insecure yet easily deployable solutions. Consequently, even a sizable fraction of enterprise networks operate with insecure configurations, vulnerable to attacks ranging from casual war-driving to exposure of sensitive information.

Based on the above problem which is faced by ABU wireless LAN and other WLAN deployment, we are proposing the use of WPA2 encryption techniques or method, which fix all known vulnerabilities in WEP and greatly enhance data protection and access control

on existing and future Wi-Fi LANs. It provides an immediate, strong, standards-based, interoperable Wi-Fi security solution.

Network managers should review the deployment scenarios outlined as above in chapter four and migrate to WPA2. If upgrading to WPA2 from WPA or otherwise, managers should begin planning the migration strategy now. There is no reason not to deploy WPA2 today to enjoy the tremendous productivity and benefits of a secure Wi-Fi network

5.2 Conclusion

Our objective in this thesis work is to analyze wireless LAN security, taken ABU wireless LAN as the case study, based on the analysis, we proposed a solution which when applied to wireless local area networks, an organization such as ABU Zaria, and others, or individual could have wireless secured communication channel for its end users.

In this work we have shown that ABU wireless LAN lacks security setting, and/or the one in place can be break through by network hackers usually using some set of simple software tools. This problem can be faced not only by ABU wireless LAN, but even those wireless network deployment that have been configured with the basic IEEE802.11 wireless security settings such as the use of WEP, SSID, MAC Address and the likes as there are one hundred and one wardriving tools freely available for cracking such encryption techniques which are widely in use.

In conclusion, we have successfully analyzed the wireless LAN security, taken ABU wireless LAN as the case study by connecting our laptop to access services at different vantage points on the network, where we have captured live signal for analysis. Based on the analysis carried out, we noticed that the WLAN security is in two forms as; security at application level and that at network level. We were able to decrypt the security at the network level based on the packet capture on the network, which indicates that the wireless LAN is vulnerable to attack. Based on this our findings, we have proposed the use of WPA2 which is an enhance security mechanism with no known decryption tool. A simulated instance of this security mechanism has also been provided.

5.3 Recommendation

The use of WPA2 which is an enhanced WPA security encryption mechanism is of no doubt as Wi-Fi Alliance has tested and concluded that Infact, no method an intruder, or intruders can employ to overcome this WPA2.

We are there for recommending not only for ABU Wireless LAN, but any other wireless LAN that want to enjoy effective and secure communication to imbibe the use of WPA2 for encrypting their wireless LAN so as to enhance security to a reasonable height.

5.4 Future Work

The main future direction is the implementation of WPA2 for organizations to foresee its advantage so as to embrace it. And also to show that it cannot be easily intruded by a hacker.

References

Ashwin P., Dan S., Glen Z., Joe S., Hao Z., and Josefsson S. (2003). *Protected EAP Protocol (PEAP) Version 2 Internet Draft*, IETF draft-josefssonpppexteap-tls-eap-07.txt.

Atheros Communication. (2004). *How Atheros define wireless Network security today and in the feature*. White Paper Building a secure wireless Network.

Bellardo and Savage. (2009). *Wireless 802.11i Network Made simple*. Cisco Coop.

Baker, D. (2003). *Wireless LAN Security for Health Care*. San Diego, CA: Science Applications International Corporation.

Cisco Aironet (2005) *Cisco Aironet 1240AG Series 802.11A/B/G Access Point*. Product Data Sheet, Cisco Systems, Inc., 2005.

Cisco Website :Packet Tracer
http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html accessed on 05/03/2011

Clement J.B, John B., and Movs, G. (2005). *Tenth Annual CSI/FBI Computer Crime and Security Survey*. Technical report, Computer Security Institute. London DC, pp 6.

Daniel, B. F. and David, R. C. (2004). *No Long-term Secrets: Location-based Security in Over-provisioned Wireless LANs*. In Proc. of the Third ACM Workshop on Hot Topics in Networks (HotNets-III), November 2004.

David, C. and Cliff, P. (2002). *A Path Loss Comparison Between the 5 GHz UNII Band (802.11a) and the 2.4 GHz ISM Band (802.11b)*. Technical report, Intel Corporation England.

ETSI (2000). *Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview*. Technical Report DTR/BRAN-00230002, London February 2000.

Government of Canada. (2003). *802.11 Wireless LAN Vulnerability Assessment*. Ottawa, Ontario, Canada: Government of Canada. P. 11

Homayoun H. (1994) *Measurements and Modeling of Temporal Variations of the Indoor Radio Propagation Channel*. 43(3):733-737, Rinehart and Winston Inc., New York. pp 2-8.

Interlink Networks (2002). *Wireless LAN Security using Interlink Networks RAD Series AAA Server and Cisco EAP-LEAP*. Interlink Networks Resource Library London.pp7-9.

Interlink Networks (2002). *Introduction to 802.1X for Wireless Local Area Networks*. White Papers at Interlink Networks Resource Library London. pp 8.

Ivan M., Glen Z., Joe S., and Hao G. (2008). *Design, Implementation, and Performance Analysis of DiscoSec – Service Pack for Securing WLANs.* University of Kaiserslautern, Germany.

Ivan M. Glen Z., Joe S., and Hao G., (2007). *Introduction of IEEE 802.11i and Measuring its Security versus Performance Tradeoff*. In Proceedings of the 13th European Wireless Conference, April 2007

Jean-Paul, S. (2002). *Techniques to resolve 802.11 and wireless LAN technology in outdoor environments*. News Article at SecurityMagazine.com.

Jeffrey, H. (2000). *SpotON: An Indoor 3D Location Sensing Technology Based on RF Signal Strength*. Technical Report UW CSE 2000- 02-02, University of Washington, February 2000.

Jonas, M. and Jan-Erik, B. (2000). *Simple and Accurate Path Loss Modeling at 5 GHz in Indoor Environments with Corridors*. In Proc. of IEEE Vehicular Technology Conference (VTC), volume 1, pages 30-36.

John, V., David R., and Robert M. (2001). *Wireless LAN Access Control and Authentication*. White Papers at Interlink Networks Resource Library, 2001. Accessed at http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.pdf on 13/12/2010

Jorgen, B., Clement D., and Joshua H.(1995). *Propagation Measurements and Models For Wireless Communications Channels*. IEEE Communication Magazine, 33(1):42-49.

Jesse R.W. (2000). *Unsafe at any key size: An analysis of the WEP encapsulation.* 802.11 Security Papers at NetSys.com. Accessed at http://www.netsys.com/library/papers/walker-2000-10-27.pdf on 13 /12/2010

Karygiannis, T., and Owens, L. (2002). *Wireless Network Security 802.11, BlueTooth and Handheld devices* IEEE Communication Magazine.

Kent, S. and Atkinson, R. (1998). *Security Architecture for the Internet Protocol, RFC 2401, IETF*. London.

LAN MAN Standards Committee of the IEEE Computer Society (2006). *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)*. Technical Report 2003 Edition, IEEE Std802.15.4.

LAN MAN Standards Committee of the IEEE Computer Society (2004). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*. Technical Report 2004 Edition, IEEE Std 802.11i.

Lidl, J., Vollbrecht J., Rago D., and Moskowitz D. (1999). *A Method for Transmitting PPP over Ethernet (PPPoE)*, RFC 2516, IETF.

Martinovic, F. A., and Simos E. (2008). *Wireless Network Security and Interworking*. IEEE Wireless Communications Magazine, Feb.2008.

Merriam-Webster Online Dictionary.
http://www.merriam-webster.com/dictionary/accountability, accessed in December 2010.

Minho, S., and Gabriel L. (2008). *Security & Vulnerability Analysis of Wireless Messaging Protocols & Applications Wireless Client Puzzles in IEEE 802.11 Networks: Security by Wireless*. Proc. ACM Conference on Wireless Network Security (WiSec 2008), pages 36–45,

Mishra, M., Vinter, R., and John L. (2004). *Pro-active Key Distribution using Neighbor Graphs.* IEEE Wireless Communications Magazine.

Dave, W. (2004). *The Implementation of a Multi-site, Wireless Network at Northumbria University.* Northumbria University London.

Naveen, S., Umesh S., and David W.(2003). *Secure Verification Of Location Claims*. In Proc. of the Second ACM Workshop on Wireless Security (WiSe'03), pages 1-10.

Nourddine, A. and Laurent, C (2007). *An Impulse Response Model for the 60 GhzChannel Based on Spectral Techniques of α-stable Processes*. 52(12):3180-3189, December 2007.

Paul, A. (2006).*Benefits of Wi-Fi Protected Access 2 (WPA2)*. INFS 612 – Fall 2006

Paramvir, B. and Venkata, N. P.(2000). *RADAR: An In-Building RF-Based User Location and Tracking System*. In Proc. of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00), Tel-Aviv, Israel.

Pierre Trudeau (2001). *Building Secure Wireless Local Area Networks*. White Papers at Colubris.com
http://download.colubris.com/library/whitepapers/WP-010712-EN-01-00.pdf Accessed on 13/11/2010.

Peter, C. and Cliffort M.(2006). *CAPWAP Protocol Specification*. IETF Internet Draft, draft-ietf-capwap-protocol-specification-01. New York.

RSA Security Inc (2005). *The Wireless Security Survey of London.* White Paper WSLN05-WP-0305 London.

Seidel, S. Y. and Rappaport, T. S. (1992). *914 MHz Path Loss Prediction Models for Indoor Wireless Communications in Multi-stored Buildings*. IEEE Transactions on Antennas and Propagation, 40(2):207-217.

The Official Worldwide Wardrive. http://www.worldwidewardrive.org/, June 2004, accessed on Nov. 2010.

Theodore S. R. (2002). *Wireless Communications - Principles and Practice*. Prentice Hall PTR, 2nd edition.

Wi-Fi Alliance(2005). Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise,

WLAN Association (1999). *Introduction to Wireless LANs*. WLANA Resource Center Accessed at http://www.wlana.com/learn/intro.pdf on 4/11/2011

WLAN Association (2002). *Wireless Networking Standards and Organizations.* WLAN A Resource Center. Accessed at http://www.wlana.com/pdf/wlan_standards_orgs.pdf on 3/11/2011

Ylonen, T. and Lonvick, C. (2006). *The Secure Shell (SSH) Protocol Architecture, RFC 4251, IETF*. London.

Zion N.(2006) 2.4 GHz 24 dBi High Performance Reflector Grid Wireless LAN Antenna, Model HG2424G. Product Data Sheet. HyperLink Technologies, Inc..