Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Detecting Fake Access Point into Wireless Network Using Clock Skews as Fingerprinting Technique

**Miss Swati Jadhav**
M.Tech Student
Department of Computer of Engineering
B.V.U College of Engineering
India

**Sandeep Vanjale**
Research Scholar
Department Computer Engineering
B.V.U College of Engineering
India

**Dr. P. B. Mane**
Professor
Department Electronic Engineering
AISSM'S IOIT, Pune
India

***Abstract —The presence of Rogue Access Point (RAP) is major security concern in wireless network. If this kind of security threat is alive into WLAN, it results into leakage of confidential information to outside network. In our implementation, we have make used of clock skew of wireless LAN access point as its fingerprint to detect the fake APs. Fingerprinting will act as unique identification like human fingerprint work. The major objective of using the clock skew interval for detecting the fake AP is to overcome the limitation of existing approach. Existing methods for detection of fake AP has limitation of detecting MAC address spoofing. We have used TSF timestamp value of beacon frame transmitted from access point for purpose of calculating the clock skew value of AP in WLAN. There are two kinds of approach exist for calculating the clock skew of AP. one of them is LPM-method and second one is LSF method. The LPM stands for linear programming and LSF stand for least square fitting method.***

***Keywords— AP, RAP, WLAN, WEP, MAC address, Man-in-middle attack, Clock skews, LPM, LSF, WLAN***

## I. INTRODUCTION

Now days, WLAN is becoming most popular communication medium. WLAN is most fastest growing technology. For communication purpose, using the communication device without requirement of cables has becoming very popular and this method is used everywhere. For providing network access to mobile device, wireless network are being derived. Advantage of WLAN over wired network is because of its features like flexibility, probabilities and its inexpensiveness. But with this advantage, we have considered some security and performance issued related to WLAN.

First we will discuss wireless security issues with respect to wired network. Any client of wired network will access the wired network through Ethernet port of that LAN network. So for accessing the wired network we will require physical access to LAN ports. As in case of wired network the data is transmitted to particular destination only, it is not broadcasted like wireless network, there is less chance of compromising the privacy until someone does not intercept data on their destination path. So in case of wired network the security break issue will only come into picture if LAN network is physically compromised.

Now we will discuss wireless security issues with respect to wireless network. In case of wireless LAN the data transmission is take place through the broadcasting technique. The wireless access point which is configuring on enterprise or organization network without authorization from network admin in enterprise is called as wireless rogue access point. It is also called as unauthorized or illegal AP or fake AP.

The legitimate employee in enterprise network will configure the wireless rogue AP because of two possible reasons. First one is that employee is unaware of enterprises security policies and second one will be he wanted to intentionally place an insider attack within enterprise network with some malicious purpose. The medium used in WLAN is wireless which will introduce a threat called eavesdropping in WLAN network over wireless data communication. In WLAN, the signals are unidirectional and spread beyond intended coverage area within WLAN. So this kind of issue in WLAN make it physical insecure.

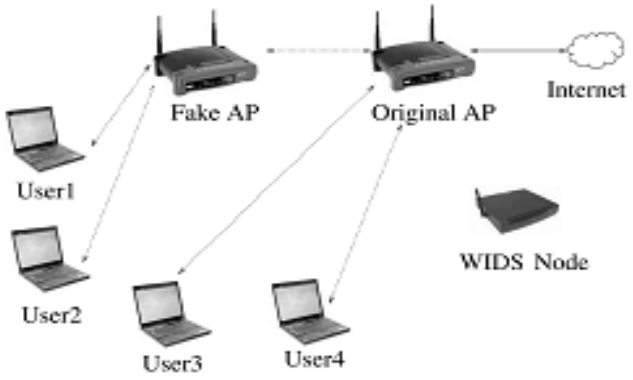


 

Fig. 1 Fake AP detection in WLAN scenario

Now days, for network admin most important issue related to security of WLAN is prevalence of rogue AP. Now in our mind the question arise, why this kind of security problem is major concerned over other security threat. Answer for this is other security threat in WLAN requires technical knowledge and require costly devices. But in case of rogue AP, one should not require to have much security knowledge of WLAN.

As rogue AP create the security hole into enterprise network, it will open the backdoors for the outsiders bypassing all wired security measures such as firewalls and network access control (NAC). In this way rogue AP poses major security threat to enterprises organizational network. RAP in literature is called as unauthorized AP. In secure network, wireless access point has been installed without authorization from the local admin. It has been created for attacker to have man-in-middle attack.

## II. SOFTWARE ARCHITECTURE

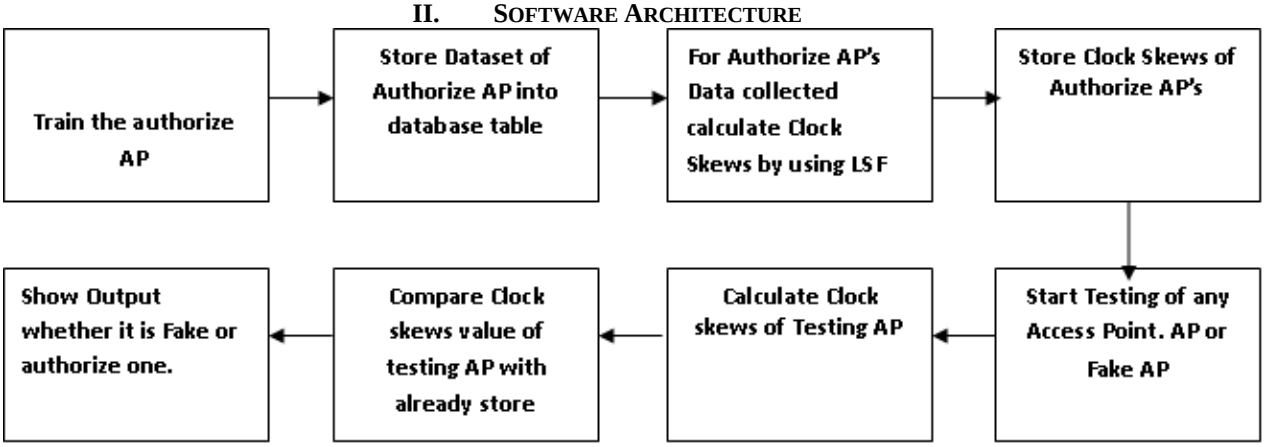


Fig.2 Architecture Diagram

The above diagram shows the software architecture of our rogue access detection system. It contains 8 main blocks. Each block has its own purposed. First block is for getting training dataset from the authorized Access point within wireless network. Dataset contains the beacon frame received from the authorized AP. For calculation of APs clock skew we have used timestamp values from this beacon frames. Once these values are retrieved from the beacon frames, we have calculated the clock skew of AP and we have store clock skew value of the AP in database for future used. The clock skew value is calculated by using LSF and LPM method. LSF has show better result as compare to the LPM method. Once we have done all processing with the authorized AP.

Next we proceed with the unauthorized AP. Same process we will do with the unauthorized AP. First we will have dataset for unauthorized AP. That dataset contain again beacon frame values. Again we calculate clock skew for unauthorized AP using same algorithm i.e. LPM and LSF. After that we will compare the clock skews value of both authorized and unauthorized AP. Depending upon comparison we will display the result weather candidate AP for given testing is fake or authorized one.

At last we will show the result in form of the graph.

## III. IMPLEMENTATION OF SYSTEM :

The authorized AP used in our case is TP-LINK. The system on which scanning and testing is perform is called as WIDS node. This system configuration for WIDS node is as Acer 4GB RAM having I3 processor running Windows. We use wireless card— Intel PRO. Wireless card used for capturing beacon frames. For Windows we have used jNetpcap and win cap libraries. While implementing the rogue access point detection system, the whole system is divided into three modules. First module is requiring for scanning and maintains the beacon frames of authorized AP. After that second module will contain the actual calculation of clock skew value of AP from store beacon frame values which are collected during first module. For calculation purpose we have used the two algorithms. First we have calculated clock skew value by using linear programming method and then by using least square fitting method. The LSF method has better result as compare to LPM method. Following are equation for LPM and LSF method for calculating clock skew.

$\frac{1}{n}\sum_{i=1}^{n}(\delta.x_i + \emptyset - O_i) = 0$ ……. By LPM (1)

$\sum_{i=1}^{n}(Oi - (\delta.x_i + \emptyset))^2$ …..... By LSF (2)

Where,

$\delta$ =is the slope of the line which the clock skew

$\emptyset$= is the y-intercept

Oi->Estimated offset of it frame

Xi -> Time difference between arrival of 1st and ith frame at fingerprinting node

Once we have done with calculation of clock skew value of authorized AP. Next we have to do testing. For testing candidate AP, the same process of calculation of clock skew is follow. After that the clock skew values of tested AP and authorized AP are compare and result are shown in form of graph.

 

Flowchart for Fake AP Detection

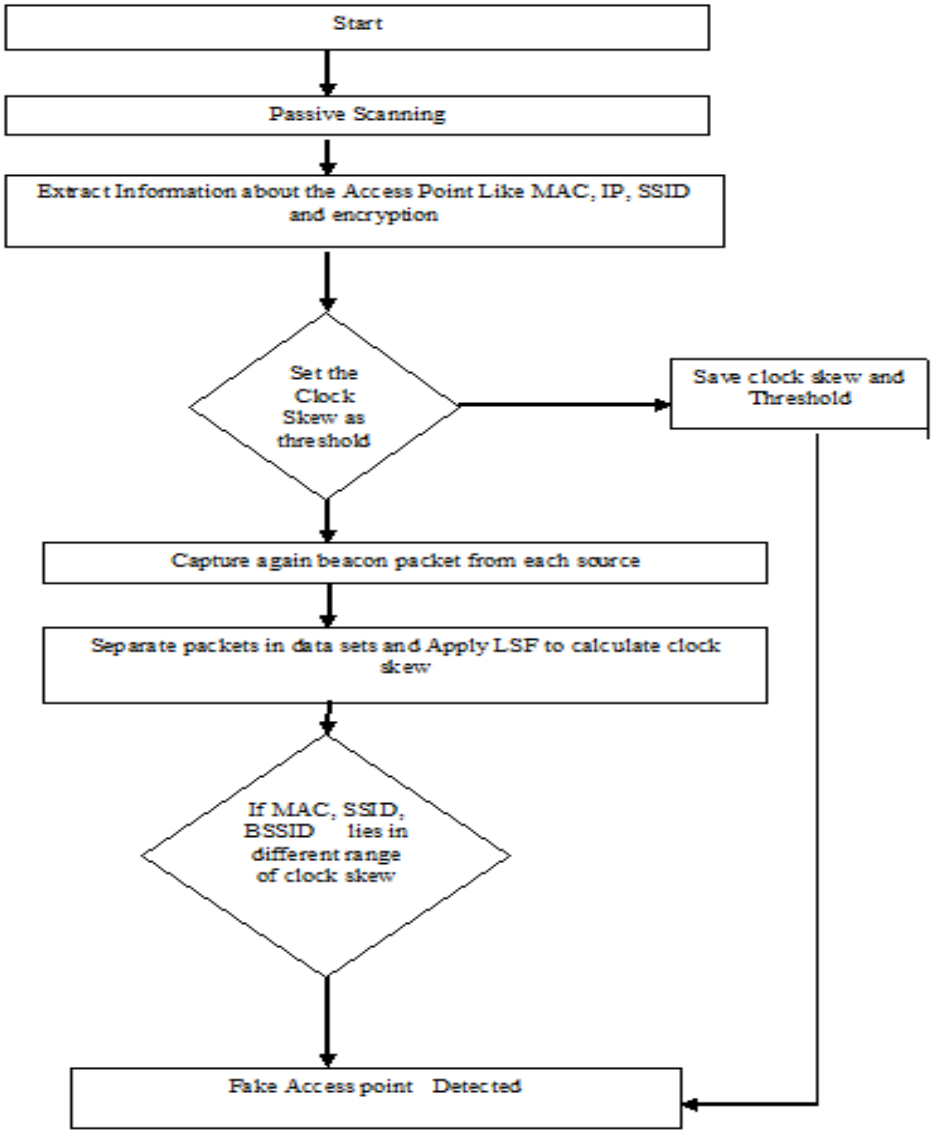


Fig. 3 Flowchart for Fake AP Detection

## IV. THE EXPERIMENTAL RESULT

Here we will show some result which come out of experimental setup.

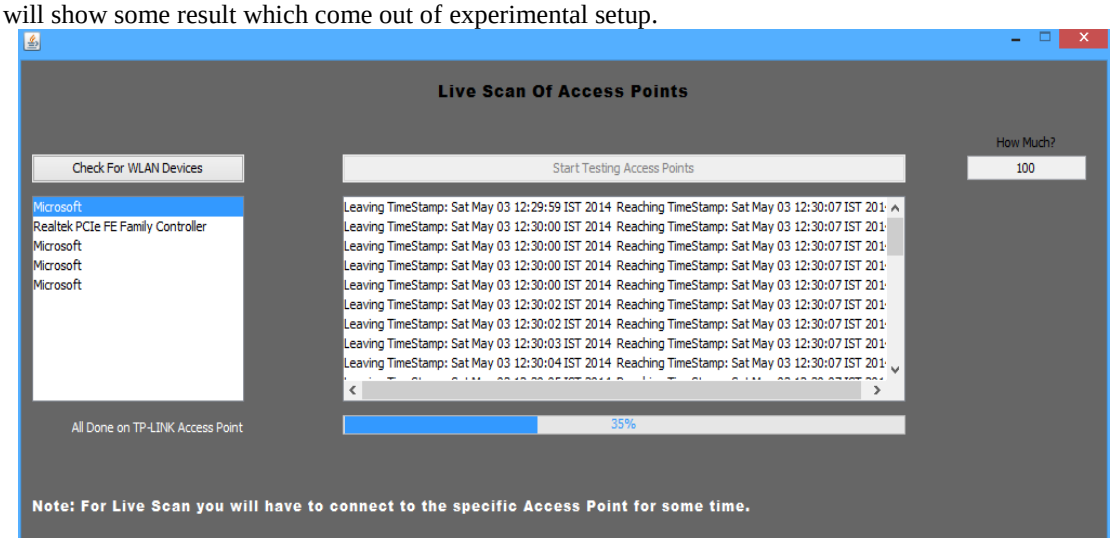


Fig. 4 Output window of Testing of Access Point.

 

The above window shows the process of receiving the beacon frames from particular AP for calculation of clock skew. For that purpose we have to connect to particular AP and then for receiving the beacon frames in our system we have select appropriate WLAN device. In above scenario, the Microsoft option is selected.

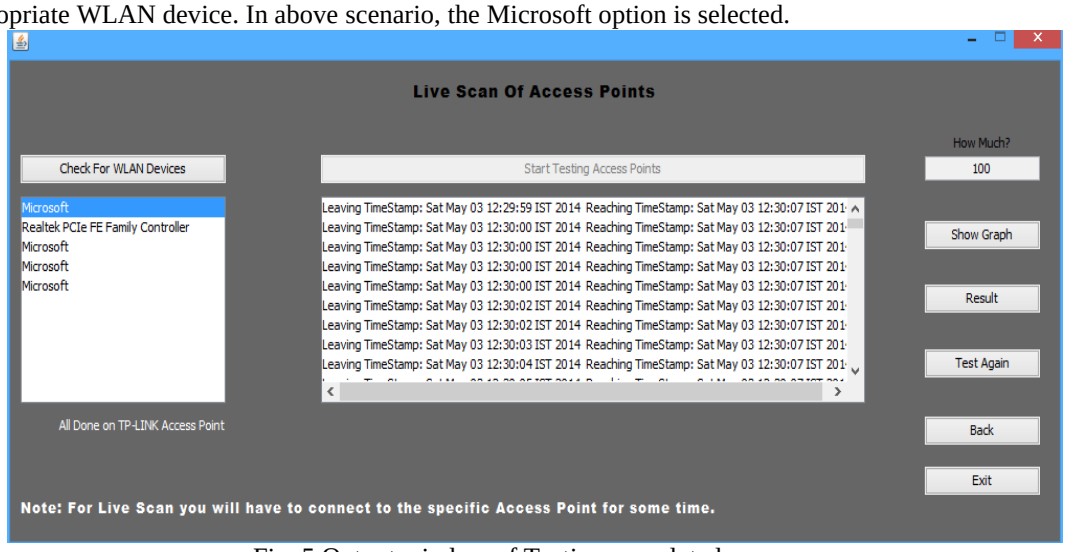


Fig. 5 Output window of Testing completed process

The beacon frame receiving process is completed and clock skew is calculated and is stored in database. Different options are shown on the window like show graph, result, test again, and exist.

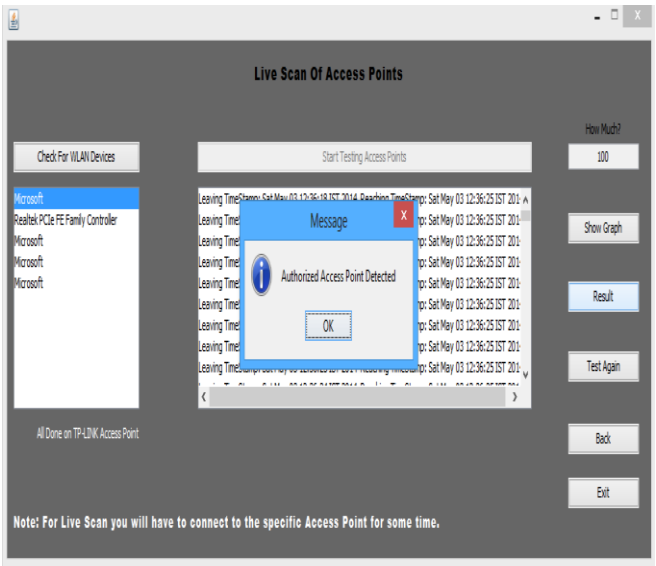


Fig. 6 Output window of Authorized AP detected.

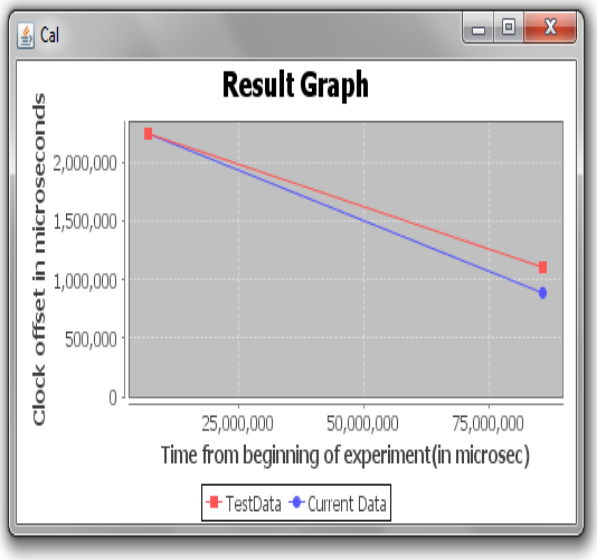


Fig. 7 Output window of Authorized AP's Graph

The above two window show the testing result of authorized AP. When authorized AP is tested clock skew is calculated for candidate AP to be tested and its result is compare with already store clock skew value of the authorized AP. Depending upon comparison result, the result of authorized AP is shown into message window and graph is shown.
In above given graph, red line shows the threshold value. Clock skew is shown by slop line. For candidate AP to be tested, slop line is shown by blue line. If clock skew line of candidate AP to be tested is below the threshold value, then authorized AP is detected.

 

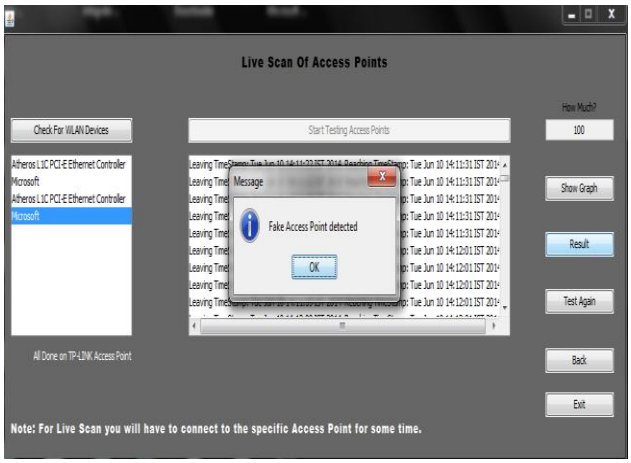


Fig. 8 Output window of Fake / unauthorized AP detected.

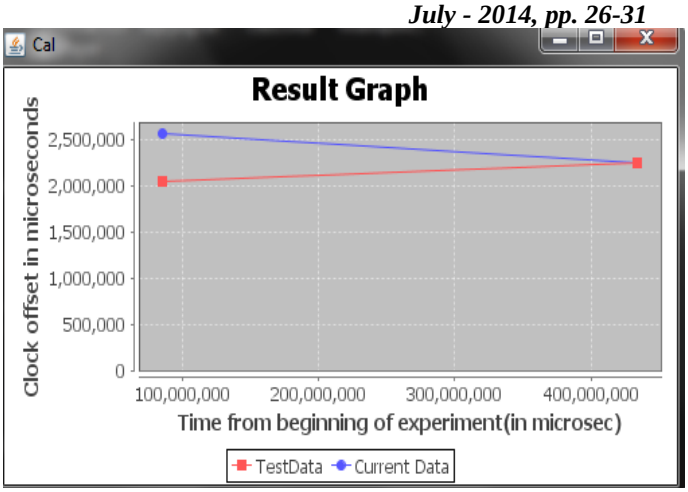


Fig. 9 Output window of Fake/ unauthorized AP's Graph

The above two window show the testing result of unauthorized AP. When unauthorized AP is tested clock skew is calculated for candidate AP to be tested and its result is compare with already store clock skew value of the authorized AP. Depending upon comparison result, the result of unauthorized AP is shown into message window and graph is shown.

In above given graph, red line shows the threshold value. For candidate AP to be tested, slop line is shown by blue line. If clock skew line of candidate AP to be tested is above the threshold value, then fake AP is detected.

| No. of Packet | LPM | LSF |
|---|---|---|
| 100 | 50.89842459542978 | 50.57207420581314 |
| 200 | 93.80088593838573 | 93.7838909881677 |
| 300 | 85.32188950561931 | 85.17843729192961 |

Fig. 10 Clock skew value of authorized AP by LSF and LPM method.

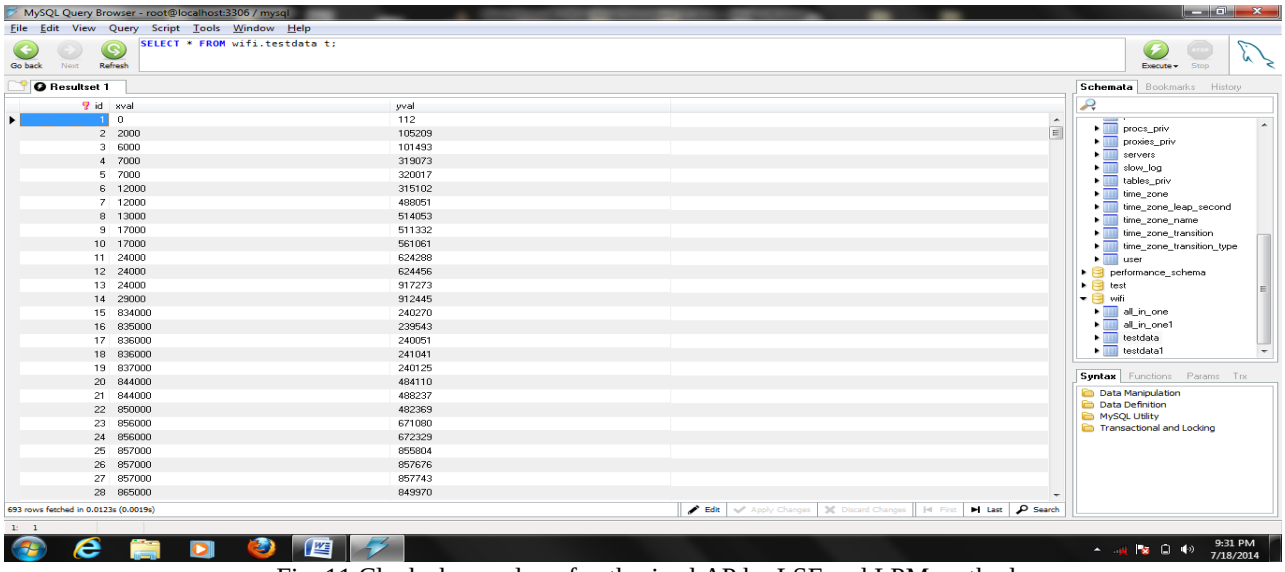


Fig. 11 Clock skew value of authorized AP by LSF and LPM method.

The above two window shows the different database values store. First window show the clock skew value of particular AP calculates by using the LPM and LSF method. The second window shows the x and y values which are required for calculation of clock skew.

## V. CONCLUSION

From experimental setup we have in our laboratory, we have collected the beacon frame from authorized AP, and from that data collected. We have calculated clock skew and save it in database for future used. Then we have collected beacon frames from candidate AP which we have to be tested and then again calculate clock skew and compare it with authorized one and come to conclusion.

 

We have make used of clock skew for purposed of detection of detection of fake AP. Clock skew of access point is calculated from beacon frame. We have successfully calculate clock skew faster and with less packet number as compare to existing TCP/ICMP based techniques.

**REFERENCES**

[1] Prof S.B.Vanjale, Mr. Jay Dave "Unapproved Access Point Elimination In WLAN Using Multiple Agents And Skew Intervals" in International Journal of engineering science and Technology, IJEST Vol. 4 , No.02 , February 2012

[2] A.V.Dhaygude, K...R.Patil, A.A.Sawant "Threats to Wireless Local Area Network (WLAN) and Countermeasures", ICONS'0, January 2007, Tamilnadu, India.

[3] Prof S.B.Vanjale, Mr. Amol Kadam "Detecting and Eliminating Rogue Access Point in 802.11 WLAN" in JERS (E-ISSN0976- 7916), Vol.2 Aug 2011-12.

[4] Prof S.B.Vanjale, Mr.Shashi Athavale "Rogue Access Point Detection using MA intelligence" In the International Journal of Computer Applications and Business Intelligence ISSN: 0975-945X April-June 2010 Volume: 01.

[5] uman Jana and Sneha Kumar Kasera" On fast and accurate detection of unauthorized wireless access-points using clock skews" IEEE Transaction on Mobile Computing, Vol.9, No.3, March 2010.

[6] Ms Sushama Shrike, Prof S. B. Vanjale "Rogue Access Point Detection using time stamp" International Journal of advanced Computer and mathematical sciences ISSN: 2230-9624 Volume: 2, June 2011.

[7] "AirMagnet" Available: http://www.airmagnet.com/.

[8] A. Adya, P. Bahl, R. Chandra, L. Qiu, Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks, in: proceedings of the International Conference on Mobile Computing and Networking MobiCom 2004

[9] Prof S.B.Vanjale, Ms. Fatima Inamadar "Illegal Access Point Detection for Wi-Fi Network by Using Hybrid Approach "in International Journal of Engineering Research & Indus Appls (IJERIA) in 2011-12

[10] Nets tumbler, http://www.netstumbler.com.

[11] Security-Standards http://www.sans.org/reading_room/whitepapers/wirelss/overview-80211-wireless-network-security standards-mechanisms_1530

[12] Wireless LAN: Security Issues and Solutions: http://www.sans.org/reading_room/whitepapers/wireless/wireless-lan-security-issues-solutions_1009.

[13] Lanier Watkins, Rahee Beyah, Cherita Corbett "A Passive Approach to Rogue Access Point Detection" 2007 IEEE

[14] Prof S.B.Vanjale , Ms.Snehal Behede "Providing Data Security for Wi-Fi network using mobile agent in distributed system" in International Journal of Advanced Engineering Technology, IJAET/Vol.III/ Issue II/April-June, 2012.

[15] J. Geier, Multipath a potential WLAN problem, Tutorial, Wi-Fi Planet, May 14,2002,http://www.wifiplanet.com/tutorials/article.php/112161.

[16] Evil Twin' fears for wireless net, BBC News, Jan 20, 2005,http://news.bbc.co.uk/2/hi/technology/4190607.

[17] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, D. Wetherall, 802.11 User fingerprinting, in: Proceedings of Mobicom 2007.

[18] Chrisil Arackaparambil, Sergey Bratus, Anna Shubina, and David Kotz "On the Reliability of Wireless Fingerprinting using ClockSkews"

[19] Wireless LAN: Security Issues and Solutions http://www.sans.org/reading_room/whitepapers/wireless/wireless-lan-security-issuessolutions_1009.

[20] L. Xu and E. Oja, "Randomized Hough Transform (RHT): Basic Mechanisms, Algorithms, and Computational Complexities," CVGIP: Image Understanding, vol. 57, no. 2, pp. 131-154, 1993.

 