International Journal of Advanced Computer and Mathematical Sciences ISSN 2230-9624.
Vol 2, Issue 2, June-2011, pp 111-116 http://bipublication.com

ROGUE ACCESS POINT DETECTION USING TIME STAMP

Sushama Shirke, S. B. Vanjale
B.V.D.U, Pune

ABSTRACT

This is an implementation of the Wireless LAN Intrusion Detection System (WIDS) using clock-skews as a fingerprinting property as suggested by Jana-Kasera [1]. Our objective is to detect the presence of a fake access point (AP) in a Wireless LAN (WLAN). Use of clock -skew enables us to effectively detect Medium Access Control (MAC) Address spoofing. The principle used in this project is that clock s k e w s remain consistent over time for the same AP but vary significantly across APs. We have also tried to explore probable points of failure and implemented algorithms to overcome these problems. Advantage of this implementation is that fake AP can be detected very quickly as WLAN Intrusion Detection System needs only 100 -200 packets in most cases.

***Index Terms*—**IEEE 802.11, fake access point, fingerprint, MAC Address spoofing, timestamps

I. INTRODUCTION

WIRELESS LAN is a broadcast service. As a result, it is quite vulnerable to the various attacks. Different encryption techniques have been devised to provide security to the Wireless Networks. Yet, it seems to be inadequate. Consider an organization X'. It has a wireless broadcast t router which provides service to its employees. A malicious attacker can set up a fake Access Point (AP) which emulates this authorized AP. Now, the attacker can lure the clients of this authorized AP and the clients get connected to the fake AP believing that they are connected to the authorized one. Now, the attacker can easily launch various types of attacks on the connected clients.

Some security mechanisms like new wireless security enhancement 802.11i RSNA (Robust Security Network association) can be used to provide strong mutual authentication between the authorized AP and its clients, But its disadvantage is that it becomes very difficult to manage and verify the digital certificates over the network across different domains. Also, practical limitations to this cryptographic encryption technique can introduce vulnerabilities in the wireless networks using 802.11i RSNA cryptographic encryption techniques. However, the system becomes robust and secure if this technique is combined with validations using the fingerprint of the authorized AP calculated by the clock- skew of the AP with respect to the fingerprinting node.

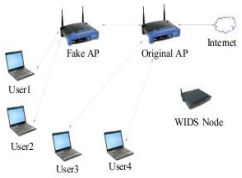


Fig.1. Structure of WLAN Intrusion Detection System.

II. WIRELESS LAN

a. Basic Information

Wireless Communication is one of the fastest growing technologies. IEEE 802.11 is a standard defined by IEEE for specifications of Wireless LAN. This specification over physical and data link layers.

b. Architecture

IEEE 802.11 defines two types of services – Basic Service Set (BSS) and Extended Service Set (ESS). BSS is a building block of wireless s LAN. It contains wireless clients and an optional Access Point (AP). BSS without AP is *ad-hoc* architecture while BSS with AP is called as an

infrastructure network. Two or more BSS connected with a distribution system form an ESS.

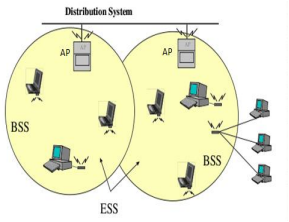


Fig.2. Architecture of the Wireless LAN

IEEE 802.11 s specifies three types of frames for communication –

i. Data Frame: This frame is used for sending receiving data

ii. Control Frame: This type includes various frames such as Request-To-Send (RTS), Clear-To-Send (CTS), ACK, etc.

iii. Management Frame: These frames are used for maintenance of WLAN. Frames such as probe request, probe response, beacon are covered in this type of frames.

In our project, we extensively make use of beacon frame for extracting Timestamp information.

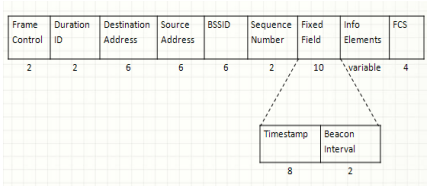


Fig.3. Frame structure of the captured beacon frame

c. Radio Tap Headers

Radio tap Header is also specified by the IEEE 802.11 protocol. It is 32 byte in length. Wireless driver (in this case, Mad Wi-Fi driver for Linux) writes time of arrival of the beacon frame in 8 byte 'Timeval' field in Radio tap header. We extract this field to get the hardware timestamp[ii].

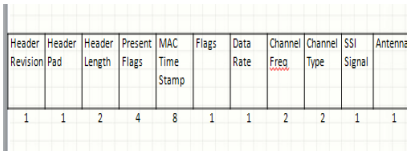


Fig. 4. Structure of Radio tap of Header

III. FAKE ACCESS POINT

A wireless network can be attacked by many ways. One such way is by creation of unauthorized fake Access Point (AP) in the network. A malicious attacker can sniff the beacon frames of authorized AP. He then extracts Medium Access Control (MAC) Address, SSID and BSSID of the authorized AP and puts it into his own frame[iv]. Thus, newly created AP now acts as a duplicate AP of the authorized AP. Once this fake AP is set up, users of authorized AP think that fake AP is the real one and connect to it. Now, the attacker can launch various attacks on these clients[iv].

Fake APs are dangerous than a direct attack on the network. This is due to following reasons.

i. When different clients try to connect to the authorized AP, they use election algorithms that are purely based on signal strength. If the attacker manages to increase its signal strength, he can easily lure the clients into using fake AP instead of authorized one. Once connected, attacker can make sure that client never uses authorized AP again by keeping its signal strength at constant level. Thus, client is now virtually quarantined from the rest of the network of authorized AP and he has no way of knowing this fact.

ii. Beacons sent by fake AP have their fields copied from beacons of authorized AP. As a result, security system can also be fooled as it thinks that packets are coming from authorized AP itself. Thus, fake AP evades its detection. It is difficult to detect the presence of fake AP in a wireless network. It is more difficult to

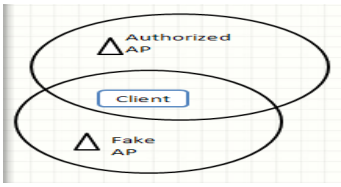
exactly identify the device and block it [ii].
iii. These fake access points can be easily created using beacon sniffers and packet injectors which only need a wireless Network Interface Card (NIC) which can work in monitor mode [iii].
iv. This is why clock-skews come into picture for detection of fake APs. They are discussed in-depth in section V.

IV. THREAT MODEL

a. Scenarios

There are two scenarios in which a fake AP can operate.

i. Authorized AP and fake AP are both active in the network. A client can receive beacons from both the APs. The attacker can keep the signal strength of fake AP above that of authorized AP s o that user will be forced to connect with the fake AP.



ii. Only fake AP is active and authorized AP cannot be reached by the client. This can happen in some situations like failure of authorized AP due to internal reasons or due to attack by the adversary. The attacker can also follow the client beyond the field of influence of authorized AP.

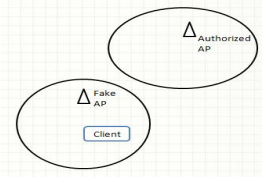


Fig.6. Threat scenario 2

For calculation of clock-s kew, we need to gather time measured by two difference devices. We have made us e of wo types of times tamps in this project as suggested by Kohno and co-authors and verified its usefulness by Jana-Kasera [1].

- Source Times tamp – Whenever a beacon is sent from an access point, the device driver of the AP writes the time of s ending in the times tamp field of Beacon Header. This is called source times tamp.
- TSF Times tamp – Whenever a client receives a frame, the device driver on the client side writes time of arrival as indicated by the client's clock into the times tamp field of Radiotap Header. It is called as Time Synchronization Function (TSF) times tamps. These times tamps help us in determining the exact clock skew between the clock of client / WIDS node and that of an Access Point.

b. Calculation Of Clock Skew

We have used the method explained by Jana-Kasera [1] for the calculation of clock skews. This method can be explained as follows.
Let, Implementation of the Passive online scheme that can detect fake APs can handle both these situations effectively.

T_i = Source Times tamp of i^{th} beacon
t_i = TSF Time Stamp of 1 beacon
We calibrate our system before actual work in the network. As a result we have accurate clock-skew of the authorized AP with which we can compare with detected APs. If more than one AP is detected with same MAC Address, SSID and BSSID but with different clock-skews, we can determine that attack des cried in scenario 1 is taking place. If an AP is found with same MAC Address, SSID and BSSID but having different frame clock-skew than pre-calibrated value, we can determine that attack explained in scenario 2 is taking place.

x_i = Time difference between arrival of 1 fingerprinting node and I frame at us
O_i = Estimated offset of i^{th}
$x_i = t_i - t1$

$o_i = (T_i - T_1) - (t_i - t_1)$

V. CLOCK SKEW

i. Definition

Clock Skew can be defined as the difference in time shown by the clocks at different nodes in the network. It can act as an identifying property for a network device. Thus, using clock-skews, we can uniquely fingerprint up to 512 different APs.Clock-skew arises in a network due to difference between the physical properties of clocks present in different devices connected to network. An electronic clock consists of two parts –

Oscillator – Oscillator is controlled by a crystal and it ticks at a fixed frequency

Counter – It keeps track of number of ticks produced by the oscillator.

Oscillator frequency depends on type of crystal and angle at which the crystal was cut relative to its axes. Practically, no two crystals can have exactly equal frequency of oscillation. This introduces skew in the time measured by different nodes .We plot the graph of (o_i) vs (x_i) which is approximately linear. Slope of this line represents the clock-skew between the AP and WIDS node.

To estimate the value of clock-skew, we can use two different methods.

a. Linear Programming Method (LPM)

In this method, we have to minimize the function

$$\frac{1}{n}\sum_{i=1}^{n}(\delta x_i - \phi - oi)$$

Where δ is the estimated clock skew.

Limitation of this method is that it has high tolerance towards the outliers. Even if a point lies outside of the line, it treats it as a point on the line. In our calculations , value of clock-skew is calculated at microsecond precision and there is high possibility that LPM will be unable to distinguish between the two APs with closely located clock-skews. As a result, we use Least Square Fitting.

b. Least Square Fit(LSF)

In this method, we have to minimize the function

$$\sum_{i=1}^{n}[o_i - (\delta x_i + \phi)]^2$$

This method allows low tolerance towards outliers. As a result it can distinguish between two APs even if their clock skew values are very closely located. Thus, it helps us in identifying fake APs that have engineered the clock skew very close to the clock skew of authorized AP[i].

Implementation of LSF:

We have already defined a function which we have to minimize.

$$f = \sum_{i=1}^{n}[y_i - (\delta x_i + \phi)]^2$$

Applying standard procedure to find minima, we differentiate it partially with respect to δ and ϕ and equate it to zero.

$\partial f/\partial\delta = 0$ and $\partial f / \partial\phi = 0$

Solving them simultaneously, we get estimated value of δ as –

$$\delta = \frac{n\sum xy - \sum x \sum y}{n\sum x^2 - (\sum x)^2}$$

Thus, we get the clock skew using this result.

VI. IMPLEMENTATION

Approximately 200 beacon frames are sufficient to determine the clock-skew accurately. When these beacons are captured, we estimate the value of δ (*clock-skew*) using the result obtained in previous section. That is, we apply Leas t Square

Fitting.

PHASE I : *Calibration of the System*

The process is described below.

i. This step must be carried out before a wireless network is deployed s o that there is guaranty that no fake AP is active.

ii. System gathers beacon packets from s elected AP.

iii. Maximum value of the s lope of line between various points is determined. This is the *threshold* of clock- skew for differentiating between frames from different APs.

PHASE II: Detection of Fake AP

Values of *threshold* and *clock -skew* are written to the file for us e in Phase II. The process is described below.

i. Capture desired number of packets. Again, 150-200 packets from each source are sufficient to determine accurate clock-skew.

ii. Now, based on *threshold* value, we separate the packets into various data sets.

iii. We apply Leas t Square Fitting (LSF) on each of the datasets and calculate its estimated clock skew.

iv. If we get beacons having same MAC Address, SSID and BSSID but lying in different ranges of clock skew, we can determine that Fake AP is present in the network.

a. Algorithm

WLAN Intrusion Detection System follows a t step process .In the first phase, system is calibrated for the desired AP. In the second phase, system searches for available beacons which are coming from the authorized AP or which seem to come from the authorized AP and then tries to establish whether a fake AP is active or not.

b. Hardware Requirement

TREND net TEW -651BR Wireless Router, HP Pavillion dv4 Laptop having AR9285 wireless network adapter with Atheros Chips et

c. Software Requirement

Platform: Ubuntu Linux 10.04 Lucid Lynx, Environment: Java 6, Additional Libraries: net.s ourceforge.jpcap package with native libpcap library support ,Customized MadWifi device drivers which write TSF times tamps in microsecond precision instead of usual millisecond precision, IDE: Eclipse.

VII. PROBLEM POINTS OF FAILURE AND IT'S SOLUTIONS

Clock-skew of a device with respect to another device remains constant under same external working conditions. But this skew may change due to change in external factors , resulting in failure of WIDS Scheme. As a result, we have to make changes in our implementation s o that the system is immune to these changes.

a. Temperature Variations

Temperature of the core of the AP can change due to various factors. The change can be due to change in atmospheric temperature or it can be due to varying loads on the CPU. The changes in clock-skew because of change in temperature are consistent and gradual. As a result, we implement a rolling signature scheme in which we update the value of clock-skew[i].

b. Virtualization

A virtual AP is an s ingle hardware AP used to simulate multiple APs with different MAC Addresses, SSIDs and BSSIDs. As all virtual APs are simulated on the same hardware, there clock-skew is in the same range as that of the real AP. Hence, even if the authorized AP is using virtualization to implement various APs, our system can detect Fake APs [i].

Engineered Clock skew which imitate that of

authorized access point

Fake AP can copy the value of times tamp from the source beacon. As a result, Fake AP that exhibits clock-skew nearly same as that of authorized AP can be constructed. But when such beacon frame is reconstructed, there is delay of few microseconds between the retransmission of the frame from fake AP. Thus, client will get duplicate frames having different sequence numbers and system will be able to detect the Fake AP. Also, we have implemented Leas t Square Fitting Technique which has very low tolerance towards outliers. Hence, a slight deviation from desired clock-skew can be detected instantaneously.

VIII. RESULTS

a. Calibration Result for TRENDnet651BR

Packets available: 228,clock skew = 5.248028109901964E-5 Calibration Success fully Performed.

b. WIDS in working conditions

Total no. of packets: 218, Set one: 218, Unique AP found!!, Network does not contain any fake AP. Number of AP's detected: 1, Their clock Skews are as follows:
AP No. 0 , clockSkew = 5.182813495610108E-5
The clocks kew of original AP is: 5.248028109901964E-5

IX. FURTHER IMPROVEMENTS

In this implementation, we can only detect the presence of Fake AP and get its clock-skew. But we cannot identify the device physically and take corrective measures to block this device. This facility can be incorporated in the WLAN intrusion Detection System.

REFERENCES

i. S.Jana and S.Kasera, –On Fast and Accurate Detection of Unauthorized Wireless Access Point s Using Clock Skews‖, IEEE T ransact ions on Mobile Computing, vol. 9, no. 3,March 2010

ii. T . Kohno, A. Broido, and K.C. Claffy, –Remot e P hysical Device Fingerprint ing‖ IEEE Trans. Dependable Secure Computing, vol.2, no. 2, pp. 93-108, Apr.-June 2005

iii. B.Forouzan, Data Communicat ion and Net working, McGraw Hill, Fourth Edition

iv. IEEE St andard 802.11 —Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, T he IEEE, Inc., 1999.

v. http://www.madwifi-project.org

vi. http://www.rfakeap.tuxfamily.org

vii. B.V.Ramana, –Higher Engineering Mat hemat ics‖, T ata McGraw Hill

viii. WireShark Net work Analyser, ht t p://www.wireshark.org

ix. Java P acket Sniffer lib

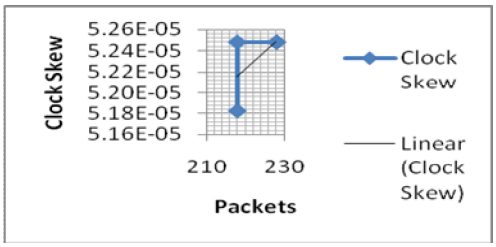


TABLE 1 EXPERIMENTAL RESULT

Packets	Clock Skew Received	Access Point
218	5.18E-05	Authorised
218	5.25E-05	Authorised
228	5.25E-05	Authorised
231	5.25E-05	Authorised
228	5.25E-04	Unauthorised

TABLE 2 OBSERVATION TABLE