AUTOMATYKA • 2011 • Tom 15 • Zeszyt 3

Łukasz Sturgulewski*, Artur Sierszeń*

System of Distance Measurement and Localization of Wireless Devices Communicating Based on Wi-Fi Technologies

1. Introduction

The presented system localizes devices in wireless networks. There are many reasons for developing systems localizing people or equipment. They include the localization of medical staff in a hospital or the needs of parents and people who take care of children (systems such as these may be used for monitoring places where children spend time).

However, the intention of the authors is that this system be used mainly for the detection of unauthorized access points and other unauthorized wireless devices in Wi-Fi technologies. Its functions will improve the developed system for detecting threats in a network.

2. Guidelines

The most fundamental requirement is that the program enable users to find a wireless device in a most precise way. A reasonable criterion is an error which does not exceed a few (2–3) meters. Devices should be localized quickly; users should obtain the required information within the maximum of a few seconds. Operation of the application should be easy and intuitive; then, everyone, even a person with no computer knowledge, would be able to start it on their own. The system is supposed to facilitate work, not hinder it.

The functioning of the whole system is based on measuring the strength of signals read on access devices in a wireless network during communication (or on attempts at establishing communication) [3, 5]. Based on this parameter, the distance to measurement points within the system is calculated.

* Computer Engineering Department, Technical University of Lodz, Poland

3. Measurement of signal strength and determining distance

One of the most important pieces of information, from the perspective of the application, is Signal Strength, which represents the strength of a signal sent by devices of users in a wireless network. This value is expressed in dBm, i.e. in decibels in respect of a miliwatt [2].

In order to calculate a distance in the application, the following formula was applied (1) for signal suppression in the air [4]:

$$A = 36.56 + 20\log_{10}(f_{\mathrm{MHz}}) + 20\log_{10}(0.621371192 * r_{\mathrm{km}}) \tag{1}$$

where:

A – signal suppression in the air,
f_{MHz} – signal frequency in MHz,
r_{km} – distance between the transmitter and the receiver expressed in kilometres.

The following transformed formula was used in the application (2).

$$r_{\mathrm{km}} = \frac{10^{\frac{A - 36.56 - 20\log_{10}(f_{\mathrm{MHz}})}{20}}}{0.621371192} \tag{2}$$

The function based on the formula presented above checks the table in which strengths of signals were registered, ones which reached subsequent Access Points from the device. If the signal was registered in the checked cell, the distance is calculated.

The next stage, after distance calculation, is the presentation of results in a transparent way. Here, the area map was applied, which has already been described. On this map, circles were marked with centres in places where access points are located and of radiuses reflecting distances between the relevant Access Point and the localized device.

4. Implementation

As a part of the engineer thesis [1], the student implemented the application in Microsoft Visual Studio Express 2008 in C#. The application localizes a device and, if the device is active in a test network, it is able to present detailed information, e.g. (Fig. 1):

- network card IP address,
- network card physical address,
- network card name,
- time period in which the device is connected with the network,
- signal parameters.

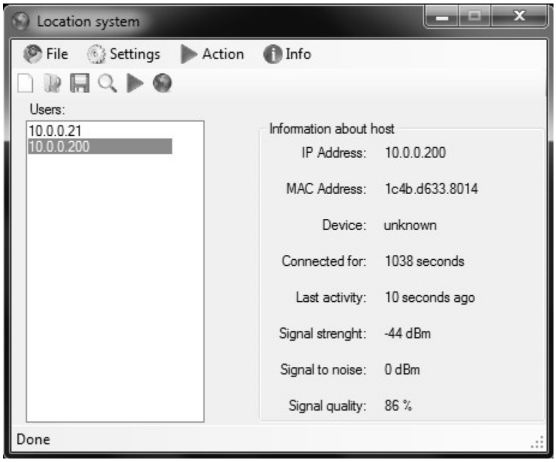

Fig. 1. Main window of the application

5. Tests of the application

Tests of distance measurements were conducted in one of laboratory rooms in the Computer Engineering Department. The room is of app. 50 m^2 area.

The Figure below presents the network in which the tests were conducted (Fig. 2). It consisted of one switch and three access points.

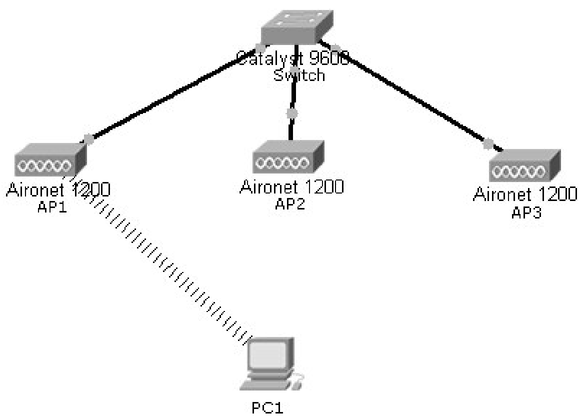

Fig. 2. Topology of the network in which tests were conducted

The locations of Access Points are presented in the Figure (Fig. 3). The application for the detection of devices in a wireless network was equipped with the area map which makes it easier for the operator to mark the location of access points.

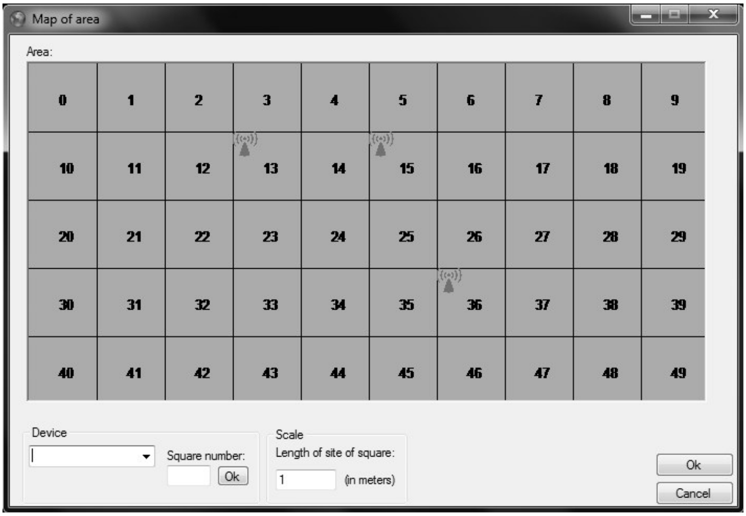

Fig. 3. Locations of access points in the room

At first, all three Access Points were in the room as well as the notebook which was a testing device. After measurements had been made, the locations of the access points and the notebook were changed.

In majority, the results were satisfactory and within the margin of error. The results are presented in the Figure 4. As may be concluded from the Figure 4, the located device should be somewhere between the sectors 13, 14, 23, and 24. In fact, the notebook was on the border of the sectors 14 and 24. It may be concluded that the test results were acceptable.

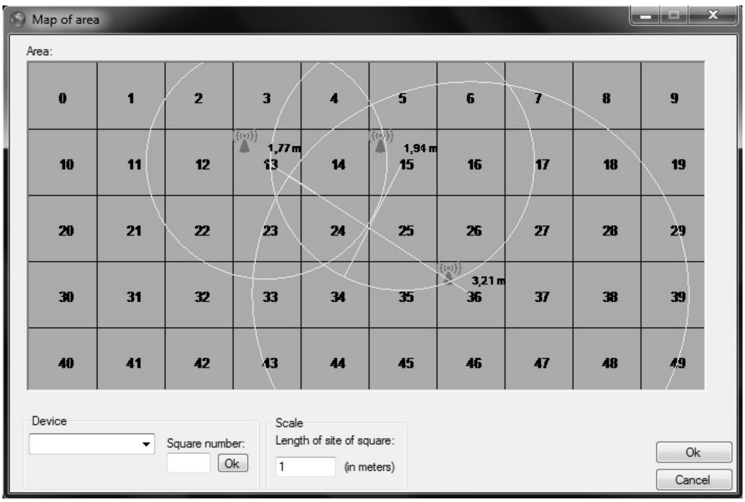

Fig. 4. Graphic interpretation of detecting the tested object location

During the second stage, the access points were distributed in a larger area, i.e. the corridor of the Computer Engineering Department. It is app. 42 metres long. The devices were located at both ends and in the middle of the corridor. The locations of Access Points are presented in the Figure 5.

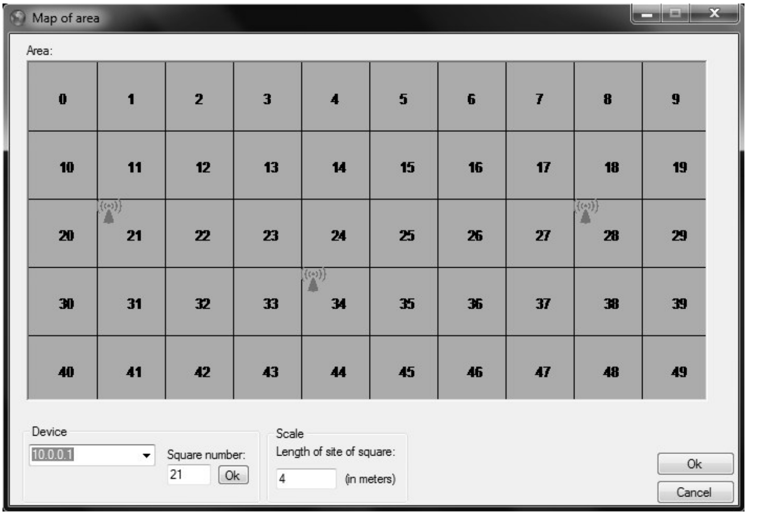

Fig. 5. Locations of the access points in the corridor

Unfortunately, in this case the results were not acceptable because in most events the measurement was even 50 metres, which was not possible.

The first factor which could have affected the results included the physical characteristics of the area. Walls and doors may disturb radio signals significantly, what certainly influenced the obtained results. The second factor was the fact that there are many wireless networks in the Department and, what is worse, they have stronger signals than that of the test network.

6. Conclusions

The tests indicated that the application gives good results in a small area; however, localization is more difficult when the area is larger. Additionally, the application gives worse results in conditions where there are more barriers for transmitted waves, e.g. walls, doors, or windows, which make the whole process more difficult. The next negative factor is the presence of other wireless networks in the area, what reduces the accuracy of measurements.

It seems that the application should be developed so that it does not give results based only on the measurements of signal strength. Using knowledge on propagation of radio waves and having been acquainted with the area by conducting advanced measurements, one may obtain much more accurate location results. Therefore, the next step will be the development of area characteristics map.

References

[1] Jasiński R., *Distance measurement and localization system for wireless devices with communication based on Wi-Fi technologies*. Technical University of Łódź, 2011 (Master's thesis, supervisor: A. Sierszeń).
[2] Ross J., *Sieci standardu Wi-Fi*. Nakom, Poznań 2004.
[3] Sankar K., Sundaralingam S., Balinsky A., Miller D., *Bezpieczeństwo bezprzewodowych sieci LAN*. Mikom, Warszawa 2005.
[4] Szóstka J., *Fale i anteny*. Wydawnictwa Komunikacji i Łączności, Warszawa 2006.
[5] Zieliński B., *Bezprzewodowe sieci komputerowe*. Helion, 2000.