MCL
Mobile Communications & Quantum Technologies Lab.

Schulcz Róbert
schulcz@hit.bme.hu

Varga Tamás
tvarga@mik.bme.hu

WiFi ranging and real time location

Room IE504 in building I

Basic principles of Wireless LANs

Nonstop Internet connectivity has become a substantial need nowadays. Most of the users prefer wireless connectivity for it is more convenient. There are several wireless network technologies out on the market, one of which is 802.11 WLAN, also named WiFi. WiFi chipsets are present in almost all smartphones and other mobile devices (tablets, laptops etc.), the only difference among them is the version of the standard which they support. We shall note here, that WiFi is not a mobile access network technology as quick handovers and technologies to enable uninterrupted connectivity for fast moving users are not supported.

WiFi network operation principles are lain down in the IEEE 802.11 standards, which have been updated and extended regularly with the advance in technology, user needs and national regulation changes. The standard family includes standards which specify the radio interface, the security and encryption possibilities and the implementation of QoS (Quality of Service) in wireless networks.

Inspecting the IEEE 802.11 standards regarding the OSI model we can declare that the standards specify operation principles in OSI Layer-1 and Layer-2 (physical and data link layer respectively). It is fundamental regarding the physical layer that the WiFi standards specify radio frequencies for radio-based WiFi (Infrared is also avaiable, even though it have not become prevalent) which are in the ISM bands of the spectrum (several licensed bands are supported though in 802.11ah,j,p,y standards). Most systems deployed operate in the 2.4GHz and 5GHz bands in Europe. As in these bands operation is not licensed several other users may use the same part of the spectrum for their communication needs. The shared nature of spectrum access and thus interference from other users should be taken into consideration while planning and deploying WiFi networks.

Access to ISM bands is unlicensed but not unregulated of course. There are several rules for the use of these bands. In Europe the output power for WiFi devices is limited at 100mW (EIRP - Effective Isotropically Radiated Power) usually, and there are regulations regarding the technology used: DSSS (Direct Sequence Spread Spectrum) and OFDM (Orthogonal Frequency Division Multiplexing) are allowed, but while manufacturing or deploying 2.4GHz WiFi systems noise from FHSS (Frequency Hopping Spread Spectrum) systems at the same frequency (e.g.: Bluetooth and Bluetooth LE) should be taken into account. Using spread spectrum allows for better narrow-band noise tolerance and uncorrelated white noise tolerance.

Maintaining high throughput over wireless networks imply that the rate of the transport errors should be as low as possible. Low error rates are possible with error detection and error correction codes and by maintaining a good signal quality. Signal quality is defined by two main factors: the power of the received signal and the ratio of the received signal and the noise (white noise, other WiFi systems, Bluetooth etc.).

RSSI (Received Signal Strength Indicator) is the most important value characterising the received signal power whose value is composed of both the useful signal power and the noise power. This is the value used commonly as the “field strength”. If the power of the useful signal is in question, RSCP (Received

Schulcz Róbert
schulcz@hit.bme.hu

Varga Tamás
tvarga@mik.bme.hu

Signal Code Power) and RSRP (Reference Signal Received Power) values are to be inspected. RSCP is the power of the signal decodeable with a specific spreading code in spread spectrum systems, while RSRP is the referece signal (pilot tone) power.

In WiFi networks the maximum received power is -20dBm in most cases (-10dBm is possible), the sensitivity of the receiver is -85dBm for the preamble, -75dBm for the rest of the transmission. Sensitivity means the minimum power of a signal still decodeable.

The Signal to Noise Ratio, SNR value declares the ratio of the useful signal and the background noise power. WiFi standards do not specifiy allowed ranges, modulation switches are done based on frame error ratio (10% and 8% in different parts of the standards).

Real time location based on RSSI

In wired networks location of a subscriber is defined by the endpoint used by the specific user, if location is needed, a database lookup is sufficient (although in very old, obsolete telephone networks identifying the caller party was far from trivial). Wireless networks allow for different degree of mobility but it is common that the location of a specific device can be determined inspecting the traffic in the network layer only to define the access point serving the device.

If the location of a mobile device should be determined more precisely supplementary technologies should be utilised. Cellular and mobile networks nowadays usually support Location Based Services, but using satellite navigation allows for location info regardless of location based services support in the access network. Location in confined spaces (office buildings, flats etc.) may not be available by neither cellular network info nor satellite based technologies. In these cases, WiFi-based location may be an option.

Traditional location methods used base the location of the device on relation to points of reference with a well-known position. Triangulation for example is a technique useful to determine location on a plane: the distance of the object from three anchor points is determined thus three circles can be drawn around them giving one exact location. Distance may be determined in radio networks by measuring the propagation time of the signal and using the fact that the speed of the electromagnetic radiation is known. Triangulation based on time measurement is not a viable option with WiFi networks as radio wave propagation is a bit more complicated in a busy and crowded office building (line of sight propagation is not common, reflections are likely on objects) and time measurement with a necessarily low quantum is also not available in cheap WiFi devices.

Measuring the signal power is the other option: though the indoor propagation of radio transmission is quite turbid, by defining a finite number of signal level ranges and creating a heatmap of the transmission power in the area affected we may do some approximations.

Schulcz Róbert
schulcz@hit.bme.hu

Varga Tamás
tvarga@mik.bme.hu

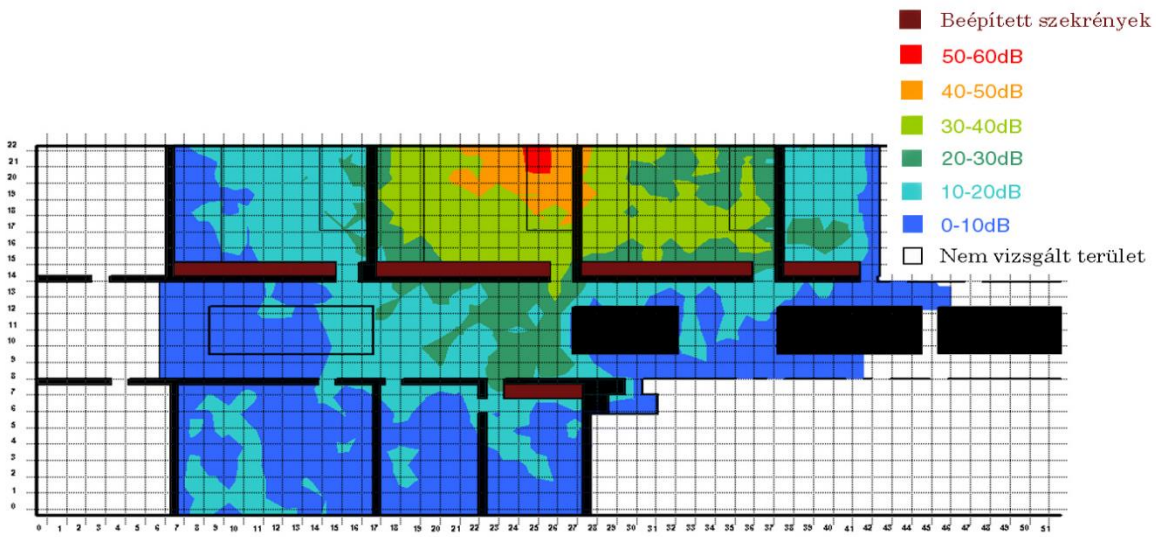

Figure 1 WiFi heatmap of an office area

Using signal level of several WiFi access points we may calculate approximations based on heatmaps for all the access points thus narrowing down the possible location of the device. Likely location of the device is the intersection of all the ranges possible on each heatmap. Of course the precision of the location is dependent on several factors: heatmap step size, the number of the access points involved in the measurement, their distribution in the area, the size of the area and the fidelity of measured RSSI value. On the figure below, the process of narrowing down the possible location of a device based on RSSI value for two networks is shown.

Schulcz Róbert
schulcz@hit.bme.hu

Varga Tamás
tvarga@mik.bme.hu

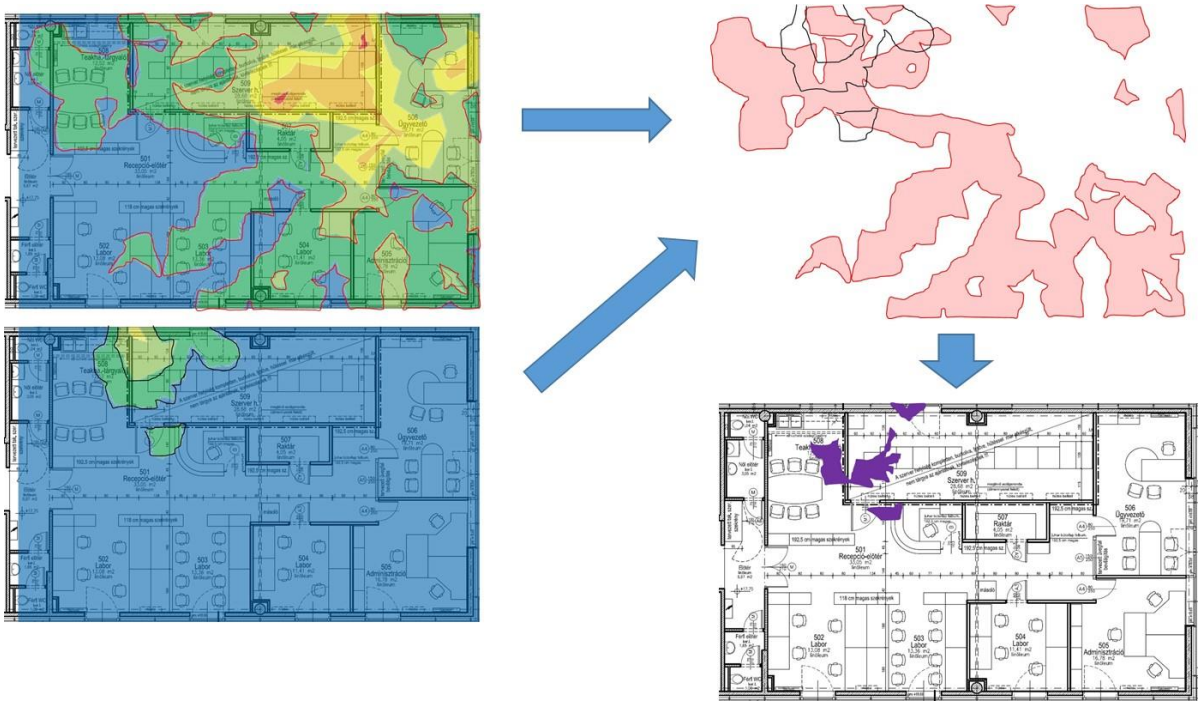

Figure 2 Narrowing down possible location.

In practice for acceptable location accuracy signal strength data of several access points is needed.

Abbreviations

BLE – Bluetooth LE – Bluetooth Low Energy

DSSS – Direct Sequence Spread Spectrum

EIRP – Effective Isotropically Radiated Power

FHSS – Frequency Hopping Spread Spectrum

ISM – Industrial Scientific Medical

LBS – Location Based Services

OFDM – Orthogonal Frequency Division Multiplexing

OSI – Open Systems Interconnection

QoS – Quality of Service

RSCP – Received Signal Code Power

RSRP – Reference Signal Received Power

RSSI – Received Signal Strength Indicator

SNR – Signal to Noise Ratio

WLAN – Wireless Local Area Network

Schulcz Róbert
schulcz@hit.bme.hu

Varga Tamás
tvarga@mik.bme.hu

Tasks

To fulfil the tasks below a mobile device running Android 4.1 os a more recent Android OS is required. If you do not have such a device, please ask the instructor for help. Please read all tasks carefully before beginning the tasks as task may depend on each other!

0. Please install Aruba Utilities on your device!

Figure 3 Aruba Utilities download link.

1. Using the WiFi monitor feature in Aruba Utilities you can see the RSSI for the surrounding WiFi networks.

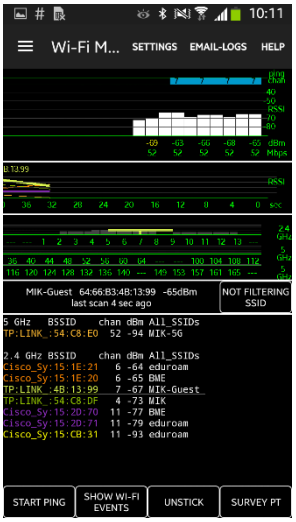

Figure 4 Aruba Utilities

   Note the RSSI values for 4 chosen access points broadcasting the SSID BME in the hall of building I on a 5m x 5m grid.
2. Draw a contour-map of the values on the map provided.
3. Using Bluetooth Low Energy is a viable option for indoor positioning as well. The last task for the measurement is a game actually. Please try to find a Bluetooth LE device hidden at the premises of the Mobile Innovation Centre (Building I, room IE504). For monitoring the RSSI value of the BLE device the Nordic Semiconductors Master Control Panel application may be used!
   The MAC address of the device to look for: **D3:DD:71:D8:DA:EC**.

Schulcz Róbert
schulcz@hit.bme.hu

Varga Tamás
tvarga@mik.bme.hu

Figure 5 Nordic Semiconductors Master Control Panel application download link

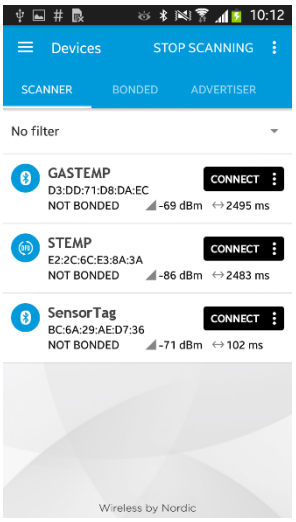

Figure 6 Nordic Semiconductors Master Control Panel application main window