Recognizing Illegitimate Access Points Based on Static Features: a Case Study in a Campus Wifi Network

Franklin Tchakounté[1], Michael Nakoe[1], Blaise Omer Yenke[2], Kalum Priyanath Udagepola[3]

[1]Department of Mathematics and Computer Science, Faculty of Science, University of Ngaoundéré; Po.Box 454, Ngaoundéré, Cameroon
[2]Department of Computer Engineering; University Institute of Technology; Po.Box 455, Ngaoundéré, Cameroon
[3]Department of Information and Computing Sciences; Scientific Research Development Institute of Technology Australia, Australia

tchafros@gmail.com, nakoemichael@gmail.com, byenke@yahoo.com, kalum_udage@yahoo.com

ABSTRACT

Wireless networks are useful to disseminate information across an institution. However, access points are often abandoned with vulnerable security protocols and the network is maliciously infiltrated by illegitimate access points called rogue access points. Research works dealing with the identification of rogue access points are limited to inaccurate information such as the strength of the signal and the communication channel. Indeed, the strength of the signal depends on the proximity to the access point. Each normal communication can be done on several channels; one cannot a priori determine a legitimate channel with such criteria. A reasoning based on two principles guided this research: the hacker needs to divert as many users as possible. For that, the security policy will be opened most of the time. In addition, since the administrator has an accurate view of the network, ad-hoc connections may reveal suspicion. This work proposes therefore an approach based additionally on the communication mode and the security protocol. Moreover, an experiment-based on wardriving reveals the Medium Access Control (MAC) address and the Service Set Identifier (SSID) as useful information for the identification of intruder access points. A test phase demonstrated that the proposed method can detect traces of intruder access points.

KEYWORDS

Intruder, MAC, Rogue Access Points, Security, SSID, Wardriving, Wireless

INTRODUCTION

Wireless equipment’s are growing increasingly at a worldwide scale due to their deployment and maintenance simplicity. These capabilities make them more preferred than wired solutions [1]. Their openness and ignorance of users in terms of security make them vulnerable. Attackers target protocol security flaws and bad management of access codes. One of the severe malicious techniques is the infiltration wireless access points unknown to the administrator of the network. Access points, in this case, are called rogue access points (RAP). Considerable efforts have been realized to solve that problem by trying to identify RAP based on static features Ease of use [2-8]. However, they are limited because they are based on imprecise information such as the signal strength and the communication channel. Indeed, the strength of the signal depends on the proximity with the access point. Moreover, each normal communication can be done on several channels. Identifying a legitimate access point (AP) based on channel is a priori infeasible. Two principles guide this work. The first one is that the attacker is concerned to lure (potential victims) that is why the security protocol is let opened. The second one is that the administrator is the only one having the complete view of its network. Ad-hoc connections are used for monitoring the network state or to make configurations. Illegitimate APs does not belong to the network architecture and ad-hoc communications on them can reveal malicious activities. This work proposes to identify illegitimate APs based on security protocol, communication type and Service Set Identifier (SSID). Information collection and extraction are done via network sniffing through wardriving techniques and

Wireshark commands. Experimentations indicate that the MAC address is to be considered. A helpful guidance on the security risks is suggested to improve user awareness.

This work is structured in four sections. The first section reviews existing works related to AP security in general and to the detection of illegitimate APs in particular. The second section defines relevant concepts exploited in the proposed scheme. The third section describes the experimentation of collecting information in campus sites using wardriving tools. An analysis is made to determine the useful information required for detection of malicious APs. The fourth section proposes a detection strategy of intruder access points. The fifth section makes some tests on real networking cases. The document ends with a conclusion and perspectives.

2 RELATED WORKS

This section studies existing works related to the improvement of the security of wireless networks

2.1 Detection of Rogue Access Points

According to [9], a rogue access point (RAP) is a wireless access point infiltrated in a deployed network any approbation of the administrator, providing unauthorized access. Some authors propose approaches to determine RAPs in a wireless network [10]. Ying et al. [2] proposed a server-side solution using clock skews of access point in a wireless network. In this approach, clock skews are used as a fingerprint to detect RAP in a network. Clock skews are calculated using the time stamp values from the beacon frames. This approach cannot detect MAC spoofing and has a lack of accuracy and speed in the calculation of clock skews in TCP/ICMP. Nikbakhsh *et al.* [6] elaborated a client-side approach checking footbridges through which packages convey in transit. It is easy to implement on mobile devices. But the attacker can easily break the security by using utility programs. Yang *et al.* proposed to exploit fundamental communication structures and properties of RAP attacks in wireless networks and to design new active, statistical, and anomaly detection algorithms. Their preliminary evaluation in real-world widely deployed 802.11b and 802.11g wireless networks shows very promising results. It can identify evil twins with a very high detection rate while maintaining a very low false positive rate. Kim *et al.* [5] proposed a client-side approach using the concept of received signal strength (RSS) for RAP detection. In this method, highly correlated RSS sequences are collected in the wireless devices. After that the received signal is normalized and classified whether the collected signal is multiple or not. For this, a sequential hypothesis technique is used. It is a lightweight solution to overcome the drawbacks of the client-side approach. But in this technique, the distance between the client node and access points while calculating the signal strength was never considered. Distance affects the signal strength, hence reducing the effectiveness of this approach. Kao *et al.* [3] proposed a client-side RAP detection technique based on bottleneck bandwidth analysis. This approach is limited because bottleneck can come from the architecture of the network. SLFAT [4] extracts the arrival time of the special frames with the same length to determine malicious behaviors. SLFAT is limited because bottleneck can impact on the real value of time. Vanjale *et al.* [8] proposed to profile RAPs by combining multiple parameters SSID, MAC address, Received Signal Strength Indicator (RSSI), channel and frequency, authentication type, and radio type. Such strategy makes the selection of parameters random, thus imprecise.

2.2 Protection of 802.11 Layers

Some efforts have been oriented to the protection of the physical layer [11-13], the MAC layer [14], the network layer [15-16] and the transport layer [17]. These works are mainly based on the authentication techniques. This work in contrast relies on static features characterizing wireless APs.

2.3 Utilization of Wardriving

Dobrilovic *et al.* [18] carried out a comparative study in two capital cities: in Hungary (Budapest) and in Serbia (Belgrade). The evaluation of security is made based on information collected using wardriving techniques to wirelessly scan AP configurations in both capital cities. They propose also ways to reduce risks. Kalniņš *et al.* [19] tested the safety of different wireless encryption methods and the Wifi Protected Setup (WPS) function. They made also an online survey to evaluate user awareness on wireless security. They conducted wardriving to collect information to identify the most used encryption methods in Riga town. They reveal that most users are unaware, and that the most of networks use vulnerable protocols. This work is based on wardriving to collect enough AP information.

2.4 Synthesis

The previous works are limited in three points.

- They lack automation in information manipulation (from collection to extraction). This work collects with wardriving tools, outputs directly to the traffic analyzer, which makes commands to facilitate decision making.
- They consider imprecise information such as signal, and channel. This work overcomes by coupling SSID, security protocol, Medium Access Control (MAC) address and communication mode.
- They lack formalism for reproducibility. This work provides an algorithm reproducible in a monitoring tool.

3. BACKGROUND

This section presents some concepts such as Wardriving, features of AP and types of RAPs.

3.1 Wardriving

Wardriving is the act of discovering wireless networks. AP discovery can occur using a variety of transportation methods such as by cars, walking on foot or by rail. This concept has been firstly thought by Pete Shipley[1]. wardriving is performed with equipments such as laptops, with wireless card supporting an external antenna and opensource wardriving software.

3.2 AP Parameters

There are several static parameters to characterize an AP [10].

Identifiers: There are only two identifiers in the IEEE 802.11 standard that can authenticate APs to users. These are the SSID and MAC address (or Basic Service Set Identifier - BSSID) of the AP.

Signal information: The quality of communication between the sensor unit and the access point is indicated by the RSSI value and it is expressed as decibels (dB).

Channel information: Channels transmit the information signals from senders to receivers. The transmitting capacity of the channel is measured in bandwidth in Hertz or its data rate in bits per second.

Security protocols: They are used to authenticate communications from one source to destination. The main authentication schemes are Wired Equivalent Policy (WEP), Wi-Fi Protected Access (WPA), WPA2, and 802.1 X authentications (pre-authentication).

3.3 Rogue Access Point

One of the most common security problems faced by WLANs is the Rogue Access Point (RAP), which is a fake AP that was not installed by the network administrator. According to [16], there are four types of RAPs: evil-twin, improperly configured, unauthorized, and compromised.

Evil-twin: In this category, an AP is imitated using a portable computer on which software such as airbase-ng[2] is installed. The fake AP simulates the SSID and the MAC address of the real AP.

Improperly Configured: This category concerns APs which has not been set with secure parameters such as security protocols.

Unauthorized: This category includes APs which have been installed on a network without authorization of the administrator.

Compromised: In this category, an attacker obtains shared keys on the access point using man-in-the-middle techniques.

This work deals with the first three categories. In this paper, rogue access points and illegitimate are interchangeably used and refer to the same meaning.

[1] www.dis.org/shipley

[2] https://www.aircrack-ng.org/doku.php?id=airbase-ng - A tool for attacking users and APs

4. EXPERIMENTS

This section describes the experimentation process of data collection in in real sites, the observation of main vulnerabilities and the analysis of information to extract useful parameters for profiling RAPs. The experimental approach includes five points: the circumscription of experimental area, selection and justification of collection tools, data collection, and analysis of results and description of parameters.

4.1 Experimentation Area

The study zone of APs is illustrated in Figure 1. This figure represents the University of Ngaoundéré's campus[3], which includes five zones of interest. They are selected because they are provided with Internet access.

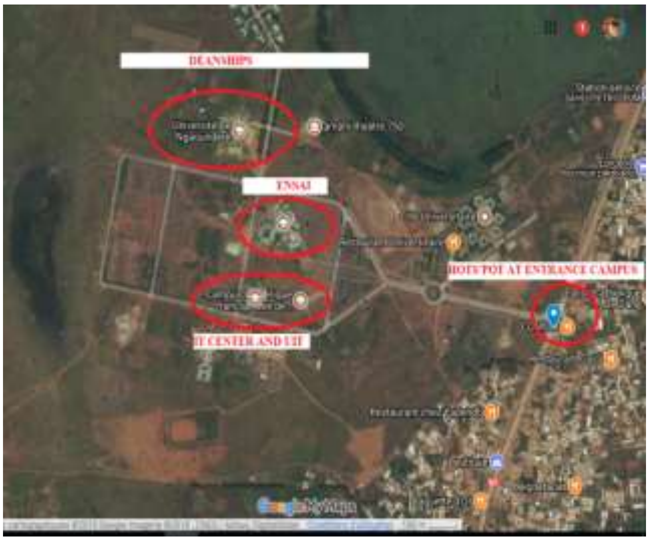


Figure 1: Experimentation area

They are

- The IT Centre (A1);
- The National School of Agro-Industrial Sciences (ENSAI) (A2);
- The University Institute of Technology (UIT) (A3);
- The Deanships (A4);
- The Hotspot at the campus's entrance (A5).

4.2 Collection Tools

Hardware

A laptop with the following characteristics has been used:

- Constructor: HP Pavilion dm4
- Processor: Intel(R) core(TM) i5 CP UM460 @ 2,53 GHZ
- Memory: 8.00 GB
- Operating system: Kali-linux-2016:2-amd64
- Wifi network card: Broadcom 802.11n

A Wireless USB Adapter antenna (USB 802.11n 150 bps) has been attached to the computer to enlarge the scanning area.
For the sake of mobility, a smartphone with the following characteristics has been used.

- Samsung Galaxy Grand Neo Plus GT-I9060I core4 4xARM Cortex - A7@1:20GHz.
- RAM: 1GB.
- Android version 4.4.4

Software

The sniffing was made with Kismet and the packet analyzer Wireshark[4]. The data collection is made via Kismet and Wigle[5]. These applications are selected because they allow exporting data from wireless access points into .kml and .xml files to manipulate maps, and .csv file for statistical analysis. They extract considerable amount of information relatively to other similar tools. The smartphone and laptop have been employed for scanning and collection purposes.

4.3 Data Collection

Figure 2 shows the data collection carried out within the campus. It presents the five areas A1 to A5. The green and red legends represent the access points scanned in those areas. Table 1 presents the number of APs per area.

[3] www.univ-ndere.cm

[4] https://www.wireshark.org/

[5] https://wigle.net/

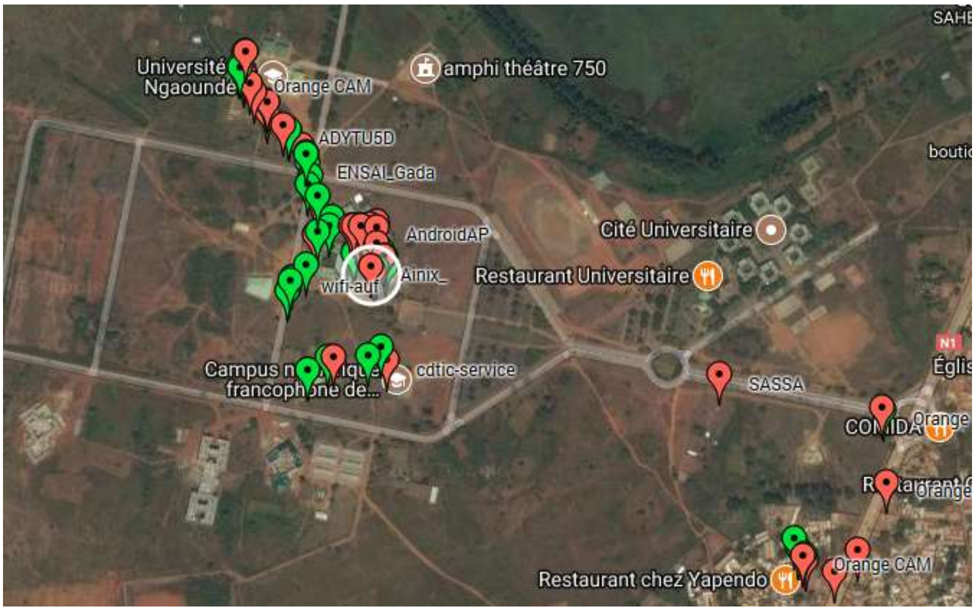


Figure 2: Experimentation area after scanning

Table 1: Number of AP per area

Areas	Number of APs
A1	15
A2	34
A3	10
A4	09
A5	13

4.4 Analysis of Results

The acquired data are processed and statistically analyzed to establish a statistical report. The following features are reported: the use of channel, SSID statistics, and information on security protocols (WEP, WPA, WPA2, WPS and in mixed mode), location information and security statistics according to the CSV format lines. A line is structured as follows: AA: AA: AA: AA: AA; BB; [WPA - PSK - TKIP] [ESS]; 6=20=201513: 57; 6; -97; 44:8185463; 20:3735048; 0; 336; WIFI. The different fields are separated with a semi-column and described as follows.

- The first field represents the AP’s MAC address of the access point.
- The second field represents the AP’s SSID.
- The third field represents the type of security of the scanned AP. In this work, 11 different types of security have been identified. The partial list is given in Table 3.
- The fourth field represents the date and the period of scanning.
- The fifth field represents the channel or the frequency used by the AP (channels varies from 1 to 13).
- The sixth field represents RSSI.
- The seventh, eighth, ninth and tenth field represent respectively the geographic coordinates of the AP including latitude, longitude, altitude, and exactitude.
- The last column represents the detected network type (Wifi or Global System for Mobile Communications (GSM)).

Statistical analysis

A. Security protocols

A set of 81 APs has been scanned. The diagram shown in Figure 3 represents their proportions. The protocol mostly used was WPA2, which is the most secured one. However, there are many users who still use WEP, the most vulnerable one (10 APs). It appeals to education and sensitization of users. Open authentications have been found but was belonging to captive portals.

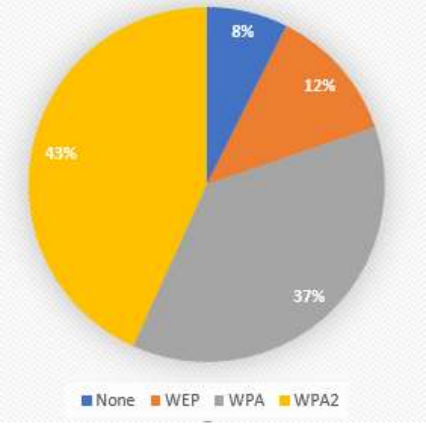


Figure 3: Repartition of security protocols

B. Communication channels

Table 2 shows proportions of use of channels (from 1 to 13) in the scanned APs. The channel the most used was the channel 6. Channels 1, 6, and 11 are the only non-overlapping one in the 2.4 GHz band. Selecting one or more of these channels is relevant to setting up network[6].

Table 2: Communication channels

Used channel	Number of APs
1	21
2	08
3	0
4	0
5	06
6	20
7	0
8	06
9	06
10	06
11	08
12	00
13	00

C. Sub-security types

Authors in literature do not consider sub-protocols of the known ones. For example, WPA includes WPA-PSK-TKIP. Table 3 represents the security type and other protocols used by APs. The frequent sub-protocol is [WPA-PSK-TKIP][ESS] according to Figure 4.

Table 3: Communication channels

Type	Security type	#AP
1	[ESS]	04
2	[WPS][ESS]	02
3	[WEP][ESS]	10
4	[WPA-PSK-TKIP][ESS]	30
5	[WPA2-PSK-CCMP][ESS]	05
6	[WPA2-PSK-CCMP][ESS][SEC80]	05
7	[WPA2-PSK-CCMP][WPS][ESS]	05
8	[WPA2-PSK-CCMP+TKIP][ESS]	04
9	[WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP][ESS][ESS]	05
10	[WPA2-PSK-CCMP+TKIP][WPA2-PSK-CCMP+TKIP][ESS][WPS][ESS]	10
11	[WPA2-EAP-CCMP+TKIP-preauth][ESS][ESS]	01

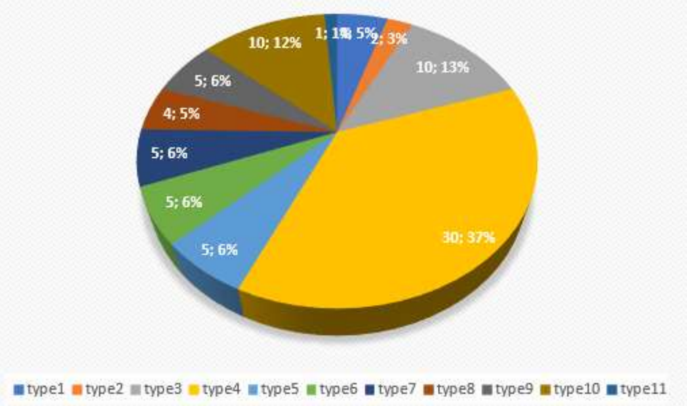


Figure 4: Repartition of security types

4.5 Observations

Some observations are important to be considered.

- It has been noticed APs with the same SSID. It means that there are illegal APs.
- Access points with considerable traffic provide high enough signals if client hosts are closer.

4.6 Justification of Selected Parameters

This experimentation demonstrates that some parameters are relevant.

- SSID: there can be many access points having the same SSID in a same network. Without SSID, it is difficult to communicate and to interact with each other.
- MAC address: It is an identifier proper to a computer.
- Types of security protocols: they are important for transmission authentication.
- Communication mode: there are two modes: ad-hoc mode and infrastructure mode. During the experimentation, this feature has

[6] https://www.metageek.com/training/resources/why-channels-1-6-11.html

been hard to be seen. It can be used to indicate abnormal activities.

5. DETECTION OF VULNERABLE AND ILLEGITIMATE APs

The experimentation has revealed vulnerabilities, the presence of illegal SSID which indicate the consideration of some features in identifying legitimate APs. This section proposes an approach to recognize illegitimate APs while taking into account information such features.

5.1. Assumptions

The detection proposal is supported by some assumptions.

Legitimate hosts: A host is considered as an access point or a computer. In the first case, it is an AP for which the MAC address and the holder can be certified by the administrator. In the second case, it is a computer client recognized as being part of the network by the administrator.

Suspected hosts: illegitimate hosts (AP or computer) are considered as potentially malicious thus are suspected.

It is assumed that the administrator detains the perfect knowledge of the entire network, and maintains databases of legitimate, illegitimate, and suspected hosts.

5.2. Architecture

As shown in Figure 5, the architecture of the proposed approach is made of four layers: collection layer, extraction layer, decision layer and alert layer.

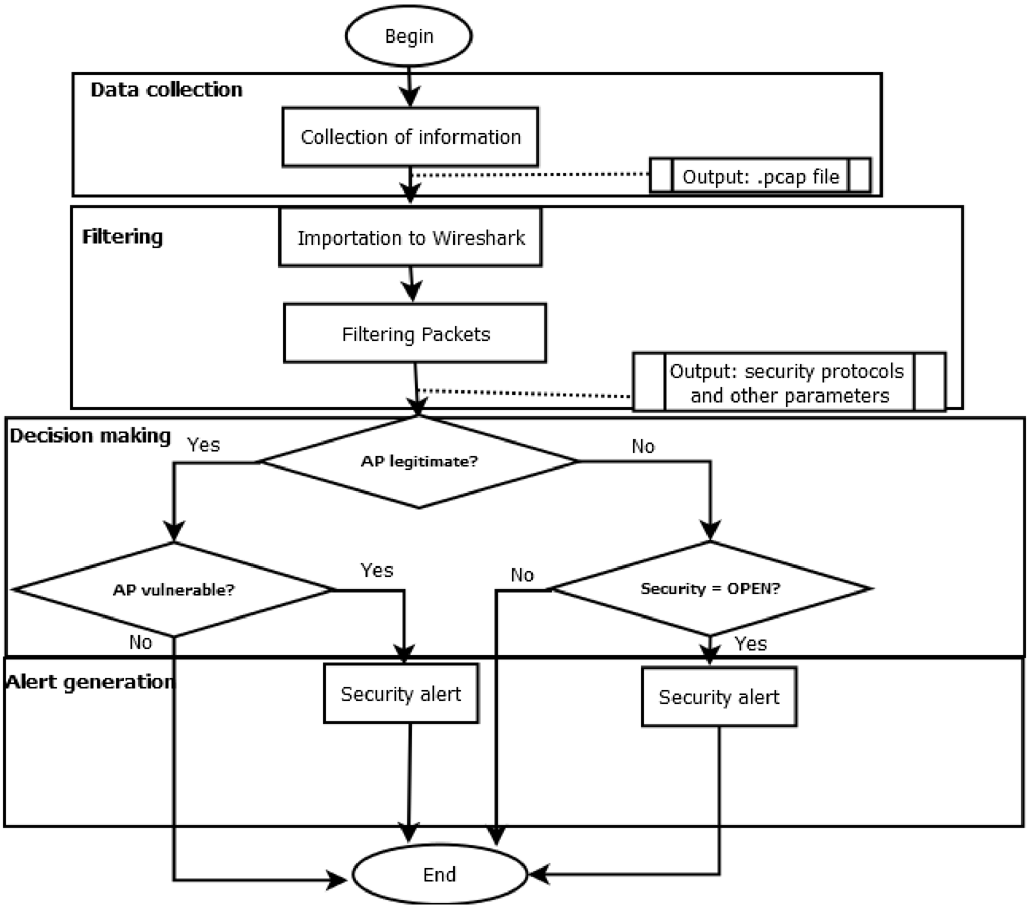


Figure 5: Architecture

Data collection

The collection of data inherent to access points is made by using wardriving tools described in the experimentation section. Information are collected via the collection equipment and then kept into a .pcap file to be used later for analysis purposes.

Filtering of parameters

This stage consists of filtering with Wireshark commands to extract useful parameters from the

.pcap file. This process enables to mark traces of vulnerabilities.

- SSID extraction: This stage checks the scanned AP names and stores in a text (.txt) file.
- Extraction of BSSID and communication mode: This stage consists to extract from the exchanged messages, MAC address and communication mode fields corresponding to SSID of scanned legitimated APs.
- Extraction of security policies: this stage consists to extract from exchanged messages the set of security protocols corresponding to the SSID of legitimate access points.

Decision making

The system takes a proper decision in terms of security to point out different security defects. The decision making is described in Table 4. For example, the rule N°3 states that if the client is connected in Ad-hoc mode then their activities are suspected. It is explained by the fact that only the administrator possesses the privileges to directly connect to network APs.

Table 4: Communication channels

Rule N°	Definition of the rule	Profiling decision
1	If the access point is in the RAP list	AP mischievous
2	If the access point is in the AP legitimate list	legitimate host
3	If the client is in the legitimate host list	legitimate host
4	If the client is connected in Ad-hoc mode	Suspect
5	If the access point uses WEP or WPA or WPA2 security	AP vulnerable
6	If the access point uses the Preauth security	AP secured

Algorithm 1 represents the code logic which determines the set of legitimate and illegitimate APs within a network. It is described as follows. Algorithm 1 is described as follows:

- Lines 1 to 6 build the list of legitimate access points. They check if a given access point is in the database and if it is secured. If such a case, it is added to the list of legitimate access points.
- Lines 7 to 11 build the list of illegitimate access points that have usurped names (SSID), or the MAC addresses (BSSID). It is checked first if APs with the same SSID as the current one exists (line 8). When the MAC addresses are the same, it is a situation of usurpation of MAC address; if not, it is a usurpation of name (SSID). In both cases, the list of illegitimate access points is updated.
- Lines 12 to 15 check another case of illegitimacy (line 12). Indeed, if the access point does not have a security policy (OPEN) and if it is connected in Ad-hoc mode, then the access point is illegitimate. So, the list of access points is updated.

Alert generation

This module triggers an alert in two scenarios.

- If an access point is mischievous or suspected, then legitimate hosts of the network are informed about an eventual an attack;
- If an access point is vulnerable, then we inform the network administrator to change security policies.

6. TESTS AND RESULTS

This section experiments the proposed strategy on a real environment.

6.1. Environment of Tests

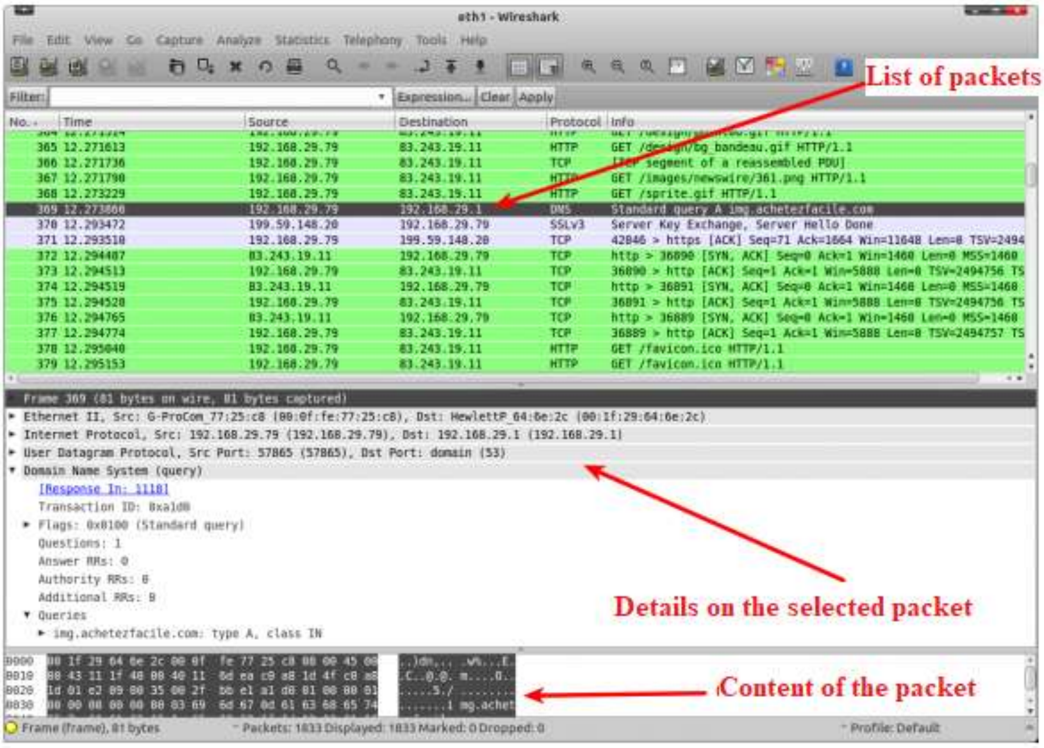
Wireshark is an open source traffic analyzer. It uses relies on GTK+ (Graphical Image Manipulation Toolkit) for the implementation of its user interface and .pcap for the capture of messages; it operates on many UNIX compatible environments like GNU/Linux, FreeBSD, NetBSD, OpenBSD or Mac OSX, but also on Microsoft Windows (Sanders 2017). Figure 6 illustrates Wireshark interfaces. It depicts the flow of packets collected through smartphone, along with details and contents. For example, it shows that the user (with the address 192.168.29.79) opens the web page www.achetezfacile.com which requires a DNS request redirected to the gateway 192.168.29.1.

Algorithm 1. Detection of legitimate and illegitimate APs

```
Inputs
L= list of APs identified by the administrator
LAP= list of current APs
Lh=list of hosts
Prot = {WEP, WPA, WPA2, PREAUTH}

Outputs
LAP=∅
LAPI=∅

Variables: x, y, z, LAP, LAPI
while L ≠ ∅ do
    if x ∈ L then
        if x.P ∈ Prot then
            LAP=LAP U {x}
            L=L\{x}
        endif
    else if ∃ z/z.SSID=x.SSID then
        if x.MAC=z.MAC then
            LAPI=LAPI U {x}
            L=L\{x}
        endif
        if x.P ∉ Prot or ∃y∈Lh/adhoc(x,y) then
            LAPI=LAPI U {x}
            L=L\{x}
        endif
        endif
    endif
endwhile
```



```
No. .  Time        Source          Destination     Protocol  Info
  365 12.271613   192.168.29.79   83.243.19.11    HTTP      GET /design/bg_bandeau.gif HTTP/1.1
  366 12.271736   192.168.29.79   83.243.19.11    TCP       [TCP segment of a reassembled PDU]
  367 12.271790   192.168.29.79   83.243.19.11    HTTP      GET /images/newswire/361.png HTTP/1.1
  368 12.273229   192.168.29.79   83.243.19.11    HTTP      GET /sprite.gif HTTP/1.1
  369 12.273860   192.168.29.79   192.168.29.1    DNS       Standard query A img.achetezfacile.com
  370 12.293472   199.59.148.20   192.168.29.79   SSLv3     Server Key Exchange, Server Hello Done
  371 12.293510   192.168.29.79   199.59.148.20   TCP       42046 > https [ACK] Seq=71 Ack=1664 Win=11648 Len=0 TSV=2494
  372 12.294487   83.243.19.11    192.168.29.79   TCP       http > 36890 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460
  373 12.294513   192.168.29.79   83.243.19.11    TCP       36890 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=2494756 TS
  374 12.294519   83.243.19.11    192.168.29.79   TCP       http > 36891 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460
  375 12.294528   192.168.29.79   83.243.19.11    TCP       36891 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=2494756 TS
  376 12.294765   83.243.19.11    192.168.29.79   TCP       http > 36889 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460
  377 12.294774   192.168.29.79   83.243.19.11    TCP       36889 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=2494757 TS
  378 12.295040   192.168.29.79   83.243.19.11    HTTP      GET /favicon.ico HTTP/1.1
  379 12.295153   192.168.29.79   83.243.19.11    HTTP      GET /favicon.ico HTTP/1.1

  Frame 369 (81 bytes on wire, 81 bytes captured)
▸ Ethernet II, Src: G-ProCom_77:25:c8 (00:0f:fe:77:25:c8), Dst: HewlettP_64:6e:2c (00:1f:29:64:6e:2c)
▸ Internet Protocol, Src: 192.168.29.79 (192.168.29.79), Dst: 192.168.29.1 (192.168.29.1)
▸ User Datagram Protocol, Src Port: 57865 (57865), Dst Port: domain (53)
▾ Domain Name System (query)
    [Response In: 1118]
    Transaction ID: 0xa1d0
  ▸ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ img.achetezfacile.com: type A, class IN

0000  00 1f 29 64 6e 2c 00 0f  fe 77 25 c8 08 00 45 00   ..)dn,.. .w%...E.
0010  00 43 11 1f 40 00 40 11  6d ea c0 a8 1d 4f c0 a8   .C..@.@. m....O..
0020  1d 01 e2 09 00 35 00 2f  bb e1 a1 d0 01 00 00 01   .....5./ ........
0030  00 00 00 00 00 00 03 69  6d 67 0d 61 63 68 65 74   .......i mg.achet

Frame (frame), 81 bytes    Packets: 1833 Displayed: 1833 Marked: 0 Dropped: 0    Profile: Default
```

List of packets

Details on the selected packet

Content of the packet

Figure 6: Wireshark snapshot

6.2 Data

The data collection has been made using Kismet. Table 5 represents features inherent to access points. Table 5 shows that the SSID Actions For Development appears twice (Line 1 and line 2) with distinct MAC and functioning on different channels. They are accessible behind APs. We also notice that the signals are different meaning that the fake one can be displayed on top on the user side.

Table 5: Data inherent to access points

Name of AP (SSID)	MAC (BSSID)	Communication mode	Channel	Signal (dBm)
Actions For Development	ec:23:3d:a0:2e:e0	AP	1	-52
Actions For Development	54:40: ad:2f:a3:49	AP	6	-64
wifi-auf	30:b5:c2:64:a3:d4	AP	2	-73
CAMTELHOTSPOT	e0:10:7f:16:e2:f8	AP	9	-89
ENSAI Djalingo	f4:f2:6d:35:16:0e	AP	1	-96
WIFASEG	00:1d:7e:03:80:6f	AP	6	-98
ADYYU00tVDU1MA	b0:47:bf:04:25:a3	AH	1	-97
ENSAI Gada	30:b5:c2:86:45:f8	AP	1	-86
WIFI IUT	10:fe:ed:c3:c6:82	AP	10	-83
ESMV	10:fe:ed:2b:b9:10	AP	1	-97
DOYEN FS	20:f3:a3:48:30:d7	AP	10	-94
TECNO W1	d6:7d:fc:ac:21:88	AP	13	-87
TECNO W5 Lite	d6:7d:fc:3f:d1:65	AP	6	-96
GOUAN	2a:be:03:ce:39:de	AP	11	-99
HUAWEI-E5573-9E97	48:db:50:cf:9e:97	AP	6	-72
Dr NGUIMBOU	d6:7d:fc:6e:f6:49	AP	6	-80
AndroidAP	1c:66:aa:d6:6a:82	AP	6	-91
Connectify-me	54:27:1e:55:ee:ff	AP	11	-81
guest network	60:83:34:cd:f6:3a	AP	6	-76
DMI ENSAI	98:fc:11:f5:8b:ae	AP	1	-92
DIR ESMV	10:fe:ed:c3:c9:b	AP	1	-98

6.3. Extraction of Useful Information

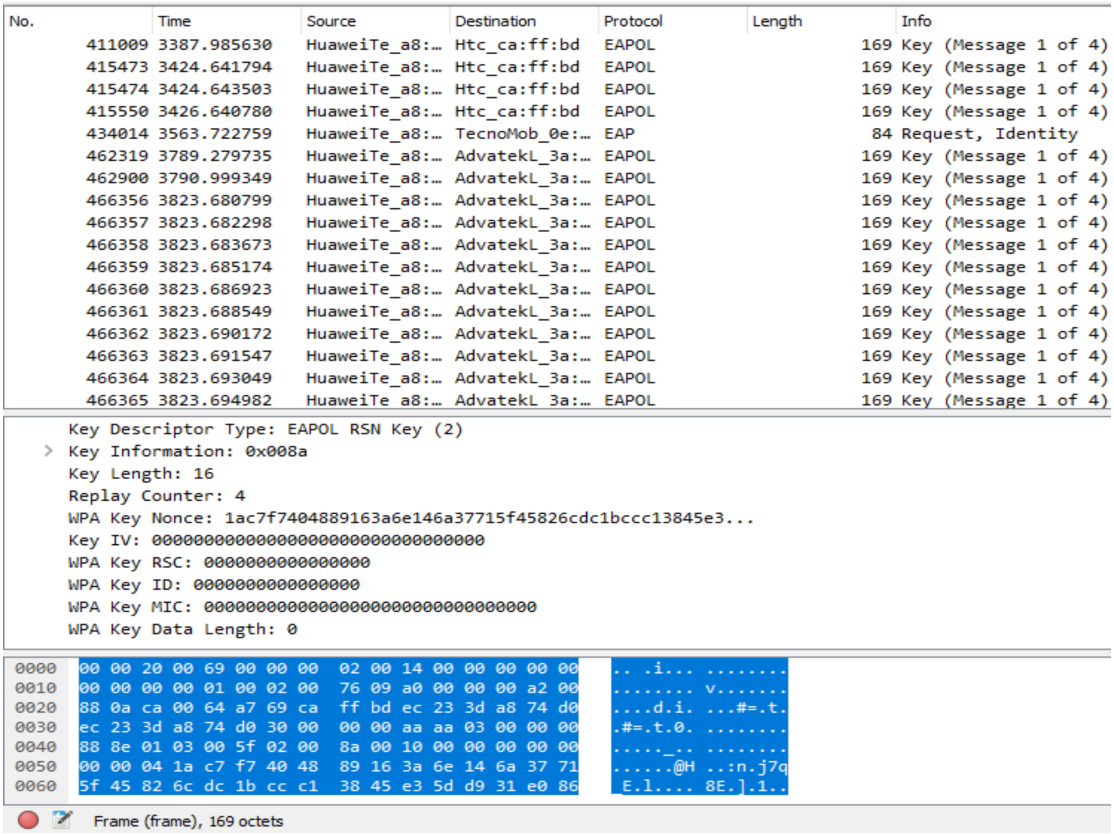
Figure 7 illustrates a capture of packets of illegitimate access points by isolating the legitimate APs. The MAC address is obtained with the filter *!wlan.bssid == ec:23:3d:a0:2e:e0*. The security protocol is then checked with the following filters:

- ***wlan.fc.protected == 0* and *wlan.fc.type eq 2***: which indicates non encoded data.
- ***eapol***: which indicates encoded data with WPA

Figure 8 overviews the packets after filtering based on security protocol with *eapol*. This filter has been performed to determine access points using authentications based on WPA, WPA2, WPA/WPA2 or preauth.

6.4 Decision Making

After frame analysis with Wireshark, the next task is to determine the legitimate and illegitimate access points. The proposed method based on filtering based on parameters helps us to evacuate fake APs. Results about benign APs are consigned in Table 6 whereas fake APs are consigned in Table 7. For example, concerning the SSID “Actions for Development”, the benign one has the MAC “ec:23:3d:a0:2e:e0” with security mode “WPA/WPA2”. The SSID “ENSAI Djalingo” appears to also be illegitimate even if it does not appear several times. In reality, investigations reveal that this SSID is on anytime since about ten years. In fact it was an old SSID used at school for various purposes. But the server which delivers behind this SSID is no more and someone mislead this SSID for bad intentions.



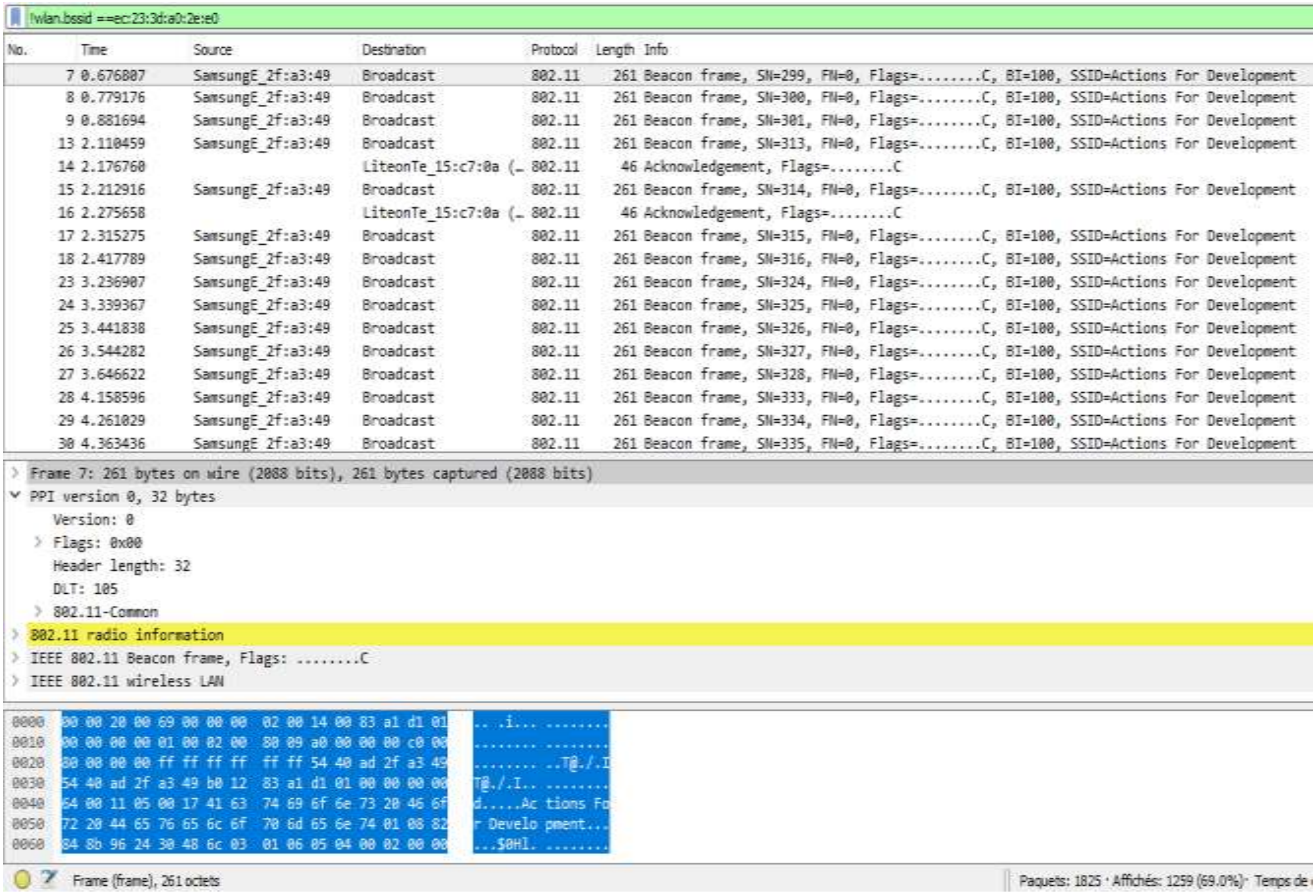
```
No.      Time          Source        Destination   Protocol  Length  Info
  411009 3387.985630   HuaweiTe_a8:… Htc_ca:ff:bd  EAPOL        169 Key (Message 1 of 4)
  415473 3424.641794   HuaweiTe_a8:… Htc_ca:ff:bd  EAPOL        169 Key (Message 1 of 4)
  415474 3424.643503   HuaweiTe_a8:… Htc_ca:ff:bd  EAPOL        169 Key (Message 1 of 4)
  415550 3426.640780   HuaweiTe_a8:… Htc_ca:ff:bd  EAPOL        169 Key (Message 1 of 4)
  434014 3563.722759   HuaweiTe_a8:… TecnoMob_0e:… EAP           84 Request, Identity
  462319 3789.279735   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  462900 3790.999349   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466356 3823.680799   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466357 3823.682298   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466358 3823.683673   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466359 3823.685174   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466360 3823.686923   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466361 3823.688549   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466362 3823.690172   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466363 3823.691547   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466364 3823.693049   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)
  466365 3823.694982   HuaweiTe_a8:… AdvatekL_3a:… EAPOL        169 Key (Message 1 of 4)

    Key Descriptor Type: EAPOL RSN Key (2)
  > Key Information: 0x008a
    Key Length: 16
    Replay Counter: 4
    WPA Key Nonce: 1ac7f7404889163a6e146a37715f45826cdc1bccc13845e3...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0

0000  00 00 20 00 69 00 00 00  02 00 14 00 00 00 00 00   .. .i... ........
0010  00 00 00 00 01 00 02 00  76 09 a0 00 00 00 a2 00   ........ v.......
0020  88 0a ca 00 64 a7 69 ca  ff bd ec 23 3d a8 74 d0   ....d.i. ...#=.t.
0030  ec 23 3d a8 74 d0 30 00  00 00 aa aa 03 00 00 00   .#=.t.0. ........
0040  88 8e 01 03 00 5f 02 00  8a 00 10 00 00 00 00 00   ....._.. ........
0050  00 00 04 1a c7 f7 40 48  89 16 3a 6e 14 6a 37 71   ......@H ..:n.j7q
0060  5f 45 82 6c dc 1b cc c1  38 45 e3 5d d9 31 e0 86   _E.l.... 8E.].1..

Frame (frame), 169 octets
```

Figure 7: Detection of mischievous access points



```
!wlan.bssid ==ec:23:3d:a0:2e:e0

No.  Time      Source             Destination           Protocol Length Info
   7 0.676807  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=299, FN=0, Flags=........C, BI=100, SSID=Actions For Development
   8 0.779176  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=300, FN=0, Flags=........C, BI=100, SSID=Actions For Development
   9 0.881694  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=301, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  13 2.110459  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=313, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  14 2.176760                     LiteonTe_15:c7:0a (…  802.11    46 Acknowledgement, Flags=........C
  15 2.212916  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=314, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  16 2.275658                     LiteonTe_15:c7:0a (…  802.11    46 Acknowledgement, Flags=........C
  17 2.315275  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=315, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  18 2.417789  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=316, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  23 3.236907  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=324, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  24 3.339367  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=325, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  25 3.441838  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=326, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  26 3.544282  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=327, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  27 3.646622  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=328, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  28 4.158596  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=333, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  29 4.261029  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=334, FN=0, Flags=........C, BI=100, SSID=Actions For Development
  30 4.363436  SamsungE_2f:a3:49  Broadcast             802.11   261 Beacon frame, SN=335, FN=0, Flags=........C, BI=100, SSID=Actions For Development

> Frame 7: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
v PPI version 0, 32 bytes
    Version: 0
  > Flags: 0x00
    Header length: 32
    DLT: 105
  > 802.11-Common
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
> IEEE 802.11 wireless LAN

0000  00 00 20 00 69 00 00 00  02 00 14 00 83 a1 d1 01   ... .i... ........
0010  00 00 00 00 01 00 02 00  80 09 a0 00 00 00 c0 00   ........ ........
0020  00 00 00 00 ff ff ff ff  ff ff 54 40 ad 2f a3 49   ........ ..T@./.I
0030  54 40 ad 2f a3 49 b0 12  83 a1 d1 01 00 00 00 00   T@./.I.. ........
0040  64 00 11 05 00 17 41 63  74 69 6f 6e 73 20 46 6f   d.....Ac tions Fo
0050  72 20 44 65 76 65 6c 6f  70 6d 65 6e 74 01 08 82   r Develo pment...
0060  84 8b 96 24 30 48 6c 03  01 06 05 04 00 02 00 00   ...$0Hl. ........

Frame (frame), 261 octets          Paquets: 1825 · Affichés: 1259 (69.0%) · Temps de
```

Figure 8: Scanned packets

Table 6: List of legitimate access points

Name of AP (SSID)	MAC (BSSID)	Communication mode	Security
Actions For Development	ec:23:3d:a0:2e:e0	AP	WPA/WPA2
wifi-auf	30:b5:c2:64:a3:d4	AP	Preauth(802.1x/EAP)
CAMTELHOTSPOT	e0:10:7f:16:e2:f8	AP	Preauth(802.1x/EAP)
WIFASEG	00:1d:7e:03:80:6f	AP	WPA
WIFI IUT	10:fe:ed:c3:c6:82	AP	WPA/WPA2
ESMV	10:fe:ed:2b:b9:10	AP	WPA/WPA2
DOYEN FS	20:f3:a3:48:30:d7	AP	WPA/WPA2
TECNO W1	d6:7d:fc:ac:21:88	AP	WPA2
TECNO W5 Lite	d6:7d:fc:3f:d1:65	AP	WPA2
GOUAN	2a:be:03:ce:39:de	AP	WPA2
HUAWEI-E5573-9E97	48:db:50:cf:9e:97	AP	WPA2
Dr NGUIMBOU	d6:7d:fc:6e:f6:49	AP	WPA2
AndroidAP	1c:66:aa:d6:6a:82	AP	WPA2
Connectify-me	54:27:1e:55:ee:ff	AP	WPA2
guest network	60:83:34:cd:f6:3a	AP	WPA/WPA2
DIR ESMV	10:fe:ed:c3:c9:b	AP	WPA/WPA2

Table 7: List of illegitimate access points

Name of AP(SSID)	MAC(BSSID)	Communication mode	Security
Actions For Development	54:40:ad:2f:a3:49	AP	OPEN
ENSAI Djalingo	f4:f2:6d:35:16:0e	AP	OPEN
ADYYU00tVDU1MA	b0:47:bf:04:25:a3	AH	OPEN
ENSAI Gada	30:b5:c2:86:45:f8	AP	OPEN
DMI ENSAI	98:fc:11:f5:8b:ae	AP	OPEN

6.5 Discussions

Algorithm 1 determines spoofing attacks and SSID usurpation by establishing the list of legitimate access points in Table 6. Table 7 represents rather the list of illegitimate access points. The clients of that network are informed of the presence of an intruder access point. The presence of vulnerable access points is due to the utilization of vulnerable security protocols. So, the users will be informed to better secure their access points in order to avoid an attack. The presence of non-secured APs incentives man in the middle attacks and the presence of duplicate SSIDs incentives spoofing attacks. The proposed approach includes alert module to prevent these attacks.

Limitations

The proposed method is limited in three points.

- It is not semi-automatic.
- It is static since it is based on deterministic criteria to take a priori decision. It is not focused on all the communications exchanged on the wireless network.
- It is unable to stop an attack that may occur in the network.

CONCLUSION AND PERSPECTIVES

This work proposed a strategy to identify RAPs based on multiple static features selected from a well-performed experimentation on real sites. The collection process has been made assisted by smartphones and laptop with installed wardriving tools. Then generated data are transmitted to a traffic analyzer to apply filter commands to extract traces of RAPs. The method has been applied on a real case and has been able to detect the presence of vulnerable access points and the illegitimate ones. Nevertheless, this work deserves to be improved on three points. The first one concerns the automation of the proposed method. The second concerns the fact of taking in account exchanges between access points and the client hosts. The third concerns the integration of the capacity to stop attack flows when it occurs.

REFERENCES

1. Prakash, A., Agarwal, D. P.: Data Security in Wired and Wireless Systems. In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. IGI Global DOI: 10.4018/978-1-5225-0105-3.ch001 (2019)
2. Ying, X., Sagong, S. U., Clark, A., Bushnell, L., Poovendran, R.: Shape of the Cloak: Formal analysis of clock skew-based intrusion detection system in controller area networks. IEEE Transactions on Information Forensics and Security, 14(9), 2300-2314 (2019).
3. Kao, K.-F., Liao, I.-E., Li, Y.-C.: Detecting Rogue Access Points using Client-Side Bottleneck Bandwidth Analysis. Computers and Security, 28(3-4), 144 – 152 (2009).
4. Lu, Q., Qu, H., Ouyang, Y., Zhang, J.: SLFAT: Client-Side Evil Twin Detection Approach Based on Arrival Time of Special Length Frames. Security and Communication Networks (2019) https://doi.org/10.1155/2019/2718741
5. Kim, T., Park, H., Jung, H., Lee, H.: Online Detection of Fake Access Points Using Received Signal Strengths. In Proceedings of the 2012 IEEE 75th Vehicular Technology Conference (VTC), pp. 1–5. IEEE, Yokohama, Japan (2012)
6. Nikbakhsh, S., Manaf, A. B. A., Zamani, M., Janbeglou, M.: A Novel Approach for Rogue Access Point Detection on the Client-Side. In Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, 684–687. IEEE, Fukuoka, Japan (2012)
7. Yang, C., Song, Y., Gu, G.: Active User-Side Evil Twin Access Point Detection Using Statistical Techniques. IEEE Transactions on Information Forensics and Security 7(5), 1638-1651 (2012).
8. Vanjale, S., P. B., M.: Detection of Rogue Access Point Using Various Parameters. In Proc. International Conference on Data Engineering and Communication Technology Advances in Intelligent Systems and Computing, Volume 468, pp. 699-710. Springer, Singapore (2017).
9. Ataelmanan, S.K.M., Hassan, M.A.: A review of threats, protocols, and solutions to enhance the security of wireless networks, International Journal of Computer Science and Network Security, 19(4), 108-115 (2019)
10. Alotaibi, B., Elleithy, K.: Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions. Wireless Personal Communications 90(3), 5021-5028 (2016).
11. Menezes, A., van Oorschot., P. C., Vanstone, S. A. : Handbook of Applied Cryptography. *CRC Press*; New York NY (1996).
12. Tang, X., Liu, R., Spasojevi, P., Poor, H. V.: A Broadcast Approach to Secret Key Generation Over Slow Fading Channels. Preprint, available at https://arxiv.org/pdf/1103.3113.pdf (2011)
13. Khisti, A.: Interactive Secret Key Generation over Reciprocal Fading Channels. In Proc. 50th IEEE Annual Allerton Conference on Communication, Control, and Computing. IEEE, (Monticello, IL, USA) (2012).
14. Li, C.-T., Wu, T.-Y., Chen, C.-L., C., Lee, C.-C., Chen, C.-M., C. : An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT Based Medical Care System. Sensors 17(7), 1482 (2017).
15. Bloch, M., Barros, J., Rodrigues, M. R. D., McLaughlin, S. W.: Wireless Information-theoretic Security. IEEE Transactions on Information Theory 54(6), 2515–2534 (2008).
16. Sharma, S., Mishra, R., Singh, P.: Authentication in Wireless Networks. In Proc. 2nd IEEE International Conference on Computing for Sustainable Global Development (INDIACom, New Delhi, India). pp. 2031-2035. IEEE (2015)
17. Refaey, A., Hou, W., Loukhaoukha, K.: Multilayer Authentication for Communication Systems Based on Physical-Layer Attributes. Journal of Computer Science and Communications 2(8), 64-75 (2014).
18. Dobrilovic, D., Stojanov, Z., Jäger, S., Rajnai, Z. : A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities. Acta Polytechnica Hungarica 13(6), 67–86 (2016).
19. Kalniņš, R., Purins, J., Alksnis, G.: Security Evaluation of Wireless Network Access Points. Applied Computer Systems, 21(1), 38–45 (2017).
20. Sanders C.: Practical Packet Analysis, 3E: Using Wireshark to Solve Real-World Network Problems. No Starch Press (2017).