This paper was presented as part of the main technical program at IEEE INFOCOM 2011

Defending Against Vehicular Rogue APs

Hao Han, Fengyuan Xu, Chiu C. Tan, Yifan Zhang, Qun Li
College of William and Mary, Williamsburg, VA, USA
Email: {hhan, fxu, cct, yzhang, liqun}@cs.wm.edu

***Abstract*—This paper considers vehicular rogue access points (APs) that rogue APs are set up in moving vehicles to mimic legitimate roadside APs to lure users to associate to them. Due to its mobility, a vehicular rogue AP is able to maintain a long connection with users. Thus, the adversary has more time to launch various attacks to steal users' private information. We propose a practical detection scheme based on the comparison of Receive Signal Strength (RSS) to prevent users from connecting to rogue APs. The basic idea of our solution is to force APs (both legitimate and fake) to report their GPS locations and transmission powers in beacons. Based on such information, users can validate whether the measured RSS matches the value estimated from the AP's location, transmission power, and its own GPS location. Furthermore, we consider the impact of path loss and shadowing and propose a method based on rate adaption to deal with advanced rogue APs. We implemented our detection technique on commercial off-the-shelf devices including wireless cards, antennas, and GPS modules to evaluate the efficacy of our scheme.**

I. Introduction

The proliferation of IEEE 802.11 access points (APs) in public spaces has provided users easy access to the Internet anytime and anywhere. Many city-wide wifi networks have already been deployed in the real world. For instance, Google provides a free wireless Internet service to the city of Mountain View [1]. APs are also proposed for deployment along the road for vehicular networks. We believe future vehicles will be equipped with wireless capabilities that enable a car to communicate over the Internet through roadside APs (also known as *Drive-thru Internet* [2], [3]), and this will become a reality in the next few years.

Due to the ubiquitous deployment of APs, the problem of rogue access points (also known as rogue APs) has emerged as a well recognized security issue. A rogue AP is a malicious AP that pretends to be a legitimate AP to induce users to connect. Once an innocent user has associated to a rogue AP, the adversary can then launch various attacks by manipulating users' packets. For example, the adversary can launch phishing attacks to redirect a user's web page request to a fake location, seeking to steal the user's private information such as bank account numbers and passwords.

In a vehicular network, rogue APs can be classified into two categories: *static* and *mobile*. In the first category, a rogue AP is set up at a fixed place, for example in public hotspots such as a building facing a busy road. Since this type of rogue AP usually keeps active for a long time and uses the same infrastructure to access Internet, it is relatively not difficult for administrators to detect such a rogue AP. Previous work [4]–[14] has already proposed several methods to detect static rogue APs. However, there is little work on how to defend against a mobile rogue AP where the rogue AP is set up in a moving vehicle to attract users on the road. Due to its mobility, such a rogue AP is able to maintain a long connection with users. Thus, the adversary has more time to launch various attacks to steal users' private information. Detecting a vehicular rogue AP is challenging because the duration for a vehicle connected to any single AP is short. When the signal strength of a connected AP is less than a threshold, the client has to take a handoff [15] and re-associate to another AP with the strongest signal strength. Hence, the time left for the rogue AP detection is restricted. We need a more efficient detecting scheme, since it is meaningless for a client to identify a legitimate AP while such an AP is out of the communication range. In addition, it is more difficult to prevent the installation of a vehicular rogue AP, since this type of rogue AP is always moving. Even if extensive sniffers are deployed along the road, the vehicular rogue will have moved to a different location before the authority can detect it. Furthermore, we consider a sophisticated vehicular rogue AP, which can mimic the roadside AP to avoid simple detection. For example, we cannot simply use the duration of the association time to indicate whether a connected AP is a rogue AP, since the adversary can control the rogue AP to reply fake messages directly.

Considering the above challenges, we propose a practical detection scheme that prevents user from connecting to a vehicular rogue AP. Our solution imposes minimal modification to existing wireless standard. The whole detection process relies on the knowledge of the transmission powers and the locations of APs in the vicinity. The clients leverage the received signal strength (RSS) of beacons which are broadcasted by the APs periodically, and tune the transmission rate of probe requests to detect rogue APs. To the best of our knowledge, we are the first to consider the vehicular rogue AP problem and propose a practical detection solution. Our main contributions are listed as follows:

1) We are the first to consider the vehicular rogue AP problem and demonstrate the feasibility of this type of rogue AP.
2) We propose a practical method to defend against vehicular rogue APs including basic attacks and sophisticated attacks. Our solution is user-centric and can apply to 802.11 based vehicular networks. Our method can be implemented with little modification to current 802.11 standard.

3) We implement our schemes using commercial off-the-shelf devices including wireless cards, antennas, and GPS modules. Also, we perform extensive experiments on realistic road conditions to evaluate our schemes.

The rest of the paper is organized as follows. Section II discusses the related work. Section III describes some background including motivation, problem formulation, and adversary model respectively. Our detection algorithm is detailed in Section IV. Our implementation and evaluation results are presented in Section V. We discuss the limitation of our solution in Section VI and conclude in Section VII.

II. Related Work

The threat of rogue APs has attracted the attention of both industrial and academic researchers. Previous research has been mainly focused on detecting static rogue APs in an enterprise or a hotspot scenario. Typically, existing schemes can be classified into to three categories.

The first category relies on sniffers to monitor wireless traffic. These sniffers usually scan spectrum to examine the 2.4 and 5GHz frequencies. Once detecting any traffic from unauthorized APs, they will alert the administrator. This approach usually demands well controlled infrastructure such as enterprise networks, where the administrator can easily deploy sniffers and cut off the access of rogue APs to Internet. Some commercial products [16]–[18] have been developed following this technique. In academic community, an architecture for diagnosing various faults in WLAN including rogue APs, is presented in [10], where multiple APs and mobile clients installing a special diagnostic software cooperate to perform RF monitoring. In [13], another monitoring infrastructure called DAIR is proposed, where USB wireless adapters are attached to desktop machines for capturing more comprehensive traffic to reduce false detection rate. Different from this type of solution, our defending scheme does not reply on sniffers. That is because a small amount of sniffers may not catch vehicular rogue APs well, but extensive deployment of sniffers is impractical.

The technique used in the second category is leveraging fingerprints to identify rogue APs. Since an advanced adversary can easily spoof a rogue AP's MAC address, SSID, vendor name, and configuration to escape from the detection, the previous work often adopted the fingerprints that cannot be easily forged. For example, the work by [19] calculated every AP's clock skew by collecting their beacons and probe responses. Since clock skew is difficult to forge , any AP with unknown clock skew is identified as a rogue AP. In addition to clock skew, RSS values [20], radio frequency variations [21] are also used. However, a major drawback of this type of schemes is that the AP validation requires to access a database containing the fingerprints of all legitimate APs. This database may not be available for end users before they connect to the AP. Our solution differs from such schemes in that we do not assume the clients know the fingerprints of legitimate APs in advance. Therefore, our detection scheme can apply to not only network administrators but also end users who use the wireless network for the first time.

The last category exploits the features of wireless traffic to detect the presence of rogue APs [4]–[6], [9]. In [4], a practical timing based scheme is proposed. The method employs the round trip time between user and local DNS server to detect rogue APs without assistance from network administrators. [11] utilizes the immediate switch connecting rogue APs to measure round trip time of TCP traffic. Other work by [12], [14] uses the spacing between packets to distinguish wireless networks from wired networks. In [6], inter-arrival time of ACK-pair is used to detect rogue APs. In [9], wired verifier and wireless sniffers are deployed at the same time to detect layer-3 rogue APs. Since we consider a new type of rogue AP, it is unclear whether previous solutions could work in vehicular networks. Although some schemes might work, it may spend much time on analyzing the network traffic. Our solution is more efficient and end-user centric.

III. Background

In this section, we discuss some background to our vehicular rogue AP problem, including problem formulation, motivation and adversary model.

A. Problem formulation

When a vehicular client tries to access Internet through roadside APs, the client will first scan all wireless channels. After scanning, the client could discover multiple APs within its communication range, where some APs are legitimate and some are rogue. According to current standard, a client will pick the AP with strongest signal strength to associate. To induce clients, the adversary will choose to drive a car along the road with a rogue AP inside. Since the rogue AP is closer to vehicular clients, the rogue AP's signal strength is very likely to be greater than a roadside AP. In addition, a sophisticated adversary could control the rogue AP delicately to avoid detection. For example, the adversary can forge a valid SSID and MAC address, or directly reply fake messages without accessing Internet first to avoid some timing-based detections. The objective of this paper is to help clients to avoid associating to such a ”smart” vehicular rogue AP. Our solution can be viewed as a complementary part to existing AP selection policies.

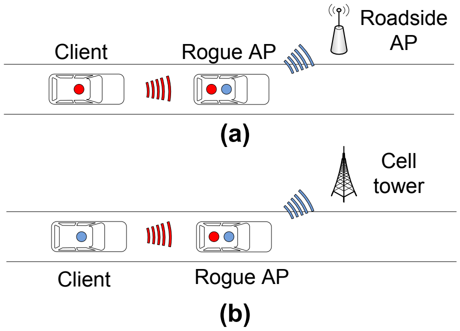


Fig. 1. Illustration of two typical setups for vehicular rogue APs

Vehicular rogue AP is assumed to be launched in a car with two wireless interfaces. The first interface pretends to be a valid AP, and the other interface is used to connect to Internet. Fig. 1 illustrates two typical setups for a vehicular rogue AP. In the first setting (a), the rogue AP is equipped with two 802.11 wireless adapters: the first adapter is configured to AP mode, whereas the second adapter is set to station mode for connection to a real roadside AP. Nevertheless, the rogue AP does not reply on roadside APs. In the alternative setting (b), the first interface still pretends to be an AP, but the second interface connects to a cellular tower. For both settings, a bridge is set between two interfaces. Once a packet is received by the first interface, it will be forwarded to the second interface, and vice versa. The adversary may choose either setting to launch attacks. We seek to detect rogue APs under both settings.

In this paper, we do not consider AP is capable of using RADIUS-based 802.1X authentication of users, since it requires each vehicle to have the correct key to access the network. While this may be possible, for example, every car when registered with the DMV is issued the appropriate credentials, it is unclear how well this will work in practice. Thus, we only consider the open 802.11 network where any car can connect.

B. *Practicality of vehicular rogue APs*

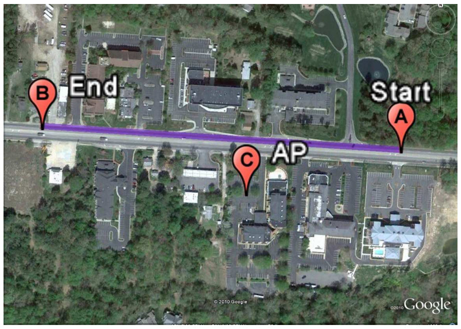


Fig. 2. Demonstration of the feasibility of vehicular rogue APs

To demonstrate vehicular rogue AP is a feasible threat, we set up a testbed shown in Fig. 2, where three laptops and two vehicles are used. The first laptop configured as a roadside AP is placed at location C. An external antenna connected to such a laptop is mounted on the top of a ladder in the height of 2 meters. A vehicular rogue AP and a vehicular client drive from location A to B, each with a laptop inside and an external antenna mounted on the roof. They maintained the distance of 10 meters away from each other. The length between A and B is approximately 500 meters.

From the vehicular client's view, we measure the RSS of beacons broadcasted by both roadside AP and the vehicular rogue AP. Fig. 3 shows the results, where the x-axis denotes the elapsed time and the y-axis presents the RSS values. As we see, the vehicular rogue AP is easy to maintain relatively larger RSS values than the roadside AP. It is true that a client will be attracted by the vehicular rogue, since the client will always pick the AP with the strongest signal strength to associate. Note that both the roadside AP and the vehicular rogue use the same maximum transmission power.

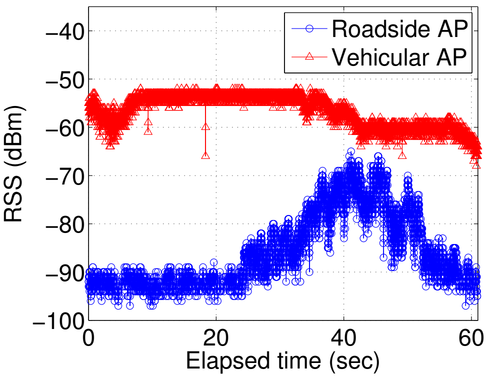


Fig. 3. Measured RSS of the roadside AP and the vehicular rogue from location A to B

C. *Adversary model*

Recall that the goal of vehicular rogues is to induce clients to connect. If any client associates to a vehicular rogue, the adversary succeeds. Next are several assumptions of vehicular rogue APs. First, we assume that the adversary uses off-the-shelf hardware to set up a vehicular rogue. The rogue AP is able to transmit a packet with arbitrary transmission (TX) power, and inject any packet with any content (including changing the 802.11 MAC header). For example, the adversary is able to forge fake re-associate frames to force clients to re-select APs immediately. Second, we assume the adversary cannot modify the firmware of hardware devices. In other words, the rogue AP cannot control ACK frames. Although any frame including the ACK can be generated, the ACK cannot be sent back to the client within an ACK timeout. It is reported that the time interval between data and ACK is a SIFS (10 μs in 802.11g [22]). Software (not firmware) ACK cannot be prepared within such a interval [23]. Last, the adversary is able to provide whatever fake information to clients. For example, the adversary can monitor the wireless channels to learn the SSID and MAC address of a legitimate AP, and then set up its rogue AP with the same information.

Based on the assumptions described above, the adversary has two types of attacks.

- **Basic attack** In the basic attack, the vehicular rogue always broadcasts beacons with the maximum TX power. That is because the maximum power will lead to the strongest signal strength with which the vehicular rogue has most probability to attract users to connect. The advantage of the basic attack is its easy setup. Without any complicated configuration, the basic attack can be launched anytime and anywhere.
- **Advanced attack** The advanced attack differs from the basic attack in two aspects. First, the advanced adversary

is able to perform background preparation before creating a vehicular rogue AP. The background preparation includes profiling the RSS values of roadside APs, investigating the road conditions (e.g. the road direction, lanes, intersection and so on) and traffic conditions. Second, the advanced adversary targets a specific area of the road. By tuning the TX power carefully, the adversary forges the signal strength received in the target area, so that it appears to be "real". Compared with the basic attack, the advanced attack is more time-consuming, but is more difficult to be detected.

IV. Our Solution

Our vehicular rogue AP detection scheme demands slight modification to APs that each AP embeds its GPS location and TX power in every beacon. The GPS location indicates the AP's coordinates in the form of a latitude-longitude pair. The TX power presents the effective isotropic-radiated power (EIRP) which equals to the power level plus antenna gain and minus cable loss. This two pieces of information can be obtained by the administrator in advance, or obtained from wireless driver automatically. A user will then use them to detect vehicular rogues. Note that the 802.11 standard allows us to add variable-length information elements at the end of each beacon frame. The form of information elements is shown in Fig. 4. Furthermore, if an AP uses static TX power, this two pieces of information can be manually set in the SSID field without any modification to APs. For example, a valid SSID is like `` ``W-M_Wireless, (37.270643, -76.712383), 20dBm'' ``.

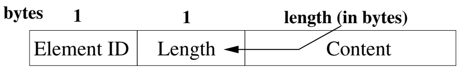


Fig. 4. Format of information elements

A. Defending against the basic attacks

Since a roadside AP has to report its TX power and GPS location. The adversary will have to decide what values should be appended in beacons. In the basic attack, the adversary is assumed to induce users in an opportunistic manner. Hence, choosing the maximum power is the best strategy for them. However, the adversary should not report its actual GPS location, since this location indicates that the AP is in the middle of the road. A user can easily detect it. Therefore, the adversary must report a fake AP location. Fig. 5 shows three possibilities.

Upon receiving a beacon, the client then obtains AP's reported location, TX power, and a measured RSS. After knowing the reported GPS location as well as its own GPS location, the client can then calculate the distance between the AP and itself. Based on that distance, TX power, and RSS, our algorithm is used to determine whether the tested AP is a rogue AP. The main idea is as follows. Let d and d' denote the actual and reported distance between the rogue AP and the client separately. Suppose the adversary picked a location such that $d < d'$ (see Fig. 5 (1)). The client is expected to receive beacons with "abnormally" large RSS values. On the other hand, if $d > d'$ (see Fig. 5 (3)), the RSS values are "abnormally" less than the expectation . Here, the abnormality is defined as exceeding (i.e. less than the lower bound or greater than the upper bound) a valid range of RSS values derived from the path loss model.

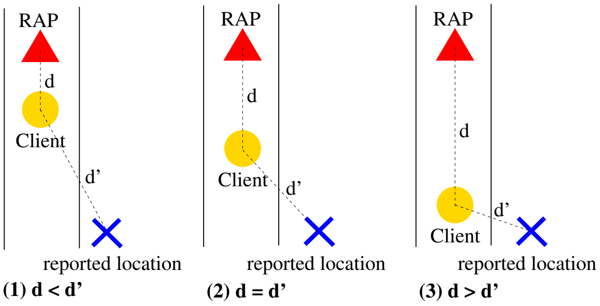


Fig. 5. Illustration of basic attacks, where triangle, circle, and cross denote vehicular rogue AP, vehicular client, and reported location respectively

We adopt a common path loss model [24] considering two factors that may incur signal attenuation: *path loss* and *shadowing*. The path loss is the attenuation of electromagnetic signal propagating through space. The model assumes the path loss (PL) is exponentially proportional to the transmit-receive distance d,

$$PL(d) \propto d^{\gamma}.$$

The shadowing that is caused by obstacles between the transmitter and receiver that attenuate signal power through absorption, reflection, scattering, and diffraction. The received signal strength P_r in dBm is then given by

$$P_r = P_t - (10\gamma \log_{10}(d) + c + X_{\delta}) \quad (dBm), \qquad (1)$$

where P_t is the transmission power in dBm. Variable γ, the *path loss exponent*, determines the rate of attenuation when the signal propagating through the space. Variable c is a correction constant which describes the additional loss or gain in the model. Variable X_{δ} is a random variable describing the shadow fading which makes the received signal strength different from the mean predicted path loss. Field measurements have verified this variation to be environment dependable and follows *log-normal* distribution [24].

Algorithm 1 presents our solution to defend against basic attacks. We use clt to denote a client and ap to denote a tested AP with the strongest signal strength discovered by the client. If ap passed the algorithm, the client will terminate the test and connect to that AP. Otherwise, the client will continue the algorithm on next AP until all the APs are tested. Eventually if no AP can pass the algorithm, the client will keep un-associated until a new AP is scanned. In Algorithm 1, the client first collects n beacons from ap and measure RSS values. Meanwhile, AP's TX powers and GPS locations, as well as client's GPS locations, are recorded (in line 1). Then, the client calculates the distance from the AP (in line 2). It is noticed that the update of GPS usually is slower than the

Algorithm 1 Detecting Basic Rogue APs

```
1:  Listen $n$ beacons from the tested $ap$ and record $\{rss_i\}$, $\{power_i\}$, $\{gps_i^{ap}\}$, and $\{gps_i^{clt}\}$ for each beacon
2:  $distance_i = \|gps_i^{ap} - gps_i^{clt}\|$
3:  for $k = 1$ to $n - 2$ do
4:      if $|rss_k - rss_{k+1}|$ and $|rss_{k+1} - rss_{k+2}| > \tau$ then
5:          $rss_{k+1} \leftarrow (rss_k + rss_{k+2})/2$
6:      end if
7:  end for
8:  Use maximum likelihood estimation to calculate $\hat{\gamma}$ by Eq. 2 and Eq. 3
9:  if ($\hat{\gamma} <$ lower bound ) or ($\hat{\gamma} >$ upper bound) then
10:     $ap$ is a rogue AP
11: end if
```

beacon interval. Thus, multiple beacons may have the same coordinates. To improve accuracy, we apply interpolation to consecutive GPS data. For example, consider the following segment of GPS coordinates included in consecutive beacons:

$$(x_1, y_1),\ (x_2, y_2),\ (x_3, y_3),\ (x_4, y_4),\ (x_5, y_5)\ \cdots$$

Suppose the median three coordinates have the same value (i.e. $x_2 = x_3 = x_4$ and $y_2 = y_3 = y_4$), since GPS was not updated at that time. After applying the interpolation, we obtain

$$(x_1, y_1),\ (x_2, y_2),\ (x_3', y_3'),\ (x_4', y_4'),\ (x_5, y_5)\ \cdots$$

where

$$(x_3', y_3') = (x_2 + \frac{x_5 - x_2}{3}, y_2 + \frac{y_5 - y_2}{3})$$

and

$$(x_4', y_4') = (x_2 + \frac{2 \cdot (x_5 - x_2)}{3}, y_2 + \frac{2 \cdot (y_5 - y_2)}{3}).$$

The detailed code of interpolation is ignored. Next, the loop from line 3 to 7 is used to filter out the extreme RSS values caused by environment interference. The client checks consecutive three RSS values. If the difference between the median value and the first/last value exceeds a threshold τ, the median value is replaced by the average of its previous and next values. After smoothing, we fit RSS values, distances, and TX powers into our path loss model (i.e. Eq. 1), and use maximum likelihood estimation (MLE) to estimate the parameter γ of the model. Without fitting, the variations of measured GPS and RSS data may lead to detection errors in practice. To minimize the squared error, the estimation of γ can be obtained by

$$f(\hat{\gamma}, \hat{c}) = \sum_{i=1}^{n} (RSS_i - Pt_i + 10\hat{\gamma}\log_{10}(d_i) + \hat{c})^2.$$

Differentiating $f(\hat{\gamma}, \hat{c})$ and setting it to be zero, the value of $\hat{\gamma}$ and $\hat{c}$ can be derived as follows,

$$\hat{\gamma} = \frac{-\sum_{i=1}^{n}(RSS_i - Pt_i + \hat{c})\log_{10}(d_i)}{\sum_{i=1}^{n} 10(\log_{10}(d_i))^2} \qquad (2)$$

$$\hat{c} = \frac{-\sum_{i=1}^{n}(RSS_i - Pt_i + 10\hat{\gamma}\log_{10}(d_i))}{n} \qquad (3)$$

If $\hat{\gamma}$ exceeds an empirical bound, we suspect the tested ap to be rogue. Previous work has pointed out that the path loss exponent normally ranges from 2 to 6 [25], where 2 is for propagation in free space, and 6 is for relatively lossy environment. Therefore, we heuristically set the lower bound of γ to 2 and the upper bound to 6. Last, in the case that $d = d'$, our algorithm cannot distinguish the rogue AP. However, we argue that the cars are continuously moving, the adversary cannot maintain this condition. Therefore, this condition is safe to be ignored.

B. Defending against advanced attacks

A more sophisticated adversary can launch advanced attacks which require more preparations than basic attacks. For example, the adversary can set up a stationary AP at a specific location and drive along the road to profile RSS values from that AP. The adversary dynamically tweaks the TX power to make the RSS received at a desired target area similar to the profiled values. Then, the rogue AP reports such a location. Within the targeted area, the client cannot use RSS to detect the rogue AP, since the RSS values appear to come from the reported location.

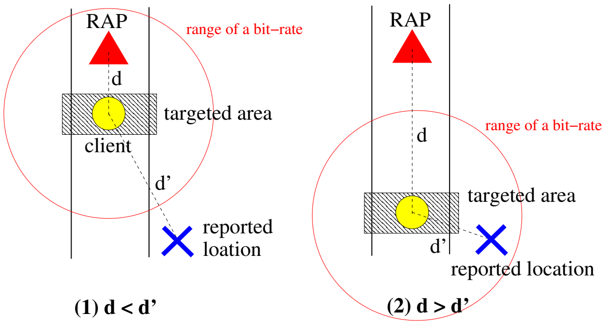
To defend against the advanced attacks, our algorithm requires the client to actively send *probe request* frames to the AP with the TX power included in beacons but different bitrates. In 802.11 standard, different modulation schemes support the packet transmission with multi-rates. IEEE 802.11a uses a multi-carrier modulation scheme (OFDM), where different data rates will use different modulation formats (BPSK, QPSK, QAM) accordingly. IEEE 802.11b uses direct sequence spread spectrum (DSSS) modulation. For the 1Mbps and 2Mbps data rates, the modulation format is set to DBPSK and DQPSK respectively. For 5.5Mbps and 11 Mbps, there are two coding schemes: CCK and PBCC, where CCK is mandatory and PBCC is optional. The details are described in Table I [26].

TABLE I
MODULATIONS FOR 802.11A/G

Rates (Mbps)	standard	Modulation	RX sensitivity (dBm)
6	802.11a/g	BPSK/OFDM	-82
9	802.11a/g	BPSK/OFDM	-81
12	802.11a/g	QPSK/OFDM	-79
18	802.11a/g	QPSK/OFDM	-77
24	802.11a/g	QAM-16/OFDM	-74
36	802.11a/g	QAM-16/OFDM	-70
48	802.11a/g	QAM-64/OFDM	-66
54	802.11a/g	QAM-64/OFDM	-65

As we see, different transmission rate requires different receiver (RX) sensitivity. According to 802.11 standard, a receiver cannot demodulate the packet with RSS less than the RX sensitivity. Thus, we can send packets with varying transmission rates to test if the AP is within a certain distance at which a corresponding rate can be demodulated with an acceptable bit error rate (BER). If the AP is out of the range of such a bit rate, the client cannot receive any ACK frame.

Otherwise, the client can receive the ACK frame. Based on that, we can verify if the AP reported its location honestly.



(1) d < d'

(2) d > d'

Fig. 6. Illustration of advanced attacks

Next, we consider two situations of advanced attacks (shown in Fig. 6): (1) the reported location is far away from the targeted area, whereas the distance between AP's actual location and the targeted area is closer (i.e. $d < d'$); (2) opposite to the first situation (i.e. $d > d'$). In the first condition, the adversary should use a relatively small TX power, since the actual distance is closer than the reported. In other words, the reported TX power is greater than the actual TX power. Suppose there is a client within the targeted area. If such a client starts a transmission with RX sensitivity greater than the received RSS, it is expected that the packet will not be demodulated at the reported location. As illustrated in Fig. 6 (1), the big circle depicts the range of the transmission rate. Within the circle, the packet can be demodulated. Out of the circle, the packet cannot be demodulated. Here, the client can receive ACKs. That implies the tested AP should not be located at the reported location. Hence, the tested AP is suspected to be a rogue AP. In the second situation that $d > d'$, the client will transmit a probe request with a transmission rate whose RX sensitivity is less than the received RSS. It is expected the tested AP will reply ACKs. However, the client does not receive the ACK. Thus, the tested AP is also suspected to be a rogue AP. At last, due to the similar reason mentioned in previous subsection, we do not consider the situation that $d = d'$.

Algorithm 2 describes our scheme to defend against advanced attacks, where some functions are described in Table II.

TABLE II
FUNCTION DESCRIPTION

function name	notation
$sen(x)$	return the RX sensitivity (dBm) of a bit-rate x
$pre(x)$	return the bit-rate slightly slower than the bit-rate x
$next(x)$	return the bit-rate slightly faster than the bit-rate x
$ratio(x)$	return the ratio of the number of ACKs replied to the number of probe requests transmitted with bit-rate x
$rateset[i]$	return the ith rate in $rateset$

In the algorithm, the client tries multiple bit-rates (smaller and larger rates) to verify both cases that $d > d'$ and $d < d'$. Since the ACK may be corrupted by noisy environment, the client does not receive the ACK not only because of the failed demodulation of probe requests, but also due to the lost ACKs. Therefore, multiple rounds are used to reduce the errors.

Algorithm 2 Detecting Advanced Rogue APs

```
procedure 1: adjust_tx_power ($rss,\ pt$)
if $rss > sen(48\text{Mbps})$ then
    return $pt - (rss - \frac{sen(36\text{Mbps})+sen(48\text{Mbps})}{2})$
else
    return $pt$
end if
procedure 2: return_bitrate_set ($rss,\ pt$)
if $rss > sen(48\text{Mbps})$ then
    return $\{24\text{Mbps}, 36\text{Mbps}, 48\text{Mbps}, 54\text{Mbps}\}$
else
    $rate \leftarrow$s.t. $sen(pre(rate)) \leq rss_i$ and $sen(rate) > rss_i$
    return $\{pre(pre(rate)),\ pre(rate),\ rate,\ next(rate)\}$
end if
Initialize $pass_k$ to $false$ where $k \in [1, 4]$
for $i = 1$ to $n$ do
    Receive a beacon and record $rss_i$ and $pt_i$
    $txpower \leftarrow$ adjust_tx_power ($rss_i,\ pt_i$)
    $rateset \leftarrow$ return_bitrate_set ($rss_i,\ pt_i$)
    for $j = 1$ to $m$ do
        Randomly pick a $rate_x$ from $rateset$
        Transmit a probe request with $rate_x$ and $txpower$
    end for
end for
for $k = 1$ to 4 do
    $pass_k \leftarrow true$if $ratio(rateset[k]) > \theta$
end for
if $pass_1 = true$ and $pass_2 = true$ and $pass_3 = false$
and $pass_4 = false$ then
    The tested AP is a legitimate AP
else
    The tested AP is a rogue AP
end if
```

During the test, a client receives n beacons from an AP, and sends m probe requests to that AP right after each beacon. After that, the client will make a decision whether to associate to that AP. The decision is based on the ACK reply ratio (which is referred to the ratio of the number of received ACKs to the number of transmitted probe requests). Particularly, once a client receives a beacon from an AP, the client will measure the RSS and extract the TX power. Then, the client determines a set of bit-rates consisting of four bit-rates. Two rates have greater RX sensitivity than the measured RSS, whereas the other two rates have the less RX sensitivity. Note that if the RSS is greater than 48Mbps, the client cannot find two higher rates since the maximum rate is 54Mbps. In that case, the client must reduces the TX power (see procedure 1). This is verified in practice that 10dBm reduction in TX power will lead to 10dBm decrease in RSS if the distance between sender and receiver is not far away.

Next, the client randomly picks a rate from the rate set to transmit a probe request frame. It is expected that the AP can demodulate two lower bit-rates but fail on two higher bit-rates. For each rate in the set, the client will compute an ACK reply ratio. If the ratio is greater than a threshold θ, it is deemed that the AP can demodulate packets with such a rate. If two lower bit-rates exceed θ but two higher bit-rates are less than θ, the client will associate to that AP. Otherwise, the AP is suspected to be rogue. Variables n, m, and θ are three adjustable parameters in our algorithm. According to our experimental results, we heuristically set that $m = n = 10$ and $\theta = 50\%$.

Lastly, our advanced detection algorithm relies on a relatively symmetric wireless channel. This is a reasonable assumption also mentioned in [27]. The symmetric channel means that the path loss between a transmitter and a receiver is similar. With the same transmission power, both the sender and receiver are supposed to receive packets with similar RSS values. To verify if this assumption is valid in outdoor vehicular networks, we conducted the experiment by recording the RSS values at both sender and receiver sides in moving vehicles. The results are shown in 7. As we see, the majority of the RSS pairs are within 3 dBm. Besides that, experimental results presented in evaluation section also show our schemes work in practice.

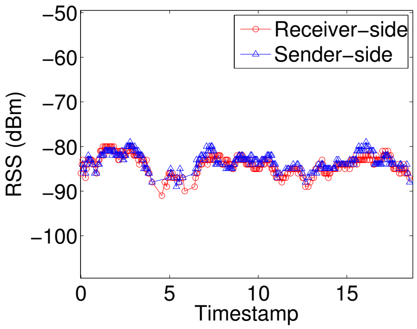


Fig. 7. Illustration of symmetric channel in outdoor vehicular scenario

V. Evaluation

In this section, we describe the setup of our experiments, followed by the experimental results.

A. Experimental setup

The experiments have three components: a roadside AP, a vehicular rogue AP, and a client.

Roadside AP A laptop connected with an external omni-antenna and a GPS receiver (see Fig. 8-left) mounted on the top of a ladder (in height of 2m) is configured as a roadside AP. The laptop was running a 2.6.27-7-generic Linux kernel with the latest madwifi driver (svn r4128). The wireless card is set to monitor mode which is easier for us to inject beacons with additional information such as GPS location and TX power. In our implementation, the field of GPS location has 18 bytes including 1 byte element ID, 1 byte length, 8 bytes latitude, and 8 bytes longitude. The field of TX power contains 1 byte element ID, 1 byte length, and 1 byte power value. The whole beacon packet is directly delivered to the wireless driver through libpcap [28].

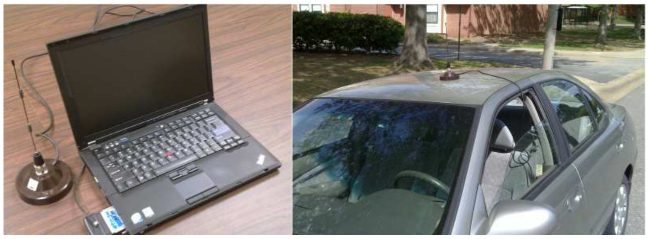


Fig. 8. Illustration of experimental equipment

Vehicular rogue AP For ease of setup, we did not set up the Internet access for the vehicular rogue AP, since it does not affect the experiments. The configuration of our vehicular rogue AP is similar to the roadside AP except that the external antenna and the GPS receiver are mounted on the roof of the car (see Fig. 8-right). For basic attacks, the TX power is fixed by executing command "iwconfig txpower [value]" with the maximum power value. For advanced attacks, tuning TX power per packet is achieved through *radiotap* header. In Linux, 802.11 MAC layer allows arbitrary injected packet composed in the following format:

[radiotap header] + [ieee80211 header] + [payload].

In the radiotap header, two types of argument are used by injection packet, namely `IEEE80211_RADIOTAP_RATE` and `IEEE80211_RADIOTAP_DMB_TX_POWER`. By filling the different value, the packet can be transmitted with the desired power level. Note that to control per-packet TX power, `hal_tpc` must be enabled while loading the madwifi module.

Client Another laptop with GPS module and external antenna is configured as a client. Similar to the APs, the client also sets the wireless interface to monitor mode. Sending and receiving packets are achieved by libpcap. Per-packet bit-rate control is done by radiotap header. Table III presents all the equipment used in our experiments.

TABLE III
Equipment description

Name	Notation
Laptop	Lenovo T61 with 2.0GHz processor and 1G RAM
GPS	GlobalSat BU-353 USB GPS receiver
Wireless card	CB9-GP Cardbus 802.11a/b/g using Atheros chipset
Antenna	7 dBi MA24-7N magnetic-mount omnidirectional

The experiments are conducted in an outdoor parking lot, where we can freely drive along the road or stop to collect measurements. We took two sets of experiment to evaluate our vehicular rogue AP detection schemes. The first set of experiments is for the basic attack. We set up a roadside AP near the road, and a vehicular rogue AP driving in front of a client. Both the roadside AP and the vehicular rogue AP use the same maximum TX power to transmit beacons. In the second set of experiments, we seek to test our solution to advanced attacks, but the difference is that the roadside AP, the vehicular rogue AP, and the client are all deployed stationary. Here, we do not conduct the experiment in moving vehicles. The reason is that we optimistically assume the vehicular rogue AP always tunes the TX power to make the RSS to look like “real”. However, it is difficult for the adversary to do that in practice. Therefore, for simplicity, we just investigate our scheme in several snapshots. Note that all the experiments were conducted extensively. We achieved similar results. The following section presents the detail.

B. Evaluation results

1) Basic attack evaluation: In this experiment, the roadside AP is static, whereas the vehicular rogue AP and the client are moving. We first test if the legitimate roadside AP can pass our algorithms. The left figure of Fig. 9 shows the RSS values of the roadside AP measured by the client and the distance between the AP and the client. Note that, the whole test was performed over 30 seconds. We ignore the periods from the starting point to 15 seconds and from 25 seconds to 30 seconds. That is because the RSS values measured in these periods are too weak for a client to connect. The right figure shows the fitting results of our algorithms for the period from 15 seconds to 20 seconds. As we see, $\hat{\gamma} = 3.06$ that is within the valid range. Therefore, the AP is not a rogue.

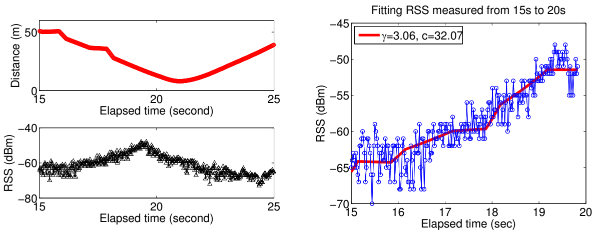


Fig. 9. Results of our algorithms in the case of the legitimate AP

To perform meaningful comparison, we assume the adversary reported the same location as the roadside AP. In that case, the distance between the client and the reported location (i.e. d') varies as shown in the left of Fig. 10, but the actual distance (i.e. d) keeps about 3 4 meters. Thus, fitting incorrect distance into the pass loss model will lead to the large departure from the valid range of model parameters. The right figure in Fig. 10 presents the incorrect fitting results. It is seen that the calculated $\hat{\gamma}$ equals to -0.4233. Therefore, such an AP is a rogue AP.

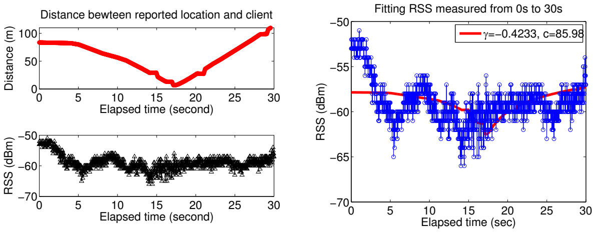


Fig. 10. Results of our algorithm in case of the basic attack

2) Advanced attack evaluation: Since the advanced attacks are more complicated, we separated our evaluation into two cases. In the first case that $d < d'$, the sophisticated adversary will decrease its TX power to make the RSS smaller, so that it appears to come from the reported location rather than the actual location. To verify if the probe requests can be demodulated at the reported location, we physically set an AP there. Thus, we have two APs at both reported location and actual location. It is expected that only the legitimate AP cannot demodulate packets with two low rates but can demodulate packets with the other two high rates. The opposite is true of rogue APs. Fig. 11 shows the results, where $d' = 42.67m$ and d is set to three values of $7.4m$, $22.3m$, and $37.5m$ respectively. As we see, all RAPs failed in passing our algorithms, even the adversary tunes the TX power carefully.

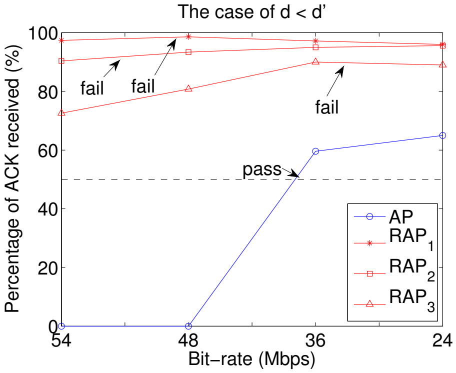


Fig. 11. Case 1: $d < d'$ where the distance between the reported location (we physically set an AP there) and the client is that $d' = 42.67m$. The distance between the vehicular rogue AP_i and the client is $d_1 = 7.4m$, $d_2 = 22.3m$, and $d_3 = 37.5m$ respectively. The reported TX power is 20dBm. The adversary will tune its TX power to make the mean RSS at client side to be 68 dBm.

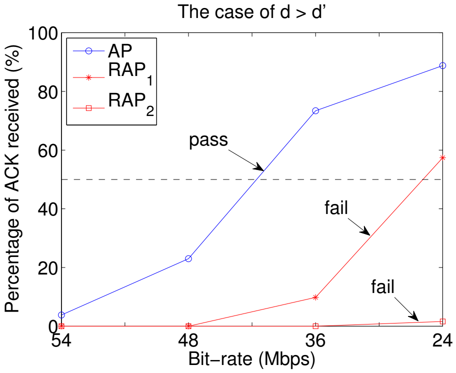


Fig. 12. Case 2: $d > d'$ where the distance between the reported location (we physically set an AP there) and the client is that $d' = 6.32m$. The distance between two locations of the rogue and the client are $d_1 = 17.7m$ and $d_2 = 30.3m$ respectively.

In the second case that $d > d'$, the adversary must increase the TX power to make the RSS larger. Again, an AP was set up in the reported location ($d = 6.32m$). Such an AP used 14dBm as the reported TX power to broadcast beacons. The mean RSS value received by the client was -60dBm, which was greater than the RX sensitivity of 48Mbps (say -66dBm). Following our second algorithm, the client then reduced TX power (6dBm) to transmit probe requests. Next, the vehicular rogue was placed at two further locations with distance that $d_1 = 17.7m$ and $d_2 = 30.3m$. The client used the same power 6dBm to test the vehicular rogue. The results are shown in Fig. 12. As we see, only the legitimate AP can demodulate the two high rates but fail on the other two low rates. Hence, the rogues are successfully determined.

VI. Discussion

Our solution makes use of physical characteristic such as path loss and RX sensitivity to determine the discrepancy between the rogue AP's actual location and its reported location. This makes our solution vulnerable to the following factors.

One factor is when the adversary picks its fake location that is very close to its current location. In other words, $|d - d'|$ is some very small value. From our experience, this is approximate 5 meters. When this happens, our scheme is unable to detect the rogue AP. However, in practice, this attack is not easily launched. The reason is that the vehicular rogue has to be continuously moving, and will quickly extend the distance between d and d'. For example, a vehicular rogue traveling with 60 miles per hour will have traveled approximately 27 meters in one second. Thus, the window of opportunity for the adversary to launch this attack is very small.

The other factor is that outdoor wireless channel condition is unpredictable. While our solution relies on the well-known signal propagation models. It is inevitable that there will be instances where the actual conditions deviate from the models. When this happens, our solution will not be able to determine the rogue AP as well. We can mitigate by adopting a more accurate model in our solution (Algorithm 1 line 8). In addition, it is unclear how well the adversary can take advantage of this limitation since the adversary is unable to predict the channel conditions as well. Finally, based on our deployment experiences, we observe that our scheme do not work as well in locations where there are a lot of buildings. This suggests that our vehicular rogue AP detection will be more suitable for interstate highways which have less physical obstacles, and less so for dense urban areas. unfortunately, due to safety concerns, we were unable to conduct experiments in highway environments.

VII. Conclusion

The ease of setting up a successful rogue AP in vehicular makes this form of wireless attack a particularly serious security problem in vehicular networks. In this paper, we are the first to demonstrate the feasibility of this type of rogue APs, and present a practical defending schemes to prevent the users to connect to vehicular rogues. We implement our approach on commercially available hardware, and perform extensive real world experiments to evaluate our solutions.

Acknowledgment

The authors would like to thank all the reviewers for their helpful comments. This project was supported in part by US National Science Foundation grants CNS-0831904, and CAREER Award CNS-0747108.

References

[1] Google Mountain View. [Online]. Available: http://wifi.google.com

[2] V. Bychkovsky, B. Hull, A. K. Miu, H. Balakrishnan, and S. Madden, "A Measurement Study of Vehicular Internet Access Using In Situ Wi-Fi Networks," in *12th ACM MOBICOM Conf.*, Los Angeles, CA, September 2006.

[3] J. Ott and D. Kutscher, "Drive-thru internet: Ieee 802.11b for "automobile" users," in *INFOCOM*, 2004.

[4] H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu, "A measurement based rogue AP detection scheme," in *The 28th IEEE International Conference on Computer Communications*, Rio de Janeiro, Brazil, 2009.

[5] L. Ma, A. Y. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity Wi-Fi networks," in *Infocom 2008.*

[6] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs," in *IMC 2007.*

[7] W. Wei, S. Jaiswal, J. F. Kurose, and D. F. Towsley, "Identifying 802.11 traffic from passive measurements using iterative bayesian inference," in *INFOCOM*, 2006.

[8] A. Venkataraman and R. Beyah, "Rogue access point detection using innate characteristics of the 802.11 mac," in *SecureComm 2009.*

[9] H. Yin, G. Chen, and J. Wang, "Detecting protected layer-3 rogue APs," in *Broadnets 2007.*

[10] A. Adya, P. Bahl, R. Chandra, and L. Qiu, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," in *Mobicom 2004.*

[11] L. Watkins, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," in *Globecom 2007.*

[12] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue access point detection using temporal traffic characteristics," in *Globecom 2004.*

[13] 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 *MobiSys 2006.*

[14] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics," in *Milcom 2007.*

[15] A. Giannoulis, M. Fiore, and E. W. Knightly, "Supporting vehicular mobility in urban multi-hop wireless networks," in *MobiSys*, 2008.

[16] Air defence. [Online]. Available: www.airdefence.net

[17] Air magnet. [Online]. Available: www.airmagnet.com

[18] Air wave. [Online]. Available: www.airwave.com

[19] S. Jana and S. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *Mobicom 2008.*

[20] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell., "Detecting 802.11 MAC layer spoofing using received signal strength," in *Infocom 2008.*

[21] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Mobicom 2008.*

[22] D. Vassis, G. Kormentzas, A. N. Rouskas, and I. Maglogiannis, "The ieee 802.11g standard fo high data rate wlans," *IEEE Network*, vol. 19, no. 3, pp. 21–26, 2005.

[23] M. Neufeld, J. Fifield, C. Doerr, and A. S. andDirk Grunwald, "Softmac - flexible wireless research platform," in *HotNets-IV*, 2005.

[24] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2004.

[25] J. Turkka and M. Renfors, "Path loss measurements for a non-line-of-sight mobile-to-mobile environment," in *ITST*, 2008.

[26] J. Yee and H. Pezeshki-Esfahani, "Understanding wireless lan performance trade-offs," *Communication Systems design*, pp. 32–35, 2002.

[27] G. Judd, X. Wang, and P. Steenkiste, "Efficient channel-aware rate adaptation in dynamic environments," in *MobiSys*, 2008.

[28] Libpcap. [Online]. Available: http://www.tcpdump.org/