Wardriving - Building A Yagi Pringles Antenna

Spyridon Antakis Mark van Cuijk Joël Stemmer

13 October 2008

Abstract

Wireless networks bring mobility to the business user and consumer and introduce networking on places where networking couldn't be brought before. With the current mass usage of wireless networking the hardware prices are lowering and the bandwidth is raising. The scanning and logging of these networks is called wardriving. Some locations might be impossible to get at without the adversary attracting unnecessary attention. By using a better antenna than the ones used in standard Wi-Fi hardware, the problem could be avoided. In this paper we describe a custom directional antenna, made using basic everyday parts and a Pringles can. Experiments will be performed to compare the antenna with a regular Wi-Fi equipped laptop in signal quality and reception range.

1 Introduction

The first operational wireless network was ALOHAnet [9], developed at the University of Hawaii and deployed in 1970 throughout the US state of Hawaii. In the decades that followed, several new technologies were developed, leading to the First IEEE Workshop on Wireless LANs [4] where the process started that would eventually lead to the IEEE 802.11 standards set [2], that specifies communication for wireless LANs from the physical layer, up to encryption and authentication standards for security.

Since the start of the twenty-first century, most sold notebooks include hardware to communicate with wireless networks using one or several of the IEEE 802.11 standards, broadband internet connection providers distribute modems with built-in wireless networking capabilities and this lead to a mass adoption of the technology. Most of these networks are connected to the internet and carry sensitive information, such as internet banking transactions, personal photographs and private email.

To provide confidentiality to the transmission channel, the original IEEE 802.11 standard, dating 1999, included the Wired Equivalent Privacy (WEP) algorithm. Because several serious weaknesses were identified in 2001 [5] and with the introduction of Wi-Fi Protected Access (WPA) as part of the IEEE 802.11i [8], WEP is now considered deprecated. For authentication purposes, the Extensible Authentication Protocol (EAP) [6] has been adopted, which had previously been used in point-to-point topologies, like phone lines.

Despite the availability of several security-enhancing technologies, a large share of the deployed wireless networks are badly secured or not secured at all. Consumers are often not aware of the security implications or do not have the required knowledge to determine what steps must be taken to secure a wireless network. Wireless devices are often left in their factory default settings (using default passwords) or with WEP and WPA completely turned off.

1.1 Wardriving

Wardriving is literally driving around scanning for wireless networks using a portable computer or PDA. Variations on the name exist, like warbiking and warwalking. In this paper we will use wardriving as a collective name for all these activities. Despite the part "war" is included in the name, wardriving has nothing to do with warfare. The name was derived from the term wardialing, the technique of calling a list of consecutive phone numbers to find modems and fax machines.

In wardriving, the only intent is to scan the availability of wireless networks and collect various security-related information of these networks. An entirely different activity is the one of actually connecting to unprotected wireless networks or breaking into protected networks to gain access to the internet, possibly for malicious purposes like sending large amounts of spam email or downloading excessive amounts of data. In the wardriving community it is considered unethical to actually connect to a wireless network without permission of the owner. The Stumbler Code of Ethics [11] that proposes "a collection of suggestions for safe, ethical, and legal

stumbling" is often referenced in discussion boards on the topic.

2 Problem statement

In this paper we will research how we can improve the reception of Wi-Fi signals by building an external, directional antenna. The reasons of using an external antenna are: a) improving signal quality and b) increasing the scanning distance. This allows you to scan a larger area while wardriving and gives you the ability to connect to networks otherwise unreachable. The Wi-Fi antenna will be constructed using basic parts available in most (web)shops related to computer equipment and electronics and a Pringles[1] can. We will then perform several experiments to compare the performance of this external antenna to a regular Wi-Fi equipped laptop in terms of signal quality and reception range.

The following research questions will be answered in this paper:

1. How do you build a simple directional antenna, suitable for reception of Wi-Fi signals?

2. How does this antenna perform compared to an antenna in a standard Wi-Fi capable laptop when scanning for networks?

3. Is a larger communication distance possible with a directional antenna at only one end?

To answer the first question, section 3 will give a basic introduction into Signal Theory to understand the workings of the antenna and explains the steps necessary to build the antenna. For the other two questions, section 4 will give an outline of the experiments we have performed. The results of these experiments are provided in section 5, followed by the conclusion in section 6.

3 Building an antenna

3.1 Antenna types

Antennas generally fall into one of the following two categories: omni-directional and directional. Although there are many different antennas, most of them are variations of these two basic types. Presenting all the different varieties of antennas is something out of the scope of this paper, we will therefore only introduce the basic antenna types.

[1]Pringles are a type of potato chips and are packaged in a cylinder-shaped can with a foil-coated interior.

Omni-directional antennas (omnis) radiate a pattern in all directions. Omnis are useful in large open areas where without any significant obstructions. Depending on the gain, most omnis are just black or white sticks in varying lengths. Others look somewhat like smoke detectors or small, flattened hockey pucks. In general, a low gain omni will have a relatively small coverage area, but it will be very broad vertically. In comparison high gain omnis radiate a signal further in a more narrow form.

Directional antennas exist in many varieties, such as Yagi, Sector Patch Panel and Parabolic [12]. Although these are all directional antennas, an important difference exists concerning the coverage patterns.

3.1.1 Yagi antennas

Yagi antennas are the most well known. The Yagi looks a lot like an older television antenna. Most common Yagi antennas for 2.4 GHz — the band where 802.11(b/g) signals are emitted — look like a long cylinder. The cylinder is just a weatherproof cover. Yagi antennas work by focusing signals in one direction like a mirror behind a light bulb. The higher the gain of the antenna, the narrower the radiated signal will be. In many cases a Yagi antenna may be able to cover up to 4 or more kilometers when used at both ends.

3.2 Signal theory for a Yagi antenna

We are using the following basic definitions in our calculations:

Frequency is a measure of the number of occurrences of a repeating event per unit time. Denoted as f (Hz).

Speed of light is the speed of all electromagnetic radiation, including visible light, in free space. Denoted as c, equals to 3×10^8 (m/s).

Wavelength is the distance between repeating units of a propagating wave of a given frequency. Denoted as λ, $\lambda = \frac{c}{f}$ (Hz).

3.2.1 Calculations

Considering the signal theory, equation 1 calculates the wavelength at the lowest end and equation 2 the wavelength at the highest end of the frequency range for Wi-Fi signals (2.412 GHz channel 1 to 2.472 GHz channel 13).

$$\lambda_{min} = \frac{c}{f_{min}} = \frac{3.000 \times 10^8}{2.412 \times 10^9} = 12.78 \text{ cm} \quad (1)$$

$$\lambda_{max} = \frac{c}{f_{max}} = \frac{3.000 \times 10^8}{2.472 \times 10^9} = 12.14 \text{ cm} \quad (2)$$

The size of the pipe, which is part of the collector, should be between 12.14 cm and 12.78 cm. In practice, the actual size of the pipe would be about 14.2 cm, because we will have also to include the lengths of the nuts at both ends. [7] [1]

3.3 Building a Yagi Pringles antenna

3.3.1 Components Used

- A Pringles can with a length of 25.5 cm and a diameter of 7 cm.
- A metallic pipe
- Ten nuts and five washers
- Two Pringles lids
- A low signal loss coax cable (an LMR 400 with N-type male connector to RPSMA male connector)
- A Flens N-type female connector
- A solid 12-gauge pin

Note: There are many different ways to build a Yagi antenna, you can use different components (Wi-Fi card, connectors, cables, can). However, the theoretical part will always be the same, only the calculations are going to change a bit. [10]

3.3.2 Combining the components

Step 1: The collector This is the most important part of the antenna. Here we apply the measurements based on the signal theory calculations in section 3.2.1. We take the 14.2 cm pipe, the 5 washers, the 10 nuts and the 2 Pringles can lids. A hole is pierced in the center of both can lids, big enough for the all-thread to pass through. The outer ridge of one can lid is trimmed off to fit inside the can. Finally we assemble the pipe. The pipe is a sandwich that goes on the all-thread as can be seen in Figure 1. The washers are fixed in the chosen distance $3.035 \leq \frac{\lambda}{4} \leq 3.195$ cm.

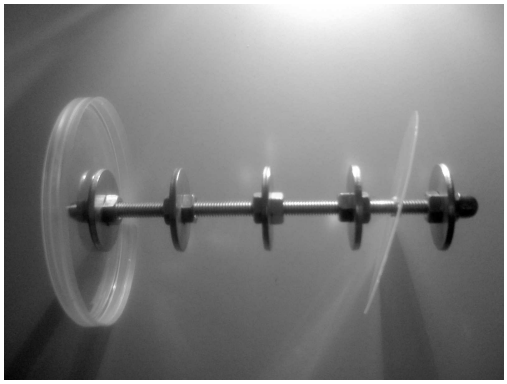

Figure 1: The collector

Step 2: Attaching the pin We solder the 12-gauge pin onto the Flens N-type female connector. Based on the Pringles can diameter (7 cm), the ideal length of this pin is about 2.7 cm [7]. It is always just shy of the middle of the can you are using.

Step 3: Building the antenna We make a hole about 8.6 cm (length based on testing performance [7]) from the bottom to the top of the can. We then insert and stabilize the N-type female connector with the attached solid pin in that hole and place it next to the collector. The Yagi Pringle antenna is connected to the Wi-Fi card using the LMR 400 cable. The completely assembled antenna is shown in Figure 2.

Figure 2: The Yagi Pringles antenna

4 Experiments

After building the antenna, there are a lot of interesting experiments that can be performed with it. We picked two basic experiments that allow us to tell something about the performance of the antenna. The first experiment is a passive one; we shall only receive signals to detect what wireless

networks can be received. The same will be done using standard Wi-Fi equipment in a notebook to create a comparison. In the second experiment we shall create a connection to another wireless device get a hint on the maximum distance that still allows communication.

4.1 Hardware and software

Notebook A: The first notebook is an Acer Aspire 1500LMi, which includes a Broadcom Corporation BCM4306 802.11b/g Wireless LAN Controller (rev 03). This notebook runs a Linux 2.6.25-2-amd64 SMP kernel with the b43 driver module loaded. The BCM4306 is loaded with firmware version 410.2160.

Notebook B: The second notebook is a MacBook 4.1, with a Zydas USB Wireless LAN Controller attached to the USB bus. The notebook runs a Linux 2.6.24-19-i686 SMP kernel with the zd1211b driver module loaded. The device is loaded with firmware version 4725.

Access Point: A Thomson SpeedTouch 580 ADSL modem, with built-in wireless access point is used as the base station in the second experiment. This device was supplied for free with an ADSL subscription with a large national provider in The Netherlands.

Software: Kismet is a well known 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. It will work with any wireless card which supports raw monitoring (rfmon) mode. Kismet identifies networks by passively collecting packets, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic. [3]

4.2 Experiment A

To compare the reception performance of our antenna with standard Wi-Fi equipment, we will use two notebooks and perform a passive scan with both of them at the same time. Two notebooks are positioned next to each other and use Kismet to process the received packets. Our main goal is to actually compare and spot the differences between the scanning results of our Yagi Pringles antenna and a common notebook antenna. The intention is to focus mostly on a possible difference in the sensitivity and the detection performance that these two antennas are going to give us in a real life situation.

Both notebooks will be placed on a table in the Auditorium of the Technical University of Eindhoven (TU/e). At start, the directional antenna will be placed in a fixed position. After setting this up, Kismet will be started on both notebooks at the same time and the program will be instructed to sort the available network by SSID. After this, the notebooks and the antenna will not be touched for a period of two minutes to allow them to capture enough packets. After two minutes, the full list of networks is noted and for all networks that appear on both notebooks, the signal strength will be noted. After the information is noted, Kismet will be closed on both notebooks. The directional antenna will be rotated 120 degrees and the experiment will be repeated.

4.3 Experiment B

Ethics prohibit a wardriver to actually connect to a wireless network, but a criminal might have different intentions after finding an interesting network. To use the network without attracting any attention, he might want to connect to it from a larger distance than regular Wi-Fi equipment is capable of. In this experiment, we will try to determine what the maximum distance between a regular wireless access point and a notebook with the Yagi Pringles antenna is. For the sake of simplicity, encryption is disabled on the SpeedTouch access point and it is configured to accept connections from any client. Notebook B will be used in this experiment.

The devices are placed next to each other and a wireless network connection is setup to verify the devices are compatible. After this has been verified, the SpeedTouch device is placed at the eleventh floor of the staircase in the main building of the TU/e. The notebook is moved just outside of the building and the antenna is pointed towards the SpeedTouch to verify connection is still possible, given the thick layer of glass in between. Now, the notebook is moved to the top of the Twinning Center, which is located approximately 800 meters from the main building, where again a connection will be created.

The outcome of this test will determine how the experiment will continue. If no connection is created, the notebook will be moved closer to the main building to find the point where a connection is possible. Otherwise, the notebook and Yagi Pringles antenna will be placed in a car and will drive the

J.F. Kennedylaan, away from the TU/e campus. We will continue until a point is found where no signal from the TU/e wireless network is received.

5 Results

5.1 Experiment A

The first thing to notice after starting up Kismet, is that notebook B detects 10 to 20 new networks every second, without being able to detect the SSID of these networks. The packet count of all these networks stay at exactly 1. We assume that they are the result of distant networks, that are too far away to interact together with standard equipment, but that get mixed and received by the Yagi antenna. Kismet is known to process packets that are almost valid 802.11 packets. We decided to sort the results by reversed packet count, to push these bogus results down and ignore them during the scanning.

Notebook A picked up 16 different wireless networks, all of which belonged to the TU/e. Many of these networks shared the same SSID, but were uniquely identifiable through their MAC address. Table 1 lists all the different SSIDs that were found. Each of these SSID had four different access points and we noticed that in all cases the last digit of their MAC address corresponded with the id in the table. Notebook B only picked up 12 different wireless network, all of which were also detected by notebook A. The four networks that were not detected by the Pringles antenna were always the same (*tue-wpa2*). We suspect the reason for not detecting those four networks are because of limitations in the drivers, but this has not been verified. We were unable to connect to any of the available wireless network because the drivers of the Wi-Fi card in notebook B did not support the necessary security protocols. These drivers were also unable to report the signal quality of the detected networks.

id	SSID
0	eduroam
1	guest
2	tue
3	tue-wpa2

Table 1: The SSIDs detected in experiment A

5.2 Experiment B

The first part of the experiment was conducted on September 26th, 2008 between 9:00 AM and 10:00 AM. The SpeedTouch device is setup and placed in the main building of the TU/e as described in section 4.3. The notebook is moved to the parking lot next to the W-hoog building, where the antenna is directed at the staircase of the main building. Kismet detects the signal and the GUI allows us to establish a connection. After this, we moved the notebook to the top of the Twinning Center and again directed the antenna to the main building. Again the signal is picked up by Kismet. Establishing the connection using the GUI took longer than normally, but it succeeded. To test the connection, we opened up the configuration webpage of the SpeedTouch device. We succeeded in loading the page, although at a much lower speed than in normal conditions.

An interesting thing we noticed on top of the Twinning Center is that Kismet detected packets with SSID *stadhuisplein*. Assuming this network is located at the Stadhuisplein in Eindhoven, the approximate distance those packets traveled is an exciting two kilometers.

The follow-up experiment was conducted on the same day between 3:30 PM and 4:30 PM. The notebook and antenna were placed in a car. During the ride, the antenna was directed towards the TU/e campus. We left the TU/e campus using the exit at the J.F. Kennedylaan. At this point, Kismet showed the *tue* SSID in the results. When driving away from the campus, the network disappeared very soon. Because of this, we decided to stop at the first bridge over the J.F. Kennedylaan (Viaduct Orpheuslaan) and perform the test outside. The *tue* network shows up on Kismet again.

After this, we moved on to the next bridge (Viaduct Sterrenlaan) and performed the same test, but the *tue* SSID did not show up anymore. From this bridge, we had a line-of-sight towards the Vertigo building on the campus, but the rest of the campus was invisible because of trees. About 300 meters east of the bridge is a building of the ROC. We requested access to the highest window with view to the TU/e campus to perform the test with a better line-of-sight. From this position the *tue* SSID did not show up either.

Afterwards we looked up the exact positions where we stopped. The Viaduct Orpheuslaan is approximately 1000 meters from the campus. The Viaduct Sterrenlaan and the ROC building are approximately 2300 meters from the campus.

6 Conclusions

We have shown how to build a Yagi antenna with some basic parts and a Pringles can. Assuming you already own a wireless network card, the total

cost to build this antenna will be about 20 euros, depending on the type of cable used. This is very reasonable considering the results we were able to achieve.

The first experiment was designed to test if the Pringles antenna was able to pick up Wi-Fi signals. The results indicate the Pringles antenna was able to successfully detect most networks, but it did uncover a problem we had not anticipated. The antenna picked up a lot of noise and interfering signals. These were incorrectly registered as new networks and flooded the list of valid networks. We have not been able to determine if this is a software problem only affecting Kismet or if it is a result of the increased sensitivity of the new antenna. Because of a limitation in the hardware drivers we were unable to determine the signal quality of these networks.

In the second experiment we were able to detect a network about 800 meters away. Using an unencrypted access point we were also able to successfully establish a connection. Even though there was an unobstructed line-of-sight view between the access point and the antenna, the signal quality was poor which resulted in a significant loss of bandwidth. Based on these results we continued experimenting to find the maximum distance achievable. Our antenna was able to detect wireless networks up to about one kilometer. During these experiments we observed some strange behaviour. The best results were sometimes achieved by slightly pointing the antenna away from the intended target. This could be explained by the fact that we did not have the proper equipment and environment to calibrate the antenna.

7 Future work

A controlled testing environment is necessary to properly calibrate the antenna and perform experiments. This controlled environment should block any sources of interference. It can then be used to test various configurations of the antenna. The effects of using cans with different lengths and diameters can be measured. It will be interesting to see the differences in using other amounts of washers, with various sizes, spread differently on the collector. The exact placement of the pin inside the can could also influence the reception and should be tested. This will result in a design with carefully chosen components, assembled and calibrated for maximum performance.

To reach more reliable results, identical hardware and software will also be required. In our experiments we compared the results acquired with laptops using different hardware configurations and software versions. To address the issue of detection of invalid wireless networks, multiple software packages should also be considered.

Once these problems have been dealt with, several other interesting ideas can be further explored. Stepping away from the strictly wardriving point of view, actual connection tests can be performed. What is the amount of packet loss and the available bandwidth, and how exactly does increasing the distance affect it. A point-to-point link could be set up. One where both parties are using an external directional antenna. What will this mean for the overall signal quality and what kind of distances can we expect to reach?

References

[1] *Build your own wireless signal booster with pringles*, [Online; accessed 26-September-2008] `http://www.truveo.com/Build-Your-Own-Wireless-Signal-Booster-with/id/3600436257`.

[2] *Ieee 802.11, the working group setting the standards for wireless lans*, [Online; accessed 25-September-2008] `http://www.ieee802.org/11/index.shtml`.

[3] *Kismet, a wireless network scan tool*, [Online; accessed 30-September-2008] `http://www.kismetwireless.net/`.

[4] *The first ieee workshop on wireless lans*, 1991, [Online; accessed 24-September-2008] `http://www.cwins.wpi.edu/wlans91`.

[5] Nikita Borisov, Ian Goldberg, and David Wagner, *Intercepting mobile communications: the insecurity of 802.11*, MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking (New York, NY, USA), ACM, 2001, pp. 180–189.

[6] B. Aboba et al., *Extensible authentication protocol (eap) key management framework*, [Online; accessed 24-September-2008] `http://tools.ietf.org/html/rfc5247`.

[7] Rob Flickenger, *Antenna on the cheap (er, chip)*, [Online; accessed 28-September-2008] `http://www.oreillynet.com/cs/weblog/view/wlg/448`.

[8] Sheila Frankel, Bemard Eydt, Les Owens, and Karen Scarfone, *Establishing wireless robust security networks: A guide to ieee 802.11i*, Tech. Report SP 800-97, National Institute

of Standards and Technology, February 2007, [Online; accessed 25-September-2008] http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf.

[9] F. F. Kuo, *The aloha system*, SIGCOMM Comput. Commun. Rev. **25** (1995), no. 1, 41–44.

[10] Gregory Rehm, *How to build a tin can waveguide wifi antenna*, [Online; accessed 27-September-2008] http://www.turnpoint.net/wireless/cantennahowto.html.

[11] Renderman, *Stumbler code of ethics v0.2*, [Online; accessed 26-September-2008] http://www.renderlab.net/projects/wardrive/ethics.html.

[12] Terry Schmidt and Ben Serebin, *Antennas 101; basic antenna concepts for 802.11*, [Online; accessed 12-October-2008] http://poitiers.sansfil.free.fr/doc/Antennas101.pdf.