International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

Detecting Unauthorized Access Points in Wireless Environment

S.P. Meenakshi[1*], Jacintha Thomas[2], K S Balaji[3], Sathya Narayanan N[4], Shankar Raman[5], V Kamakoti[6]

Department of Computer Science and Engineering, Indian Institute of Technology, Chennai 600036, India

[*]*Corresponding Author: spmeenakshi@vit.ac.in*

Available online at: www.ijcseonline.org

Abstract— The exponential growth in wireless environment ensures extended mobility to the end-users. Mobility provides different levels of flexibity in operation but induces certain security risks. The security risks exist mainly in the form of unauthorized or fake access points to which end users can connect. The illegitimate connections could lead to eavesdropping on the end users and initiating security attacks (such as evil twins exploit). In this paper, we propose a method which uses label-hopping technique to detect fake wireless Access Point (AP). Once detected, such fake AP could be identified and removed from the wireless environment. We use Wireless Local Area Network (WLAN) based environment, as an example for applying the proposed technique. The proposed technique is extensible to mobile wireless networks such as 4^{th}=5^{th} generation mobile.

***Keywords*:** The concept of mobility for end users has intro-duced both security risk and an exponential growth of base stations and Wireless Access Points.

I. INTRODUCTION

Wireless communication is growing at a rapid pace till recently and will be playing an important role in access networks. This can be seen by the widespread adoption of WLANs, cellular networks and emergence of cognitie radio networks [1]. These wireless access networks will be usually interconnected through a wired backbone network. The wired backbone could host a server or could be connected to a wired high-speed router, which then connects to the Internet. The overall architecture described here is shown in Figure 1.

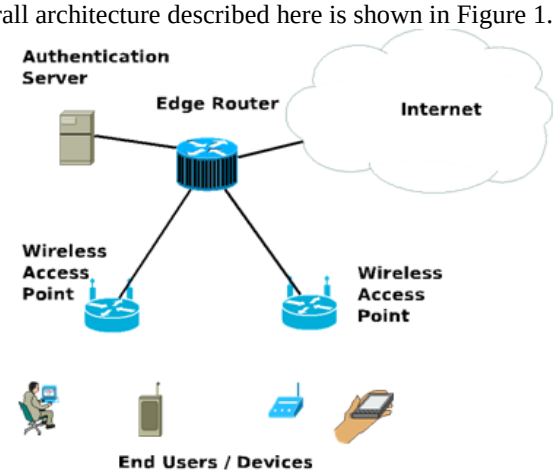

Figure 1. Wired Backbone connecting wireless networks

A fake 802.11 Wireless Access Point (WAP) also called as a rogue AP can be plugged into an organizational network with a valid SSID of another WAP. This is a form of evil twin attack [2]. Available security measures, such as Wired Equivalent Privacy (WEP) etc which are available for preventing unauthorized access have its own pitfalls such as security flaws [3]. The fake APs could as well disrupt the authentication mechanisms and have been identified as one of the most riskier device to have in WLAN environment.

The presence of a fake AP has been discussed detail in literature [3]. Various methods have been pro-posed to detect fake APs. WLAN Intrusion Detection Systems (WIDS) [4] are the first line of defense. Such devices can detect various wireless security threats including fake APs. In the authors have proposed a method to sniff the airwaves to detect presence of fake APs. A set of wireless sniffers can scan the airwaves in its periphery for packet analysis [5]. These sniffers are integrated with APs to perform intrusion detection. These sniffers can be overlaid with APs, by strategically deploying as a separate infrastructure network. Sniffers detecting fake wireless devices listen to all the WLAN channels in the near vicinity. The APs are scanned either sequentially or non-sequentially by using various channel surfing strategies [6].

The other method is to authenticate the access point with a predefined data base [12], or techniques similar to two-factor authencation. A useful technique could be to make use of sound of fan as discussed in [13].

In this paper, we propose a label-hopping technique to detect fake wireless APs. Once detected, such fake APs could be identified and removed from the wireless environment. We

use the IEEE 802.11 protocol used in Wireless AP as an example. The idea can be extend for detection in mobile networks. The advantage of our approach is that the algorithm used here is generic and could be modified to suit wide variety of situations for detecting fake devices.

The rest of the paper is organized as follows: Sec-tion 2 gives a brief introduction to the label hopping al-gorithm. Section 3 discusses how fake Wireless AP can be detected using label hopping and a protocol. The issue of addressing fake devices in mobile networks is addressed in Section 4. The drawback and some mitigation schemes for the label hopping technique is discussed in Section 5. We discuss our future work in Section 6 and conclude with Section 7.

II. LABEL HOPPING TECHNIQUE

In the label hopping technique [7] a router (either the backbone or the Wirelss AP) R_i is initially pro-vided with a set of labels $K = (k_1; k_2; k_3; k_n)$; $n > 1$ and, k_i 6= k_j if i 6= j. Along with this a set of algorithm indices in the form of integers $A = (a_1; a_2; a_m)$; m 1 in the control-plane exchange. Each algorithm a_i generates the set of its own labels which are mutually exclusive with the labels generated by another algorithm a_j in A given a_j 6= a_i. Addi-tionally, we could also generate label d for each data packet where d is based on a random bit selection pattern known only to the backbone router and the wireless AP. This label d when appended as an inner-most label, (with k_i acting as the outer label with respect to d), offers a combination that is hard to spoof by an intermediate attacker.

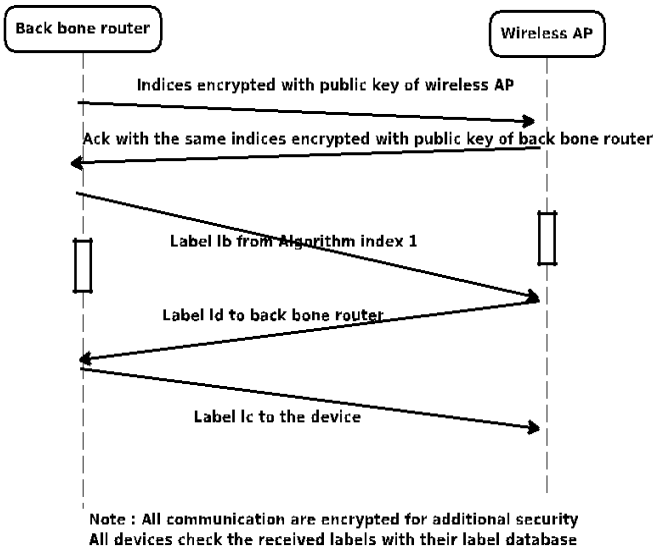

Figure 2. Protocol for detecting and eliminiating fake Wireless AP

The use of additional inner-most label also increases the size of the labels thereby providing protection against attacker guess-ing the labels. We can choose an universal hashing algorithm [8] to ensure that the labels generated are collision-free and are mutually exclusive. However, even if there is a collision, the bit pattern generation for d is not revealed to the hacker. Further, the labels in the set K can be frequently changed and then exchanged by the routers, thereby providing additional security Having understood the basis of the label hopping technique, we will consider its application to two relevant domains, namely fake Wireless AP detection and fake Base Station detection.

III. DETECTING FAKE WIRELESS AP

We will now apply the label hopping technique de-scribed above, to detect fake Wireless AP. There are three parts to the problem,

1) Preventing fake Wireless AP from connecting to the backbone network.
2) If a fake Wireless AP connects the preventing it from continuing operation on the network.
3) Disrupting or removing the fake Wireless AP from the network.

We will discuss each one of them in detail. Figure 2 gives a detail working of the protocol.

3.1. Preventing fake Wireless AP

The label hopping algorithm discussed earlier will provide a direct solution to the problem. Initially, the backbone router and legal wireless AP will exchange the order in which the algorithms will be chosen by transferring the indices. The secure exchange is similar to Diffie Hellman key exchange or any such key ex-change algorithm [9]. Once the indices are exchanged, the back bone router creates a challange by choosing the first algorithm and a random label l_b from the set of labels generated by the algorithm. The wireless AP will then send a label l_d in response, from the set of labels associated with the same algorithm. Note that l_d 6= l_b. The back bone router must again respond with a new label l_c also from the same set from the algorithm. The algorithm will mutually authenticate the back bone router and the device (wireless AP) when l_d 6= l_c 6= l_b. At frequent time intervals the algorithm will change the algorithm indices and re-initiate the exchange process. Given m such algorithm we allow m! number of indices themselves. Therefore detecting the indices themselves becomes a difficult problem to solve by a fake Wireless AP. We now consider the second case.

3.2. Preventing function of fake Wireless AP

Let us assume that somehow a fake Wireless AP is able to guess the index and join the network. In this case the fake wireless AP will be active until the first indices are active.

From the next time period where a different index is chosen the fake Wireless AP will have to guess the newer index and then reproduce the labels. This becomes difficult as choosing 1 index out of m! is a difficult problem. Note that if m is large i.e., the problem becomes more hard. A next logical ques-tion is "How does increasing the labels with respect to an algorithm impact security?". Increasing the labels helps in reducing the m! permutations to be quickly exhausted. However if the number of labels is large, developing a dictionary-based attack [10] will be hard.

3.3. Disruption or removal of fake Wireless AP

Assuming that the backbone router detects a fake Wireless AP, how does it ensure that it does not become live in the network. In this case, a network ad-ministrator can pinpoint the location of fake Wireless AP and remove it physically or they could employ a mechanism similar to cell barring [14], whereby the communication between the backbone and the fake Wireless AP is disrupted. The second part is achieved by deploying a server with the same ethernet medium access control identifier as that of the fake Wireless AP. In this case, any traffic going to the router could as well be rerouted to the server thereby starving the fake Wireless AP of data. We now show how the label hopping technique can be used to detect fake Base Station.

IV.DETECTING FAKE BASE STATION

4.1. Root Cause of the problem

A base station search represents the combined proce-dure of Measurement, Evaluation and Detection pro-cess. A end-user device goes through the search pro-cess first and then the base station selection procedure. A base station search is very tightly related to the base station selection. During base station search, a list of base stations in the near vicinity are scanned. The end-user device internally generates a list of base stations sorted based on decreasing Received Signal Strength Indication (RSSI) order. The final list is generated after carefully measuring and sampling the quality of each base station's synchronization signal. Once the list is completed, the selection procedure starts. The selection procedure involves selecting a suitable base station and decoding the broadcast signal. A suitable base station is the one, that has the best RSSI and within the allowable frequency range. The end-user device camps on to the base station that is suitable.

The end-user device camps to the base station which is having the greatest signal strength (RSSI). The algorithm used in all the end-user devices is a greedy algorithm. The idea of identifying a locally optimal choice based on RSSI leads to selecting the strongest base station. The side effect of this approach is that, the selection method is predictable. This behav-ior is exploited by the rogue base stations, imsi catch-ers and spy devices. In a wireless network, the attacker captures the identity of a legitimate base station. Then builds control frames using the legitimate base station's identity. It then injects the crafted messages when the medium is available. The control signal is broadcasted at same time slots as legitimate base station with high quality and strength. This way the fake base station takes control of the end-user device. Without the ability to detect the legitimacy of a base station, the end-user device might connect to the fake base station everytime. The reason to stick to the same base station is due to a greedy approach in base station selection and not barring the fake base station once detected.

4.2. Algorithm to detect fake base stations

The 802.11 authentication is the first step in network attachment. 802.11 authentication requires a mobile device (station) to establish its identity with an Access Point (AP) or broadband wireless router. In current implementation, a end-user device sends an authenti-cation request to the base station. Then the base station sends a authentication response message. Based on the contents of the message the end-user device tries to attach. If it is not possible it attempts the same procedure on other base station. At this point, there is no data encryption or security mechanisms is available to prevent fake base stations advertisements. All the fake base station can do is just mimic the legitimate base station. Then the fake station can manipulate the frame and send broadcast at legitimate base station time slots.

We present an algorithm that can authenticate the credibility of a base station, thereby removing the fake base station from authenticating itself. Our approach is based on a modified label hopping technique. We assume the access points and end-user devices in near vicinity as issued August 25,set of nodes in a undi-rected graph. Each node in the graph will be connected to a AP/base station. Each base station nodes broad-cast control messages during its own time slot. The control message has necessary information for time synchronization, frequency, channel modes and base station identity. Our idea here is to add one more field namely the label field. The label field will have a random number based on the label hopping algorithm. The same is shown in Table 4.2.

Frame	Id	Addr....	Sequence No	Addr 4	....

QoS control	HT control	Label	Frame body	FCS

TABLE 1. MODIFIED 802.11 FRAME FORMAT

The algorithm A1 used by the base station, can generate a set of random labels. The same algorithm also runs on the end-user device side. Whenever a broadcast message is send by the base station, the end-user device receives the control message and decodes the label. The decoded label is compared with the labels present in the bucket of end-user

device. The presence of label conformsthe validity of the base station.
The advantage of such a method is

(1) Mutual authentication: The label mechanism guarantees only a legal base station and AP could communicate in the wireless network.

(2) Session key establishment: The base station and AP can establish a session based on unique random label. The session guarantees confi-dentiality and integrity of the communication session.

(3) Provision of user revocation: service of the fake base station can be terminated for a definite period of time.

```
Algorithm1 Base station authentication algorithm
Require: None
Begin
    packet = CP-ReceivePacket(node: base sta-tion);
    C[] = ExtractIE(packet); // extract Infomration Elements
    K[] = ExtractLabels(C); // extract the labels TS[] = ExtractTimeSlices(packet); // extract the time slices
    B = selectHashAlgorithm enduser(A[i], TS); // hash algorithm to use
                    If compare key(B, K),
        Camp on base station
    else
        Terminate connection and bar base station.
End
```

$$\text{legitimacy}_i = \begin{cases} 1; & \text{if } BT_{key}^{i} \; MS_{key}^{j} \; 8\text{keys} \\ 0; & \text{Otherwise.} \end{cases} \quad (1)$$

where BT is the base station and MS is the mobile station.

V. DRAWBACKS OF THE LABEL HOPPING APPROACH

There are certain drawbacks in the current scheme. We now discuss a few of them. The proposal is vulnerabe to dictionary-based at-tacks where the person in the middle (PITM) can observe the labels that are passed and then group them. However this requires detecting m disjoint mutually exclusive groups and then the corresponding labels. Even if the person sees all the labels ("M K"), grouping them becomes extremely diffcult as there could be KC_M groupings possible. If K and M are large the problem becomes hard to solve.

A random number based attack is possible. In this case, as discussed in Section 3.2, the fake Wireless AP or the fake device will be present in the network for a brief period of time before it is shut off from the network.

VI. DISCUSSION AND FUTURE WORK

We will divide the future work into two parts (a) on wireless AP and (b) on base stations. In both the cases, the algorithm could use asymmetric encryption using public and private keys. Since many of these devices support SSL, we could as well use these certificates. From the implementation point of view, the foot print of the code is very minimal and based on our implementation experience it runs to less than 2000 assembly language instructions. This excludes the labels that are generated. We had implemented a mechanism similar to the hashing technique discussed in [11].

We will also study the algorithm for performance of this technique in a live network. One other area for work is to study the different types of attacks that are possible on this technique and methods to mitigate them. We had already mentioned dictionary based attack and technique to mitigate the same. Rushing attacks, Byzantine attacks and replay attacks will be studied in the future.

VII. CONCLUSION

The concept of mobility for end users has intro-duced both security risk and an exponential growth of base stations and Wireless Access Points. The security risk comes in terms of fake Access Points, Base Sta-tions to which a device might associate itself, there by exposing its data to unauthorized users. We presented a technique by whcih fake access points could be detected in a wireless network using label hopping technique. The proposed technique is extensible to other forms of Wireless Networks such as 4=5 Gener-ation mobile networks.

ACKNOWLEDGMENT

The authors would like to thank M Ramya, Balaji Venkat Venkataswami and R Monica, for helping us during critical course of the work.

REFERENCES

[1] N. Sathya Narayanan, Milan Patnaik, V. Kamakoti, ProMAC: *A proactive model predictive control based MAC protocol for cognitive radio vehicular networks, Computer Commu-nications*, Volume 93, 2016, Pages 27-38,ISSN0140-3664, https://doi.org/10.1016/j.comcom.2016.05.012.

[2] K. Bauer, H. Gonzales and D. McCoy, *Mitigating Evil Twin Attacks* in 802.11, IEEE International Performance, Com-puting and Communications Conference, Austin, Texas, 2008, pp. 513-516. doi: 10:1109/PCCC.2008.4745081

[3] M. Martellini, A. Stanislav, S Gaycken, and C. Wilson, *Information Security of Highly Critical Wireless Networks*, Springer International Publishing, 2017, pp. 11-15. doi: 10.1007=978-3-319-52905-9 4

[4] D. Pleskonjic, S. Omerovic, and S. Tomazic, *Network Sys-tems Intrusion: Concept, Detection, Decision, and Prevention, IPSI BgD Transactions on Internet Research*, vol. 3(1), 2007.

[5] Anik Shah, Animesh Shah, *"A Survey: Wireless Lan Security Protocols",* IJECS, vol. 4, no. 3, pp. 10968-10971, March 2015.
[6] U. Deshpande, T. Henderson, D. Kotz. *Channel sampling strategies for monitoring wireless networks., In: Proceedings of the second workshop on wireless network measurements*, Boston, April 2006.
[7] S Raman, B Venkat, G Raina, *Mitigating Some Security Attacks in MPLS-VPN Model "C",* International Journal on Advances in Networks and Services, vol. 5(3 4),2012.
[8] J.Lawrence Carter, M. N.Wegman, Universal classes of hash functions Elseveir Journal of Computer and System Sciences, vol. 8(2), pp. 143154, 1979.
[9] V Boyko, P MacKenzie, and S Patel, *Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman*, *Advances in Cryptology — EUROCRYPT* 2000, Springer, Ed.B Preneel, pp.156171, 2000.
[10] D Wang, P Wang, *Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards., In: Desmedt* Y. (eds) Information Security. Lecture Notes in Computer Science, vol 7807. Springer, 2015.
[11] T H Cormen, C E Leiserson, R L Rivest, C Stein, *Introduction algorithms*, MIT press, 2009.
[12] Ting, M T David, O Hussain, and G LaRoche, *Systems and methods for multi-factor authentication*, U.S. Patent 9; 118; 656, 2015.
[13] N Karapanos, M Claudio Marforio, S Claudio and C Srdjan, *Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound*,In USENIX Security Symposium, pp. 483 498,2015.
[14] Romero, Francisco Javier Dominguez, Kyriakos Exadactylos, and Andrea De Pasquale. *"Cell barring in a cellular communi-cation network."* U.S. Patent 8,718,655, issued May 6, 2014.

