

Development and Implementation of a Bluetooth Networking Infrastructure for the a Notebook-University Scenario

Ana Zapater, Kyandoghene Kyamakya, Silke Feldmann, Marc Kruger, Isaac Adusei
Institute of Communications Engineering
University of Hannover
Appelstr. 9A, 30167 Hannover (Germany)
{zapater, kyandogh, feldmann, mkrueger, adusei}@ant.uni-hannover.de

Abstract

In the context of the UbiCampus project, the Notebook-seminar was developed in the Institute of Communications Engineering (Institut für Allgemeine Nachrichtentechnik, IANT) at the University of Hannover. In this seminar the students worked in groups in order to provided a Bluetooth infrastructure for the rooms of the IANT. In this paper the UbiCampus project is described, as well as the most interesting results of the 3 groups that participated in the seminar.

1. Introduction

The first part of this paper is the description of the UbiCampus project and the Notebook Seminar developed in its context

1.1. The UbiCampus Project

The UbiCampus project [1], [2] of the University of Hanover (Universität Hannover, UH) and the medical university Hanover (Medizinische Hochschule Hannover, MHH) is promoted as one of 22 projects in the context of the advertisement Notebook University by the BMBF (*Bundesministerium für Bildung und Forschung*), with the initiative “Neue Medien in der Bildung” (New Media in Education) [3].

Goal of the UbiCampus project is the development and introduction of mobile multimedia technologies for the interactive presence teaching. The aim is to obtain constructive learning attempts with frequent changes between presentation and independent learning.

In order to do it 4 scenarios are implemented on basis of different interaction samples in the context of pilot attempts.

The 4 scenarios are:

Interaktive Vorlesung (interactive lecture) - lecture introduction to the operating systems at the Notebook *Notebook seminar* - autonomous development of a project task

Mobile Projektgruppe (Mobile project group) - pair programming in the context of a software project
Zielgruppenoptimierte Veranstaltung (goal group-optimized meeting) - physics for the medical profession and biomedical technology

These 4 scenarios will be implemented during the course of the project, integrated in the normal learning process in the scope of the pilot attempts and finally evaluated.

A new learning style is proposed, which results from the permanent use of the Notebook. It becomes the central and continuously available medium of the study, which use goes clearly beyond the previous occasional one of the stationary computers. It concerns not only the access to teaching and learning materials, but particularly around the extension on the interaction by direct computer access and simulations. Furthermore the interactive co-operation between the students within a team plays an important role.

1.2. The Notebook-Seminar

One of the 4 scenarios to be implemented in the UbiCampus project is the Notebook-seminar, which has been developed in the Institute of Communications Engineering.

The educational objective was to achieve with an independent work of the project tasks both an intensive insight into the Bluetooth technology and to learn the methods of working in a project. Notebooks are used as typical “engineer instrument” to the procurement, preparation and representation of the information. Assistants attend advising and looking after the project realization.

The first seminar took place in the winter semester 2002-2003. In this seminar a Bluetooth infrastructure for the seminar rooms, the labs and the hall area of the IANT had to be designed. The infrastructure

should allow the mobile end-devices (notebooks, PDA's etc.) different services, such as secure mobile and wireless access to inter- and intranet, or the communication between devices among each other (e.g. Broadcast-Function).

The following demands on the project were set:

- In the seminar rooms the network had to be able to be used with enough capacity by at least 25 people simultaneously.
- The temporal use of the Bluetooth infrastructure had to be known, in order to deduct the available services.
- The network should have a good "Quality of Service" to show for itself.
- The network should have a high security standard to enjoy.

To provide these demands the following tasks were formulated:

- a) Provide a total concept for the networking.
- b) Selection and dimensioning of the network elements.
- c) Provide a security concept.

Each of these tasks was developed for one group, each with 4-5 members. The most interesting results are detailed next. Each student worked with his own notebook, and a Bluetooth USB-dongle was provided for each student.

2. Results

Some of the obtained results are the development of a handover concept, the use of Bluetooth to do location and positioning, or the implementation of a program to measure the signal strength and represent.

2.1. Handover Concept

There are different motivations to induce a handover, such as the movement of the user, the results of the measurement of the radio hop, high traffic load or service measurements. To create a concept of handover in Bluetooth the handover method of the other cellular networks can be adjusted and converted.

If the received signal power is too weak, a handover should be induced. We can define a critic handover limit (i.e. Received Signal Strength Indicator (RSSI) = -5), and if the received signal power reaches or exceeds this limit the handover is induced, but the connexion should be maintained.

The criteria to choose a new Access Point (AP) are:

Accessibility: select the Base Station (BS) from which the signal is strongest. For indoor networks the signal strength depends not only on the distance, but also on the objects that are in the room. The signal strength can be the only criterion of the accessibility. An example is represented in Fig.1.

The signal strength of AP1 in the red area is smaller from the one of AP2 because of the object S. However in the green area is stronger than the one from AP2. In the blue area is the signal strength of AP2 under the critical border.

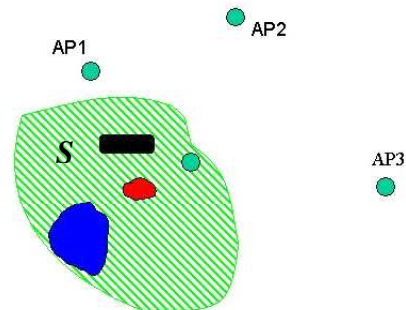


Fig.1: Example of accessibility

Access Point – load: The maximum number of Mobile Stations (MS) that can access at the same time an AP is 7. The effective connecting rate of individual MS is $1Mbit/n$, where n is the number of MS connected to an AP. The more number of MS connected to an AP, the slower is the connection. With the Handover procedure we should select, if possible, an AP with few load.

Distance to the AP: the distance between the BS and the future AP should be as short as possible (more signal strength).

With these 3 criteria a hypothetical decision factor is formulated:

$$h = d \times s \times l$$

Here d is the distance in meter, s is the signal strength in $RSSI - RSSI_0$ (with $RSSI_0$ the critic handover limit) and l is the load or number of MS.

Taken into account this decision factor, the algorithm to select a new AP during the handover process is the following:

1. Calculate the actual position of the MS
2. Calculate the decision factor for each AP, and sort the AP according to the obtained valued (The list of AP is obtained at the first connection from the handover agent)
3. Choose the AP with the smallest factor
4. If the selected AP is not accessible, select the next AP. Otherwise completed.

Handover Procedure by Bluetooth: proposed procedure

If the handover conditions are achieved, the MS selects a new AP and sends to the server the measured data and a *Handover Request*.

When the server receives this request writes the data in a table and sends an *Allocation Inquiry* to the preferred AP. If the answer of the AP is positive, the server “breaks” the old connection, creates a new one with the new AP and sends the MS a *Handover Response*. If the answer of the AP is negative, the server search from the table an AP with the lowest decision value and sends an allocation inquiry to it. The process starts again until a new AP is found.

When the MS receives the *Handover Response* from the server according to the connection type there are two possibilities.

With a SCO connection the MS interrupts the transmission with the old AP and creates a new one with the new AP. The MS sends to the server a *Disconnection Acknowledge*, and once the server receives it are transferred the contents of the buffers. After that the server sends a *Ready Response*.

If the connection is ACL, the transmission is broken and the position of the break point is marked. The MS sends to the server a *Disconnection Acknowledge*, and once the server receives it the transmission continues at the marked place. After that the Server sends a *Ready Response*.

If the MS uses LAP, is used the PPP tunnelling, which server is located in the handover-agent. The AP is only responsible for the redirection of the PPP packet. The PPP connection will be retained when the handover occurs.

But if the MS uses PAN, the handover agent has a Routing table, which contains the IP address of the MS of the AP with which is connected AP. After the handover the routing table is updated.

2.2. Location using Bluetooth

The *Received signal Strength Indicator* (RSSI) is defined in order to show whether the received signal strength lies in the golden receiver power rank, so that the transmitter can place their sending achievement. The golden receiver power rank (Fig.2) is defined by two thresholds. The lower threshold level corresponds to the received energy, which has at least 6dB over the actual sensitivity of the receiver, however maximum of -56dBm. The upper threshold level is 20dB over the lower threshold level with an accuracy of ±6dB.

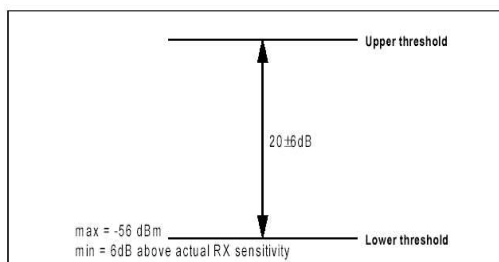


Figure 2: The golden receiver power rank

The RSSI measurement compares the received signal strength with the two thresholds. The command of the HCI-layer *HCI_Read_RSSI* offers the possibility of querying the RSSI. This command returns a positive difference, if the received signal strength lies above the upper threshold of the golden receiver power rank. If it lies under the lower threshold, returns a negative difference. If the received signal strength lies in the golden receiver power rank, a zero is returned.

If we call S the received signal strength, the following equations are determined by the definition of RSSI:

$$S = \text{RSSI} + T_0, \text{ for } \text{RSSI} > 0$$

$$S = \text{RSSI} - T_u, \text{ for } \text{RSSI} < 0$$

$$T_0 = T_u + 20\text{dB}$$

where T_0 designs the upper threshold and T_u the lower threshold of the golden receiver power rank.

In order to determine the distance by means of RSSI it is accepted that there is no obstacle between transmitters and receivers. As a result the following equation is obtained:

$$\text{RSSI}(d) = \text{RSSI}(d_0) + 10\lg(d/d_0), \text{ for } \text{RSSI} > 0$$

$$\text{RSSI}(d) = \text{RSSI}(d_0) + 10\lg(d/d_0), \text{ for } \text{RSSI} < 0$$

From this equation a design for the qualitative relationship between the distance and the RSSI can be provided. The distance where the RSSI is always zero is the golden receiver power rank. Since the RSSI values are constant in this distance, they are not applicable for the computation of the distance. The distance between the transmitter and the receiver can be computed in the ideal case (no obstacle, no reflecting, RSSI not equal 0) with this equation.

To determine the geometrical position of one point, the method of triangulation can be used. Before doing it the positions of several reference points must be determined in a coordinate system, and the distances between the determining goal point to the points of reference must be also measured. But the triangulation method could be a little difficult, and the method of least-square estimation (LSE) will be used.

To define the position of a Bluetooth device (MD) the distances between the MD and a few reference devices (RD) must be measured. The measurement with Bluetooth has however some disadvantages:

First of all, the concept of Bluetooth actually is the replacement of cable between different devices. A Bluetooth equipment has the advantage of low power consumption, which supposes a relative small range

of coverage. This involves the limitation of the measurement to the indoor range.

Secondly Bluetooth does not have an efficient method available for measurement of the signal strength. The Bluetooth specification defines two HCI instructions, *HCI_Read_RSSI* and *HCI_Get_Link_Quality*, which can be used for this purpose. The *HCI_Read_RSSI* instruction returns the difference between the measure of the received signal strength and the delimitations on the golden receiver power rank. The accuracy of the RSSI value depends on the Bluetooth hardware manufacturer. The *HCI_Read_RSSI* instruction always returns zero, which is not used to determine the distance, if the RSSI is in the golden receiver power rank. Unfortunately the golden receiver power rank has a width of 20dB, which is already a large range, where the received signal strength is also optimal for the receivers. For the determination of the distance only the positive and negative RSSI values can be used, which shortened the measuring range again. Since the length and the width of a room is normally under 20m, the RSSI values will not lie in the negative range, and only the positive RSSI values will be possible. The *HCI_Get_Link_Quality* command returns an unsigned 8-bits Integer as indication of the connection quality. However the Bluetooth specification does not supply guidance over the meaning of this number.

Thirdly, we have supposed transmission in free area, which means no obstacle or objects which reflects the radio wave on the transmission path. But in the real indoor environment there are many objects which can affect the transmission of the radio wave, such as walls, window, doors, roof, soils, tables, chairs, etc. Almost in every case the object whose position is to be determined is held by a person in the hand, and the person has also effect on the radio transmission.

Because of these reasons the received signal strength depends not only on the distance between the transmitter and the receiver, and the equation said before is not useful. Instead of it we have to measure the RSSI at different points and use a function approximation.

2.3 Location algorithm

In the room, where the location should be done, N Bluetooth devices are placed as reference station (RS). The number of RS and the position of each of them are stated in such a way that the transmitted power is so strong that the RSSI of those is always positive.

The RSSI of all RS is measured in some cells, which should be uniform distributed. In order to reduce the external effect to the RSSI, it has to be measured

several times and take an average value. The measured RSSI and the associated positions of the cells are stored. After sufficient data are collected, the approximation of the appropriate functions can be accomplished. The distance of each cell to all BS is computed considering the coordinates of the cell as the position of it. The coordinate of the centre of the cell is (x_z, y_z) , and (x_b, y_b) is the coordinate of the RS. The RS is h meter over the cell. The distance d is then:

$$d = \sqrt{(x_z - x_b)^2 + (y_z - y_b)^2 + h^2}$$

To do the approximation three-function type are used, the logarithmic function and polynomial function with 2 and 3-Order. To each function type is determined a function with the method LSE, and the value of R^2 is calculated. R^2 designates the *similarity* degree of the function with the measuring points and is defined as

$$R^2 = 1 - \frac{SSE}{SST}, SSE = \sum (Y_j - \hat{Y}_j)^2, SST = \sum Y_j^2 - \frac{(\sum Y_j)^2}{n}$$

The function with the largest R^2 -value is used for the later computation of the distance. This procedure must be accomplished once for each RS, so that each RS possesses its own function for the determination of the distance.

Finally the position of the MS is computed by means of the measured RSSI at its position. The MS measures the RSSI from each RS several times and the average value is taken. Then the distances of the MS are computed to the respective RS with the determined function. The coordinate of the position of the MS can be computed then with LSE method.

2.4 Propagations conditions

The prediction of radio propagations is generally difficult. It is still more difficult to predict or compute the radio propagations in buildings with their specific absorptions, reflections and overlays. With the simulations is tried to copy the reality as well as possible so that an approach prediction can be done. A simple simulation in the programming language C++ was written, in order to measure the radio propagation of the Access Points distributed along the institute (14th and 15th floor of the building).

Neither in the data sheets of the dongles, nor in those of the AP, data concerning the kind of antenna used was described, therefore reliable conclusions about the antenna gain and the directional characteristic cannot be reached. Thus as basis for the computation

is supposed an isotropic spherical source, whose power is uniformly distributed in all directions.

Other aspect to consider is the data of the devices. In Bluetooth are specified 3 power classes, each of one with a different power transmission and range: class 1 (100mW or 20 dBm, 100 m), class 2 (2,5mW or 4 dBm, 40m) and class 3 (1mW or 0 dBm, 10m). All ranges refer to free area, thus for Line of sight (LOS) connections. These ranges cannot be achieved because of the absorptions caused in buildings due to its construction. The AP used in the Institute of Communications Engineering have 20 dBm of power transmission, while the USB adapters only 4 dBm.

The receiver sensitivity of the USB adapters is approx. -80 dBm and the AP more than -85 dBm. In the computation was supposed always a sensitivity of -80 dBm for all devices, which brings an additional safety level for the accessibility to the AP.

As the search for a suitable program with which one can simulate wave propagation within buildings was not successful, a C++ simulation program had to be written, which computes the wave propagation and is restricted to the dependence on the walls and free space attenuation.

In the following paragraphs is described the algorithm used in this program. First the plans of the two floors, with dimensions 870 x 450 pixels, were stored in the computer. During the model production of the walls were specified 2 different types, one to represent the normal partition walls, and the other one to represent the thick concrete walls in the area of the elevators and the toilets. The wall types were already considered as a fixed value. Variable specifications were the safety level, the power transmission as well as the receiver sensitivity. The safety level is defined, because during the transfer absorption are considered only the walls. Objects such as cupboards, shelves, people, contribute also to the absorption, however are almost impossibly to be simulated in the context of this project. The algorithm for the computation of the field strength is with exception of the reflection and the diffraction, both not considered, equal to the algorithm of the Raytracing software. After the location of the AP, which is marked by one mouse-click on the graphic surface and represents the transmitting antenna, the surface is drawn line by line. For each 3rd pixel the program determines the distance pixel-AP on the basis a mathematical linear equation. It serves as basis for the computation of the free space attenuation (Figure 3)

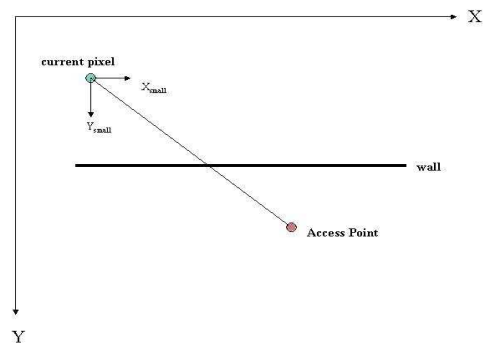


Figure 3: Computation of the field strength

If between the current pixel and the AP are one or more walls, the field strength must be decreased by the appropriate portion of the wall absorption. Whether a certain wall on the way is penetrated along the determined straight lines, determines the following algorithm. The current pixels serves as origin of a new, small coordinate system ($x_{small}|y_{small}$). For each point on the distance $x_{small} = 0$ to $x_{small} = X_{AP}$ is determined the y-value in accordance with the linear equation. If the point determined is identical to one point of the stored positions of the wall, then no LOS connection exists, and the receipt level must be weakened in the place of the current pixels additionally for free space attenuation around the absorption value of the type of wall concerned. In the developed program could be problems if the upward gradient of the linear equation became too large. Then it could happen that with any x the pertinent y-value was the far below y-value of the wall, and which next y-value was with x+1 the far over y-value of the wall. This problem was gone around thereby as the determined y-values are successively put down in an array, and after each new point computation it is queried whether between the current y-value and the preceding possibly the y-value of a wall lies. With this algorithm it is now possible to recognize whether a jet (linear equation) a wall penetrates, or not. Some results are represented in Fig.4.

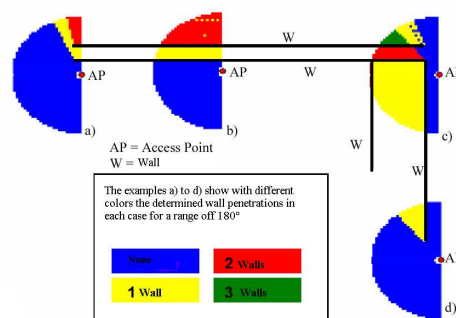


Figure 4: Example of propagation measurement

For unexplainable reasons the algorithm described does not function at high upward gradient values always satisfyingly. Therefore occasionally error samples are with high upward gradients to recognize (Fig.4, example b: Yellow pixels within the red range). After the algorithm functioned became the formula for the free space attenuation added, and the receipt levels graphically represented (see Fig.4).

After the test phase of the algorithm of recognition of the wall penetrations the formula for the free space attenuation was added and a total test with the graphic surface was accomplished. The result is represented in Fig.5. The frequency was 2.4 GHz, the safety level was 2 dB, the transmitted power 0 dB, the receiver sensibility -80 dB, the attenuation of the walls model 1 5 dB and the attenuation of the walls model 2 13 dB. The strength of the receipt levels are coloured represented. Red means that a very good receipt level prevails there, while yellow represents a very bad. The blue points represent the used Bluetooth devices.

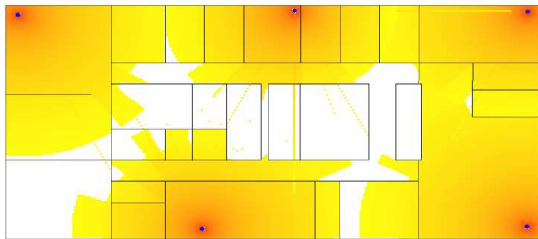


Figure 5: Simulation results

On the basis of practical field strength measurements the Bluetooth infrastructure already existing was examined and the results were compared with the theoretically determined values of the simulation program. At some points theoretically according to the results of the simulation no receipt would have been more possible. However a receipt could be proven in the mentioned places. This effect was to be noticed particularly clearly in the corridors. The receipt of the signals must have come by reflections at the walls and by the smaller absorption of the opened doors, because this effect was not considered in the simulation.

2.5. Security issues

Wireless networks and its problems

The open access to wireless communications networks makes the safety attitudes one of the most significant factors to be examined and understood. Most of the available technologies use nowadays the radio frequency spectrum. This frequency band could be without large expenditure for almost everyone

intercepted and subjected to a large number of disturbances subjected. Because the wireless communication is momentarily already used for business purposes and will be in the near future still much more strongly used, this vulnerable conditions is not acceptable and is need a security concept.

In cable-based networks the cables used to interconnect the devices offer a certain physical protection against manipulations. The cables normally are within a building, which is protected by certain access controls. Within the areas, where the devices are, the cables are freely accessible. A potential aggressor must break in the cables thus into the building and look for them in the appropriate area. In order to arrive at the data, the cable must be intercepted. In mobile, wireless networks the data are simple openly over air transferred and thus in a certain spatial periphery to receive. It can even be that the transmission is receivable outside of a building. The data communication is thus accessible over the air interface very much more easily, than with a network connected with cable. Due to the easy listening receptivity in the wireless surrounding field are necessary an authentication, a coding and an access control with strong cryptography.

Additionally in ad-hoc networks the participants do not know each other when network is constructed, therefore is it not possible to construct the network using common information as for example secret keys. Possibly they use even different safety standards.

General security aspects and its solutions

In nearly all the applications where Bluetooth can be used, private or personal data of the users is administered or used. Therefore it is particularly important that no strange user can log in into a network and/or a computer and access its data. Beside the contamination by so-called "Virus" and the unnoticed falsification the data, an additional danger results if a strange user accesses to the data by imitation of an acquaintance into a network and using a wrong identity obtain unnoticed access and if necessary in further networks too(account abuse). Also without login for potential aggressors can be possible to arrive into the possession of confidential data to falsify. The radio interface could be heard or the data could be manipulated on the way from the sender to the receiver.

Nevertheless, using coded traffic another overview of the activities of the network can be noted by monitoring of the radio interface and if necessary a conclusion can be drawn. With mobile Bluetooth users a transaction log can be provided, which betrays critical habits of a user.

There are several possibilities for the solution of the safety problems. A first attempt for a safe network would be a participant identification using clear characteristics, e.g. the MAC address. These were registered into an Access Control List (ACL). If a client with a strange MAC address tries to access the network, he is rejected. Authentication would be the next step toward a safe net. The authentication could be solved e.g. in terms of software using passwords, and/or on the hardware side by Smart Cards or similar. Further different groups of users for different safety-relevant ranges could be created. So it could be prevented that networks were abused, or data were seen or changed by unauthorized users.

In the case of data transmission in the network it is important the maximum permitted load to code e.g. WEP (Wired Equivalent Privacy). Here is worked with different key lengths, i.e. 64 or 128 bits. Enclosed are 24 bits called the initialization vector (one of the random numbers which are changed by the hardware from packet to packet) and the remainder (40 and/or 104 bits) is defined by the user. Secure end-to-end connections using the IP protocol can be realized by using VPN (Virtual private network).

A very simple characteristic for the safety increase is the delimitation of the range of the Access Points. In Bluetooth this is already given by the standard, which contains a range of approx. 10 m. In the WLAN functionality there is the possibility to switch the functionality off.

Frequency Hopping in Bluetooth is too a safety aspect. Here the frequency is changed 1600 times per second. If a potential aggressor wants to hear the signal, first he must synchronize himself with the signal.

Bluetooth security

Bluetooth signals can be easily heard. For that reason were necessary in the Bluetooth specification special safety mechanisms to avoid the falsification of data during the transmission. In particular the link layer makes available features, with which authentication and coding of data are possible.

Bluetooth contains 3 different security modes for the authentication of devices, which are used depending upon equipment and safety need.

Mode 1: this mode refers to missing safety precautions and is used when there are not implemented critical applications on the appropriate devices. In this mode the devices ignore the safety functions of the link layer, so that the access to databases that do not include sensitive data is released.

Mode 2: this mode offers security on the service level and makes possible the appropriate access

procedures in applications which run in parallel or processes with different safety requirements.

Mode 3: this mode offers security on the safeguard level, by which the link manager provides on a uniform level during the connecting fittings for all applications for safety precautions. This mode is less flexible, however it can be implemented by the security level more easily than mode 2, in which each application has its own safety level.

With the security mode 2 the safety stages can be specified for devices and services separately. For devices there are 2 stages of confidence, trusted and untrustworthy. Trusted devices stand in a firm relationship to each other (paired devices) and have unrestricted access to all services.

Untrustworthy devices are not located in permanent relationship, and/or connection, because they are not trustworthy. There can be cases, in which devices stand to each other in a firm relationship although they are untrustworthy. In these cases the access to services is limited.

The trust level of equipment can be set in such a way that it has only access to a service, and/or a group of services. The requirements for authorizing, authentication and coding are specified depending upon access of the devices independently of each other:

- With services, which require authorizing and authentication, the access will be only permitted to trusted devices; all other devices must authorize it manually.
- Services, which require only an authentication.
- Services, which stand open for all

A safety approach is the employment of a security manager, who is queried during the establishment of a connection. The security manager can make possible for so trustworthy devices, after inquiry of the internal database, services and access of the appropriate safety stage. However this inquiry of the security manager cannot replace existing network-specific safety precautions. During extremely strict requirements, security would have to be supplemented by safety mechanisms on the application layer. A characteristic of the Bluetooth security architecture is that actions are avoided if possible with the access to services. Actions are necessary only if a limited use of services is to be granted to devices, or if trustworthy relations with devices has to be arranged, which permit unrestricted data access.

In order to be able to satisfy different requirements in view of the availability of services without user interferences, the authentication must take place after the definition of the security stage of the requested service. The authentication takes place when a connection requirement for the service is transferred. The following events arise with the access to trustworthy equipment successively:

- The connection requirement is made by L2CAP
- L2CAP requests the access with the security manager
- The security manager queries the service data base
- The security manager queries the equipment data base
- If necessarily the security manager forces the Authentication and coding
- The security manager allows the access
- L2CAP continues with the mechanism of the connection

Thereby the authentication can take place into both directions, so that the client must authenticate itself with the server, or in reverse.

Even if the Bluetooth security architecture is not coordinated with the mode 3 (security on the connecting level), it can support nevertheless this mode easily. The security manager can order the link manager that the authentication is forced, before a base band connection is made by the HCI. Before the transition of mode 2 on mode 3 there are however some steps necessary, to avoid that trusted devices do not receive access. The security manager must remove all connecting codes for not trusted devices, which are stored in the radio module. In addition it can use the HCI.

For arriving connections is required the access control of the L2CAP-level and sometimes also the upper multiplex protocols (e.g. RFCOMM). With the reception of the connecting desire the protocol object sets an inquiry with the security manager, both are passed on the multiplex information. The security manager decides, whether the connection may be initiated or not. It answers then the protocol object. If the entrance is granted on the part of the security manager, the procedure is continued for the mechanism of a connection. If the connecting desire is rejected, the connection is terminated.

3. Conclusions

In this paper is exposed the results of the project Notebook Seminar developed at the Institute of Communications Engineering at the University of Hannover in the context of the UbiCampus project. In this seminary the students have worked in groups in order to provided a Bluetooth infrastructure for the rooms of the IANT. The most interesting results were exposed.

4. References

[1] UbiCampus–Notebook University Hannover
<http://www.ubicampus.uni-hannover.de/>

[2] Learning Lab Lower Saxony (L3S)
<http://www.learninglab.de/deutsch/projekte/ubicampus.html>

[3] Projektträger Neue Medien in der Bildung
<http://www.gmd.de/PT-NMB/>

[4] <http://www.qsl.net/n9zia/wireless/>

[5] Modern Approaches in Modeling of Mobile Radion Systems Propagation Environment, Aleksander Neskovic, Natasa Nestovic and George Paunovic, University of Belgrade

[6] <http://www.sfb425.uni-karlsruhe.de/A2/12000/index.htm>

[7] Script „Wellenausbreitung“, Prof Marquart, Uni Hannover

[6] Specification of the Bluetooth System

[7] Bluetooth - Sicherheitsmodelle der Bluetooth Spezifikation – Nathan J. Muller – 2001

[8] Wireless Security – Randall K. Nichols, Panos C. Lekkas – 2002

[9] <http://www.niksula.cs.hut.fi/~jiitv/bluese.html>

[10] Security Weakness in Bluetooth - Markus Jakobsson, Susanne Wetzel

[11] Security of Bluetooth: An Overview of Bluetooth Security - Marjaana Träskbäck