

# Authentication of Wireless Devices using Radio Frequency Fingerprinting

by

Jeyanthi Hall

A thesis proposal submitted to  
the Faculty of Graduate Studies and Research  
in partial fulfilment of  
the requirements for the degree of  
Doctor of Philosophy

Ottawa-Carleton Institute for Computer Science  
School of Computer Science  
Carleton University  
Ottawa, Ontario

October 2003

© Copyright  
2003, Jeyanthi Hall

The undersigned recommend to  
The Faculty of Graduate Studies and Research  
acceptance of the thesis proposal,

**Authentication of Wireless Devices using Radio Frequency  
Fingerprinting**

submitted by  
**Jeyanthi Hall**

---

Dr.  
(Director, School of Computer Science)

---

Dr. Evangelos Kranakis  
(Thesis Supervisor)

---

Dr. Michel Barbeau  
(Thesis Co-Supervisor)

---

Dr.  
(External Examiner)

Carleton University

October 2003

# Executive Summary

To be completed at the end.

# Contents

<b>I</b>	<b>Current State of Wireless Network Security</b>	<b>1</b>
<b>1</b>	<b>Wireless Network: An Overview</b>	<b>2</b>
1.1	Introduction to Wireless Networks . . . . .	2
1.2	General Threats and Countermeasures . . . . .	2
1.3	Authentication Functions and Protocols . . . . .	2
<b>2</b>	<b>Wireless Network: Wireless Wide Area Network: AMPS/GSM</b>	<b>3</b>
2.1	Attacks and Countermeasures . . . . .	3
2.2	Future Enhancements . . . . .	3
<b>3</b>	<b>Wireless Local Area Network: 802.11b</b>	<b>4</b>
3.1	Attacks and Countermeasures . . . . .	4
3.2	Authentication Protocol . . . . .	4
3.3	Weaknesses in Authentication Protocol . . . . .	4
3.4	Potential Solutions . . . . .	4
3.5	Future Enhancements . . . . .	4
<b>4</b>	<b>Ad-Hoc Network: Bluetooth</b>	<b>5</b>
4.1	Attacks and Countermeasures . . . . .	5
4.2	Authentication Protocol . . . . .	5
4.3	Weaknesses in Authentication Protocol . . . . .	5

4.4	Potential Solutions . . . . .	5
4.5	Future Enhancements . . . . .	5
<b>II</b>	<b>Outstanding Problem with Device Authentication</b>	<b>6</b>
<b>5</b>	<b>Problem to be addressed</b>	<b>7</b>
5.1	Disadvantages of Current Approaches . . . . .	7
5.2	Problem Statement . . . . .	7
5.3	Requirements for Robust Device Authentication . . . . .	7
<b>6</b>	<b>Proposed Solution</b>	<b>8</b>
6.1	Biometrics-based Authentication . . . . .	8
6.2	Use of Radio Frequency Fingerprinting . . . . .	8
<b>III</b>	<b>Device Authentication using Radio Frequency Fingerprinting</b>	<b>9</b>
<b>7</b>	<b>Radio Frequency Fingerprinting</b>	<b>10</b>
7.1	Process . . . . .	10
<b>8</b>	<b>Detection of Start of Transient</b>	<b>11</b>
8.1	Current Approaches . . . . .	11
8.2	New Approach . . . . .	11
8.3	Comparison of Approaches . . . . .	11
8.4	Experimental Platform . . . . .	11
<b>9</b>	<b>Characterization and Classification of Transceiverprint</b>	<b>12</b>
9.1	Objectivehyperlink . . . . .	12
9.2	Methodology . . . . .	12

9.3	Current Approaches . . . . .	12
9.4	Validation . . . . .	12
9.5	Experimental Platform . . . . .	12
<b>10</b>	<b>Implementation of Authentication Protocol</b>	<b>13</b>
10.1	Objectivehyperlink . . . . .	13
10.2	Methodology . . . . .	13
10.3	Validation . . . . .	13
10.4	Experimental Platform . . . . .	13
<b>11</b>	<b>Bibliography</b>	<b>14</b>

# List of Tables

# List of Figures



# List of Algorithms

# Part I

## Current State of Wireless Network Security

# Chapter 1

## Wireless Network: An Overview

### 1.1 Introduction to Wireless Networks

### 1.2 General Threats and Countermeasures

### 1.3 Authentication Functions and Protocols

## Chapter 2

# Wireless Network: Wireless Wide Area Network: AMPS/GSM

### 2.1 Attacks and Countermeasures

### 2.2 Future Enhancements

# Chapter 3

## Wireless Local Area Network: 802.11b

### 3.1 Attacks and Countermeasures

### 3.2 Authentication Protocol

### 3.3 Weaknesses in Authentication Protocol

### 3.4 Potential Solutions

### 3.5 Future Enhancements

# Chapter 4

## Ad-Hoc Network: Bluetooth

### 4.1 Attacks and Countermeasures

### 4.2 Authentication Protocol

### 4.3 Weaknesses in Authentication Protocol

### 4.4 Potential Solutions

### 4.5 Future Enhancements

## Part II

# Outstanding Problem with Device Authentication

# Chapter 5

## Problem to be addressed

### 5.1 Disadvantages of Current Approaches

### 5.2 Problem Statement

### 5.3 Requirements for Robust Device Authentication



# Chapter 6

## Proposed Solution

### 6.1 Biometrics-based Authentication

### 6.2 Use of Radio Frequency Fingerprinting

## Part III

# Device Authentication using Radio Frequency Fingerprinting

## Chapter 7

# Radio Frequency Fingerprinting

### 7.1 Process

# Chapter 8

## Detection of Start of Transient

### 8.1 Current Approaches

### 8.2 New Approach

### 8.3 Comparison of Approaches

### 8.4 Experimental Platform

## Chapter 9

# Characterization and Classification of Transceiverprint

9.1 [Objective](#)

9.2 Methodology

9.3 Current Approaches

9.4 Validation

9.5 Experimental Platform

# Chapter 10

## Implementation of Authentication Protocol

### 10.1 Objectivehyperlink

### 10.2 Methodology

### 10.3 Validation

### 10.4 Experimental Platform

Test for a citation [4] and [3] and [1] and [2] this should do it.

## Chapter 11

## Bibliography

# Bibliography

- [1] Jen Hall. Overview: Wireless LAN Security.  
[http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w\\_ov.html](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.html), 2001.
- [2] Jen Hall, Tom Smith, and Vice Rioy. Title called testing. *Some Journal*, 1998.
- [3] HomeRF Working Group. *A Comparison of Security in HomeRF versus IEEE802.11b*, 2001.
- [4] Wireless Ethernet Compatibility Alliance. *802.11b Wired Equivalent Privacy (WEP) Security*, 2001.