TKN Telecommunication Networks Group

Technical University Berlin

Telecommunication Networks Group

Variations in Wi-Fi RSSI due to different types of Interferences

Aravinth, Sivalingam Panchadcharam

contact@aravinth.info

Berlin, March 2014

Project in advanced network technologies

Supervisors: Dr. Arash Behboodi, Filip Lemic

Abstract

WiFi Beacon packets are transmitted periodically to announce the presence of WLAN. RSSI is Received Signal Strength Indicator which indicates the power of signal that is received at the receiver. Beacon Packet RSSI values are extensively used for ranging and localization purpose. However, RSSI value changes with various interferences, different chipsets and distance. This project work includes an implementation of a software tool to visualize the raw data obtained during the experiments and examines how these RSSI values changed by controlled interferences.

Contents

Chapter 1

Introduction

Beacon Packet

In Wireless Local Area Network (WLAN) Beacon Packets are transmitted periodically to announce the presence of WiFi Network. It contains information of the network such as SSID, BSSID and type of encryption.

Received Signal Strength Indicator (RSSI)

It indicates the power of signal which is received at the receiver and included into the beacon packet by Network Interface Card.

Chapter 2

Problem Statement

Chapter 3

RSSI Visualization Tool

Chapter 4

Design

4.1 Interference

4.1.1 Introduction

This document shortly presents initial interference scenarios that will be artificially generated in TKN Wireless Indoor Sensor network Testbed (TWIST) testbed in order to benchmark different indoor localization solutions in the environments with controlled interference. The reason for benchmark representative indoor localization solutions in the environments with con- trolled interference is to determine if and to which extend different types and amounts of Radio Frequency (RF) interference can influence the indoor localization performance.

4.1.2 Interference Scenarios

Reference Scenario

This reference scenario is instantiated on the 2nd floor of the TWIST testbed in Berlin. It is called "Reference scenario", while no artificial interference is generated and the presence of uncontrolled interference is minimized. Ac- cording to the EVARILOS Benchmarking Handbook (EBH), this scenario is an instance of the "Small office" type of scenarios. In this scenario 20 measurement points are defined and their locations are given in Figure 1.

At each measurement point the indoor localization System Under Test (SUT) is requested to estimate location. The SUT device is carried to each measurement location using the robotic platform. The navigation stack of the robotic platform gives one order of magnitude more accurate location estimation than considered SUTs and the location obtained from the robotic platform is considered as the ground truth.

The experiments were performed at the weekend afternoon, so the influence of interferes has been minimized. Furthermore, the wireless spectrum has been measured using the WiSpy device attached to the robotic platform and all measurements with the interference threshold above certain level have been repeated. Finally, before each experiment a more detained measurement of the spectrum has been taken with the spectrum analyzer at a predefined location.

Interference Scenario 1

First interference scenario instantiated in TWIST testbed uses the testbed's Wireless Fidelity (WiFi) nodes as interference sources. Interference type is jamming on one IEEE 802.11 channel with the maximum transmission power. Three of such jamming nodes are present at different locations in the testbed environment. Summary of this interference scenario is given in Table 1.

Table 4.1: Interference scenario summary

Types of interference sources	
WiFi	✓
Microwave	×
DECT	×
Bluetooth	×
3G	×
ZigBee	×
Types of interference sources	
Number of sources	3
Power	20 dBm
Waveform	Carrier jamming
Specific pattern	
Start & stop time	Beginning & end of experiment
Traffic model	
Traffic parameters of interference	
Packet size	
Inter-packet gap	
Bit rate	
File size	
Start & stop size	
Traffic model	
Network parameters	
Network size	
Node density	
Node mobility	
Node failures	

Interference Scenario 2

In this interference scenario instantiated in TWIST testbed interference is created using the IEEE 802.15.4 Tmote Sky nodes. The interference type is jamming on one IEEE 802.15.4 channel with a constant transmit power equal to 0 dBm. Five of these jamming nodes will be present in the testbed environment. Summary of this interference scenario is given in Table 2.

Table 4.2: Interference scenario summary

Types of interference sources	
WiFi	×
Microwave	×
DECT	×
Bluetooth	×
3G	×
ZigBee	✓
Types of interference sources	
Number of sources	5
Power	0 dBm
Waveform	Carrier jamming
Specific pattern	
Start & stop time	Beginning & end of experiment
Traffic model	IEEE 802.15.4 radio
Traffic parameters of interference	
Packet size	
Inter-packet gap	
Bit rate	
File size	
Start & stop size	
Traffic model	
Network parameters	
Network size	
Node density	
Node mobility	
Node failures	

Interference Scenario 3

Second interference scenario instantiated in TWIST testbed defines inter- ference types that is usual for the office and home environments. Namely, interference is emulated using 4 WiFi embedded Personal Computers (PCs), namely a server, email client, data client, and video client. The server acts as a WiFi Access Point (AP) and a gateway for the emulated services. The email client will "check email" once every 15 seconds for a duration of one second. The data client is emulated via TCP streams one starting at 45 sec- onds for a duration of 22.5 seconds and the other starting at 105 seconds for a duration of 45 seconds. The video client is emulated as a UDP stream of 100 kbps for half the experiment cycle and it will start at the middle of the experiment. In total, the experiment takes 150 seconds. Summary of this interference scenario is given in Table 3.

Table 4.3: Interference scenario summary

Types of interference sources	
WiFi	✓
Microwave	×
DECT	×
Bluetooth	×
3G	×
ZigBee	×
Types of interference sources	
Number of sources	3
Power	20 dBm
Waveform	
Specific pattern	
Start & stop time	Beginning & end of experiment
Traffic model	WiFi traffic
Traffic parameters of interference	
Packet size	
Inter-packet gap	
Bit rate	
File size	
Start & stop size	
Traffic model	
Network parameters	
Network size	
Node density	
Node mobility	
Node failures	

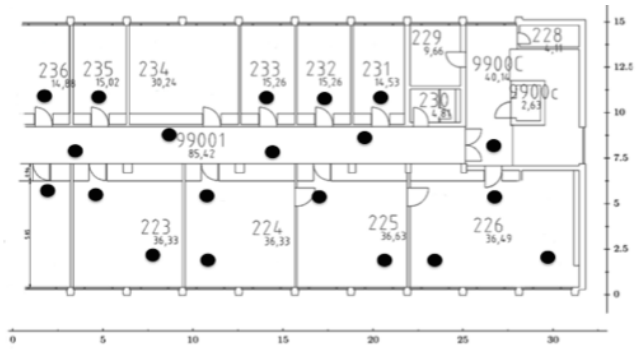

Figure 4.1: Locations of measurement points

Chapter 5

Experiments

Chapter 6

Results

Chapter 7

Conclusion

Bibliography

[1] Leslie Lamport

[2] Leslie Lamport