

**Masters Project Final Report December 2015**

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Title** | Privacy and Security Implications on Wireless (Wi-Fi) Tomography | | |
| **Student Name** | J R O Sirimanne | | |
| **Registration No. & Index No.** | 2013/MIS/021  13 | | |
| **Supervisor’s Name** | Dr. Chamath Keppitiyagama | | |
| **Please Circle the appropriate** | **Masters Program** | **Type** | |
| **MIS** | **Research** | **Implementation** |
| **For Office Use Only** | | | |
|  | | | |

**Privacy and Security Implications on Wireless (Wi-Fi) Tomography**

**J R O Sirimanne**

**2015**



**Privacy and Security Implications on Wireless (Wi-Fi) Tomography**

**A dissertation submitted for the Degree of Master of  
Science in Information Security**

**J R O Sirimanne**

**University of Colombo School of Computing  
2015**



**Declaration**

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Students Name: J R O Sirimanne

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: Date:

This is to certify that this thesis is based on the work of Mr. J R O Sirimanne under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name: Dr. Chamath Keppitiyagama

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: Date:

Abstract

This research is aimed to be a proof of concept for a Privacy and Security Implications on Wireless (Wi-Fi) Tomography. Wi-Fi is a popular wireless networking technology used today which uses radio waves to transmit data. For this research Radio tomographic imaging (RTI) technologies are used to prove that the privacy can be breached just by analyzing the wireless signals receive signal strength indicator (RSSi) value. This analysis can be done by anyone who has a simple wireless card that shows the RSSi value. Hence one’s privacy can be breached even without him knowing his movements are being analyzed by an outsider.

In this I have used statistical methodologies and probability analysis to prove that there is a significant difference in RSSi when a human is obstructing the wireless signal and that difference is clearly visible in the gathered data set. By using probability we can predict the position of a person inside a room.

Acknowledgement

Firstly, I would like to express my sincere gratitude to my advisor Dr. Chamath Keppitiyagama for the continuous support for my research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis.

Secondly I would like to express my appreciations to Mr.Asanka Sayakkara who provided the necessary scripts to gather data and his continued guidance for analysis of gathered data and also for the support given to me to complete this thesis.

I would like to express a special thanks to all the staff members of the Network Operating Center of University Of Colombo School Of Computing for their immense support on providing the technical support and required hardware to make this research a success.

Beside those my heartiest appreciation should go to all the lecturers, assistant lecturers, demonstrators and other staff members in the University Of Colombo School Of Computing who sincerely helped me in numerous ways.

Table of Contents

[Table of Figures ix](#_Toc439266477)

[1. Introduction 1](#_Toc439266478)

[1.1 Definitions 1](#_Toc439266479)

[1.1.1 Decibel 1](#_Toc439266480)

[1.1.2 Received Signal Strength Indicator (RSSI) 2](#_Toc439266481)

[1.1.3 Privacy 2](#_Toc439266482)

[1.2 Technologies 3](#_Toc439266483)

[1.2.1 Wi-Fi 3](#_Toc439266484)

[1.2.2 Radio Tomographic Imaging 3](#_Toc439266485)

[1.3 Hardware Devices 4](#_Toc439266486)

[1.3.1 Wireless access point 5](#_Toc439266487)

[1.3.2 Signal Strength Capturing device 6](#_Toc439266488)

[1.4 Motivation 6](#_Toc439266489)

[1.5 Aims and Objectives 7](#_Toc439266490)

[1.6 Research Question 7](#_Toc439266491)

[2 Literature Survey 8](#_Toc439266492)

[3 Design 9](#_Toc439266493)

[3.1 Scenarios 9](#_Toc439266494)

[3.2 Scenario Diagrams 9](#_Toc439266495)

[References 14](#_Toc439266496)

[Appendix A 16](#_Toc439266497)

[Data Gathering Code 16](#_Toc439266498)

[Appendix B 18](#_Toc439266499)

[Gathered Data 18](#_Toc439266500)

# Table of Figures

[Figure 1- Wi-Fi logo 8](file:///C:\Users\jithendra\Documents\research\thisi_jithendra.docx#_Toc431970738)

[Figure 2 - An illustration of an RTI network. Each node broadcasts to the others, creating many projections that can be used to reconstruct an image of objects inside the network area. [2] 9](#_Toc431970739)

[Figure 3- Wireless Access point Simplest usage 10](file:///C:\Users\jithendra\Documents\research\thisi_jithendra.docx#_Toc431970740)

[Figure 4 - DSL-2750U Wireless N ADSL2+ Wi-Fi Router 10](file:///C:\Users\jithendra\Documents\research\thisi_jithendra.docx#_Toc431970741)

[Figure 5 - Dell 14R n4010 General Purpose laptop 11](file:///C:\Users\jithendra\Documents\research\thisi_jithendra.docx#_Toc431970742)

[Figure 6 - Dell Wireless DW1501 Mini Card 11](file:///C:\Users\jithendra\Documents\research\thisi_jithendra.docx#_Toc431970743)

List of Abbreviations

|  |  |
| --- | --- |
| RSSI | Receive signal strength indicator |
| RTI | Radio tomographic imaging |
| MAC | Media access control |
| dBm | decibel-milliwatt |
| WLAN | wireless local area network |
|  |  |
|  |  |

Chapter 1

# Introduction

At present day Wi-Fi is the popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. Wi-Fi connections support millions of people in homes, businesses, and public locations around the world supporting them to be connected at every possible time. According to statistics there is a huge growth in Wi-Fi enabled devices and Wi-Fi hotspots within past few years and it is expected to grow more and more. There is a possibility to track people movements by observing just the signal strength of these Wi-Fi networks.

## Definitions

Definitions section describes the meanings of terms used in this document.

## Decibel

The decibel (dB) is a logarithmic unit that expresses the ratio of two values of a physical quantity, often power or intensity. One of these quantities is often a reference value and in this case the decibel expresses the absolute level of the physical quantity. The number of decibels is ten times the logarithm to base 10 of the ratio of two power quantities or of the ratio of the squares of two field amplitude quantities. One decibel is one tenth of one bel, named in honor of Alexander Graham Bell; however, the bel is seldom used. The definition of the decibel is based on the measurement of power in telephony of the early 20th century in the Bell System in the United States. Today, the unit is used for a wide variety of measurements in science and engineering, most prominently in acoustics, electronics, and control theory. In electronics, the gains of amplifiers, attenuation of signals, and signal-to-noise ratios are often expressed in decibels. The decibel confers a number of advantages, such as the ability to conveniently represent very large or small numbers, and the ability to carry out multiplication of ratios by simple addition and subtraction. By contrast, use of the decibel complicates operations of addition and subtraction. [7]

## Received Signal Strength Indicator (RSSI)

In telecommunications, received signal strength indicator (RSSI) is a measurement of the power present in a received radio signal. RSSI is usually invisible to a user of a receiving device. However, because signal strength can vary greatly and impact functionality in wireless networking, IEEE 802.11 devices often make the measure available to users. In an IEEE 802.11 system, RSSI is the relative received signal strength in a wireless environment, in arbitrary units. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.

There is no standardized relationship of any particular physical parameter to the RSSI reading. The 802.11 standard does not define any relationship between RSSI value and power level in mW or dBm. Vendors and chipset makers provide their own accuracy, granularity, and range for the actual power (measured as mW or dBm) and their range of RSSI values (from 0 to RSSI\_Max). One subtlety of the 802.11 RSSI metric comes from how it is sampled, RSSI is acquired during only the preamble stage of receiving an 802.11 frame, not over the full frame. [10]

## Privacy

Privacy has many meanings. The most general is freedom from interference or intrusion, the right "to be let alone," a formulation cited by Louis Brandeis and Samuel Warren in their groundbreaking 1890 paper on privacy. [4] This recognizes that each person has a sphere of existence and activity that properly belongs to that individual alone, where he or she should be free of constraint, coercion, and even uninvited observation. As we would say today, each of us needs our own "space." Most would recognize the protected sphere to include personal opinions, personal communications, and how one behaves behind closed doors, at least as long as these do not lead to any significant threats to society. Many would also include behavior within the family and other intimate relationships in that sphere. [3]

## Technologies

Technology sections describe the technologies used for this study.

## Wi-Fi

Wi-Fi (or WiFi) is a local area wireless computer networking technology that allows electronic devices to network, mainly using the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF ISM radio bands. [5] Wi-Fi standards are defined by IEEE 802.11 standard. IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the market place, each revision tends to become its own standard. [6]



Figure - Wi-Fi logo

*(Source: https://upload.wikimedia.org/wikipedia/commons/thumb/3/32/Wi-Fi\_Logo.svg/2000px-Wi-Fi\_Logo.svg.png)*

## Radio Tomographic Imaging

Tomography refers to imaging by sections or sectioning, through the use of any kind of penetrating wave. Radio tomographic imaging (RTI) is an emerging application which offers a new way to image passive objects in buildings and outdoor environments using received signal strength indicator (RSSI). [1]



Figure - An illustration of an RTI network. Each node broadcasts to the others, creating many projections that can be used to reconstruct an image of objects inside the network area. [2]

*(Source: http://span.ece.utah.edu/uploads/RTINetwork.png)*

## Hardware Devices

For this study an ordinary wireless access point and a Laptop with wireless (Wi-Fi) interface that is capable of publishing signal strengths in decibel (dB) values will be used as hardware devices. By this I’m trying to generalize this study and match it maximum to a real world scenario.

## Wireless access point

In computer networking, a wireless access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself. [8].

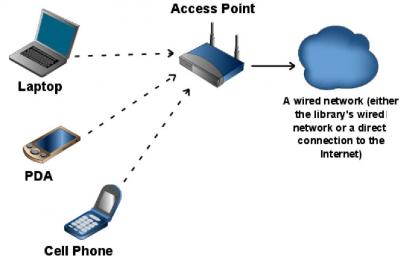


Figure - Wireless Access point Simplest usage

*(Source: http://www.techsoupforlibraries.org/files/images/wireless\_network.img\_assist\_custom.jpg)*

For this study I used a D-Link Wireless N300 ADSL Modem Router (Model Number DSL-2750U) which is a very common wireless access point used in Sri Lanka. The DSL-2750U Wireless N ADSL2+ Wi-Fi Router connects a group of users to the Internet, allowing multiple computers at home or the office to share an integrated high-speed ADSL2/2+ interface. It provides high-performance 802.11n wireless access for wireless networked computers, 4 built-in Ethernet ports, firewall protection, and QoS for smooth and secure download/upload of photos, files, music, video, and e-mail over the Internet. [9]



Figure - DSL-2750U Wireless N ADSL2+ Wi-Fi Router

*(Source: http://115.124.123.225/new/products/DSL-2750u/DSL-2750u.png)*

## Signal Strength Capturing device

Captured received signal strength indicator (RSSI) values are the main input data for this study. As mentioned earlier [10] hardware manufacturers are not oblige to provide RSSI value. So when we choose a computer/laptop to capture the RSSI values the wireless card should advertise the RSSI value. Here for the data capturing we have used a general purpose Dell Laptop (model no: Dell Inspiron 14R (N4010) Laptop) with DW1501 Wireless-N Wlan Half-Mini Card which is again a very common device in Sri Lanka market. This wireless card supports IEEE 802.11b/g/n single band mode in 2.4GHz mode. [12]



Figure - Dell 14R n4010 General Purpose laptop

(*http://1.bp.blogspot.com/-jPEiZYrgbc8/VAx1\_-yiOtI/AAAAAAAAAF0/DGvRA2iAIRw/s1600/dell-inspiron-14r-disassembly.png*)



Figure - Dell Wireless DW1501 Mini Card

(*Source: http://www.wireless-driver.com/wp-content/uploads/2011/11/DellWireless1501802.11bgMiniCard.jpg*)

## Motivation

There are many security implementations to preserve privacy of a person when connected and using the network. Research shows when an object moves inside a wireless area that objects causes the received signal strength indicator (RSSI) to be dropped. By tracking these drops we can map the path and movements of the object. Apart from providing internet and network access Wi-Fi is used in sensor networks to transfer data gathered from sensors. These sensor networks power and enable modern concepts like smart homes, smart power, smart cities, Internet of things etc. With all these usage of Wi-Fi increases rapidly and in a small area there can be many Wi-Fi networks. Issue with this is by using wireless tomography technologies we can track movements of people unknowing to them that someone is tracking them.

Currently there are no security implementations to safeguard people for above type of privacy breaches and many are unaware about the security issues related to available tomographic techniques.

## Aims and Objectives

Wireless internet is a very common method of providing Internet and networking facilities to people and devices. With such common used technology it should be safe to use. In this research, I will design, test and evaluate diffident real world scenarios of wireless implementations to determine and prove the effects to wireless signal strength when a human is present and find the scenarios that are vulnerable to privacy breaches.

## Research Question

With this study I’m researching to answer two questions that arise with above mentioned problems.

1. Is there a significant amount of wireless signal strength drop when there is a human inside the line of sight of the wireless access point and data gathering computer?
2. How accurately we can identify human presence by observing received signal strength indicator (RSSI) values.

Chapter 2

# Literature Survey

Wi-Fi uses radio waves to create networks and transmit data. Radio waves are electromagnetic waves. Electromagnetic waves have a large range of frequency starting from as low as 3 kHz and ranging up to 300 GHz. From this vast range Wi-Fi uses 2.4GHz band to do the communications. Electromagnetic waves can be affected by many reasons when they are traveling through space.

* Signal Frequency
* Transmission medium
* Objects encountered

These reasons will result in reflection (the wave partially bounces of an object), refraction (change of direction when passing from one medium to another), absorption (loss of energy when an object is hit), diffraction (when waves are bend and spread around an obstacle), scattering (wave bounces off in multiple directions) and polarization (orientation of the oscillations of the waves can change upon interaction) of the signal.

Chapter 3

# Design

In the design stage, scenarios are developed to answer research questions and test them.

## Scenarios

In the initial design face primary scenarios are developed to answer first research question(Is there a significant amount of wireless signal strength drop when there is a human inside the line of sight of the wireless access point and data gathering computer?).

For initial scenarios there are three variables

1. Data gathering computer
2. Wireless access point
3. Person

## Scenario Diagrams

In these diagrams we have used symbols to represent objects below table describes the symbols.

|  |  |
| --- | --- |
| Symbol | Resemblance |
|  | Wireless access point |
|  | Data gathering computer |
|  | Human |

Table - Symbols and resemblance

Scenario 1

Scenario 2

Scenario 3

Scenario 4

Scenario 5

Scenario 6

Scenario 7

Scenario 8

Scenario 9

Scenario 10

Scenario 11

Scenario 12

Scenario 13

Scenario 14

Scenario 15

Scenario 16

Chapter 4

Testing

Scenario 12.1

Scenario 12.2

Scenario 12.3

To be continued

Chapter 5

Evaluation

To be continued.

Chapter 6

Conclusion and Future Work

To be continued

# References

[1] University of Utah. (2015 October, 01). *Radio Tomographic Imaging* [Online]. Available: http://span.ece.utah.edu/radio-tomographic-imaging [Accessed 3 Oct. 2015].

[2] J. Wilson and N. Patwari, “Radio tomographic imaging with wireless networks,” IEEE Transactions on Mobile Computing, vol. 9, no. 5, pp. 621–632, May 2010. Published, 01/08/2010.

[3] Michael McFarland, SJ. *What is Privacy?* [online] Scu.edu. Available at: http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/what-is-privacy.html [Accessed 3 Oct. 2015].

[4] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, 4 (5), (1890): 193-220, p. 195, citing Judge Cooley in Cooley on Torts, 2nd ed.

[5] Wikipedia, (2015). *Wi-Fi*. [online] Available at: https://en.wikipedia.org/wiki/Wi-Fi [Accessed 5 Oct. 2015].

[6] Wikipedia, (2015). *IEEE 802.11*. [online] Available at: https://en.wikipedia.org/wiki/IEEE\_802.11 [Accessed 5 Oct. 2015].

[7] Wikipedia, (2015). *Decibel*. [online] Available at: https://en.wikipedia.org/wiki/Decibel [Accessed 5 Oct. 2015].

[8] Wikipedia, (2015). *Wireless access point*. [online] Available at: https://en.wikipedia.org/wiki/Wireless\_access\_point [Accessed 5 Oct. 2015].

[9] Dlink.co.in, (2015). *D-Link Wireless N ADSL2+ 4-Port Wi-Fi Router*. [online] Available at: http://www.dlink.co.in/products/?pid=452 [Accessed 5 Oct. 2015].

[10] Wikipedia, (2015). *Received signal strength indication*. [online] Available at: https://en.wikipedia.org/wiki/Received\_signal\_strength\_indication [Accessed 5 Oct. 2015].

[11] En.community.dell.com, (2015). *DW1501 Wireless-N Wlan Half-Mini Card Specifications*. [online] Available at: http://en.community.dell.com/cfs-file/\_\_key/communityserver-discussions-components-files/3324/4338.1501.1.jpg [Accessed 6 Oct. 2015].

[12] Goldsmith, A. (2005). *Wireless communications*. Cambridge: Cambridge University Press.

[13] RADAR: An In-Building RF-based User Location and Tracking System. (2000). [online] Available at: http://research.microsoft.com/en-us/people/padmanab/infocom2000.pdf [Accessed 7 Oct. 2015].

# Appendix A

## Data Gathering Code

import matplotlib.pyplot as plt

import time

import random

from collections import deque

import numpy as np

import os

def read\_wifi():

while True:

f=os.popen('sudo iwconfig wlan0 | grep -e "Signal level"')

line = f.read()

splitted\_line = line.split()

level = splitted\_line[3].split('=')

print level[1]

val = level[1]

yield val

time.sleep(0.1)

a1 = deque([0]\*100)

ax = plt.axes(xlim=(0, 100), ylim=(0, 10))

d = read\_wifi()

line, = plt.plot(a1)

plt.ion()

plt.ylim([-90,0])

plt.show()

for i in range(0,10000):

a1.appendleft(next(d))

datatoplot = a1.pop()

line.set\_ydata(a1)

plt.draw()

print a1[0]

i += 1

time.sleep(0.1)

plt.pause(0.0001)

# Appendix B

## Gathered Data