Rogue Access Point Detection by Analyzing Network Traffic Characteristics

Sachin Shetty, Min Song
Department of Electrical and Computer Engineering
Old Dominion University
Norfolk, VA 23529

Liran Ma
Computer Science Department
The George Washington University
Washington DC 20052

Abstract

One of the most challenging network security concerns for network administrators is the presence of rogue access points. Rogue access points, if undetected, can be an open door to sensitive information on the network. Many data raiders have taken advantage of the undetected rogue access points in enterprises to not only get free Internet access, but also to view confidential information. Most of the current solutions to detect rouge access points are not automated and are dependent on a specific wireless technology. In this paper, we present a rogue access point detection approach. The approach is an automated solution which can be installed on any router at the edge of a network. The main premise of our approach is to distinguish authorized WLAN hosts from unauthorized WLAN hosts connected to rogue access points by analyzing traffic characteristics at the edge of a network. Simulation results verify the effectiveness of our approach in detecting rogue access points in a heterogeneous network comprised of wireless and wired subnets.

Key words: Rogue access point, traffic characteristics, detection

1. Introduction

One of the most challenging security concerns for network administrators is the presence of rogue wireless access points [6, 7]. A rogue access point (RAP) is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network management or has been created to allow a cracker to conduct a man-in-the-middle attack. RAPs can pose a security threat to large organizations with many employees, because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless router that can potentially allow unauthorized parties to access a secured network. In commercial and military organizations, employees have the capability to deploy RAPs and build large scale wireless networks without the knowledge or approval of their network administrators. These RAPs are a serious threat to the overall network security. Typically employees connect their RAPs to a network port behind the corporate firewall. The RAPs are vulnerable as employees rarely enable the most basic security settings, making it relatively easy for unauthorized outsiders to use the access point and perform a man-in-the middle attack by eavesdropping on the network traffic. Although commercial products of detecting RAPs are available on the market, there is very little research effort on RAP detection. In this paper, we propose a novel approach for RAP detection based on traffic analysis at the edge of a network. Particularly, in a network comprising of wired and wireless devices, we first determine whether packets originated from a WLAN connection or an Ethernet connection. For packets originating from a wireless link, we proceed to check whether the host (packets originator) is authorized to use the wireless network. This determination is done based on the frequency of access of a particular port and the increase in cross-port communication. If a host shows a remarkable increase in the above two statistical categories, we conclude the host is connected to a RAP.

The rest of the paper is organized as follows. Section 2 describes the related work. We present the problem statement and our approach in Section 3. In Section 4, we present simulation results. Section 5 concludes the paper.

2. Related Work

A comprehensive taxonomy of RAP detailing different categories of RAPs has been presented by Ma *et al*. [13]. The authors have categorized access points in the following four classes: improperly configured, unauthorized, phishing, and compromised. The first three classes of RAPs are easier to detect by performing a manual audit in the vicinity of the organization premises. But the compromised AP is the most difficult to detect due to no malfunction and lack of anomalous behavior in network traffic produced. A RAP detection scheme should be effective in detecting activity produced by all the above classes of RAPs.

1-4244-1513-06/07/$25.00 ©2007

The brute-force approach of RAP detection used by most enterprises is to equip IT personnel with wireless packet analyzer tools and scan the network traffic [6, 9]. This approach, however, is ineffective and time-consuming. Scans are not effective as a RAP can easily be unplugged when the scan takes place. In addition, IT personnel must upgrade their detection devices to accommodate multiple frequencies. The improvement over an employee-equipped scanner is to initiate an enterprise-wide scan from a central location. This is possible by using separate hardware devices [11, 12], such as sensors, and transmitting the information back to the central management platform containing the wireless network policy for analysis. This approach is expensive as one must place sensors or access points throughout the entire enterprise to monitor the air waves. Also this approach can be ineffective if a malicious employee uses a directional antenna, or reduces the signal strength to cover the small range within his/her office.

To the best of our knowledge there are only five academic research efforts on detecting RAP [1, 2, 3, 4, 13]. Prior research studies [3, 4] adopt a similar approach as commercial products to detect RAP by monitoring the RF air waves. The approach adopted in [3, 4] focuses on providing a framework for network fault diagnosis and security. This leads naturally to RAP detection. In [3], wireless clients are instrumented to collect information about neighboring access points and send the information to a central server. On receipt of the information, the central server checks whether this access point is registered to determine whether it is a RAP. This detection approach is similar to those taken by commercial products of [8, 10] and has similar limitations as described above. For example, this approach is ineffective because it assumes that RAPs use standard beacon messages in IEEE 802.11 and respond to probes from the clients, which is impractical. Furthermore, all unknown access points are flagged as RAPs, which may lead to large number of false positives.

The crux of the research effort in [4] is to enable dense RF monitoring through wireless devices attached to desktop machines. This approach improves upon [3] by providing more accurate and comprehensive RAP detection. However, it has a similar limitation as [3] that it heavily relies on certain specific features of IEEE 802.11, which can be easily turned off or violated. The research effort proposed by authors in [2] takes a completely different approach from others. The focus of the research effort in [2] is to detect RAPs through temporal characteristics of wireless networks. This approach is based on the intuition that inter-packet arrival times of wireless traffic are more random than those of wired traffic. However, this research effort suffers from the following limitations. First, it is mandatory for the wireless access points to be directly attached or one-hop away from the monitoring point. Secondly, the detection is effective only when wireless hosts are uploading data. Third, the approach is based on visual inspection, which makes it difficult to detect RAPs automatically.

Wei *et al*. have proposed an online scheme based on real time passive measurements collected at a gateway router [1]. The authors developed sequential hypothesis tests by analyzing *M/D/*1 queues and the medium access mechanisms of 802.11. This research effort has a similar flavor as [2] in the sense that both utilize the temporal characteristics of wireless traffic. But the research effort focuses more on differentiating wired traffic from wireless traffic. The approach does not provide an effective scheme to differentiate between wireless traffic from authorized and unauthorized APs. The authors propose the usage of access control lists to detect unauthorized wireless hosts. Access control lists are not an effective solution due to the ease in which unauthorized hosts can perform IP spoofing.

More recently, Ma *et al*. have proposed a rogue AP protection system to detect four classes of rogue APs [13]. According to the authors, the system provides comprehensive protection against rogue APs for commodity Wi-Fi networks. The system can also detect RAPs which have the ability to violate the IEEE 802.11 standard. The rogue AP protection system comprises of packet collector, rogue AP preemption, and detection components. The preemption component probes potential eavesdroppers and performs network integrity checks to trap sniffers and thwart activity that can lead to a compromised AP. The detection components are responsible for defending against four classes of rogue APs. To defend against the first three classes of rouge APs (improperly configured, unauthorized, and phishing), an AP probing technique is employed to lure rogue APs into revealing their presence. To detect the class 4 AP (compromised), a combination of MAC address and OS fingerprinting techniques are employed. Based on availability of hardware and software resources on an AP, these components can be installed on a single AP or on separate devices connected to AP in a plugin fashion. To the best of our knowledge, real-world empirical results have not been provided to justify the claims of RAP.

Our research effort tackles the main problem of detecting a rogue access point based on analyzing traffic

patterns. In the next section, we present the main problem statement and our approaches to address the problem.

3. Problem Statement and Approach

In this section, we describe the problem statement and description of our approach. Consider a heterogeneous local area network (Fig. 1) that comprises three subnets which communicate with the Internet via a gateway router at the edge of the network. Subnet 1 consists of authorized wired hosts that communicate via Ethernet interfaces. Subnet 2 consists of authorized WLAN hosts that communicate via IEEE 802.11b WLAN interfaces Subnet 3 consists of unauthorized WLAN hosts connected to a RAP, communicating via IEEE 802.11 WLAN interfaces. The main goal of our research is to detect the RAP in Subnet 3.

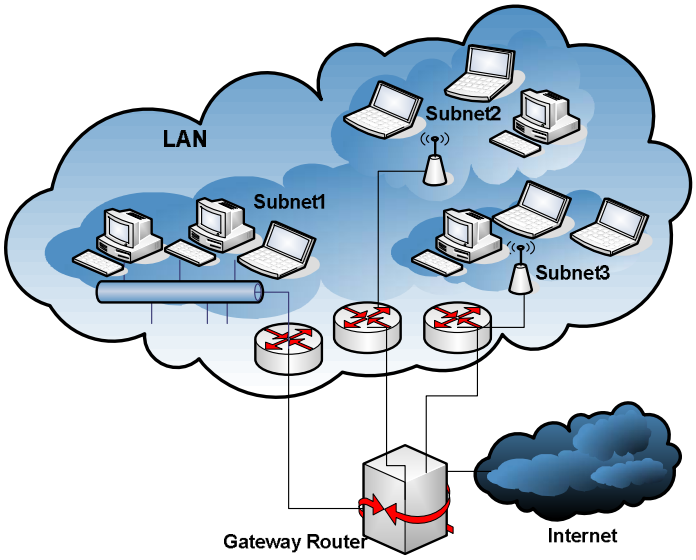

Fig. 1 A LAN comprises wired and wireless subnets.

We propose a novel approach to detect RAP in a heterogeneous network comprised of wired and wireless subnets. The approach is implemented in two consecutive phases. The premise of both the phases is traffic analysis performed at the gateway router by a network traffic analyzer (NTA). In the first phase, the NTA analyzes both inbound and outbound traffic and determines whether an end-host belongs to an Ethernet or WLAN. In the second phase, the NTA analyzes the traffic from end-hosts on WLANs to compute the frequency of straight-access and crossing-access attempts. If a WLAN end host generates traffic which causes the access point to access the port on the gateway router to which the access point is connected physically, then the access attempt is considered straight-access. If a WLAN end-host generates traffic which causes the access point to access the port on the gateway router to which the access point is not connected physically, then the access attempt is considered crossing-access. If the frequency values of these access attempts exceed a threshold, the NTA then alerts the network administrator that the end-host is connected to a RAP.

3.1 Ethernet and WLAN traffic classification phase

As discussed in the previous section, the first phase in our traffic analysis is to identify hosts connected to a wireless network by differentiating the traffic between Ethernet and WLAN.

We assume that majority of the ports on the gateway router are connected to Ethernet subnets. The traffic characteristics are influenced by the number of hops between the end host and the gateway router. We assume that the wired and wireless end hosts are connected to the gateway router by at most two links. Ethernet links are considered very reliable and do not affect their traffic characteristics. The traffic characteristics of Ethernet links are dependent on the performance of TCP. However, traffic characteristics of wireless links are dependent on the link and TCP layers. The link layer for wireless networks is not as reliable as Ethernet links due to variations in channel conditions. This causes a variation in wireless link capacity and introduces random delays.

When two back-to-back packets are sent on a perfect wireless channel, the inter-departure time of the packet pair is uniformly distributed between 500 µs and 1130 µs, with a median of 810 µs [1]. Although an Ethernet connection uses shared media, the randomness caused by the shared media in Ethernet is negligible compared to the one in a wireless network because of its high bandwidth and ability to detect collisions. Fig. 2 compares the inter-packet spacing for traffic originating from Ethernet and wireless links.

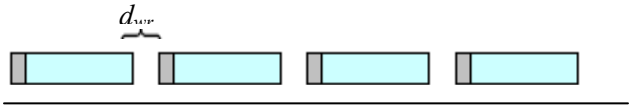

Fig. 2 (a) Traffic originating from Ethernet links.

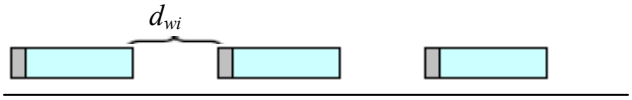

Fig. 2 (b) Traffic originating from wireless links.

Fig. 2 (b) shows that wireless links cause more random temporally different spreading of packets as compared to wired links. Wireless links uses a contention based MAC

protocol to access the shared link. Ethernet links use a non-contention based access to a switched wired link. Ethernet links have a greater data rate as compared to wireless links. These are the reasons for the differences in the inter-packet spacing. Specifically, the spreading of packets caused by wireless links is normally greater than that caused by wired links ($d_{wi} > d_{wr}$).

The psuedocode to distinguish Ethernet and Wireless LAN traffic is presented below. We collect data from the first N packets, where N is a configurable parameter dependent on the amount of traffic flowing at the gateway router.

Psuedocode to distinguish Ethernet and WLAN traffic

```
for (each flow between sender and receiver) {
     n = 0
    for (the first N packets) {
        n = n + 1
        ΔT_n = T_n – T_n-1
        // T_n is the arrival time of the n^th packet
     }
    compute median of inter-arrival times M(ΔT_n)
    if ( M(ΔT_n) <= 5 ms)
      then classify sender connection as Ethernet
   else
      classify sender connection as wireless
}
```

3.2 RAP detection phase

After applying the first phase to distinguish between Ethernet and WLAN traffic, the second phase to detect a RAP is applied.

In this section, we demonstrate the detection of RAP, by distinguishing traffic generated by authorized WLAN hosts from unauthorized WLAN hosts. One of the most common activities performed on an unauthorized WLAN host is port scanning. When a malicious user gains access to an unauthorized WLAN host connected to a RAP, he first performs a port scanning operation to find end hosts with vulnerabilities. For example, an attacker may be interested in identifying active hosts, as well as the network services that run on those hosts. In principle, an attacker is connected to a RAP, if the frequency of straight-access and crossing-access exceeds a nominal threshold. So the initial traffic originating from the unauthorized WLAN hosts consists of frequent application layer client request packets to a particular server. This application layer client requests translates into heavy volume traffic on a specific port on the gateway router. As the increased unusual traffic exceeds a threshold, the NTA will detect the unauthorized WLAN host as connected to a RAP due to the increase of straight-access attempts. In their pursuit for vulnerable ports, the traffic generated from unauthorized WLAN hosts could also cause an increase in crossing-access on the gateway router. As the unauthorized users are interested in gaining access to any vulnerable host, the request packets are sent to random end host machines, thereby increasing the crossing-access. If the frequency of the crossing-access exceeds a threshold, the NTA detects the unauthorized WLAN host as connected a RAP.

Given a train of packets arriving at the gateway router from wired and wireless networks, we would like to analyze the access attempts made to specific networks. We define the first type of access from a wireless source host s_i to the port on the gateway router as $<s_i, p_j>$ as straight-access, where p_j represents the port to which the access point of s_i is connected. We define the second type of access from a wireless source host s_i to the port on the gateway router as $<s_i, p_{cj}>$ as crossing-access, where p_{cj} represents the port to which the access point of s_i is not connected. Once we have extracted the two types of access attempts from a given train of packets, we classify the source s_i as an attacker based on the frequency of accesses to p_j and p_{cj}.

To detect the increase in the frequency of accesses, we have to first define normal accesses to p_j and p_{cj}. In the collected packet trace, let $f(s_i, p_j)$ represent the frequency of accessing port p_j by s_i, and $f(*, p_j)$ represent the frequency of accessing port p_j by all source hosts. We can define the parameter for acceptable access for a source host s_i as

$$Per(s_i) = \frac{f(s_i, p_j)}{f(*, p_j)}$$

Similarly, we define a parameter for acceptable access for source host s_i in presence of crossing-access as

$$Perc(s_i) = \frac{f(s_i, p_{cj})}{f(*, p_{cj})}$$

If $Per(s_i) > thresh$ or $Perc(s_i) > threshc$, the source host s_i is an attacker, where $thresh$ and $threshc$ are empirically derived alert thresholds. If source host s_i exceeds the threshold, then it is detected as connected to a RAP. The psuedocode for identifying wireless traffic and detecting RAPs are presented below. To compute the statistical measures, we collect data from the first N packets, where N is a configurable parameter dependent on the amount of traffic flowing at the gateway router.

Psuedocode for detecting RAP

```
for (each wireless traffic flow) {
    n = 0
    for (the first N packets) {
        n = n + 1
        for every source host in the trace
            compute f(s_i, p_j), f(s_i, p_cj)
            compute f(*, p_j), f(*, p_cj)
        if ((f(s_i, p_j) / f(*, p_j) > thresh or
            (f(s_i, p_cj) / f(*, p_cj) > threshc))
                s_i is a attacker
    }
}
```

4. Simulation Study

In this section, we present the simulation results for the two phases discussed in section 3. We adopted the ns-2 simulator to model a local area network similar to Fig. 1. The traffic flow was observed in forward and reverse directions at the gateway router. At the gateway router, the forward path is defined as the traffic originating from any end host in the local area network and terminating at any host in the Internet. Simulations are conducted on TCP and UDP traffic.

4.1 Ethernet and WLAN traffic classification

To simulate the first phase, we simulated scenarios with both TCP and UDP traffic in the forward and reverse directions. For TCP traffic, an ftp application with 10 different file sizes ranging from 1 Megabytes to 10 Megabytes using increments of 10 Megabytes were used. The number of repetitions performed with each file size was 10. The end host initiated the traffic flow by uploading a file to a server which was located in the Internet.

Fig. 3 compares the interarrival times for traffic sent from the Ethernet subnet and the two wireless subnets connected to the gateway router. The number of nodes in each subnet was 30. The size of the file uploaded was 1 Megabyte. The interarrival time for Ethernet connections does not vary much over time with a mean of 3 ms. But the wireless connections on both subnets depict a significant variable in delay due to unreliable wireless channel, increase of collisions and the unpredictable effects of random backoff mechanism.

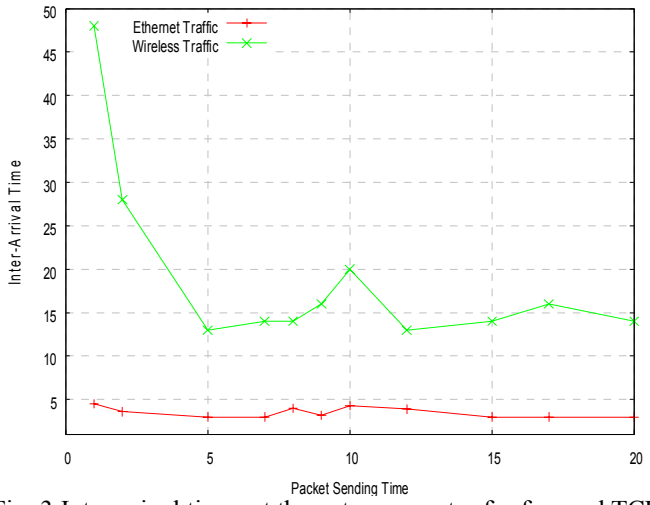

Fig. 3 Interarrival times at the gateway router for forward TCP traffic.

We observe similar differences for larger networks and larger file sizes. One can observe from Fig. 3 that when traffic is being uploaded from the hosts to the internet, the interarrival time provides an easier mechanism to distinguish between the two wireless subnets and Ethernet enabled hosts.

Fig. 4 shows the interarrival time for the reverse traffic between the internet and the three subnets. The figure compares the difference in the interarrival time between the Ethernet and the two wireless subnets. In this scenario, hosts are downloading traffic from the external network. At the gateway router, we monitor the interarrival time of the *ACK* packets. The figure shows that the difference between interarrival time for hosts on the Ethernet subnet and the hosts connected to the two wireless subnets is very large, which makes the detection process easier.

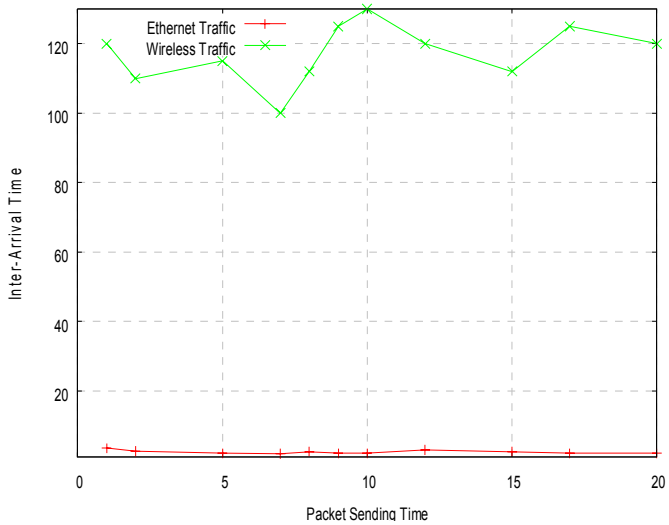

Fig. 4 Interarrival times of *ACK* packets at the gateway router for reverse TCP traffic.

Fig. 5 illustrates the difference between interarrival times from the Ethernet subnet and the two wireless subnets connected to the gateway router for UDP traffic sent at a constant rate of 1 Mbps. The figure confirms that the inter-packet characteristics are preserved even under the presence of constant UDP traffic.

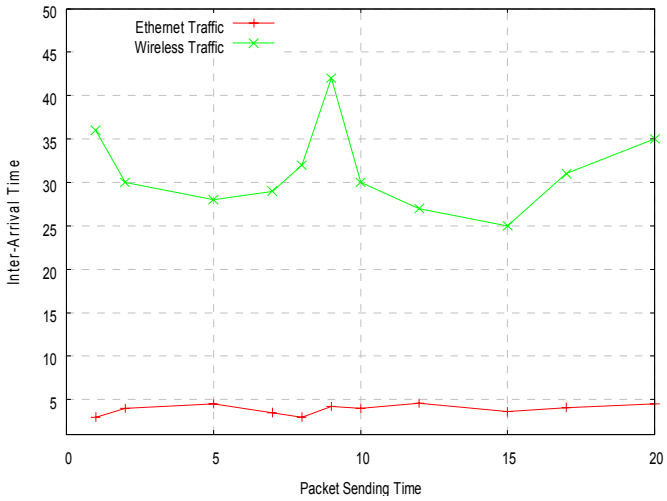

Fig. 5 Interarrival times at the gateway router for forward UDP traffic.

4.2 Detecting RAP by identifying unauthorized WLAN hosts

To simulate the second phase, we analyzed the traffic generated by WLAN hosts which were identified in phase 1.

Fig. 6 demonstrates the effectiveness of our approach in distinguishing authorized WLAN hosts from unauthorized WLAN hosts connected to RAP based on the straight-access attempts. The identification of unauthorized WLAN hosts connected to RAP is successful for all values of threshold. A large number of false positives (i.e., authorized WLAN hosts identified as connected to RAP) occur for $thresh \leq 0.35$. But for higher values of threshold only unauthorized WLAN hosts connected to RAP are identified. As described in Section 3, the alert threshold controls the number of surveillance alerts produced; only unauthorized WLAN hosts connected to RAP that perform enough scans to cross the threshold will be considered an attacker. The selection of threshold is critical for system optimization. A high threshold may result in many scans going undetected, while a low threshold may result in an overwhelming number of alerts.

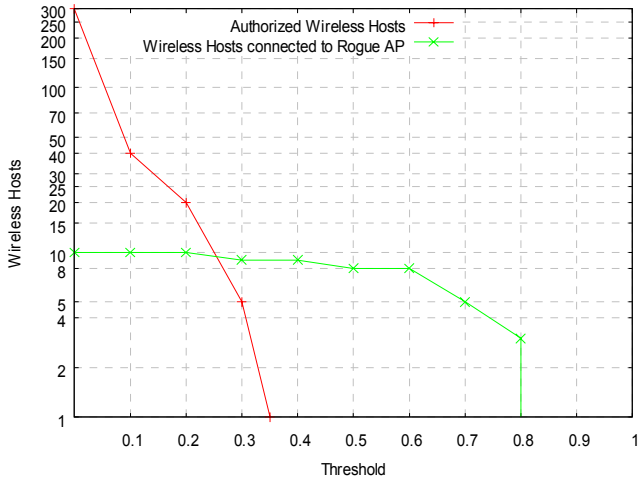

Fig. 6 Number of authorized WLAN hosts detected as connected to a RAP by analyzing straight-access traffic.

Fig. 7 demonstrates the effectiveness of our approach in authorized WLAN hosts from unauthorized WLAN hosts connected to RAP based on the crossing-access attempts. Similar to Fig. 6, a large number of false positives occur for $threshc \leq 0.4$. But for higher values of threshold only unauthorized WLAN hosts connected to RAP are identified.

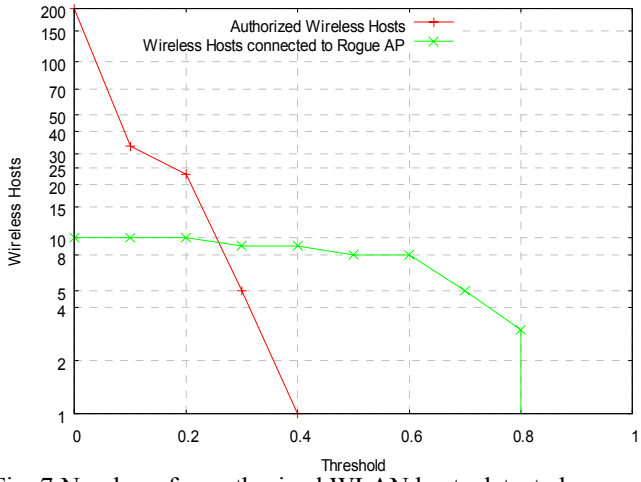

Fig. 7 Number of unauthorized WLAN hosts detected as connected to a RAP by analyzing crossing-access.

As can be seen in Figs. 6 and 7, the number of alerts can be drastically lowered with relatively small alert thresholds. This means that most authorized WLAN hosts access the external network at most a small number of times. Hence relatively low threshold settings will eliminate all the infrequent accesses, and therefore only alert on a small fraction of the rogue sources that attack. The ability to exclude the abundance of authorized WLAN hosts with a low threshold is a beneficial, positive result. This means that the number of detection

alerts displayed for the human analyst can be controllably low.

Fig. 8 illustrates the number of unauthorized WLAN hosts detected as connected to a RAP with increasing attack length. Here the attack length is defined as the total duration of the monitoring attempt (i.e., the time between the first and last monitoring points). In Fig. 8, the cumulative number of attackers for each attack length is shown. The figure shows that majority of attack lengths last for a very short time.

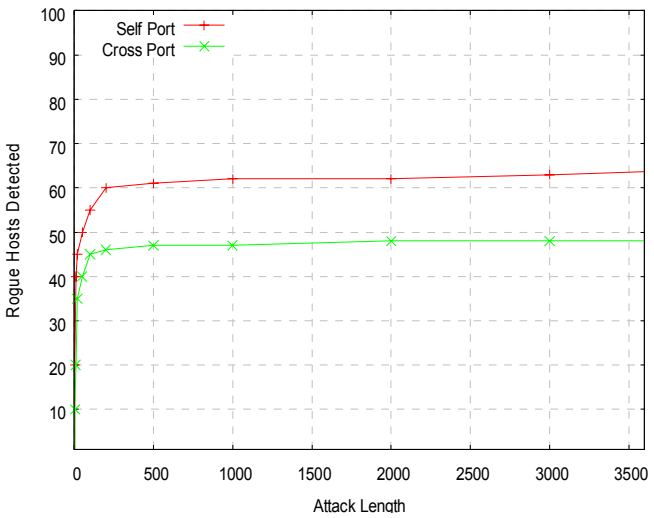

Fig. 8 Number of unauthorized WLAN hosts detected as connected to a RAP with increasing attack length.

5. Conclusions

In this paper we present an approach to detect RAP in a heterogeneous network comprised of wired and wireless subnets. Our approach is implemented by analyzing traffic characteristics in two phases. The first phase demonstrates the differences between Ethernet and WLAN traffic patterns. This difference helps to detect WLAN hosts. The second phase analyzes wireless traffic identified in first phase to detect unauthorized WLAN hosts connected to a RAP. The second phase relies on two configurable threshold parameters based on straight-access and crossing-access attempts. Our simulation results show that interarrival time is a good criterion to distinguish between Ethernet and wireless traffic. To identify unauthorized WLAN hosts connected to a RAP, proper choice of threshold values helps an analyst to eliminate false detection of large number of authorized wireless hosts.

References

[1] Wei Wei, Kyoungwon Suh, Yu Gu, Bing Wang, Jim Kurose, "Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs," Technical Report, UM-CS-2006-060, Nov. 2006.

[2] Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and John Copeland, "Rogue Access Point Detection using Temporal Traffic Characteristics," *in Proc. of IEEE GLOBECOM*, Dec. 2004.

[3] A. Adya, V. Bahl, R. Chandra, and L. Qiu, "Architecture and Techniques for Diagnosing Faults," *in Proc. of ACM Mobicom*, Sept. 2004.

[4] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," in *Proc. of ACM MobiSys*, 2006.

[5] AirDefense, http://airdefense.net

[6] AirMagnet, http://www.airmagnet.com.

[7] Airwave, Airwave Management Platform, www.airwave.com

[8] Cisco Wireless LAN Solution Engine, www.cisco.com

[9] NetStumbler, http://www.netstumbler.com.

[10] Proxim, http://www.proxim.com

[11] Wavelink, http://www.wavelink.com

[12] Highwalltech,. http://www.highwalltech.com

[13] Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng, and Min Song, "RAP: Protecting Commodity Wi-Fi Networks from Rogue Access Points," Proceedings of Qshine 2007.