POSTER: Highly-Accurate Rogue Access Point Detection using Intentional Channel Interference

RhongHo Jang, Jeonil Kang, Aziz Mohaisen†, and DaeHun Nyang
Department of Computer Engineering of Inha University, Korea
†Department of Computer Science and Engineering, University at Buffalo, USA
r.h.jang211@gmail.com,dreamx@isrl.kr,mohaisen@ieee.org,nyang@inha.ac.kr

ABSTRACT

In this work, we introduce a powerful hardware-based rogue access point (PrAP), which can relay traffic between a legitimate AP and a wireless station, and act as a man-in-the-middle attacker. To defend against PrAPs, we propose PrAP-Hunter based on intentional channel interference. We demonstrate close to 100% of detection rate, compared to 60% detection rate by the state-of-the-art.

1 INTRODUCTION

Rogue Access Point (rAP) can be easily created with a laptop and an additional network adaptor to launch a large array of attacks on innocent users connecting to it. Such attacks are facilitated by Man-In-The-Middle (MITM) [2]. A rAP can be detected in many ways, but mainly using time-based technologies. We developed a powerful hardware-based rAP (PrAP) and defeated existing time-based solutions that depend on the characteristics of inter-packets arrival time or the round trip time of traffics. We propose and validate a channel interference-based detection technology to defeat this kind of powerful hardware-based rAP (PrAP), which we call PrAP-Hunter (see Fig. 5). Our solution achieved close to 100% detection rate.

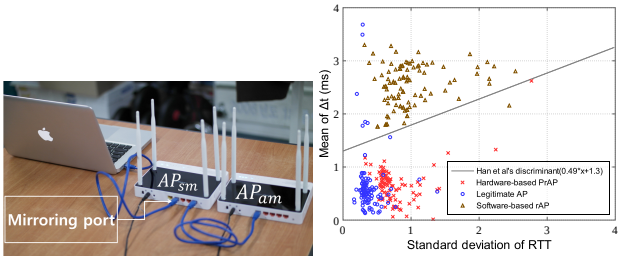
2 DEFEATING EXISTING DETECTORS

In many time-based rAP detection methods, researchers stated that when packets were sent through rAPs, packet delay would occur because rAPs used an additional wireless path, and used this delay for detection. However, we note that the observed delay was not the result of an additional wireless path, but rather the result of a computational delay caused by the software bridging. To show that, we implemented a time-based detector described by Han *et al.* [1], where they used the round trip times between station and a DNS server and between station and AP to determine whether the used AP is rogue or not. Then, we performed experiments for Han *et al.*'s algorithm under the rAP and the PrAP using the following:

Software-based rAP. The rAPs are defined using a laptop and an additional WLAN USB adapter. This type of rAP can easily be set up by adding rules to the `iptable` or by setting up the Internet sharing functionality of Microsoft Windows or Mac OS.

WiSec'17, Boston, MA, USA

DOI: 10.1145/nnnnnnn.nnnnnnn



(a) (b)

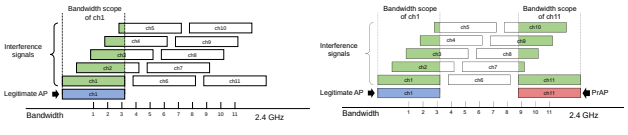
Figure 1: (a) Hardware setting of the PrAP (EFM ipTIME N8004R). AP_{sm} is responsible for repeating signals to and from the legitimate AP. AP_{am} and AP_{sm} are interconnected with a LAN cable via a wireless bridge function, and AP_{am} is assigned a valid IP from a DHCP server of AP_{sm} with a spoofed SSID and MAC address. (b) Results of Han *et al.*'s [1] algorithm for two different rogue APs: software- and hardware-based.

Hardware-based PrAP. Fig. 1(a) shows a setup of a PrAP costing under $100. Our PrAP is built of two dedicated wireless routers interconnected physically, and can relay traffic rapidly between a station and a legitimate AP.

Through experiments, we demonstrate that the state-of-the-art time-based rogue AP (rAP) detectors cannot detect our PrAP, although effective against software-based rAP. Fig. 1(b) shows clearly that Han *et al.*'s algorithm could successfully distinguish the legitimate AP and the software-based rAP. However, we also see that the same technique did not work against the hardware-based PrAP (i.e., the mean of Δt is mixed for both the legitimate AP (blue circles) and the PrAP (red crosses), which supports our conclusion).

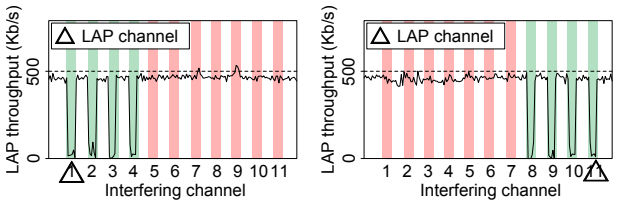
3 PRAP DETECTION STRATEGY

Now, we turn our attention to the detection method and strategy (a prototype of the detector is shown in Fig. 5). Fig. 2 shows our PrAP detection strategy, considering the wireless bandwidth standpoint. In Fig. 2(a), we show a detection scenario where the legitimate AP uses channel 1 without PrAP. First, PrAP-Hunter generates



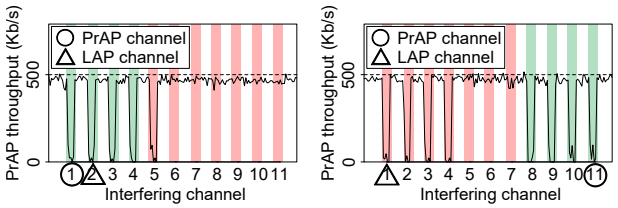
(a) With legitimate AP (b) With PrAP

Figure 2: Channel interference under IEEE 802.11n



(a) Channel 1 (b) Channel 11

Figure 3: Legitimate AP on various channels. Green bars indicate the overlapped channels with the connecting AP's (here, a legitimate AP) channel affected by interferance, which confirms the channel overlapping model of IEEE802.11n.



(a) PrAP on channel 1 and legitimate AP on channel 2 (b) PrAP on channel 11 and legitimate AP on channel 2

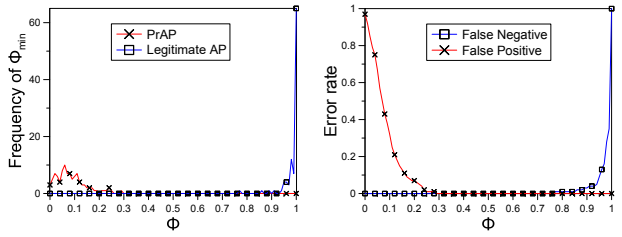
Figure 4: PrAP with varying channels for PrAP and the legitimate AP. Red bars indicate the non-overlapped channels. The non-overlapped channels are affected by interference with the channel of the connecting AP (here, a PrAP).

traffic through the currently connected AP, while the interference device is transmitting data on channel 1 to 11 with a rest time between each channel interference. Then, when the interference device transmits on channels 1 to 4, the throughput of the legitimate AP at channel 1 is obstructed because of bandwidth sharing as shown in Fig. 3(a). Channel 5 also shares a 2 MHz bandwidth with channel 1. However, we note that 2 MHz bandwidth sharing is not enough to interfere substantially. As a result, we obtained the scenario in Fig. 3(a). Fig. 2(b) shows a detection scenario where a PrAP (ch 11) repeats a signal of legitimate AP (ch 1). If the AP connected on channel 11 was legitimate, the results of detection should look similar to the results reported in Fig. 3(b). However, because we experienced an unexpected throughput degradation on channel 11 as shown in Fig. 4 when we interfered on channels 1-4 (throughput degradation should have occurred only when interfering on channels 8-11 without a PrAP), we conclude that the connected AP is a PrAP, providing wireless connectivity by repeating signals. In summary, if the number of obstructed channels is more than that of the "legitimate AP's only scenario" (that is, if the number of throughput degradation in Fig. 4 is greater than in Fig. 3), there must be a PrAP in the system.

4 PERFORMANCE

We examined the proposed method against both legitimate AP and PrAP 100 times, respectively. The repeated experiments were conducted to marginalize the effect of randomness in the results and to establish the detection results with higher confidence. As a result,

Figure 5: A prototype of PrAP-Hunter. (A) PrAP-Hunter, (B) channel interference device



(a) Distribution of Φ_{min} (b) Error rate against Φ

Figure 6: Results. (a) PrAP-Hunter: the distribution of Φ_{min} in our experimental setup. The detection trials were repeated 100 times for the rogue and legitimate AP measurements, respectively. y-axis ($= f(\Phi_{min})$) shows the frequency of Φ_{min}. (b) The CDF of the false negative and false positive rates against various values of Φ.

our experiments showed 100% success rate in detecting both legitimate AP and PrAP. As shown in Fig. 6(a), the legitimate APs and PrAPs could clearly be distinguished, because all Φ_{min}s for each PrAP detection were less than 0.3, and for legitimate AP detection, they were greater than 0.85.

Fig. 6(b) shows the legitimate AP and the PrAP detection error rate against Φ. As shown in the figure, we can keep both false positive and false negative rates at 0% when we setting the detection threshold between 0.3 and 0.78, respectively.

5 CONCLUSION

We introduced a PrAP that can evade the most widely accepted and used time-based detection techniques. We showed that while time-based techniques were indeed suitable for software-based rAP detection, they were obsolete against our new PrAP. To defend against its threat, we developed a new mechanism that used channel interference and defeat showed a high detection rate.

ACKNOWLEDGEMENT

This work was supported by the Global Research Lab. (GRL) Program of the National Research Foundation (NRF) funded by Ministry of Science, ICT and Future Planning (NRF-2016K1A1A2912757).

REFERENCES

[1] Hao Han, Bo Sheng, Chiu Chiang Tan, Qun Li, and Sanglu Lu. 2011. A timing-based scheme for rogue AP detection. *IEEE Transactions on parallel and distributed Systems* 22, 11 (2011), 1912–1925.

[2] Rhongho Jang, Jeonil Kang, Aziz Mohaisen, and DaeHun Nyang. 2017. Rogue Access Point Detector Using Characteristics of Channel Overlapping in 802.11n. In *2017 IEEE International Conf. on Distributed Computing Systems (ICDCS)*.