EXPERIMENTAL ASSESSMENT OF PRE-SHARED KEY AND WPA_RADIUS SERVER IN WIRELESS NETWORK SECURITY

Adekunle M. Ibrahim[1*], Abdulwahab Funsho[2].
[1]Department of Information and Communication Technology, Osun State University, Nigeria
[2]Department of Computer Science, University Utara Malaysia, Malaysia

ABSTRACT

Wireless network security is very important in security, privacy and confidentiality of our data and resources. It requires the use of network resources through encryption keys of packets to achieve authentication or authorization of users. It is therefore very paramount to investigate the effects and performances of pre-shared keys and radius servers to improve user quality of service and experience in data management. In this work, wireless local area (WLAN) connections and security access were explored using roaming approach across access points with the help of ad-hoc Network and sharing internet access via ADSL router. WLAN packets were captured and analyzed with wire shack analyzer to detect and evaluate security measures for efficient control of access to multiple networks. The paper demonstrates the effectiveness and performance of WPA- PSK and WPA_RADIUS in terms of access security control in wireless networks.

Keywords: *Wire shark, Encryption, Pre shared key, Radius, ADSL, Packets*

1. INTRODUCTION

Wireless networking can cause a revolution in computing and Internet access. Wireless Local Area Networking (WLAN) frees users from the constraints of cables in office or home environment. Ideal for notebook PC users wanting mobility and desktop users require access to networks where the normal wired method is impractical or prohibited like in listed buildings or across public highways. The arrival of the IEEE 802.11b Wi-Fi standards meant that majority vendors could provide a small cost compatible solution for wireless communication over the local area at speeds on a par with basic wired Ethernet technology. Before the invention of IEEE 802.11, brand x radio could not properly communicate with brandy access point and this problem has drastically reduced the communication channels between these devices. The WLAN standard continues to evolve to provide higher speeds, greater range and better security than the earlier systems. Both radio and optical (laser or infrared light) transmission methods have been used for wireless connectivity of computer systems, but radio systems are by far the most popular as they have greater range and do not require line of sight. Wireless versions of *Network Interface Card* (NIC) are employed to transmit and receive signals, and *Access Points* are used to concentrate and repeat these transmissions or bridge to wired network equipment such as hubs or switches as presented in Figure 1 **(**White, 2010).

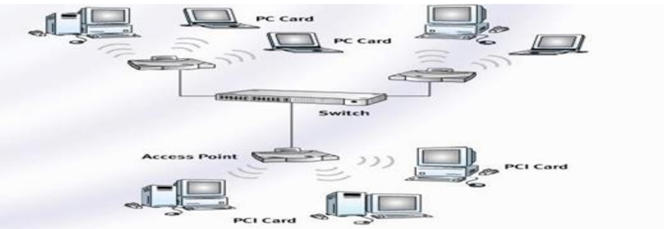


Figure 1: Wireless access points for data protection

In wireless networks, many attacks or threats such as eavesdropping, spoofing and denial (Isaac and Mohammed, 2007) can cause severe damages to our data or secret information, hence there is need for analysis and investigation of network security protocols in data protection. Much emphasis has been laid on the need to implement security on wireless networks, but very little efforts have been placed on the effect or performance of security protocols on wireless network.

1.1 Security issues with WLAN and IEEE 802.11i

Every aspect of wireless network including secure and efficient routing (Deng et al.,2002; Karp and Kung,2000; Papadimitratos and Haas,2002; Tanachaiwiwat et al., 2003), data aggregation (Ganeriwa and Srivastara,2002; Hu and Evans, 2003;Madden et al.,2002;Przydatek et al.,2003;Shrivastara,2004; Ye et al.,2004), group formation (Przydatek,2003) could be effectively applied for solving problems in network security. Apart from the traditional security issues, it can be observed that many general-purpose wireless techniques ensured that all nodes are trustworthy. In (Tasoluk and Tanrikulu, 2011), security protocols applied encryption keys to protect data and information that might take long time for hackers to crack. These keys are usually use for authentication and authorization when a client is trying to connect a wireless network, and it involves exchanging of keys between an access point and the client. This research work would apply WLAN with WPA2PSK protocol based on the IEEE 802.11i standard (Hassan,2015) to address bothering issues in wireless security. WPA (Wireless Protected Access) originated from the problems detected in WEP is a security system created for wireless networks (Maluenda et al.,2000). Security has been a major concern in any wireless network since any computer or PDA equipped with a WLAN card can pick up the signals. Also the WEP (Wired or Wi- Fi Equivalent Privacy) layer2 encryption method used by IEEE 802.11b can be seen as insecure (easily cracked). There are many ways to make WLANs as secure as wired networks. WPA (Wi-Fi Protected access) technology is now being used by most IEEE 802.11g technology, which is a subset of the new IEEE 802.11i standard designed to be used with the IEEE 802.1X extensible authentication protocols for stronger data link encryption. WPA2 provides authentication support via IEEE 802.1X and PSK (Pre Shared Keys) for the following applications:

I. **Personal Mode** is a process when products tested communicate only in PSK mode of operation for authentication access. It involves manual configuration of a pre-shared key on the access point and clients. PSK verifies users with a password or identifying code for easy access to client station and access point.

II. **Enterprise Mode** is a process that allows products to be tested for easy communication between PSK and IEEE 802.1X/EAP modes of operation for authentication purpose. When IEEE 802.1X is used, authentication, authorization, and accounting server (the RADIUS protocol for authentication and key management and centralized management of user credentials) are required. Enterprise Mode is targeted to enterprise environments (Figure 2) (Holroyd, 2009).

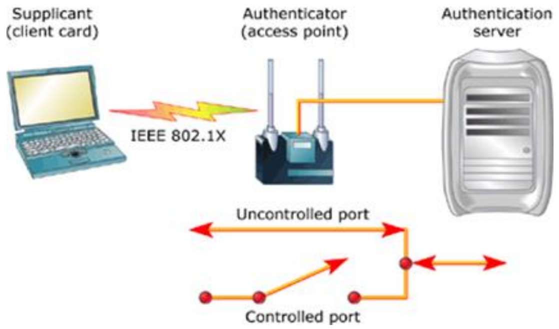


Figure 2: Access Control in Enterprise mode

2. METHODS FOR ACCESS CONTROL

Data link access control via the access point identifiers (SSIDs) offer some degree of protection against unauthorized access, if a station does not know this value then it is not allowed to associate. Putting off SSID broadcasting that is always on by default on some access points could be a mild deterrent to hackers as packet sniffing will easily reveal the name of the access point when an authorized node transmits a frame. Access control lists of MAC addresses can also be included in the Access Point used to restrict access to known users entered into a table, but again hackers can easily spoof (or clone) MAC addresses (pretend to be a valid user) to gain access. If security is a major concern, however, users are being advised to implement higher layer authentication methods or use Virtual Private Network (VPN) or VLAN techniques. For mid to large networks, WLAN switches can simplify administration and Enterprise Wireless gateways (EWGs) to ease the authentication and connectivity issues (Schaefer, 2003;Bauman, 2007).

3. ASSOCIATION, INTER-CELL COMMUNICATION AND ROAMING

Association involves connection between a node and an access point. It usually occurs when a node moves within range and tunes its radio channel to what the access point is set to.

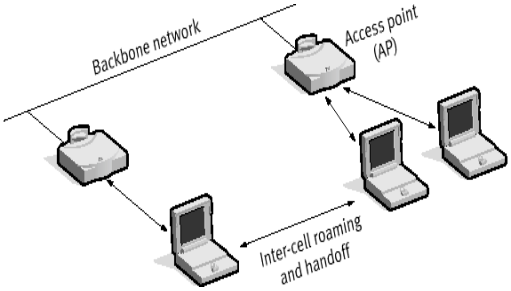


Figure 3: Inter-cell Communications and Roaming

Inter-cell communication of nodes connected to different access points by a distribution system or backbone network as in Figure 3 is accommodated by a frame structure that contain four MAC addresses. The setting on the DS bits in the control field determines how these addresses are interpreted. In the simplest case, two addresses identify the source and target wireless nodes (DS=00) but in most complex (DS=11), two additional intermediate addresses are needed. The first address is the destination node, second address is source node, and third address is the local access point that forwards the frame to the destination access point Address.

Roaming, the ability of a mobile computer to move between access points is an important feature of larger WLANs. The wireless node assesses the received signal level from each access point within range and then resynchronizes (adjusts channel settings) to the stronger as the user moves between service areas using either active or passive scanning. Active scanning adopts four steps involving an interchange of frames: (1) node sends a probe frame, (2) all APs within range reply with a probe response, (3) node selects an AP by sending an association request and (4) the AP replies with an association response. In passive scanning, the APs send out Beacon frames periodically and nodes wishing to change AP send back an association request. Beaconing is also used to awaken nodes in power save polling mode and advertise other access point services. Dynamic process with access points allows network managers to set up WLANs with a very broad coverage by creating a series of overlapping cells as in Figure 4, but care must be taken to ensure that channels do not overlap. The wireless node assesses the received signal level from each access point within range and then resynchronizes (adjusts channel settings) to the stronger as the user moves between service areas using either active or passive scanning. In IEEE 802.11b, there are only three of the 14 channels that do not overlap at all; these channels should be used at times if possible. If two partially overlapping channels are used they may cause interference for one another, leading to reduced bandwidth in the overlapping area. Not all channels are available in some regions (Kizza, 2011). WPA–PSK has been the only method recommended for home use and small business networks without a RADIUS server for several years.

EAP authentication packets would be captured on the client PC with Wire shark as it is authenticated by the AP. WPA supports two modes of operation. WPA Enterprise is meant for environments with a RADIUS infrastructure and uses an EAP authentication method while WPA Personal is meant for environments without a RADIUS infrastructure and uses a pre-shared key for authentication. For a home or small business, WPA (Wi Fi Protected Access) provides a pre-shared key authentication method for infrastructure mode wireless networks. Some experimental analysis to demonstrate the effectiveness of the AP using WPA- PSK were considered, the procedures for the experimental setup are as follows:

I. Figure the AP to use WPA-PSK and enter a pre-shared network key (passphrase) to generate the key.
II. Create a new profile for your WLAN connection called wpa1 and configure it to match the new AP security settings, and then test access as before.
III. Test connections between PCs by Pinging another client as before and determine if the data is now encrypted.

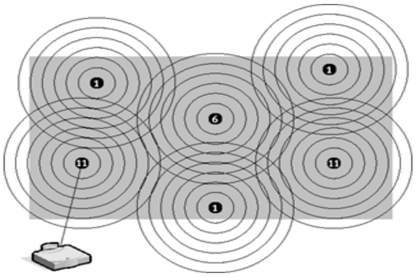


Figure 4: IEEE 802.11b DSSS cell overlap

4. COMPUTATIONAL METHODS WITH IEEE 802.1X - WPA RADIUS

This is the recommended method for enterprise wireless networks with the use of IEEE802.1X and Radius server for authentication and key distribution. In this process, standard method for Microsoft enterprise WLAN installations called PEAP could be used. This can be used to overcome security issues for wireless connections where EAP occurs during the IEEE 802.1X authentication process, before wireless frames are encrypted. The IEEE 802.1X standard helps to create port-based, network access control used to provide authenticated network access for Ethernet networks. Although this standard was designed for wired Ethernet as it has been adapted for use by 802.11. IEEE 802.1X, which uses EAP and specific authentication methods known as EAP types to authenticate the network node. The IEEE 802.1X standard imposes authentication of a network node before it exchanges data with the network. IEEE 802.1X provides stronger authentication than open system with shared key and recommended solution for large networks (Fenna,2010). This port-based uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. If the authentication process fails, access to the port can be denied. Although this standard was designed for wired Ethernet networks, it has been adapted for use on 802.11 wireless LANs as shown in Figure 5.
In the second experiment, the authenticator's port- based access control defines the following different types of logical ports that access the wired LAN via a single physical LAN port:

1. Reconfigure the AP to use WPA-with Radius and specify the Radius server details as shown in Figure 5. Review the Radius server settings to show how it is configured in conjunction with the AP.
2. Create a new profile for your WLAN connection called WPArad1 and configure it to match the new AP

settings. Supply login details when requested.

3. Test connections between PCs using Ping as before and determine if the data is now encrypted.
4. Analyze the packets to see the authentication procedure shown in Figure 5 is now being used. To do this you will need to capture EAP packets on the client and Radius PCs using Wire shark while authentication takes place.

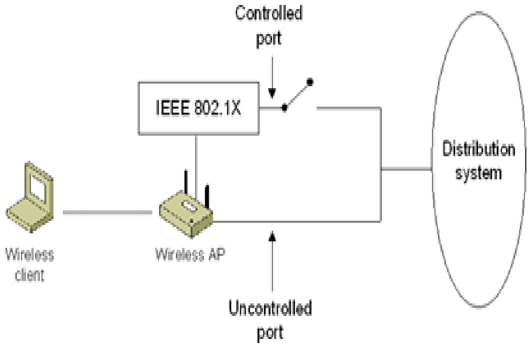
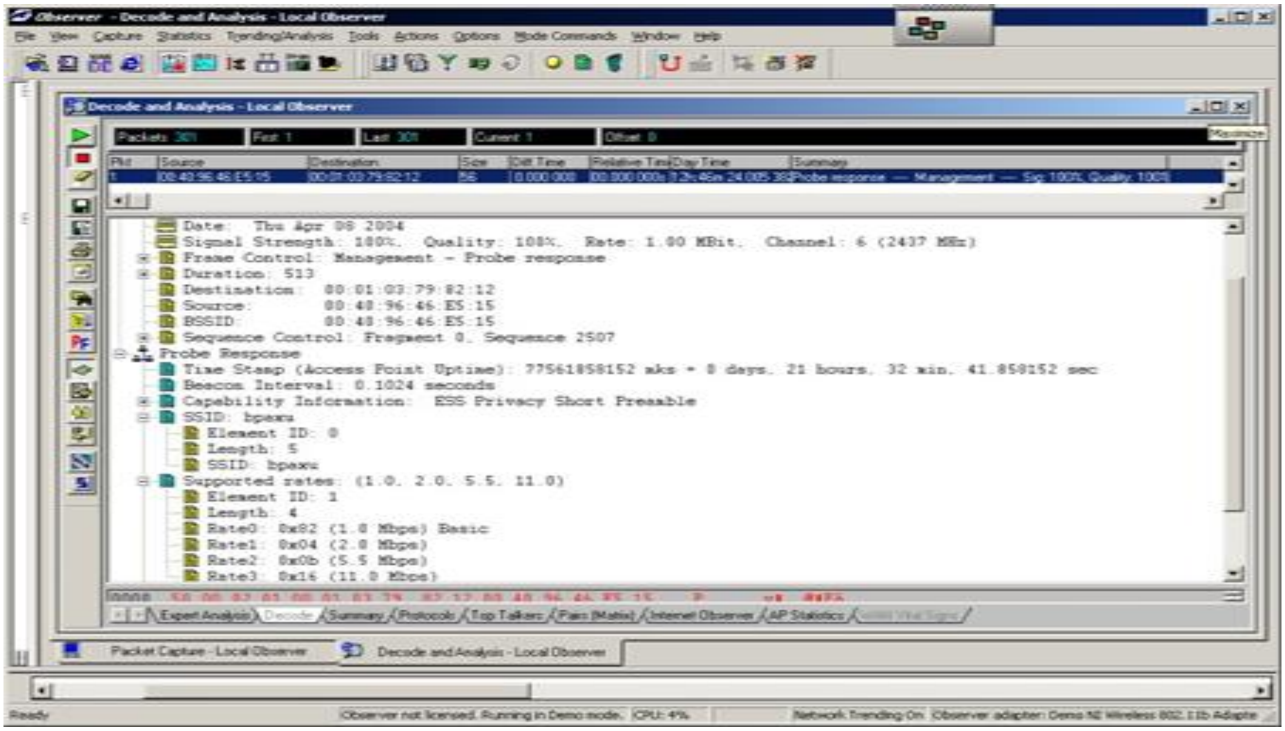


Figure 5: Wireless Network Access Control

5. RESULTS AND DISCUSSION

Analyses of packets to see that WPA and IEEE 802.1X EAP are now being used for demonstrating authentication packets behaviour are presented in Figure 6.


Observer - Decode and Analysis - Local Observer
File View Capture Statistics Trending/Analysis Tools Actions Options Mode Commands Window Help
Decode and Analysis - Local Observer
Packets 301
First 1
Last 301
Current 1
Offset 0
Expert Analysis
Decode
Summary
Protocols
Top Talkers
Pairs (Matrix)
Internet Observer
AP Statistics
Packet Capture - Local Observer
Decode and Analysis - Local Observer
Ready

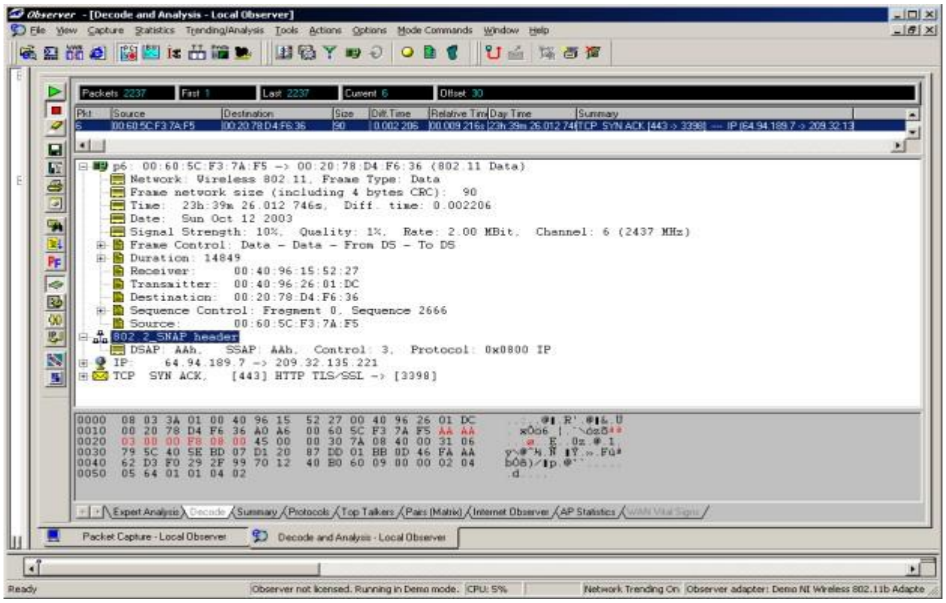
```
Pkt  Source             Destination        Size  Diff Time  Relative Time  Day Time          Summary
1    00:40:96:46:E5:15  00:01:03:79:82:12  56    0.000 000  00.000 000s    12h:46m 24.005 38 Probe response — Management — Sig: 100% Quality: 100%
```

```
    Date:  Thu Apr 08 2004
    Signal Strength: 100%.  Quality: 100%.  Rate: 1.00 MBit.  Channel: 6 (2437 MHz)
  + Frame Control: Management - Probe response
  + Duration: 513
    Destination:   00:01:03:79:82:12
    Source:        00:40:96:46:E5:15
    BSSID:         00:40:96:46:E5:15
  + Sequence Control: Fragment 0. Sequence 2507
- Probe Response
    Time Stamp (Access Point Uptime): 77561858152 mks = 0 days. 21 hours. 32 min. 41.858152 sec
    Beacon Interval: 0.1024 seconds
  + Capability Information:  ESS Privacy Short Preamble
  - SSID: bpaxu
      Element ID: 0
      Length: 5
      SSID: bpaxu
  - Supported rates: (1.0. 2.0. 5.5. 11.0)
      Element ID: 1
      Length: 4
      Rate0: 0x82 (1.0 Mbps) Basic
      Rate1: 0x04 (2.0 Mbps)
      Rate2: 0x0b (5.5 Mbps)
      Rate3: 0x16 (11.0 Mbps)
```

```
Observer not licensed. Running in Demo mode.  CPU: 4%  Network Trending On  Observer adapter: Demo NI Wireless 802.11b Adapte
```

Figure 6: Local observer for a four way handshake

From Figure 6, the initial WPA encryption key was derived from the authentication process, which verifies that both wireless client and wireless AP can be configured with the same pre-shared key. Each initial WPA encryption key is unique and 4 way handshake was done by EAP packets. As can be seen in Figure 7, it was observed that authentication procedure could be used when the EAP packets on client and PCs were captured. Please see the details of the packets analysis as follows:


Observer - [Decode and Analysis - Local Observer]
File View Capture Statistics Trending/Analysis Tools Actions Options Mode Commands Window Help
Packets 2237
First 1
Last 2237
Current 6
Offset 30

Pkt	Source	Destination	Size	Diff.Time	Relative Tim	Day Time	Summary
6	00:60:5C:F3:7A:F5	00:20:78:D4:F6:36	90	0.002 206	00.009 216s	23h:39m 26.012 74	TCP SYN ACK [443 -> 3398] --- IP [64.94.189.7 -> 209.32.13

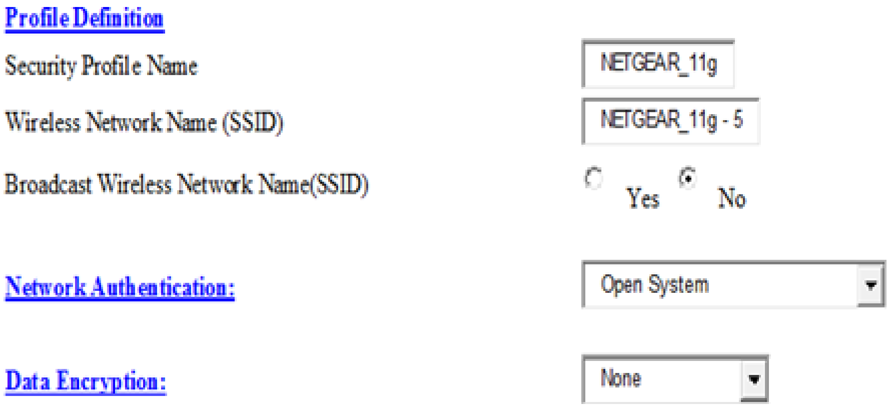
```
p6: 00:60:5C:F3:7A:F5 -> 00:20:78:D4:F6:36 (802.11 Data)
    Network: Wireless 802.11, Frame Type: Data
    Frame network size (including 4 bytes CRC):  90
    Time:  23h:39m 26.012 746s,  Diff. time: 0.002206
    Date:  Sun Oct 12 2003
    Signal Strength: 10%,  Quality: 1%,  Rate: 2.00 MBit,  Channel: 6 (2437 MHz)
    Frame Control: Data - Data - From DS - To DS
    Duration: 14849
    Receiver:      00:40:96:15:52:27
    Transmitter:   00:40:96:26:01:DC
    Destination:   00:20:78:D4:F6:36
    Sequence Control: Fragment 0, Sequence 2666
    Source:        00:60:5C:F3:7A:F5
802.2_SNAP header
    DSAP: AAh,  SSAP: AAh,  Control: 3,  Protocol: 0x0800 IP
IP:     64.94.189.7 -> 209.32.135.221
TCP  SYN ACK,   [443] HTTP TLS/SSL -> [3398]

0000   08 03 3A 01 00 40 96 15   52 27 00 40 96 26 01 DC
0010   00 20 78 D4 F6 36 A0 A6   00 60 5C F3 7A F5 AA AA
0020   03 00 00 F8 08 00 45 00   00 30 7A 08 40 00 31 06
0030   79 5C 40 5E BD 07 D1 20   87 DD 01 BB 0D 46 FA AA
0040   62 D3 F0 29 2F 99 70 12   40 B0 60 09 00 00 02 04
0050   05 64 01 01 04 02
```

Expert Analysis
Decode
Summary
Protocols
Top Talkers
Pairs (Matrix)
Internet Observer
AP Statistics
WAN Vital Signs
Packet Capture - Local Observer
Decode and Analysis - Local Observer
Ready
Observer not licensed. Running in Demo mode.
CPU: 5%
Network Trending On
Observer adapter: Demo NI Wireless 802.11b Adapte

Figure 7: Observer for packets analysis

In addition to WEP encryption, the following techniques can be used to protect 802.11 wireless networks**:** Non-broadcast wireless networks and MAC address filtering. In the third experiment, the wireless APs for non-broadcast mode prevents the casual wireless client from discovering your wireless network. On the other hand, even the most unsophisticated malicious user can capture the messages containing the wireless network name sent by wireless clients or your wireless AP and determine your wireless network name. Here, we determined the SSID of a Net gear AP that has had its broadcasting name facility disabled as shown in Figure 8. Configuration and set up for the AP for open access and disable SSID broadcasting are shown in Figure 8.



Profile Definition

Security Profile Name: NETGEAR_11g

Wireless Network Name (SSID): NETGEAR_11g - 5

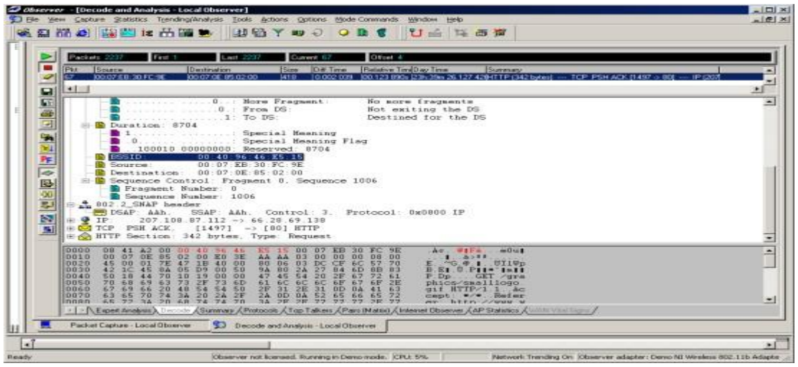
Broadcast Wireless Network Name(SSID): ○ Yes ● No

Network Authentication: Open System

Data Encryption: None

Figure 8: Security Profile configuration for WEP encryption

Probe or response packets with observer could be used to demonstrate encryption analysis to reveal the SSID of another client connecting to the network. The Kismet scanner will reveal hidden SSID without having to analyze probe packets.


Observer - [Decode and Analysis - Local Observer]
File View Capture Statistics Trending/Analysis Tools Actions Options Mode Commands Window Help
Packets 2237
First 1
Last 2237
Current 67
Offset 4
Pkt Source Destination Size Diff Time Relative Time Day Time Summary
Expert Analysis
Decode
Summary
Protocols
Top Talkers
Pairs (Matrix)
Internet Observer
AP Statistics
Packet Capture - Local Observer
Decode and Analysis - Local Observer
Ready
Observer not licensed. Running in Demo mode.
CPU: 5%
Network Trending On
Observer adapter: Demo NI Wireless 802.11b Adapte

```
67  00:07:EB:30:FC:9E  00:07:0E:85:02:00  418  0.002.039  00.123.890s  23h:39m:26.127.42  HTTP (342 bytes) --- TCP: PSH ACK [1497 > 80] --- IP:207

       .......0..: More Fragment:      No more fragments
       ........0.: From DS:            Not exiting the DS
       .........1: To DS:              Destined for the DS
   Duration: 8704
       1..............: Special Meaning
       .0.............: Special Meaning Flag
       ..100010 00000000: Reserved: 8704
   BSSID:          00:40:96:46:E5:15
   Source:         00:07:EB:30:FC:9E
   Destination:    00:07:0E:85:02:00
   Sequence Control: Fragment 0, Sequence 1006
       Fragment Number: 0
       Sequence Number: 1006
 802.2_SNAP header
   DSAP: AAh,  SSAP: AAh,  Control: 3,  Protocol: 0x0800 IP
 IP:    207.108.87.112 -> 66.28.69.138
 TCP  PSH ACK,   [1497]  -> [80] HTTP
 HTTP Section: 342 bytes, Type: Request

0000  08 41 A2 00 00 40 96 46  E5 15 00 07 EB 30 FC 9E
0010  00 07 0E 85 02 00 E0 3E  AA AA 03 00 00 00 08 00
0020  45 00 01 7E 47 1B 40 00  80 06 03 DC CF 6C 57 70
0030  42 1C 45 8A 05 D9 00 50  9A 80 2A 27 84 6D 8B 83
0040  50 18 44 70 10 19 00 00  47 45 54 20 2F 67 72 61   P.Dp....GET /gra
0050  70 68 69 63 73 2F 73 6D  61 6C 6C 6C 6F 67 6F 2E   phics/smalllogo.
0060  67 69 66 20 48 54 54 50  2F 31 2E 31 0D 0A 41 63   gif HTTP/1.1..Ac
0070  63 65 70 74 3A 20 2A 2F  2A 0D 0A 52 65 66 65 72   cept: */*..Refer
```

Figure 9: SSID packet analyzer for resolving security issues

The results of this experiment in Figure 9 reflected that without SSID, the packets captured can reveal the SSID of other clients connected to the network. In other words, turning off SSID broadcasting is useless because a hacker can use packet sniffing software to capture the SSID even if broadcasting is turned off. Turning off broadcasting would not deter a serious hacker, but it will protect from the casual "piggy backer".

6. CONCLUSIONS

This paper has presented the development of WPA_PSK and WPA_RADIUS for efficient and effective wireless communication. The effects and performances of models have been demonstrated with several experimental analyses conducted using wire shark analyzer and observer. In terms of security and bandwidth consumption, the network systems developed have proven to be very robust such that it is almost impossible for hackers to crack the network guided with these latest protection measures.

REFERENCES

[1] Bauman, Z. (2007). Globalization and culture, Polity Press, Oxford.

[2] Besanko, D, Dranove, D, Shanley, M & Schaefer, S (2003). Economics of strategy, 3rd Ed, Wiley, New York.

[3] Coates, K & Holroyd c. (2009). Japan and the internet revolution, Palgrave Macmillan, New York.

[4] Deng J., Han R., and Mishra S.(2002). INSENS: Intrusion-tolerant routing in wireless sensor networks. In Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado.

[5] Denzin, NK & Lincoln, YS (2010). The landscape of qualitative research: theories and issues, 2nd edition, Sage, Thousand Oaks, CA.

[6] Fenna, A. (2010). Australian public policy, 2nd Ed, Pearson Education Australia, French’s Forest, NSW.

[7] Ganeriwal S. and Srivastava M.(2004). Reputation-based framework for high integrity sensor networks. In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington, DC.

[8] Hassan A. (2015). “A comparative study of WLAN security protocols: WPA, WPA2,” in International Conference on advances in Eletronical Engineering (IEEE), Dhaka, Bangladesh.

[9] Hu L. and Evans D.(2003). Secure aggregation for wireless networks. In SAINT-W ‘03: Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), page 384. IEEE Computer Society.

[10] Karp B. and Kung H.T. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pages 243-254. ACM Press.

[11] Kizza, J.M. (2011). Computer network security and cyberethics, McFarland, Jefferson, N.C.

[12] Madden S., Franklin M.J., Hellerstein J.M., and Hong W.(2002). Tag: A tiny aggregation service for ad-hoc sensor networks. SIGOPS Oper. Syst. Rev., 36(SI):131-146.

[13] Maluenda J. R., Vasquez B. R., and Escobar A.V. (2017), “Redes WPA/WPA2,” [Online] Available: http://profesores.elo.utfsm.cl/~agv/elo322/1s12/ project/reports/RuzRiverosVaras.pdf [Accessed May. 20, 2017].

[14] Papadimitratos P. and Haas Z.J.(2002). Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference.

[15] Pfeiffer, J.W.(2009). Theories and models in applied behavioural science, vol. 4, Organizational, Pfeiffer, and San Diego.

[16] Przydatek B., Song D., and Perrig A.(2003). Sia: Secure information aggregation in sensor networks.

[17] Shrivastava N., Buragohain C., Agrawal D., and Suri S.(2004). Medians and beyond: New aggregation techniques for sensor networks. In SenSys '04: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, pages 239-249. ACM Press.

[18] Tanachaiwiwat S., Dave P., Bhindwale R., and Helmy A. (2003). Poster abstract secure locations: Routing on trust and isolating compromised sensors in location-aware sensor networks. In Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, pages 324-325. ACM Press.

[19] Tomlinson, J (2008). Globalization: the human consequences, Routledge, London.

[20] Watts, M.M. (2010). Technology: taking the distance out of learning, Josser-Bass, San Francisco.

[21] Wynn, J. & White, R. (2010). Rethinking youth, Allen & Unwin, St Leonards, NSW.

[22] Ye F., Luo H., Lu S., and Zhang L.(2004). Statistical en-route detection and filtering of injected false data in sensor networks. In IEEE INFOCOM.