BALTIC CONFERENCE

Advanced Topics in

Telecommunication

Tartu, 22.08. - 23.08.2008

Universität Rostock 2008

Herausgeber: Prof. Dr. Clemens Cap
Wissenschaftsverbund IuK
„Informations- und Kommunikationstechnologie“(IuK)

Erstellung der Druckvorlage:
Sebastian Engel

Entwurf des Umschlagbildes:
Dr. Christine Bräuning

CIP-Kurztitelaufnahme:

ISBN:

Bezugsmöglichkeiten:

Universität Rostock
Institut für Informatik
Frau Kerstin Krause
Albert-Einstein-Straße 21
18059 Rostock

Universität Rostock
Wissenschaftsverbund IuK
Frau Dr. Christine Bräuning
Albert-Einstein-Straße 23
18059 Rostock

Druck: Universitätsdruckerei Rostock

Table of Contents

Preface

In 2005, the University of Bremen, the University of Lübeck, the ISNM - International School of New Media at the University of Lübeck, and the University of Rostock joined forces for the first Baltic Summer School in Technical Informatics (BaSoTi). Supported by a sponsorship of the German Academic Exchange Service (DAAD - Deutscher Akademischer Austausch Dienst), a series of lectures was offered between August 1 and August 14, 2005 at Gediminas Technical University at Vilnius, Lithuania. The goal of the Summer School was to intensify the educational and scientific collaboration of northern German and Baltic Universities at the upper Bachelor and lower Master level.

In continuation of the successful program, BaSoTi 2 was again held at Vilnius, from July 31 to August 14, 2006, BaSoTi 3 took place in Riga, Latvia at the Information Systems Management Institute, from August 26 to September 10, 2007, and BaSoTi 4 was held at the University of Tartu, Estonia, from August 8 to August 23, 2008. BaSoTi 5 presently is planned for August 2009, again in Tartu.

Since BaSoTi 3, the Summer School lectures have been complemented by a one day scientific event on Advances in Telecommunications. The goal is to give young, aspiring PhD candidates the possibility to learn to give and to survive an academic talk and the ensuing discussion, to get to know the flair and habits of academic publishing and to receive broad feedback from the reviewers and participants. Moreover, the Summer School students would have a chance to participate in what most likely would be their first academic research event.

The present proceedings give proof of the research results submitted by the participants and lecturers of BaSoTi 4.

Clemens H. Cap
Rostock, October 2008.

Basics of Optical OFDM

Daniils Dikanskis, Henning Paul and Karl-Dirk Kammeyer
Department of Communications Engineering
University of Bremen
28359 Bremen, Germany
Email: ddikanskis@inbox.lv, {paul,kammeyer}@ant.uni-bremen.de

Matthias Schuster
Fachgebiet Hochfrequenztechnik
Technical University Berlin
10587 Berlin, Germany
Email: matthias.schuster.ext@nsn.com

Daniils Dikanskis and Matthias Schuster are with Nokia Siemens Networks, Munich, Germany.
This work was in part supported by the German Research Foundation (DFG) under grant Ka814/19.

1 Introduction

Orthogonal Frequency Division Multiplexing (OFDM) is a promising method of digital modulation in which a signal is split several parallel narrowband signals at different frequencies. The technology was first conceived in the 1960s and 1970s during the research into minimizing interference among channels near each other in frequency domain. Since that time, OFDM technology is widely used as a standard for many wireless and wire line applications, like IEEE 802.11 wireless local area network (WLAN), digital audio broadcast (DAB), digital video broadcast (DVB), asymetric subscriber line (ADSL) etc. Recently it has been shown that OFDM can also be utilized for optical communication, and it has many advantages in comparison to conventional optical systems.
One of the main advantages of optical OFDM is that the need for optical channel dispersion compensation is eliminated in long-haul transmission links. OFDM transmission and reception is computationally less complex due to the use of fast Fourier transform (FFT) and inverse fast Fourier transform (IFFT) algorithms compared to conventional equalizers. As OFDM sub-carriers are orthogonal and

overlap each other, the bandwidth is utilized more efficient.
Fiber-optic OFDM systems can be realized either with direct detection optical (DDO) or with coherent optical (CO) detection. Whereas DDO-OFDM is more suitable for cost-effective short reach applications, the superior performance of CO-OFDM makes it an excellent candidate for long-haul transmission systems. DDO-OFDM requires half of the optical power to be allocated for the transmission of the carrier. Also it requires that a guard band is used between the optical carrier and the OFDM band, in order to avoid intermodulation impairments that occur at the photodiode [JMS+08]. This guard band effectively halves the optical spectral efficiency and increases the bandwidth requirements of the optical front end of the transmitter and receiver. On the other hand, DDO-OFDM requires fewer components at transmitter and receiver than CO-OFDM and is therefore more cost-effective. A major concern of CO-OFDM is the phase noise of the local oscillator that must be compensated, especially since the impact of phase noise on the performance of OFDM systems is much larger than the impact of the thermal noise [SvdHFS07].
Besides the advantages of OFDM there are few main issues with OFDM systems. The first problem is the the sensitivity of OFDM to synchronization errors and the second is its high peak to average power ratio. In this paper the problem of synchronization of OFDM receivers will also be discussed.

2 OFDM

In this section the main concept of OFDM transmitter and receiver will be presented. For better understanding the block diagram figures are given. The basic idea behind OFDM is the division of a high bitrate data stream into several low bitrate streams.

2.1 Transmitter

Figure 1 shows the block diagram of a typical OFDM transmitter. A binary

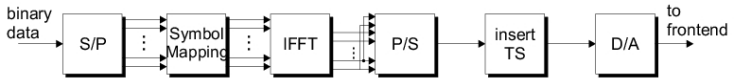

Fig. 1: *Block Diagram of OFDM Transmitter Base Band Processing*

data stream is converted from serial to parallel. After symbol mapping, the low bitrate streams are simultaneously modulated onto orthogonal subcarriers by means of the Inverse Fast Fourier Transform (IFFT). The resulting subcarriers have sinc-shaped spectra with zeros at integer multiples at $\Delta f = \frac{1}{T_s}$.

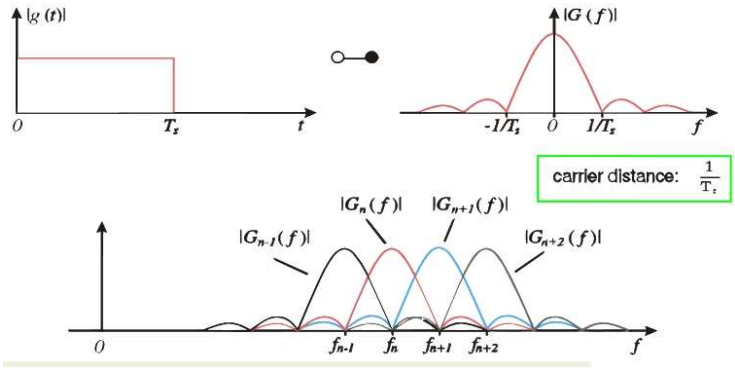

Fig. 2: *Orthogonality of OFDM subcarriers*

As a result, it is possible to put all subcarriers overlapped to each other, but such a way that the amplitude of one subcarrier is the zero values of all other neighboring subcarriers. It is shown in Figure 2. This would lead to no interference between them, which is called orthogonal. The time domain signal is generated, when all frequency domain subcarriers are passed through the IFFT block:

$$\begin{aligned} x(k) &= \sum_{n=0}^{N-1} X_n e^{jn2\pi\Delta fkT} \\ &= \sum_{n=0}^{N-1} X_n e^{jn2\pi\Delta f/f_s k} \\ &= \sum_{n=0}^{N-1} X_n e^{jn\Delta\Omega k}. \end{aligned} \tag{1}$$

If the normalized subcarrier spacing is chosen to be $\Delta\Omega = 2\pi/N$, $x(k)$ can be synthesized by means of the Inverse Fast Fourier Transform (IFFT). The cyclic prefix (CP) is added to the signal, as a method to eleminate the some effects of the optical channel (it will be explained in next section "Optical Channel"). The special Training Symbols (TS) are added for estimation of the optical channel or for synchronization of the signal sequence. The resulting signal can now be transmitted over the channel. For fiber-optical communication, the "Front end" block can directly be an optical modulator, mostly a Mach-Zehnder Modulator (MZM), or an intermediate frequency (IF) stage which will explained in a later section.

2.2 Receiver

Figure 3 shows the block diagram of a typical OFDM receiver. The front end

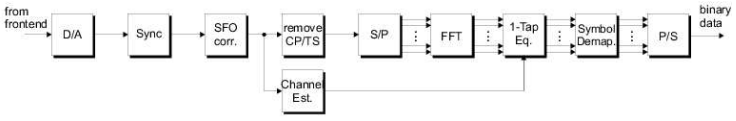

Fig. 3: *Block Diagram of OFDM Receiver Base Band Processing*

consists of an either coherent or direct detector, as will be explained in a later section. As already mentioned, the training symbols are used for signal sequence synchronization and for compensation of several elements of the optical channel. The cyclic prefix is cut off, the remaining OFDM core symbol is then transformed into frequency domain by means of FFT. The influence of the channel can now be equalized by division of every subcarrier symbol by a complex channel coefficient gained by a channel estimation based on the training symbol which is known to the receiver. Finally, the binary data is recovered after demapping of the equalized subcarrier symbols. Usually the quality or correctness of the received signal is dependent on the power of the transmitted signal and on effects of the optical physical channel.

3 Optical Channel

An optical fiber consists of a central glass core surrounded by a cladding layer whose refractive index n_2 is slightly lower than the core index n_1. Two parameters that characterize an optical fiber are the relative core-cladding index difference $\Delta = \frac{n_1 - n_2}{n_1}$ and the so-called V parameter $V = k_0 a (n_1^2 - n_2^2)^{1/2}$, where $k_0 = 2\pi/\lambda$, a is a core radius, and λ is the wavelength of light. The V parameter determines the number of modes supported by the fiber. If $V < 2.405$, it is called single-mode fiber (SMF), where only 1 mode is able to propagate.

3.1 Effects of the optical fiber

Several effects have to be considered:

Fiber losses Fiber loss is an important parameter, which shows the power loss during the transmission of optical signals inside the fiber. If P_0 is the power launched at the input of a fiber of length L, the transmitted power P_T is equal

$P_T = P_0 e^{-\alpha L}$, where the attenuation constant α is a measure of total fiber losses from all sources. Usually it is expressed in units of dB/km. The fiber loss is dependent on the wavelength of the light.

Chromatic dispersion Chromatic dispersion is a broadening of the input signal as it travels down the length of the fiber (Figure 4). It consists of both

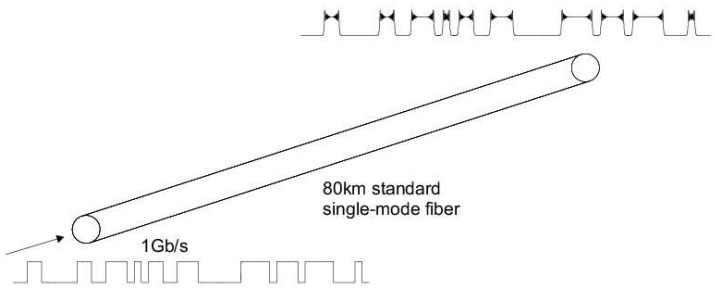

Fig. 4: *Chromatic Dispersion*

material dispersion and waveguide dispersion. Both of these phenomena occur because all optical signals have a finite spectral width, and different spectral components will propagate at different speeds along the length of the fiber. One cause of this velocity difference is that the index of refraction of the fiber core is different for different wavelengths. This is called material dispersion and it is the dominant source of chromatic dispersion in SMFs. Another cause of dispersion is that the cross-sectional distribution of light within the fiber also changes for different wavelengths. Shorter wavelengths are more completely confined to the fiber core, while a larger portion of the optical power at longer wavelengths propagates in the cladding. Since the index of the core is greater than the index of the cladding, this difference in spatial distribution causes a change in propagation velocity. This phenomenon is known as waveguide dispersion, which is relatively small compared to material dispersion.

Polarization mode dispersion (PMD) The electric field $\vec{E}$ of the electromagnetic wave can be decomposed into two transversal components which are orthogonal to each other called polarizations. In the ideal optical fiber, the core has a perfectly circular cross-section. It means that both polarized components travel at the same speed. But in real case the situation is totally different. There are random imperfections that break the circular symmetry of the fiber's cross-section, causing the 2 polarizations to propagate with different speeds. As the result, the 2 polarization components of a signal will slowly differ from each other in time, causing a delay. It is called as a differential group delay, which is shown in Figure 5. In a conventional optical transmission system, such a pulse

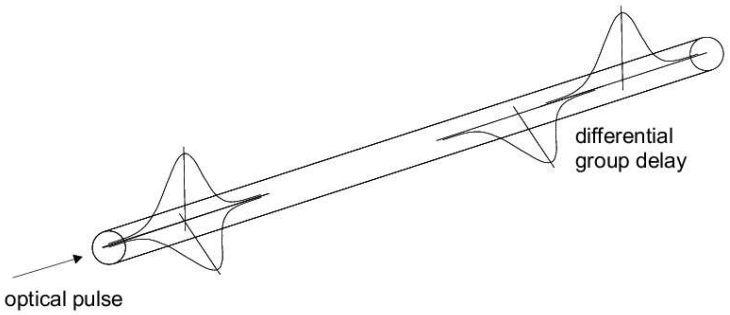

Fig. 5: *Polarization Mode Dispersion*

separation may lead to transmission impairments, especially at bit rate of 40 Gb/s and above. An OFDM system is able to equalize such a channel.

Nonlinear effects Nonlinear optics is the branch of optics that describes the behaviour of light in nonlinear media, where the dielectric polarization responds nonlinearly to the electric field $\vec{E}$ of the light. The nonlinearity is typically only observed at very high light intensities such as provided by pulsed lasers. Nonlinear effects are the consequence of interaction of the photons with the glass material of the fiber at the subatomic level. The most important effects in this context are:

- Raman scattering
- Brillouin scattering
- Self phase modulation
- Cross phase modulation
- Four wave mixing
- Photorefractive effect

3.2 Cyclic Prefix

The use of cyclic prefix, or guard interval, is the key to OFDM's ability to eliminate the inter-symbol interference (ISI) introduced by the optical channel: The chromatic dispersion (but also the Polarization Mode Dispersion) can be described by a channel impulse response, and the guard interval – the length of the cyclic prefix – has to be chosen long enough so that the transient phase at

the start of each OFDM symbol caused by channel impulse response is caught up completele. Since for optical channels, the impulse response theoretically is infinitely long, an approximation is used, the maximum propagation delay between lowest and highest subcarrier serves as an estimate for the required guard interval duration.
Non-linear effects, however are very difficult to compensate due to their dependency on the instantaneous electric field $\vec{E}$ on the fiber.

4 Detection Principles

4.1 Direct Detection

Figure 6 shows the model of a DD-OFDM transmission system employing an Intermediate Frequency concept.

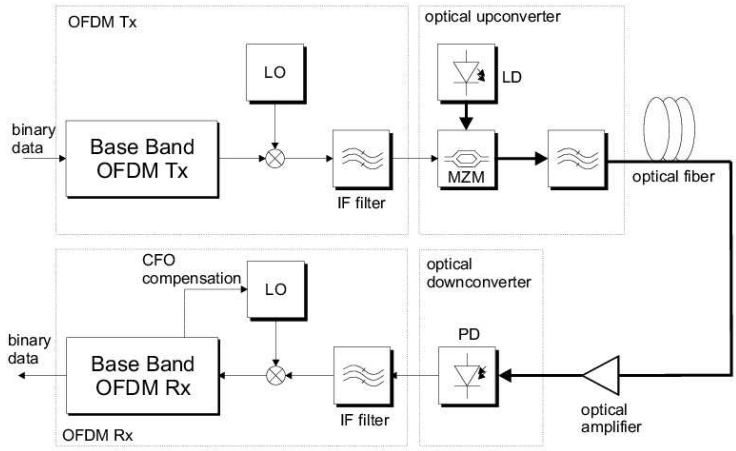

Fig. 6: *Block diagram of DD-OFDM transmission system*

After base band processing as described in 1, the complex valued time domain signal is digital to analog converted into two separate in phase (I) and quadrature (Q) branches. This analog signal is then up converted to an intermediate microwave frequency f_{RF}. Then I and Q branch signals are combined to form a real valued radio frequency OFDM waveform consisting of a band of frequencies shifted from DC.
The real valued OFDM signal is then used to modulate a laser onto an optical carrier using an Mach-Zehnder Modulator. Since Single Side Band (SSB) must be used in direct detection due to cancellation effects that might occur,

the output of optical modulator is filtered by an optical filter to remove the lower or upper sideband. The band after optical modulator and filter is shown in Figure 7 (left). It can be seen that the lower side band is suppressed by the optical filter. This band must be placed at a special gap from the carrier with the same width B as the signal itself. This is necessary because after the square law detector in the receiver (Figure 7 right) the intermodulation products fall in this band so the OFDM signal must be displaced from these distortion terms.

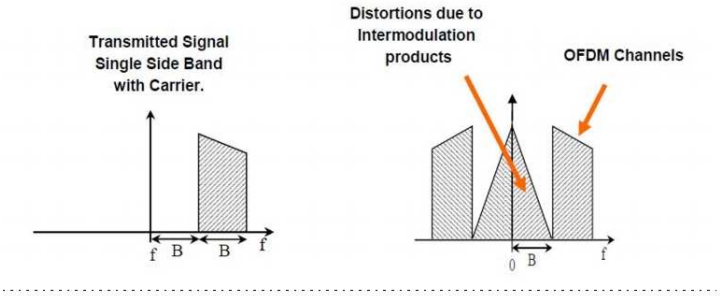

Fig. 7: *Transmitted and detected signals in Optical OFDM with SSB*

At the receiver end the optical signal is detected with the help of a photo diode that detects the instantaneous optical power and output an electrical waveform proportional to this quantity. This wave form is converted into I and Q components by mixing with radio frequency f_{RF} local oscillator. After analog to digital conversion, FFT operation is performed to transform the OFDM time domain signal into OFDM subcarriers, as already described in 3.

4.2 Coherent Detection

Figure 8 shows a conceptual diagram of a complete CO-OFDM system. The function of the optical upconverter in transmitter is to linearly shift the OFDM spectrum from the RF domain to the optical domain, using a single optical Mach-Zehnder modulator (MZM). At the receiver side, the received signal is first passed through an optical downconverter, which consists of a pair of balanced photodetectors. It is very critical to use an optical bandpass filter before the photodetectors to eliminate interference and optical noise from the image frequency to the OFDM spectrum. The signal entering the OFDM receiver is further downconverted to base band with RF IQ demodulation, sampled with sampling rate in the observation period, and the received information symbol for each subcarriers is extracted after performing FFT [BH07].

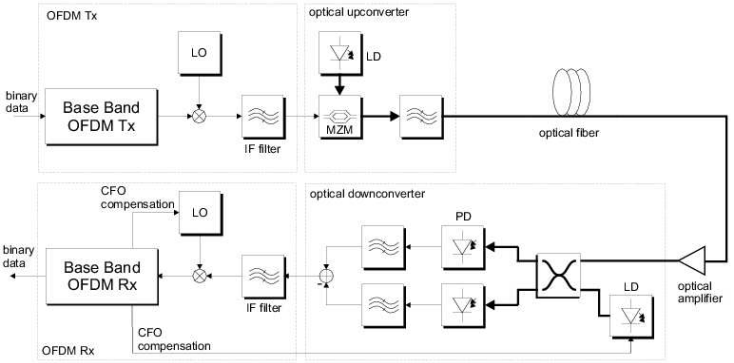

Fig. 8: *Conceptual diagram of complete CO-OFDM transmission system*

5 Introduction to Synchronization

Synchronization is an important issue in all communication systems. For OFDM the synchronization requirements are even more strict because the loss of synchronization can bring some negative effects such as loss of orthogonality. Usually there are 3 options which are necessary to be fulfilled:

- **Symbol timing:** The start of the OFDM core symbol has to be known. If the synchronizer estimates that the useful part of the symbol starts at any time within the guard interval, then there is no effect to performance. However, if synchronizer estimates that the start of the symbol is outside of the guard interval, there will be a decrease in signal energy and an increase in interference. This occurs because samples from the previous or next symbol are input into the FFT along with samples from current symbol.
- **Carrier frequency offset (CFO):** The local oscillator at the transmitter and receiver will usually not generate exactly the same frequency, and this difference can lead to degradations in demodulating the signal at the receiver. A carrier frequency offset f_o causes a phase rotation ϕ, which shows the rotation of constellation.
- **Sampling frequency offset (SFO):** The sampling rate for the A/D converters at the receiver may be different than the rate for the D/A converters at the transmitter. Because these oscillators can be accurate to a factor of about 10^{-5}, the difference in sampling rate is typically much less that one sample per OFDM symbol. Because the deviation from the correct sampling rate is very small, there is not much distortion caused by the FFT, but there will be some phase rotation from one symbol to next,

which linearly accumulates. In case of many symbols, this phase rotation can accumulate so much that it will cause errors in decoding the data.

There exist many different methods for synchronization, but the one best trade-off between performance and complexity is the Schmidl algorithm [SC97]. The symbol timing estimation relies on searching for a training symbol with two identical halves, which will remain identical after passing through the channel, except that there will be a phase difference between them caused by the carrier frequency offset. The property that two halves have correlation between each other, is employed for detection of the begin of the symbol. The two halves of the first training symbol are made identical by transmitting a pseudo-noise (PN) sequence on the even frequencies, while zeros are used on the odd frequencies. The second training symbol contains a PN sequence on the odd frequencies to measure these subchannels, and another PN sequence on the even frequencies to help to determine frequency offset. The resulting time domain OFDM symbol structure is shown in Figure 9.

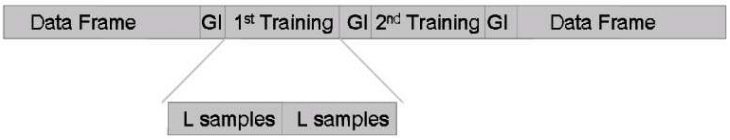

Fig. 9: *Schmidl's Training Symbols*

6 Conclusion

In this paper, the basics of optical OFDM were discussed. The schematic representations of transmitter and receiver were shown and their components were explained. The applicability of OFDM to high speed transmission in optical fiber due to its ISI elimination capability was motivated. The characteristics of optical channel have been presented. The dispersion introduced by the optical fiber causes a broadening of the input signal. Employing the cyclic prefix in OFDM, it is possible to combat dispersion and allow simple equalization. Furthermore, 2 different receiver concepts were presented and compared. Finally, an introduction to synchronization issues in optical OFDM has been given.

References

[BH07] H. Bao and H.Haunstein. Coherent Optical Orthogonal Frequency Division Multiplexing. *Opt.Express*, 15:4410–4418, 2007.

[JMS+08] S. L. Jansen, I. Morita, T. C. W. Schenk, N. Takeda, and H. Tanaka. Coherent optical 25.8-Gb/s OFDM transmission over 4160-km SSMF. *JOURNAL OF LIGHTWAVE TECHNOLOGY*, 26(1):6–15, 2008.

[SC97] T. M. Schmidl and D. C. Cox. Synchronization Algorithm for Wireless Data Transmission using Orthogonal Frequency Division Multiplexing. *A Dissertation at Stanford University*, pages 1–129, 1997.

[SvdHFS07] T. C. W. Schenk, R. W. van der Hofstad, E. R. Fledderus, and P. F. M. Smulder. Distribution of the ICI term in phase noise impaired OFDM systems. *IEEE Trans. Wireless Commun.*, 6(4):1488–1500, 2007.

QoS Aware Routing for Wireless Ad Hoc Networks

Q. Mushtaq, C. An, K. Kuladinithi, A. Timm-Giel, C. Görg
TZI/Mobile Research Centre, University of Bremen
{qm,chunlei,koo,atg,cg}@comnets.uni-bremen.de

Abstract

Routing protocols designed for ad hoc networks enable a node to communicate over a longer distance through multi-hops. The available routing protocols always strive to make multi-hop route between the source and the destination through the lowest possible hop count. However, the lower hop count cannot always guarantee the higher throughput if the link quality among the nodes is degrading. In such situations, routes with higher hop count may give better throughput. In this work, standard ad hoc routing has been improved by discovering the paths with better link quality to provide better application performance. The mostly used reactive protocol of AODV (Ad hoc On-demand Distance Vector) routing is modified to incorporate link quality when discovering routes as a deciding parameter in addition to a lower hop count. The Quality of Service (QoS) requirements are considered in order to satisfy the user requirements in terms of throughput, packet loss rate, end-to-end delay etc. The proposed protocol, called as QoS AODV (QAODV), is implemented and tested for performance against AODV in a real test-bed setup with mobility. Experiments show improved performance compared to original AODV in terms of throughput and delay.

1 Introduction

Wireless ad hoc communication is suitable for some environmental conditions where there is no possibility of using wired or infrastructure based communications. However, the performance in wireless multi-hop networks, especially with mobility is still an open issue. The ease of setting up and operating makes these protocols attractive in different applications where networking infrastructure is not available. Mobile workers in a factory can reap multiple benefits and improve their work processes accessing the IT infrastructure. Deployment of

IEEE 802.11 based ad hoc WLAN networks is a feasible method of providing connectivity to access the IT infrastructure. This work is carried out within SiWEAR[1] project funded by the German Ministry of Economy and Technology (BMWi) in the framework of the SimoBIT initiative. The main focus of the project is the improvement of work processes by secure wearable information and communication technology in production. This paper investigates the required communication technologies, specifically focusing on how to improve the performance of ad hoc networking in a vehicle production environment.

In this work, standard ad hoc routing has been improved by detecting and selecting the paths with better link quality to provide better application performance, especially considering situations where the user is mobile. When multiple paths are available between the source and destination, the shortest hop count is considered as the selection criteria for most of the standard ad hoc routing protocols. This criterion only assures better throughput and lower delay between the source and destination, if the link quality of each link is good. This is idealized environment may not be true in most cases due to different distances between nodes result in different Signal-to-Noise Ratios (SNR) and different noise sources might affect the quality of some links. Furthermore in a mobile environment, the link quality varies with node movements. A bad link quality (lower SNR) leads to degraded application throughput giving higher delay. In such cases, selecting the path with higher hop counts but with better link quality improves the application performance.

Therefore, this work proposes a solution on adding QoS parameters to the existing ad hoc routing protocol. The discovered routes are evaluated periodically and better routes are discovered when the SNR goes beyond a predefined threshold. Nodes in the network are able to monitor the SNR values to their neighbors. The proposed solution is implemented based on the IETF standardized AODV (Ad hoc On-demand Distance Vector) routing protocol [Per00, PBRD03]. Therefore, this proposal is termed as QoS AODV (QAODV).

This paper is structured as follows. The next section gives an overview to the existing research done in improving the quality of the route discovery process in ad hoc networking. The fourth section details the protocol description of the QAODV. The fifth section discusses the detailed performance analysis of QAODV taken in a real test-bed environment with mobility of nodes. Section 6 concludes the paper.

[1] www.simwear.de

2 Related Work

There are many proposals suggesting how to enable the QoS awareness to the existing mobile ad hoc routing protocols. Each method has its own merits and demerits in attempt to provide QoS. Most of these approaches take AODV as the basic routing protocol, and then modify to incorporate QoS.

An approach in [Fan04], considers a unique parameter to meet QoS in ad hoc networks. The MAC delay is proposed as a routing metric. MAC delay of a packet is defined as the time it takes to send a packet from a sender to receiver and plus the time to receive the acknowledgement at the MAC layer. The lower MAC delay is desirable for high performance. It is a parameter, which is useful to identify congested links. The network layer uses this information to discover a better route avoiding the congested links. [CN99] proposes to use the maximum tolerable end-to-end delay as the QoS metric. Minimum required capacity is used in [LL99] and maximum tolerable Packet Loss Ratio (PLR) is used as a QoS metric in [WK05] to meet the QoS requirement in wireless ad hoc networks.

The approach discussed in [TWT06] suggests using the link quality of the path as a criterion to select the route in addition to the minimum hop count. The simulation results in [TWT06] show that path with better link quality has a lower packet loss as compared to a shorter path with bad link quality. This proposal is similar to QAODV proposed in this work. However, only simulation results are available in [TWT06], without any real implementation. QAODV is implemented and tested in real test-bed for scenarios considering the mobility. [TWT06] avoids the creating of routing loops by appending a list of the IP addresses of intermediate nodes, through which a RREQ has already passed. In QAODV, a different approach is used to avoid loops during propagation of the RREQ in route discovery process. The approach restricts each intermediate node to forward a RREQ only if, it is the first one or is better than the one already forwarded. The initiation of route repair is also different from the one suggested in [TWT06]. The formula presented there, to find whether a route repair should be triggered, creates computational overhead. In QAODV, a simple mechanism is followed to eliminate this overhead. QAODV waits for a predefined number of consecutive link quality values below a predefined threshold to trigger a new route repair.

3 QoS Awareness in AODV (QAODV)

The use of link quality information into the standard AODV protocol incorporates the QoS awareness to AODV protocol [PBRD03]. In this work, AODV protocol has been modified to select a path based on link quality information

in addition considering the lower hop count of the path. The discovered routes are evaluated periodically and the better routes are discovered when the link quality goes beyond a predefined threshold. Therefore, in addition to the new route discovery process, AODV operations have also been extended to evaluate the existing routing paths periodically.

3.1 QAODV: Path Selection

When a source node wants to communication with a destination node, for which it does not have a route in its routing table, it initiates a route discovery process similar to the standard route discovery in AODV. Since, the route selection is also based on link quality information; this information has to be carried out with the RREQ packet. Therefore, a 8-bit field is appended in the standard RREQ packet called RREQ_SNR. The value of RREQ_SNR is initially set to 255 before broadcasting by the source. Each node in the network is configured to calculate the link quality to the neighboring node upon receiving data/control packet from it. The local routing tables for each node also have a field to store RREQ_SNR.

Upon receiving a broadcasted RREQ, the intermediate node compares the current value of RREQ_SNR to the calculated value of SNR to its neighbor. The lowest among the two is written in the local routing table. Moreover, this smaller value is also updated in the RREQ_SNR. The result of this mechanism is that the smallest value of SNR in the path reaches the destination node. The RREQ packet is rebroadcasted by the intermediate nodes only if the destination node for the RREQ is unknown and the updated value of RREQ_SNR higher than the SNR value in the local routing table for this destination.

The conditions above make sure that the RREQ is propagated from all the possible routes to the destination. This is helpful in providing the destination node with all the possible options to connect to the source node. The destination node upon receiving a RREQ starts a timer to wait, for a predefined time, to receive the RREQ packet propagating through all the other possible routes from the source to the destination. The destination node selects the RREQ with the highest value of RREQ_SNR. After the expiry of the timer, the RREP is sent to the selected RREQ. The intermediate nodes guide the RREP to reach back to the source using the best path. The source node upon receiving the RREP can start communicating with the destination using the newly found path.

3.2 QAODV: Path Evaluation

The performance of the discovered best path may degrade at any point of time, especially when the nodes are moving. Therefore, QAODV introduces a periodic evaluation of the link quality of currently used path. In this process, a new search for a better path is initiated upon detecting the link quality degradation the currently used path. The current routing path does not change until there is a better route found.

At the network layer, each node periodically measures its SNR with immediate neighbors during the data transmission. If any node in the existing route can experience degradation in the link to its neighbor and if it goes beyond a predefined SNR threshold, this node should initiate the path evaluation process, called as route repair. Upon detecting the degrading link with immediate hop, an intermediate node should send a route error message [PBRD03] to the upstream neighbor, which further forwards it to the source or the destination node. Those nodes then can initiate a route repair process similar to a new route discovery. If the destination or source detects the degradation of link quality, those nodes themselves can start the route repair process. The main difference between the route repair and route discovery process is that the route repair is done while using the existing route. This helps to make the new route before breaking the existing route. The degradation is defined to be that a predefined number of consecutive samples of SNR values are lower than a predefined threshold. Fig. 1 shows the flowchart for the path evaluation process.

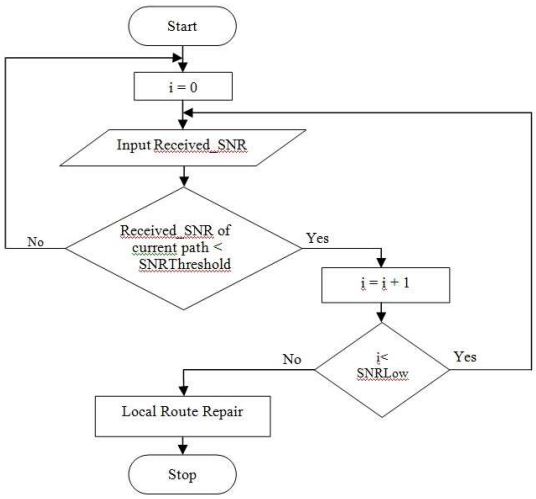

Fig. 1: *Path Evaluation Process*

QAODV concept described above is implemented by extending the AODV implementation by Uppsala University called AODV-UU[2] . The link quality is measured using the Linux command called iwspy. This command is able to calculate the values of both signal and noise as any packet is received by the sender. Each sender is uniquely identified by its MAC address. Mainly, the route discovery process of AODV-UU is modified and new functions are added to evaluate the paths in QAODV routing. The current implementation of QAODV does not support the path evaluation process initiated by intermediate nodes.

4 Analysis of Results - QAODV and AODV

The performance of AODV and QAODV is evaluated in two different test-beds to evaluate the behavior of UDP and TCP protocols. A brief description of each test bed setup and then the results are explained in the next subsections. The major difference between QAODV and AODV is the criteria for selection of the route between the source and the destination. AODV always finds and connects to the route, which has the lowest possible number of hops, whereas QAODV prefers good link quality. AODV is realized by using the original AODV-UU software.

4.1 First Test-bed Setup

The test bed setup shown in fig. 2 is used to demonstrate the principle of QAODV, i.e. to use link quality as the selection criteria. There are five identical laptops used in this test bed scenario. The source node, S wants to establish a connection with destination node D, over the intermediate nodes A, B and C. In this setup, node A is unable to hear node C and D and node B is unable to hear node C and S.

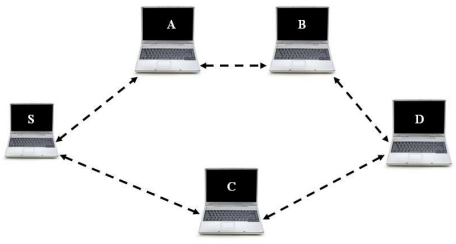

Fig. 2: *First Test Bed with Two Routes*

[2]http://moment.cs.ucsb.edu/AODV/aodv.html#Implementations

Since the link quality to C from S and D are very good and having lower hop counts, both AODV-UU and QAODV connect node S and D via intermediate hop C (S-C-D). However, as node C is moved away from node S and D, the link degradation at certain point establishes a route from S to D via A and B (S-A-B-D). This route is taken only by QAODV, whereas AODV-UU continues to keep the initial connection, even with very low link quality. AODV-UU only switches to the other longer hop count route (S-A-B-D) in case of C becomes out of reach for node D or S.

Iperf tool is used to generate the UDP and TCP applications. The experiments, repeated 6 times, show better performance of QAODV over AODV-UU, in terms of TCP throughput, UDP throughput and the UDP packet loss rate. Table 1 and Table 2 show the statistical analysis of all the six experiments carried out to analyze the both TCP and UDP behavior.

Exp. Nr.	*AODV-UU*			*QAODV*		
	Avg. Throughput (kbps)	*Delay (ms)*	Packet Loss (%)	*Avg. Throughput (kbps)*	*Delay (ms)*	Packet Loss (%)
1	944	594.9	12	1490	2.309	0.86
2	1110	83.4	6.3	1490	2.551	0.67
3	906	62.02	10	1490	2.008	0.59
4	1240	4.817	12	1490	3.511	0.91
5	1250	22.00	4.5	1490	1.909	0.59
6	1120	955.15	16	1490	2.145	0.83
Avg	***1095***	***287***	***10.1***	***1490***	***2.40***	***0.74***
Std. dev	***144.5***	***395***	***4.19***	***0***	***0.58***	***0.14***

Tab. 1: *Statistical Analysis of experiments for UDP performance in first test-bed*

Exp. Nr.	*AODV-UU*		*QAODV*	
	Avg. Throughput (kbps)	*Total (Mbytes)*	*Avg. Throughput (kbps)*	*Total (Mbytes)*
1	996	16.2	1900	27.6
2	996	16.3	1910	27.5
3	1020	17.1	1890	27.7
4	899	15.5	1960	28.3
5	925	15.9	1950	28.2
6	999	15.8	1940	28.1
Avg	***972***	***16.1***	***1925***	***27.9***
Std. dev	***48.4***	***0.55***	***28.8***	***0.34***

Tab. 2: *Statistical Analysis of Experiments for TCP performance in first test-bed*

4.2 Second Test-bed Setup

The second test bed presents a more real life scenario for mobile workers, shown in Figure 3. This shows the placement of the nodes at the different points of the floor plan. The source nodes S and the intermediate nodes A, B and C are stationary whereas the destination node D moves along the path shown by dashed lines. The source node uses the intermediate nodes to communicate with the destination node D. The number of intermediate nodes used to establish a route depends upon the location of the D during its mobility.

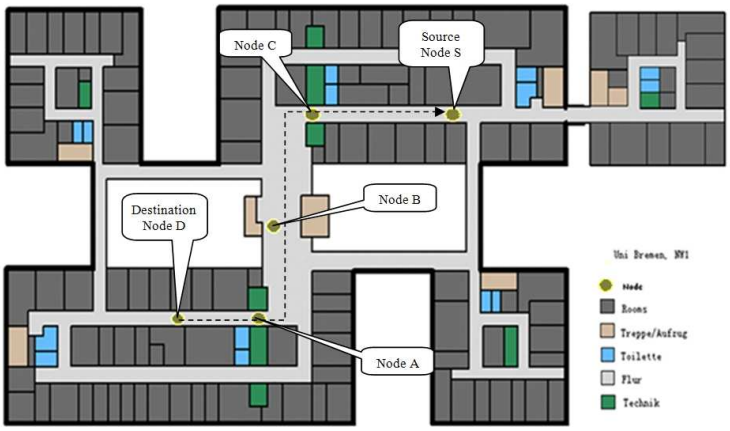

Fig. 3: *Floor Plan of Second Test-bed*

The results of multiple tests carried are presented in Table 3 and Table 4.

Exp. Nr.	*AODV-UU*			*QAODV*		
	Avg. Throughput (kbps)	*Delay (ms)*	Packet Loss (%)	*Avg. Throughput (kbps)*	*Delay (ms)*	Packet Loss (%)
1	418	0.165	15	434	0.115	3.6
2	367	0.215	10.9	440	1.011	1.7
3	411	0.172	9.5	484	0.210	2.4
4	372	0.210	19.9	433	0.160	2.4
5	349	0.230	10.1	496	0.392	0.95
6	364	0.101	27	453	0.200	1.3
Avg	***380.1***	***0.182***	***15.4***	***456.6***	***0.348***	***2.05***
Std. dev	***27.7***	***0.04***	***6.9***	***27.05***	***0.338***	***0.95***

Tab. 3: *Statistical Analysis of experiments for UDP performance in second test-bed*

Exp. Nr.	*AODV-UU*		*QAODV*	
	Avg. Throughput (kbps)	*Total (Mbytes)*	*Avg. Throughput (kbps)*	*Total (Mbytes)*
1	1130	27.0	1590	38.1
2	996	23.9	1360	32.6
3	959	23.0	1450	34.8
4	912	21.9	1670	40.2
5	858	20.6	1480	35.4
6	868	20.8	1440	34.5
Avg	***953.8***	***22.9***	***1498.3***	***35.9***
Std. dev	***101.1***	***2.4***	***112.32***	***2.7***

Tab. 4: *Statistical Analysis of Experiments for TCP performance in second test-bed*

Fig. 4 details the performance of TCP when using AODV-UU in one of the test runs. Initially, node D is connected with node S through a three hop connection (S-C-B-D). The degradation in the SNR values does not initiate any route discovery until there is a complete disconnection at the link layer. When D is moving towards S, a new path is found that is a direct connection (S-D) after a complete disconnection with node B. Fig. 4 shows that the TCP throughput is very low during the node D has very low SNR before finding the direct hop connection.

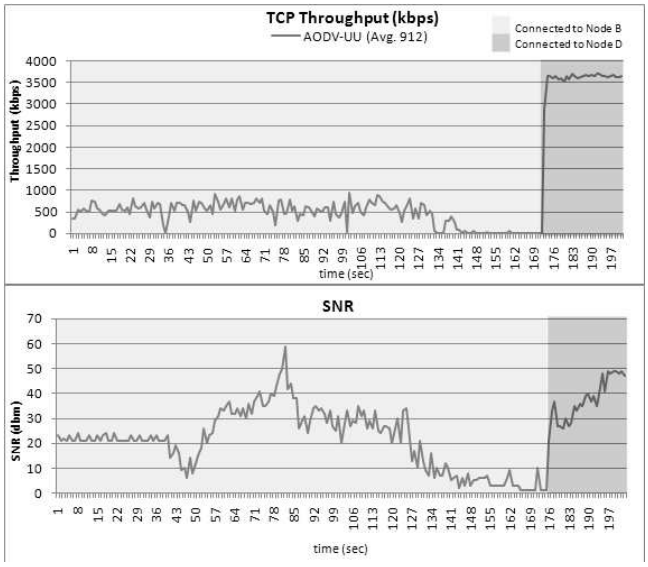

Fig. 4: *Test run Results for TCP Performance in second test-bed using AODV-UU*

Fig. 5 shows the performance of TCP when using QAODV as ad hoc routing for the same scenario. In this case, initially, the node D is connected with node S through a four hop connection (S-C-B-A-D). When D is moving towards S, the SNR values of the link (D-A) starts to decrease and the path evaluation process of QAODV triggers to discover a better route after the SNR values goes beyond a predefined threshold. The better route in this case turned out to be a three hop connection (S-C-B-D). A similar degradation is experience in the link (D-B) which forces to initiate the 3rd route repair. This leads to finding the direction connection as the best path between S and D. Compared to AODV-UU, QAODV does 2 more route changes in the same set up. Though there are more route discoveries, fig. 5 shows that the throughput that can be achieved with QAODV is more compared to AODV-UU. And also, TCP communication is not interrupted as a better path is in process of being found since QAODV uses make before break approach during the route discoveries. This leads to uninterrupted TCP transmission and ultimately leads to higher average throughput.

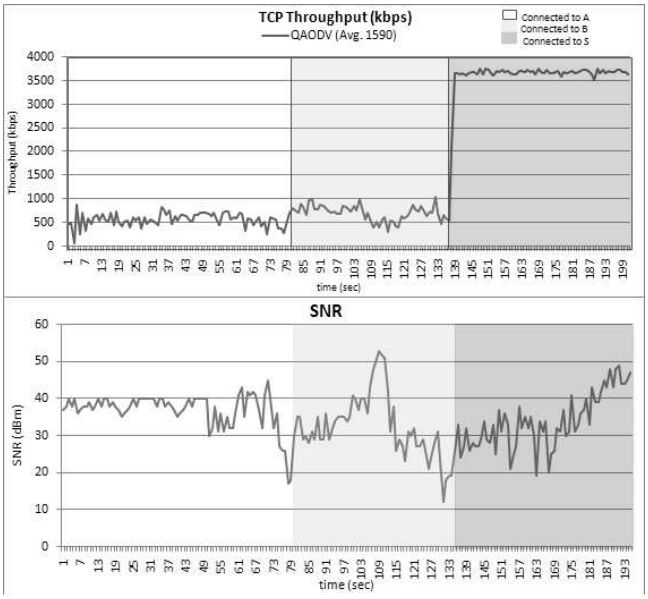

Fig. 5: *Test run Results for TCP Performance in second test-bed using QAODV*

Similar to TCP performance, fig. 6 and fig. 7 show how UDP throughput varies when using AODV-UU and QAODV ad hoc routing protocol. The UDP transmission during bad link quality resulted in higher packet loss. The average UDP throughput and packet loss are lower when using QAODV.

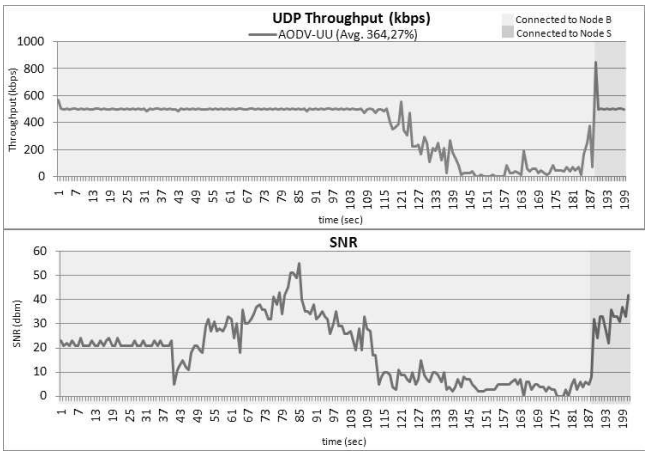

Fig. 6: *Test run Results for UDP Performance in second test bed using AODV-UU*

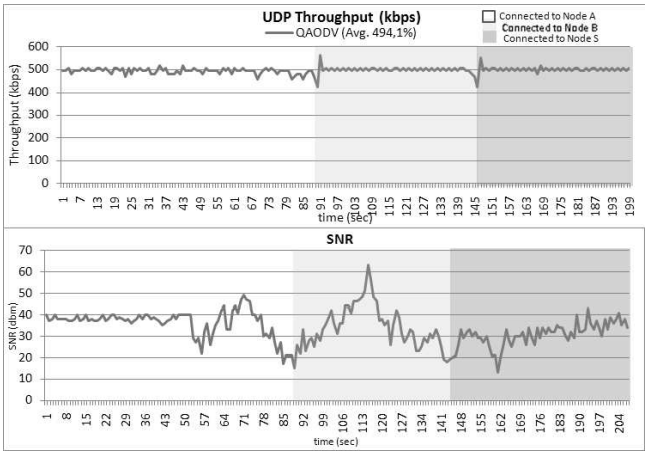

Fig. 7: *Test run Results for UDP Performance in second test-bed using QAODV*

5 Conclusion

In this paper, a solution is proposed to guarantee QoS for wireless multi-hop ad hoc networks. The popular reactive ad hoc routing protocol, AODV, is modified to incorporate the consideration of link qualities to choose the best path among all the available. Modifications in the route discoveries enable exploring all the possibilities of a route from a source to the destination. The destination can decide to select a path based on, not only the current standardized criteria, but also the link quality. The results are taken in a real test-bed

environment. QAODV shows promising improvement compared to AODV in mobile scenarios. The better performance of QAODV is due to reacting quickly to link quality degradation, which is not supported in the standard AODV. Although the decision to choose the best route is based only on SNR values in the current proposal (in addition to standardized criteria), an extension can be made to include other QoS parameter of interest such as minimum throughput and end-to-end delay. The improvement of the proposed QAODV solution with more parameters will be considered as further work. However, the overhead in considering more parameters has also to be kept in focus when incorporating improvements.

Acknowledgement

This work has been partly funded by the German Ministry economics and technology under contract 01MB07029A. The authors are responsible for the content.

References

[CN99] S. Chen and K. Nahrstedt. Distributed quality-of-service routing in ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 17(8):1488–1505, Aug 1999.

[Fan04] Z. Fan. Qos routing using lower layer information in ad hoc networks. In *15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, volume 1, pages 135–139, Sep 2004.

[LL99] C.R. Lin and J.S. Liu. QoS routing in ad hoc wireless networks. *IEEE Journal on Selected Areas in Communications*, 17(8):1426–1438, Aug 1999.

[PBRD03] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-demand Distance Vector routing, 2003. Request For Comments (Proposed Standard) 3561, Internet Engineering Task Force.

[Per00] C.E. Perkins. *Ad Hoc Networking*. Addison-Wesley, 2000.

[TWT06] H.-M. Tsai, N. Wisitpongphan, and O.K. Tonguz. Link-quality aware ad hoc on-demand distance vector routing protocol. *Wireless Pervasive Computing*, page 6, 16-18 Jan 2006.

[WK05] M. Wang and G.S. Kuo. An application-aware QoS routing scheme with improved stability for multimedia applications in mobile ad hoc

networks. In *Proc. IEEE Vehicular Technology Conf.*, pages 1901–1905, Sep 2005.

Telco Enabled Social Networking: Russian Experience

Manfred Schneps-Schneppe
Ventspils University College, Latvia
manfreds.sneps@venta.lv

Dmitry Namiot
Moscow State University, Russia
dnamiot@abavanet.ru

Abstract

The paper relates to the 7FP ICT topic concerning intelligent content and semantics. The aim of paper is a search for research partners in this field. Our main goal is to change the paradigm relating to the voice data usage in web applications. The idea is seamlessly integrate telecom data (voice) into web applications. We are planning to add new software applications to Asterisk for content providers. The document is exampled by mashup service for fixed line phones - audio-records collected right from phones being mapped on the Google Maps.

Keywords
Open source, telephone exchange, Web 2.0, mashup, Google Maps API, geo tagging

1 Introduction

The paper relates to the 7FP ICT topic concerning intelligent content and semantics. The aim of paper is a search for research partners in this field. Our main goal is to change the paradigm relating to the voice data usage in web applications using Web 2.0 technology, namely: support user-generated content by well known techniques: Ajax-based rich Internet application techniques, semantically valid XHTML and HTML markup, folksonomies (in the form of tags), REST (Representational State Transfer) Web APIs, mashups merging content

from different sources, etc. In telecommunication applications, Web 2.0 technology corresponds to Telco 2.0 and Mobile 2.0 [SSN08] containing the essence of online social networks.

A social network service uses software to build online networks for communities of people who share interests and activities or who are interested in exploring the interests and activities of others. Most services are primarily web based and provide a collection of various ways for users to interact, such as chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups, and so on. We are looking for medical applications, namely: cared living for handicapped and elderly inhabitants.

To attract user-generated content we need open programming interfaces. And it is what we do from the very foundation of AbavaNet company [NSS04]. As a nearest and newiest prototype of our research could be named British Telecom experience on open APIs for the 21th century network [McK07]. The Web21C SDK is a set of libraries that makes it simple for developers to consume Web Services exposed by BT. The Web21C SDK provides the developer with a simple object model to interact with. The Web21C SDK provides the following functionalities: Short Message Service (SMS), Voice Call service, Conference Call service, Presence service (allows the application developer the ability to store and retrieve an individual's current status and availability for communication), Authentication service (allows the application developer to create and control an authentication realm for their application), Information About Me (IAM) service (allows the application developer a way to store and retrieve data about an individual in key value pairs), Location service (allow the application developer to add the ability to determine the geographic location (latitude, longitude, altitude) of a mobile device).

2 The main idea of the proposal

The current trend for content management dictates the growing role of multimedia data. Another obvious tendency is integration. Customers (users) should be able do deploy all the available channels for content distribution and delivery. Our main area of interest during our professional activity has been related to telecom applications. Our main goal is to change the paradigm relating to the voice data usage in web applications. The idea is seamlessly integrate telecom data (voice) into web applications. Such achievement seriously explodes the possibility for social services. Just one simply explanation: all the mobile phones become the main devices for posting/getting data from new services.

We are planning to add new software applications to Asterisk using our application server Abava Gateway (Fig 1). Asterisk provides a central switching

core, with four APIs for modular loading of telephony applications, hardware interfaces, file format handling, and codecs. It allows for transparent switching between all supported interfaces, allowing it to tie together a diverse mixture of telephony systems into a single switching network. And what is very important in the context - Asterisk is free open source software. Until now Asterisk is used (reviewed) mostly in the traditional telecom sense - as a free replacement for the traditional PBX. But by our opinion it could be (and should be) used mostly as a software service integrates voice data into modern Web 2.0 applications (Figure 1). We are planning to introduce new software for service development as well as pre-build services for Asterisk. Service development tools will allow new development for non-telco oriented staff. We are planning to convert telecom development into web development. Telecom domain tasks will be converted right into Web domain tasks. Merging telecom and web applications makes our proposal unique. We are not offering a new development tools for the concrete programming language but targeting the whole platform.

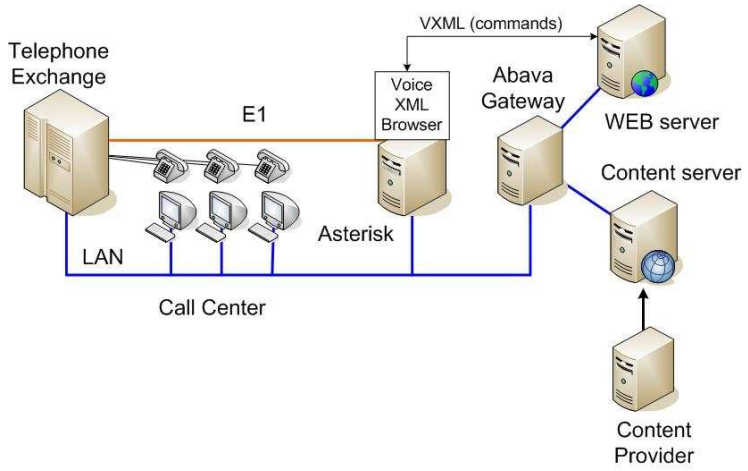

Fig. 1: *Application server Abava Gateway plays middleware role between real-time telco world including IP-PBX Asterisk and call center functionality, from one side, and internet world with content providers based on web services, from another.*

Our idea is to bring web developers into PBX programming world. As seems to us it is more than ambitious goal. Web development and Telecom development exist in parallel. For reaching this goal we are going to deploy a set of new Java based tools for Asterisk. Using Java let anyone the ability to extend our own tools in the future. But again our primary goal is not add new Java based tools. The idea is to completely change the way telecom services are developed. We are intending to bring telecom stuff right into web development world via scripting languages, typical for web development and via pre-build set of widgets for the mail telco-related tasks.

3 Current stage of the research

Our own experience and extensive market study shows the two groups of applications around the open source PBX: completed applications (e.g. call centers, messengers etc.) and embedded solutions on the base of PBX. Nobody actually targets web developers as potential customers for telecom platform. But most the applications developed nowadays are actually web applications. And corporate development anyway is unable to create all the potentially demanded applications. So the key issue for adding telco to existing and future social networks is to satisfy web development crowd with simply tools let them deploy telecom enabled applications without any expertise in telecom world.

The main area of interest during our professional activity has been related to telecom applications following Parlay/OSA concept [SSNZ06]. These applications are carried on in cooperation with Ericsson, Iskratel and other operators and vendors. The following are several Mobile 2.0 services available currently by means of Russian operator AudioTele (Fig 2):

1) Voice mail. Access will be provided via IVR interface and via the web. Voice mail server will provide also an open API for access to voice mail from third party web sites.
2) Automation voice info. User-defined voice fragments.
3) Voice Recorder. To record and publish voice messages.
4) Call to Web. Telecom mashup lets you accept voice calls in any web application. Application will receive recorded calls as ordinary HTTP callback requests. One of the most interesting approaches developed by AbavaNet. Really integrates phones and web.
5) Pay call. Navigation through web site confirmed by the call. The idea is to allow site navigation only after the call to some premium call number. Could be integrated with any web-site via Ajax interface.
6) Voice SMS. Service combines voice messages and SMS notifications [Mob07].
7) Network microphone. Lets you record voice messages and automatically publish them on the public web site.
8) Voice blog. This service lets you publish voice messages to blogs. Service deploys public API's available from the popular blog platforms.

For more detail see "AbavaNet" web resources: http://www.abavanet.ru/, http://abava.blogspot.com/, http://www.linkstore.ru/.

Let's give two concrete examples of the applications of the work proposed: 1) embed access to voice mail right into concrete web page. It is a typical example of integration. Threat voice mail data as an ordinary content the web scripts dealing with, 2) process incoming calls as ordinary HTTP requests in CGI (common gateway interface) scripts. This feature creates the ability to

program telecom applications as standard CGI script all web developers are familiar with.

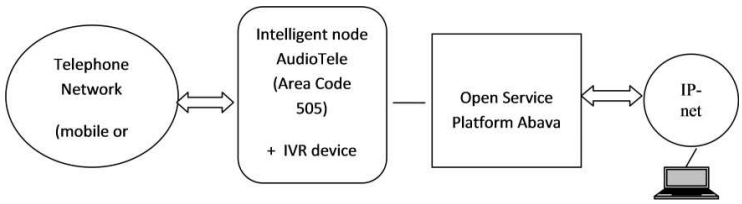

Fig. 2: *Implementation of Open Service Platform Abava for user generated content delivery (in the framework of above listed services and Intelligent node AudioTele).*

4 The problem be solved

We are planning to convert telecom development into web development. Telecom domain tasks will be converted right into Web domain tasks. Our study shows that this area is relatively empty at this moment. And of course the question step after the standard voice connection is how to program services for PBX. So our extensive background in the J2EE standards as well as in the Open telecommunication protocols lets us suggest a simple and useful approach for the developing applied services on the Asterisk. That project includes the following tasks:

- introduce Java libraries for developing Asterisk scripts right in JSP (web scripting technologies)
- add custom JSP tags for Asterisk based development
- prepare manuals and examples for access to Asterisk platform from various popular web frameworks
- prepare widgets for the main telecommunication tasks
- implement Voice XML and CCXML over Asterisk scripts particularly for personalized IVR with semantic Web features

XML based languages are completely independent of programming systems. So it is a way we will bring PBX development into web world. At this moment we can list the following Java oriented sub-tasks for the planned consortium members:

1. system support for Asterisk scripts integration
2. custom JSP tags for Asterisk scripts
3. widgets for scripts
4. CCXML implementation
5. VXML implementation

6. Service examples implementations
7. Preparing manuals and documents

5 Example. Geo tagging for fixed line phones

Let's give an illustration of our approach. The following describes a mashup service for fixed line phones - audio-records collected right from phones being mapped on the Google Maps. The idea is very simple: for the fixed line phones we know the location of the phone. So voice messages recorded by phone could be geo tagged (connected to the map) for the future access either from the net. Internet users can collect messages for the selected area or download automatically created podcast for that area. Phone users can call and listen messages by the geo proximity. Phone users can also reply to the messages without discovering the original (author's) phone. So with this application we can provide Web 2.0 (or Telco 2.0) service (actually - the class of services) that mixes internet and telephony.

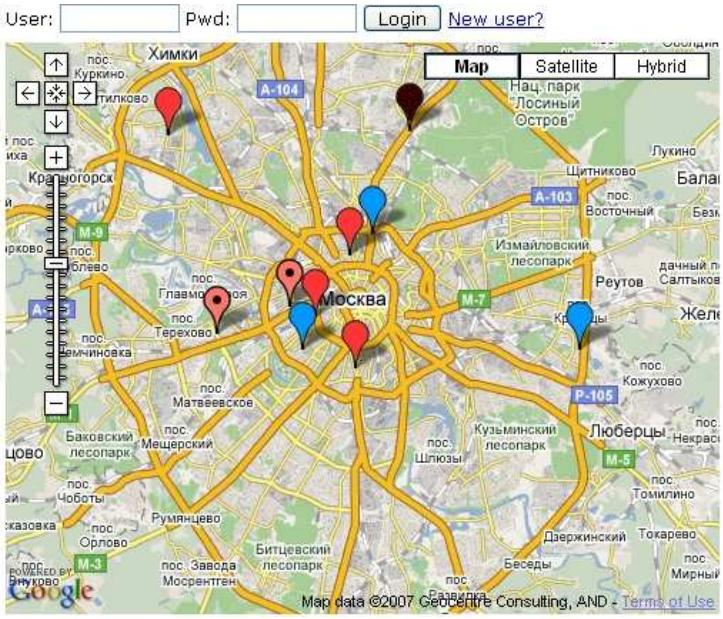

Fig. 3: *Moscow map right from Google Maps. Markers there show some user-generated voice messages.*

The fixed line phones can actually have one advantage over mobiles (at least from the point of view services) - the location of customer is known. The features that are getting available in the mobile world via Location Based services and

API's could be deployed in the fixed line world much more easily. The service (actually as we will describe below - the whole class of services) deploys the very simple idea - as soon as we are getting call we know (at that moment) where to find the originating party of this call. And "where" here means the location in geo sense - we can simply get latitude/longitude for the originating phone. So the next step was almost obvious: let us record messages by the phone and plot them on the map, using Google Maps API. So we will get user generated voice content (simply mp3 files in our case) attached to the map. See Figure 3 contained user generated voice messages. Marker type and color are indicating the various topics for the messages.

What can we get from such a service: a) internet users can now pickup messages from telco users right from the map (get all the messages for the selected area), b) telco users can call a service number and simply listen the messages, selected by the geo proximity (e.g.: listen all the messages within the 10 km area, etc.). So how does it work: there is a service number telco users can call and Voice XML based application on that number simply records the message. Messages will be stored as MP3 files. Now the service application will request address information for the originating phone.

Here are two options for address information: 1) a public service that returns address information by the phone, 2) some simplifying versions of that service. In both cases after getting the address we can use geo-coding service from Google Maps API (actually we've used in some services Yahoo geo coding too). Geo coding service accepts address information and returns latitude/longitude info for the given address. And ¡latitude, longitude¿ pair could be used in Google Maps API for drawing the marker on the map. That is all actually. All the rest is absolutely transparent.

Internet users can see the Google map mashup. So they can narrow the area, listen the records from that area (build-in flash based player right on the site), download the records from the selected area as a podcast (RSS feed will be generated by the service) or even embed the map (selected area from the map) into own web site/blog. Phone users can call a service number and listen back all the records closest to their location. "Closest" here means right the distance calculation on the pap. Also the telco users can respond to the messages right from the player, so they do not need to know the originating number (and the originating number is not discovered here).

6 Comments and discussion

Let's give a few comments on the services for getting address information for the given phone. The whole version includes simply XML over HTTP (REST) based

web service. It the practical tests for Moscow we've used the simplified versions of that - right on the service side (so no operator's resources were involved) we've used a simply mapping: 'The number corresponds to the nearest underground (metro) station'. So actually it was a simple pattern based rules: the first 3 digits of number correspond to the nearest metro station. And for metro stations the (latitude, longitude) pair is well known of course. Actually such a service does not require the precise location (up to the building). The key issue here is just to use the same (equal) precise everywhere. All the messages that are not classified (e.g. geo coding could not detect the coordinates, or even the originating number could not be detected) could be simply mapped to the pre-selected default area.

Actually here we are introducing the whole class of services. At the first hand it is used in the operator's network as a service or set of services, where the different services numbers mark different topics (tags) for voice messages: looking for help, service request, dating, garage sale etc. At the second the operator can offer such a platform for businesses in the area. They (businesses) will get own service numbers from the operator and the web application (service platform) for the voice geo tagging/collection. Conclusion: this service demonstrated on the practice how even the minimal openness on telco side (very simple call control plus voice record abilities) creates in the same time a whole new look for the old applications.

References

[McK07] R. McKenna. Interview: BT's open platform, 2007. Available at: http://sdk.bt.com/.

[Mob07] Mobile2.0. Golosovbje SMS ot AbavaNet, 05.04.2007. Available at: www.cforum.ru (In Russian).

[NSS04] D. Namiot and M. Schneps-Schneppe. Interfaces for telco service development, 2004. Otkrytye sistemy, No.5 (In Russian).

[SSN08] M. Schneps-Schneppe and D. Namiot. On intelligent services into Web 2.0 environment, 2008. Elektrosviaz, No.2 (In Russian).

[SSNZ06] M. Schneps-Schneppe, D. Namiot, and D. Zepic. Open Parlay X interfaces for NGN access nodes, 2006. Vestnik sviazi, No.1 (In Russian).

A Bayesian Approach to Context Based Information Disclosure

Christian Bünnig*
University of Rostock, Institute of Computer Science
Chair for Information and Communication Services
christian.buennig@uni-rostock.de

Abstract

Handling private data in ubiquitous computing scenarios is a challenging task for users. Often the decision whether to reveal a certain piece of information or not can only be decided in the moment when the information is requested, i.e. when the context of disclosure is known. In our work we suggest using machine learning techniques for supporting a user in managing private data. We present and evaluate an approach for learning disclosure of personal information by using a naive Bayes classifier.

1 Introduction

One key feature of ubiquitous computing environments and its applications is the utilization of personal information in order to specialize behaviour for individual needs of its users. While this can be seen as a benefit for users, obviously users do not want to disclose personal information unconditionally. Any user should be able to carefully handle private data. To do so a user needs an understanding about the potential flow of her data, which privacy implications may occur when data actually gets communicated and how data disclosure can be controlled.

* Christian Bünnig is funded by the German Research Foundation (DFG), Graduate School 1424 (Multimodal Smart Appliance Ensembles for Mobile Applications - MuSAMA)

Exemplary scenario

Consider the following scenario as an introducing example. A smart room equipped with several devices (e.g. displays, communication devices, sensors) provides various services to the persons in that room. Not all devices need to be visible and least of all the services. So a first step in order to enable a user to carefully practice privacy is to inform her about available services, which personal data they require and what are the effects if the required data gets disclosed to the services. At this point there are two privacy aspects which needs to be considered. The first one is a static aspect: a user initially has to decide whether to trust the infrastructure (respectively the services) she is going to use. The second aspect is more dynamically: what are the effects of disclosing a certain information to a service? The disclosed information may appear on a public display or it may alter the room's state which is also perceptible by other persons in the room. Here the actual recipients of the information are dynamic. Another example outside the smart room scenario is location disclosure. The dynamic aspect here is that the location itself is dynamic as well as other information which can be derived from the location. The crucial point is that fully understanding privacy implications of using a system is sometimes only possible in the moment when the information is requested. Or in other words when the context of disclosure is known.

Context based disclosure

The simplest approach to decide information disclosure based on context is to explicitly ask the user every time a service requests a certain personal information from. While this guarantees that the decision absolutely expresses the intention of the user, it overloads the user's awareness. This can be prevented by expressing in advance rules (or policies) which describe situations and how to decide information disclosure in that situations. This works good for simple cases. Consider a document which may only be visible by three persons. Then a rule like "only disclose this document to a public display service if no one else than these three persons are present" would do the job. For more complex cases specifying rules becomes harder. Users may simple not be able to abstract their privacy preferences sufficiently to describe it by rules. Even if they are, there probably will be unexpected situations which do not get caught by rules or, even worse, where rules make wrong decisions. Further the effort to specify and maintain good rules bears the risk that users tend to use simple but either too public or too private rules. The problem here is that working on rules means handling privacy separated from the actual use of a system. In an ideal situation managing privacy is directly linked to the normal interaction with a system [PD03]. One approach to fill the gap between accurate but obtrusive ad hoc user decisions and imprecise but automated rule systems is to learn a user's

disclosure behavior. A learning approach is not intended to replace rules or explicit user decisions. It may complement them in order to increase accuracy of automated disclosure decisions while reducing direct user interaction.

Overview

This paper is about integrating learning into context based information disclosure by using a naive Bayes classifier. We start with a look at related work. We continue with describing our Bayesian classifier based approach for learning context based information disclosure. Subsequent we evaluate and discuss how well our approach performs in learning disclosure behavior. Finally we conclude this paper and give an outlook to upcoming work.

2 Related work

There exist several work on deciding disclosure of personal information based on context but only a few pick up the idea of using learning techniques for automating disclosure decisions. In most cases disclosure is controlled via policies. Myles et al. [MFD03] focus on disclosure of location information and try to ease the specification of rules by starting on default rules and let users refine them with the support of "wizards". While this reduces the degree of abstracting privacy preferences it still won't be able to catch situations which do not match typical disclosure behaviour. Lederer et al. [LMDB03] present an application which let users describe rules that decide the disclosure of their location and activity based on a fixed set of contextual information (location, activity, time and nearby identities). However, there may be more contextual information which influences the disclosure decision and still a user has to abstract her privacy preferences. Indeed Lederer analyzes the limitations of its own approach in another work [LHDL04] which comprehensively discusses typical problems of managing privacy in ubiquitous computing scenarios, including the limitations of a priori defined privacy policies. A further example for policy based disclosure can be found in [Lan02] where rules are described in a P3P-like format. One approach that mentions the idea of *learning* disclosure is the work by Prabaker et al. [PRF+07]. It is about managing location privacy in a friend finder application and suggests case based reasoning for learning disclosure – however, they do not provide further details on this approach and concentrate on location as the private information to manage.

3 Learning with a naive Bayes classifier

The idea of learning disclosure decisions is to initially observe the user in her disclosure behavior and try to detect correlations between the context of disclosure and the disclosure decision. While there are several possibilities to learn such correlations we initially applied a naive Bayes classifier for decision learning. A naive Bayes classifier needs a relatively small amount of training data. Further it can give expressive user feedback since it is traceable how individual features influence the classification.

Using the Bayes theorem one can express the probability to disclose a certain piece of information D_I in a specific situation S:

$$P(D_I|S) = \frac{P(S|D_I) \cdot P(D_I)}{P(S)} \tag{1}$$

Type	**Value**
nearby-person nearby-service building	identifying string
day-of-week	*monday*, *tuesday*, ...
weekday	*yes*, *no*
time-of-day	*morning*, *afternoon*, ...

Tab. 1: *Example context information types and values.*

A situation S is composed of several context information while a context information is a pair (t, v) of a context information type t from a fixed type set T and a value v from a type dependent value set V_t. Example types of context information and corresponding values are listed in table 1. Context in its originally sensed form might be different, e.g. time is typically a timestamp and a location might be present in a geometric description. However, such *raw* context information can be transformed into the types listed in the table and then it is possible to say that a context is either present or not – this binary context description simplifies calculating disclosure probabilities. After decomposing a situation into context information elements it is possible to calculate the disclosure probability for each context information. For this let d and $\bar{d}$ be the number of situations where an information I has been disclosed respectively not disclosed. Further, let $d_{(t,v)}$ and $\bar{d}_{(t,v)}$ be the number of situations where context (t, v) was present and I has been disclosed respectively not disclosed. Finally let w_t be a weight to apply to the occurrence number of a context information of type t. Given this parameters we calculate the conditional disclosure probability for a given context as:

$$P(D_I|(t,v)) = \frac{\frac{min(d, w_t \cdot d_{(t,v)})}{d}}{\frac{min(d, w_t \cdot d_{(t,v)})}{d} + \frac{\bar{d}_{(t,v)}}{\bar{d}}} = \frac{min(d, w_t \cdot d_{(t,v)})}{min(d, w_t \cdot d_{(t,v)}) + \bar{d}_{(t,v)} \cdot \frac{d}{\bar{d}}} \quad (2)$$

The above equation is not exactly the result one would get when starting from the Bayes' theorem. It uses d and $\bar{d}$ as denominators instead of their sum $d + \bar{d}$. Initial tests have shown that this modification strongly reduces false disclosure decisions[1]. A naive Bayes' classifier assumes that the individual features (context information) are conditionally independent. This assumption allows to combine the probabilities calculated for each context information to express the disclosure probability for a situation like follows:

$$P(D_I|S) = \frac{\prod_i P(D_I|(t_i, v_i))}{\prod_i P(D_I|(t_i, v_i)) + \prod_i (1 - P(D_I|(t_i, v_i)))} \quad (3)$$

Which weights w_t to apply to a context information type strongly depends on a concrete scenario, since only then it is possible to decide which context information type has most influence on the disclosure decision. To improve the classifier it is further possible to not only calculate the disclosure probability for a context information when it is present but also when it is not present.

4 Evaluation

For a first test of the classifier we've compiled a virtual scenario. This scenario is a smart meeting room with several public screens which may display various personal information in order to improve the collaboration of the participants of a meeting in that room. Depending on the kind of meeting participants might wish to disclose certain information while keeping other information private. Examples are meeting dependent views and access rights on personal calendars or sharing of virtual workspaces (a set of documents which can be accessed by other meeting participants). The context information used for calculating disclosure behavior are *nearby-person*, *day-of-week* and *building* (see table 1). We then created a history of disclosure decisions for a specific information in various situations (training set) and a list of potential upcoming situations with corresponding disclosure decisions (test set). Initial processing of this data by the naive Bayes classifier has shown that using a greater weight for the context types *nearby-person* and *building* improve the results of the classifier. Further we could improve the results by not only regarding the presence of context (e.g.

[1] Graham suggests a similar modification for Bayes based spam filtering [Gra02].

a nearby person) but also the absence of context (e.g. an absent person). The training set was made up of 50 situations. The test set contained 20 situations of which the classifier calculated 16 correct decisions. In 3 cases the classifier falsely did not disclose the information (false negative) and in 1 case it falsely disclosed the information (false positive).

Discussion

These first test results must be handled carefully. One reason is that the situations and disclosure decisions in the training and test set have been compiled manually and do not come from real user behavior. Further it is fixed to a specific scenario. However, the results are sufficient to give an impression of the capabilities and limitations of the classifier.

One limitation of the classifier is the assumption of conditionally independence of individual context information. As a result it performs well where a direct correlation between a single context information and the disclosure decision exists. In our test set this was true for the context information types *nearby-person* and *building*. This correlation origins in the fact that these context information is associated with the recipients of the information to disclose (nearby persons may see the disclosed information on present displays and the building indicates the provider of the used infrastructure who potentially has access to the data communicated within the infrastructure). In contrast the classifier fails where a single context information is a bad disclosure indicator. Often combinations of context information must be regarded, i.e. analogies between situations must be detected to decide a disclosure.

Concluding one can say that a naive Bayes classifier can be used for disclosure decisions when the context used for classification is linked to the (potential) recipients of the information to disclose – then it is most likely that there really is a conditionally independence between the individual context information.

5 Conclusion and outlook

In this paper we discussed the problems of handling private data when the decision of its disclosure is mainly influenced by dynamic i.e. contextual aspects. We argued that explicit user interaction and rule based policies have practical limitations because the first one might be too obtrusive when a disclosure has to be decided frequently and because the latter one might either be inaccurate or hard to create and maintain. Learning disclosure decisions is one possibility to balance these limitations. We presented a naive Bayes classifier to learn the

disclosure of personal information based on the context within the information is requested. The evaluation has indicated in which settings a naive Bayes classifier performs well and where it fails.

The tests done until now are not enough to fully judge a naive Bayes classifier for context based disclosure decisions. We are going to do more manually compiled and real user studies in the future. If these tests show that a naive Bayes classifier alone is not suitable to decide the disclosure of personal information based on context, it may still be useful in combination with rule based information disclosure. The Bayesian approach could then be used to detect weak points in the rules, e.g. if the Bayes classifier predicts different disclosure decisions than the rule system.

To tackle the limitations of the conditionally independence of naive Bayes classifier it looks promising to do further research on learning algorithms which do not assume such independence. As mentioned above this is required if the context information available is not directly linked to the recipients of the personal information.

References

[Gra02] Paul Graham. A plan for spam, August 2002. Online valiable at `http://www.paulgraham.com/spam.html` (accessed May 23, 2008).

[Lan02] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *Proc. of UbiComp 2002*, volume 2498/2002 of *LNCS*, pages 315–320. Springer, 2002.

[LHDL04] Scott Lederer, Jason I. Hong, Anind K. Dey, and James A. Landay. Personal privacy through understanding and action: Five pitfalls for designers. *Personal Ubiquitous Computing*, 8(6):440–454, 2004.

[LMDB03] Scott Lederer, Jennifer Mankoff, Anind K. Dey, and Christopher P. Beckmann. Managing personal information disclosure in ubiquitous computing environments. Technical Report UCB/CSD-03-1257, EECS Department, University of California, Berkeley, July 2003.

[MFD03] Ginger Myles, Adrian Friday, and Nigel Davies. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 02(1):56–64, 2003.

[PD03] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *CHI '03: Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, pages 129–136, New York, NY, USA, 2003. ACM.

[PRF+07] M. Prabaker, J. Rao, I. Fette, P. Kelley, L. Cranor, J. Hong, and N. Sadeh. Understanding and capturing people's privacy policies in a people finder application. UBICOMP'07: Workshop on UBICOMP Privacy, September 2007.

A Two-way Approach to Service Composition in Smart Device Ensembles

Florian Marquardt, Christiane Reiße,
Adelinde Uhrmacher and Thomas Kirste
{florian.marquardt,christiane.reisse,
adelinde.uhrmacher,thomas.kirste}@uni-rostock.de
University of Rostock
Albert-Einstein-Straße 21
18059 Rostock, Germany

Abstract

The aim of research in the field of smart environments is to explore techniques which allow us to build dynamic ensembles of devices in such a fashion that the user can interact with them in a natural way, without requiring him to manually control the devices. These devices are likely to be heterogeneous and offer different services. Based on user intentions and the capabilities of the devices, the challenge is to provide suitable combined services.

This problem can be addressed top-down by decomposing goal tasks into plans or bottom-up by synthesizing chains of atomic services. In this paper, a proposal for both approaches and how those can work together to provide services will be introduced. In combination, both approaches allow an adaptive, intention-based user assistance in smart device ensembles.

1 Introduction

Different smart environments exist that require different strategies regarding user assistance. A concrete example of a smart environment is a smart meeting room. Like other meeting rooms it contains stationary devices such as fixed video projectors, canvasses, or automatic blinds. In addition, users can bring in mobile devices such as notebooks, PDAs or cell phones. The entirety of the devices in a smart meeting room forms the *ensemble*.

It is augmented by sensors, e.g. cameras and presence sensors, and exhibits some kind of coherent behavior as a whole. The purpose of a smart meeting room is to pro-actively assist users in their activities. For example, a user who wants to give a presentation should be supported by a notebook automatically connecting to a projector, starting the presentation program with the respective slides, and possibly darkening the room. To provide such a combined service, the intention of the user and the accessible services have to be known. We assume that every device offers one or more services. For example a video projector can project slides on the wall or a microphone can record speech in the meeting room. Information about the user's intention is typically provided by a separate component which employs sensor data and models of the users' behavior in deriving the user's intentions. Based on the users' intentions [BK07] suitable atomic services, e.g. dimming the lights, or composed services, e.g. supporting a presentation, can be identified (see Figure 1). In order to achieve this strategy synthesis, we distinguish between a top-down and a bottom-up approach. Typically, top-down approaches are applied for service composition in ambient intelligence applications [HK02, VRV05]. They utilize structural knowledge. The combination with a self-organizing bottom-up approach promises additional adaptability and flexibility.

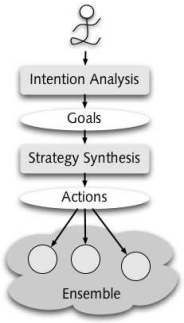

Fig. 1: *From user intentions to combined services.*

Typically, service composition in smart environments is also constrained by the limited resources of the devices, i.e. some devices will not be able to offer services in suitable representations nor to execute combined services. Smart devices mostly tend to be small and poor of resources. Our approach does not explicitly deal with this issue. We assume that a suitable middleware will enable resource-rich devices to provide computing facilities for resource-poor devices [ZDLT08].

The remainder of this paper is structured as follows. Section 2 discusses related work. The following sections will describe our approach in more detail: Section 3 will deal with the top-down part, which is based on HTN planning, Section 4 will discuss the bottom-up part, which relies on self-organization. Section 5 will bring both together and describe the potential benefits. The paper concludes with a summary in Section 6.

2 Current approaches to services in smart environments

Services in smart environments have been a topic of research which increasingly received attention during the last years.

Some of those approaches rely on a fixed hardware configuration and thus are able to plan the device cooperation in advance. Approaches that exploit fixed action schemes, like plan recognition (as pursued e.g. in the Intelligent classroom project [Fra98]) or condition-action rules (as in the EasyLiving project [BMK+00]) are not feasible in our scenario as we do not know the participating devices. Observing the users in order to automate routine tasks (as in the Adaptive House [Moz05]) is neither an option. Defining suitable training sets for our scenario of an ad-hoc ensemble is hampered by the effort it would require in beforehand and thus would not allow ad-hoc cooperation of devices.

Others focus on service matching as part of the service composition problem. E.g. the DIANE [KKRSK07] project developed a service description language called DSD (DIANE Service Description) and an architecture for device cooperation. For the generation of non-atomic services DIANE pursues an integrated approach that combines service discovery, matchmaking and composition. Finding services is based on graph matching, in which requests for services are trees that state precisely the required effects a composed service should exhibit. The available services are rated according to how many of the desired effects they fulfill. This approach works well if a precise description of the required composed service is available. In our scenario this would correspond to an abstract plan for the cooperation of devices which has to be instantiated with the available services or combinations of these services. But often there are scenarios where the user does not know or does not want to know in detail how to describe the required service. A more general description would be easier to understand and to formulate for the user.

The Amigo project [VRV05] pursues a similar approach. This project also aims at composing higher-level services based on graph matching. To fulfill a user's goal, a predefined abstract task description is required. This task description is then matched against the descriptions of the available services. The main problem of this approach is the need for a library of abstract plans designed for all possible situations that might occur. For ad-hoc scenarios this prerequisite can not be fulfilled because at design time it is unknown which devices will join the ensemble.

Another project concerned with the cooperation of devices in smart environments was the EMBASSI project [HK02]. In theory, EMBASSI is able to use a variety of approaches for service combination. In practice partial-order-planning

was used. By using distributed HTN Planning we will follow up the planning approach of EMBASSI and enhance it. A shortcoming of EMBASSI was that only atomic services were supported. We will also combine already combined (an thus non-atomic) services.

The approach Amigoni et al. [AGPR05] pursued for ambient intelligence is called D-HTN. It is based on agents and uses hierarchical task network planning with distributed aspects. The used HTN planner planner D-NOAH [Cor79] is central, but the decompositions of higher-level tasks are provided by the agents and therefore stored decentrally.

Although we follow Amigoni et al. in decentralizing task decompositions, we will in contrast use SHOP2 [NAI+03] as HTN Planner. Several publications [SPW+04, WPS+03] have already shown that HTN planning with SHOP2 is feasible in Web service environments.

In many current approaches, including that of Amigoni et al., services are only described by their interfaces. In that case only syntactical information is available for service composition. For dynamic ad-hoc scenarios it is crucial to use semantical information in addition. Here WSMO fits our needs best [RBMK08]. WSMO descriptions can provide the services' interfaces as well as their semantics. Using WSMO we are able to store pre- and postconditions.

3 Top-down planning

With this approach we propose to use Hierarchical Task Network (HTN) planning to gain composed services. HTNs are a well-known AI planning technique [EHN94] that has already proven successful for service composition [Pee05]. Planning in general can be divided into online and offline planning [Nau07]. For this approach we will consider offline planning and thus distinguish between plan generation and plan execution. The focus will be on plan generation.

Figure 2 shows a simple example of a plan decomposition in a smart meeting room. The initial goal task is to give a presentation. We assume that *Get Slides* is an atomic task that can be fulfilled by an available service directly. In contrast *Presentation* can not be executed directly as a service. But we have a decomposition in our library that splits *Presentation* up into the tasks *Darken* and *Prepare projector*, whereas *Prepare projector* has *Get slides* as a precondition. Unfortunately neither is atomic, hence decompositions for both have to be found in the task library. In the third line of Figure 2 we finally can see that task *Darken* was replaced by the sequence *Switch off lights* and *Lower blinds* as well as *Prepare projector* was replaced by *Switch on projector*, *Lower canvas* and *Show slides*. All five tasks are atomic, so now the whole resulting

plan consists of atomic tasks that can be executed as services. Hence, our goal task is fulfilled.

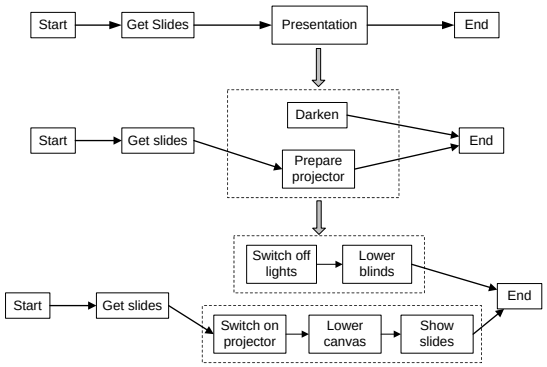

Fig. 2: *Task decomposition example for smart meeting room scenario*

HTN planning differs from other planning approaches. According to [Nau07] HTN planning is domain-configurable, which means that knowledge about the environment can be added during runtime of the system. In contrast to this, domain-specific planners include knowledge about the environment, resulting in effective planning but inflexibility. On the other hand, this kind of knowledge is omitted in domain-independent planners, resulting in wide applicability but weak efficiency. For this reason domain-configurable planning like HTN is a good compromise between reusability and effectiveness. The ability of adding domain specific knowledge to the planner during runtime is crucial in our ad-hoc scenario, because we have no a priori knowledge of the respective constellation of devices in our ensemble. Any additional knowledge about the environment can only be added to the planner when a plan is to be created.

Besides, HTN planning comes along with some restrictions compared to classical planning. The methods in the plan library confine the search space of the planner. Tasks that are not stored in the library cannot be found even if all necessary atomic tasks are available. This makes HTN planning less explorative than e.g. partial-order planning. Storing and handling of decompositions initially requires additional data structures, memory and computing time in contrast to traditional planning techniques that only require operators. But once it is available using this environmental knowledge results in much less planning steps.

The possibly most important challenge using HTNs for service composition is the need to acquire domain knowledge, namely the decomposition methods. To be applicable in real life this knowledge must be provided by the manufacturer of the devices or accessible for instance via the internet. This approach gives the responsibility for reasonable decomposition methods to the manufacturers of devices in the first place. We are aware that this prerequisite is questionable. But due to the usage of open standards it becomes possible that additional

repositories of task decompositions from different sources can be used in a smart environment [RBMK08].

After introducing HTN planning theoretically we will describe how top-down planning will work in our ensemble. To gain an executable plan we first need a planner which performs the planning. As a consequence of our approach a list of operators (atomic services) as well as library of methods (decompositions) must be provided in the smart ensemble. As proposed in [AGPR05] the decompositions are distributed over the devices. To let the planner know which atomic services and which decompositions are available a repository is accessible where the devices are listed, so the planner can contact them. We have to be a bit more detailed here. As mentioned above a device offers its functionalities as services. Furthermore the device can offer some possible decompositions wherein its own services are involved as part of the distributed library (see Figure 3). In this state a decomposition and a composed service are two different things. To make use of decompositions, the planner must build composed services out of them. These composed services then can be used in the ensemble, as long as all its involved services remain available. The number of available atomic services can change by joining or leaving of devices. In the majority of cases a whole device together with all its services will join or leave. But due to the fact that deriving a new composed service either by the top-down or the bottom-up approach correlates to a join of this service into the ensemble, we consider joining and leaving of single services instead of whole devices. If a device joins the ensemble new decompositions become available. If it leaves the ensemble its decompositions can be kept since they are generally applicable and not preassigned to one specific device or atomic service. To keep decompositions of leaving devices they must be saved in the repository.

4 Bottom-up synthesizing

As described in the last section, the top-down approach works well if all required decompositions of higher-level tasks are available and there is a component in the ensemble that may coordinate the cooperation of all the other components. However, in situations where neither is the case, the top-down approach will fail. How can this issue be addressed?

The problem of missing decompositions could be solved, for example, by partial-order planning. As long as the ensemble contains devices which offer suitable atomic services and the service descriptions are available via a repository, as explained in Section 3, a partial-order planner may find a solution. However, a major drawback of partial-order planning is the need for a central component that collects information about all possible actions, their preconditions and effects, the current state of the world and the user's goals and is thus able to

generate a plan, i.e. an action sequence that will fulfill the goals. In dynamic ad-hoc environments, however, one cannot rely on the existence of such a central component as the ensemble structure is not fixed and may change at any time. The devices the user brings into the room should integrate seamlessly with the devices installed in the room. There might even be ensembles without any fixed devices – in that case, the users build up the ensemble entirely of resource-constrained devices. The room provides merely a network infrastructure. One user brings a projector, another brings a canvas, and everyone has a notebook. The devices may have heterogeneous interfaces, were not designed to work together and were never before used together. Nevertheless, users expect the ensemble to show coherent behavior and to support them in their activities. Generating useful action sequences in such environments is therefore not trivial.

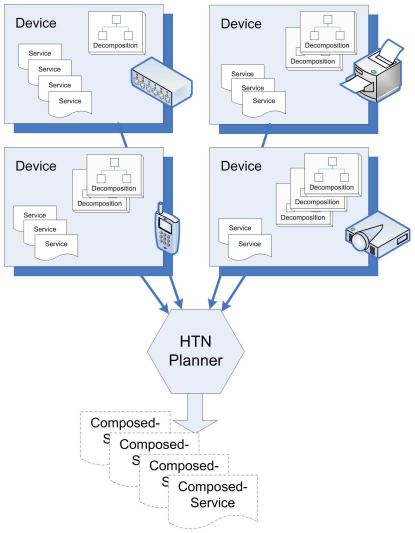

Fig. 3: *Top-down planning process for smart ensembles*

One could argue that distributing partial-order planning in such a way that each device takes part in the planning process might be a solution. However, looking at the smart meeting room domain, we find that interaction sequences among devices are rather short, such that a "heavyweight" approach like partial-order planning is probably not necessary. Furthermore, a distributed version of partial-order planning would impose severe computation overhead onto the devices. Assuming that in the domain of smart meeting rooms the devices' computation capabilities can be limited, we might run into problems with this approach. Therefore, we have developed a decentral approach based on an idea of Maes [Mae90]. We assume that all devices have some memory, possess elementary computing capabilities and are connected to a common network. Because no single device has global knowledge, the devices have to cooperate to generate action sequences. In this paper, we merely give an idea of this approach. Details can be found in [RK08a] and [RK08b].

```
(:action ShowDoc
    :parameters (?Doc - Document ?Canv - Canvas)
    :precondition (and (SentToDisp ?Doc Projector1) (CanvasDown ?Canv))
    :effect (and (DocShown ?Doc ?Canv)
                 (forall (?OtherDoc - Document)
                         (when (not (= ?OtherDoc ?Doc))
                               (not (DocShown ?OtherDoc ?Canv))))))
```

Fig. 4: *ShowDoc operator in PDDL.*

Just as planning, our approach requires that all possible actions a device can perform are described as operators with preconditions and effects, e.g. in PDDL [McD98] (see Figure 4 for an example). These operators are distributed across the devices. The devices build up a network of operators according to the preconditions and effects at run time. To this end, operators that share preconditions and effects are connected via different types of virtual links: predecessor and successor links between identical preconditions and effects, conflicter links between a precondition and its opposite effect (see Figure 5). If there is an open user goal, the device ensemble uses this network to generate an action sequence that will fulfill this goal. It gradually "selects" actions which are executed right away. Selection is no explicit process, but results from the dynamics of the network. The action chosen is always the one that is most likely to lead towards a goal at that moment. This probability is implicitly encoded in virtual "energy" that operators exchange according to the links.

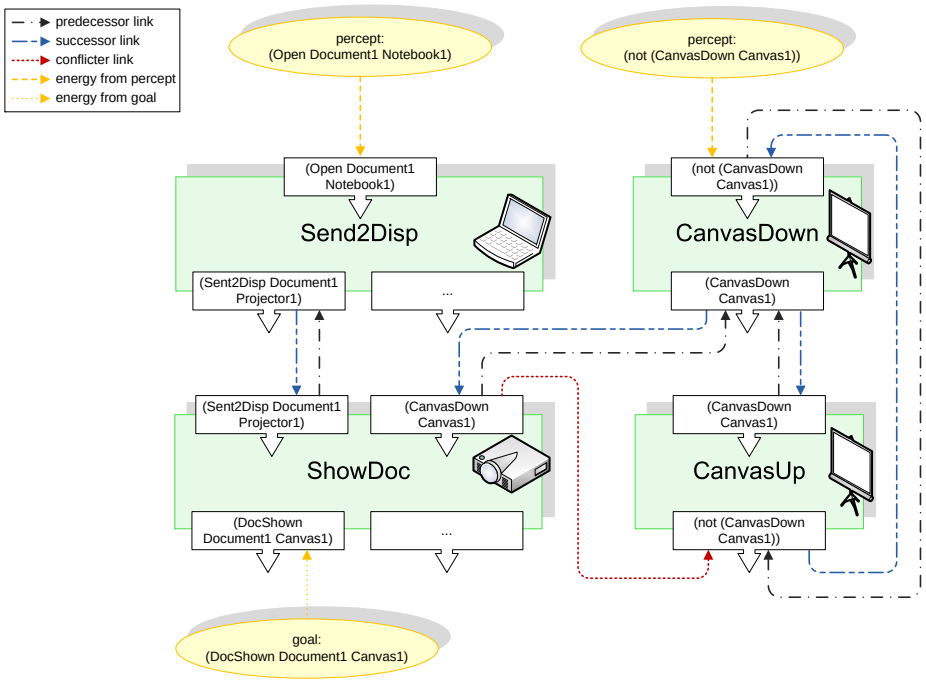

Fig. 5: *Four operators and the links between them. Additionally, the flow of energy from percepts and goals to operators is depicted.*

Consider the example in Figure 5: Initially, the *ShowDoc* operator receives energy from the open goal because its effect might fulfill this goal. *Send2Disp* and *CanvasDown* receive energy from the current world state (the percepts) because their preconditions are fulfilled. The operators then send energy to one another along the links. If either of *Send2Disp*'s or *CanvasDown*'s energy level is above a certain fixed threshold and no other operator has a higher energy

level, it is executed. Once both have been executed, *ShowDoc*'s preconditions are fulfilled. If it has enough energy it can be executed, which fulfills the goal.

The bottom-up approach has several advantages. It does not require a central component that manages the cooperation of all the operators. Each operator takes part in the planning process by computing e.g. its own activation level and sending messages to other operators. Useful behaviour of the entire system arises as a side-effect of the operators' interactions. One can call this emergent behaviour. Furthermore, no operator needs global knowledge. Each operator has just a very constrained world model which comprises its predecessors, successors, conflicters, the current world state, and the user goals.

5 Benefits of combining both approaches

Although both approaches result from rather different paradigms we propose that in combination both will be a step towards intelligent behaviour of devices in smart environments. Each approach is suitable for certain scenarios. In well-known situations the centralized planner generates fast and reliable results with a minimum of communication effort and only central computing power for generating the plan is needed. Furthermore due to its hierarchical structure it scales very well in large ensembles. In most cases top-down planning finds a solution for a demanded goal task, this solution can be regarded as optimal. The drawback of HTN planning is that this approach will fail in situations where no suitable task decompositions can be found to fulfill a demanded task. Top-down planning is also not applicable if no device is capable of hosting the planner.

The bottom-up approach, on the other hand, is suitable for situations where creativity is required. It may find solutions the top-down approach is not able to, and it can find solutions in situations where the top-down approach produces no result at all. Furthermore, the bottom-up approach can identify solutions using services which are only described by their interfaces and thus cannot be used by the top-down approach. The drawback is that the bottom-up approach is not guaranteed to find a solution even in well-known situations because it uses so little information. It also makes the assumption that all the devices have at least some computing power and are able to take part in the strategy synthesizing process. Another requirement for the bottom-up approach is that communication channels have sufficient bandwidth. This is due to the fact that the devices have to communicate a lot while finding a solution for the goal task.

Combining these approaches will result in a system that enables device cooperation in ensembles with very low computational power as well as in large scale ensembles with lots of different devices. In ensembles that allow for both approaches, it can combine them in several ways. One possibility is serializing the

top-down and the bottom-up approach. At first, the top-down approach tries to find a solution. In case it fails the bottom-up approach will be considered. If the bottom-up approach generates a feasible action sequence, it will be stored in the plan library of the top-down approach.

A more sophisticated idea is to interweave both approaches. That is, whenever one approach gets stuck, it can consult the other one. This situation might occur if the top-down approach lacks in a branch of the decomposition tree. In this case it can start the bottom-up approach using the available pre- and postconditions of the non-primitive task. If the bottom-up approach finds a solution the service sequence is given to the top-down planner which can now continue planning.

6 Summary and conclusion

In this paper we have described two approaches for identifying services in smart environments and how a combination of both can enrich user assistance in smart environments.

The combination of both approaches can handle more situations in smart environments than each of them could handle alone.

The top-down approach using HTN planning in a smart environment is based on devices that carry their service descriptions as well as their decompositions. The bottom-up approach requires only service descriptions, no decompositions. Both need information about the user's intention and goals.

Both approaches have their strengths and weaknesses. Top-down planning is comparably fast and produces reliable results but will fail if no suitable decompositions are available. Compared to top-down planning, bottom-up synthesizing is able to produce unforeseen results. This creativity is the great advantage of bottom-up synthesizing as it enables completely new solutions to be generated. The combination of both approaches increases the number of possible solutions for combined services and thus higher level functionalities in smart device ensembles can be achieved.

Acknowledgements

This work was conducted within the graduate school MuSAMA which is founded by the Deutsche Forschungsgemeinschaft (DFG).

References

[AGPR05] F. Amigoni, N. Gatti, C. Pinciroli, and M. Roveri. What planner for ambient intelligence applications? *Systems, Man and Cybernetics, Part A, IEEE Transactions on*, 35(1):7–21, 2005.

[BK07] Christoph Burghardt and Thomas Kirste. Inferring intentions in generic context-aware systems. In Timo Ojala, editor, *MUM*, volume 284 of *ACM International Conference Proceeding Series*, pages 50–54. ACM, 2007.

[BMK+00] Barry Brumitt, Brian Meyers, John Krumm, Amanda Kern, and Steven Shafer. EasyLiving: Technologies for intelligent environments. In *Proc. Handheld and Ubiqitous Computing, 2nd International Symposium*, pages 12–29, Sep 2000.

[Cor79] Daniel Corkill. Hierarchical Planning in a Distributed Problem-Solving Environment. In *Proc. 7th Intl. Joint Conf. on AI*, Tokyo, January 1979.

[EHN94] Kutluhan Erol, James Hendler, and Dana S. Nau. HTN planning: Complexity and expressivity. In *Proceedings of the Twelfth National Conference on Artificial Intelligence (AAAI-94)*, volume 2, pages 1123–1128, Seattle, Washington, USA, 1994. AAAI Press/MIT Press.

[Fra98] David Franklin. Cooperating with people: the intelligent classroom. In *AAAI/IAAI*, pages 555–560, 1998.

[HK02] Thomas Heider and Thomas Kirste. Supporting goal based interaction with dynamic intelligent environments. In *ECAI*, pages 596–600, 2002.

[KKRSK07] Ulrich Küster, Birgitta König-Ries, Mirco Stern, and Michael Klein. Diane: an integrated approach to automated service discovery, matchmaking and composition. In *WWW '07: Proceedings of the 16th international conference on World Wide Web*, pages 1033–1042, New York, NY, USA, 2007. ACM Press.

[Mae90] Pattie Maes. Situated Agents Can Have Goals. In Pattie Maes, editor, *Designing Autonomous Agents*, pages 49–70. MIT Press, 1990.

[McD98] Drew McDermott. PDDL — The Planning Domain Definition Language, 1998.

[Moz05] Michael C. Mozer. Lessons from an adaptive home. *Smart Environments: Technology, Protocols, and Applications*, pages 273–298, 2005.

[NAI+03] Dana Nau, Tsz-Chiu Au, Okhtay Ilghami, Ugur Kuter, J. William Murdock, Dan Wu, and Fusun Yaman. SHOP2: An HTN planning system. *Journal of Artificial Intelligence Research*, 20:379–404, December 2003.

[Nau07] Dana S. Nau. Current trends in automated planning. *AI Magazine*, 28(4):43–58, 2007.

[Pee05] Joachim Peer. Web service composition as AI planning - a survey. Technical report, University of St. Gallen, Switzerland, 2005.

[RBMK08] Christiane Reisse, Christoph Burghardt, Florian Marquardt, and Thomas Kirste. Intelligente Umgebungen und das Semantic Web. *Information Managment & Consulting*, 23(2):28–33, May 2008.

[RK08a] Christiane Reisse and Thomas Kirste. A Distributed Action Selection Mechanism for Device Cooperation in Smart Environments. Proceedings of Intelligent Environments 2008, Seattle, USA, July 21-22, 2008.

[RK08b] Christiane Reisse and Thomas Kirste. A distributed mechanism for device cooperation in Smart Environments. In *Advances in Pervasive Computing. Adjunct proceedings of the 6th International Conference on Pervasive Computing*, pages 53–56, Sydney, Australia, May 19-22 2008.

[SPW+04] E. Sirin, B. Parsia, D. Wu, J. Hendler, and D. Nau. HTN planning for web service composition using SHOP. *Journal of Web Semantics*, 1 (4):377–396, 2004.

[VRV05] M. Vallée, F. Ramparany, and L. Vercouter. Flexible composition of smart device services. In *The 2005 International Conference on Pervasive Systems and Computing (PSC-05)*, Las Vegas, USA, Jun 27-30 2005.

[WPS+03] Dan Wu, Bijan Parsia, Evren Sirin, James Hendler, and Dana Nau. Automating DAML-S web services composition using SHOP2. In *The SemanticWeb - ISWC*, 2003.

[ZDLT08] R. Zender, E. Dressler, U. Lucke, and D. Tavangarian. Meta-Service Organization for a Pervasive University. In *Proceedings of PerEL 2008, Workshop at 7th IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 400–405, Hong Kong, China, 2008. IEEE Computer Society.

On an Integrated PBX Infrastructure Security Programme

Iosif I. Androulidakis
University of Ioannina, Network Operations Center
University Campus
GR 45110, Ioannina
GREECE
sandro@noc.uoi.gr

Abstract

Private Branch Exchanges (PBXs) are privately owned equipment that serve the communication needs of a private or public entity making connections among internal telephones and linking them to other users in the Public Switched Telephone Network (PSTN). There are millions of lines installed in every country and they essentially complement the public network. Economy, Health, Security, Private and public sector they all rely on communication capabilities. Even if the core public network is operating normally, unintentional or targeted damages and attacks in PBXs can cause significant instability and problems. Furthermore interception of calls is a very sensitive issue that affects all of us. In that sense, it is not an exaggeration to state that PBXs are part of a nation's critical infrastructure. Much has been said and done regarding data communication security but PBXs have been left unprotected, forgotten and waiting to be attacked. This contribution presents a survey of security issues and actions. It aims at both educating the users and securing their telephony systems compromising of educational, policy, auditing, technical, documentation, hardware and software solutions and actions.

1 Introduction

Contemporary societies rely on telecommunication infrastructure more than ever. Economy, Health, Security, Private and public sector have extended telecommunication networks to serve their communication needs. Organizations, Ministries, Public bodies, Hospitals, Companies, Factories etc have their

own telephone exchanges, called private branch exchanges (PBXs). They are just like the telephone exchange (central office) that serves our home but in a smaller configuration, dedicated to serving only the telephones of the owner.

PBXs make connections among the internal telephones of a private organization - usually a business - and also connect them to the public switched telephone network (PSTN) via trunk lines. A PBX is a telephone exchange serving an individual organization or company with connections to the PSTN (Public Switched Telephone Network) [Wik07]. It is actually a private switch or router that connects a group of telephones and provides a wealth of features. It is because they incorporate telephones, fax machines, modems, and more, that the general term "extension" is used to refer to any end point on the branch.

Initially, the primary advantage of PBXs was cost savings on internal phone calls: handling the circuit switching locally reduced charges for local phone service. As PBXs gained popularity, they started offering services that were not available in the operator network, such as hunt groups, call forwarding, and extension dialling.

With such an array of services and cost savings it is of no wander that there are millions of PBX lines installed in every country. PBXs essentially complement the public network. Even if the core public network is operating normally, unintentional or targeted damages and attacks in PBXs can cause significant instability and problems. Furthermore interception of calls is a very sensitive issue that affects all of us. In that sense, it is not an exaggeration to state that PBXs are part of a nation's critical infrastructure.

Traditional, ethical hackers, who were only investigating and were acting out of curiosity, have nowadays been replaced by professional ring operations acting only for economic gains. Given this fact it is only a matter of time before a PBX is attacked. Many articles have been written to alert users and help administrators deal with the problems and much work has been carried out to safeguard the computing and network infrastructure. Regrettably, classical telephony service security field lacks such rigorous work. This is why the basic problems that threaten telephones' security are being taxonomized and addressed in this essay in an easy way, useful for both administrators and simple users.

2 Frauds and Fraudsters

As telephony security is usually lacking compared to IT security, the opportunities for crime are numerous. The first thing that comes into mind is of course unauthorized access of our telephones and the relevant results. Losses due to computer incidents are usually estimated and it is indeed a very complex pro-

cedure yielding wrong results many times. Economic losses due to a telephony incident on the other hand are immediately obvious. Imagine a telephony fraud taking place unnoticed for a substantial period. The phone bills will grow so high that it will be impossible for the company to pay them. As a matter of fact substantial damage can be done by only a weekend of full access to the company's telephones, by rings that engage in call sell operations. Apart from the apparent cost of the bill, lost revenues and additional expenses can skyrocket the total loss to astronomical amounts. Such economic frauds include usage of services by unauthorized persons, stealing of company information and secrets, call selling operations, abuse of premium rate services, abuse of freephone 800 numbers and third party billing. There have been cases where hackers were taking advantage of radio and TV stations PBXs in order to win contests (i.e. the 1st caller will win) blocking other users.

Who is actually engaging into such actions? Telecom fraudsters fall into three basic groups: those who do it for fun, those who do it to save money and those who do it for profit [Wes00]. Attacks can originate from the inside (employees) or outside (hackers, competitors, foreign governments, terrorist groups and the organized crime) At the lower end of the impact scale are skilled individuals, usually teenagers trying to break in just for the challenge. The most common threat to a network is the malicious hacker who is usually trying to earn personal benefits by employing his skills in network management and programming to deploy various illegal activities such as call sell operations using stolen codes and accesses. He could also intercept phone calls and logs providing valuable information, especially in cases of industrial spying. It is interesting to note that apart from phone voice calls, fax calls or even low speed modem data communications can be intercepted and extracted. In a category by themselves, people with increased communication needs such as soldiers, students, foreigners, refugees and prisoners devise surprising means in order to communicate freely. Last but not least do not forget the most mighty of all: Nature and its elements such as floods, hurricanes, fires can bring chaos and complete loss of communication.

Typical methods of abuse by malicious hackers involve the misuse of common PBX functions such as DISA (Direct Inwards System Access), call forwarding, voicemail and auto attendant features. DISA is designed to allow remote users to access a PBX to place log distance calls as if they were at the same site as the PBX. Fraudsters unfortunately are another category of remote users. Voicemail use pauses two possible threats. One is that if wrongly configured, they can give access to dial tone in order to place a call. The second one is the inherent dangers of stealing the information contained in them or even taking them over [Ava02].

Wireless calls can passively be intercepted using the proper gear. A classical way of interception is the use of special devices, the well known "bugs". A more elaborate technique is that of "the man in the middle". In order to intercept

a wireless communication a hacker can sit in the middle pretending to be the other party and relaying the information to the intended party. That is why revealing sensitive information during a phone call is not a good idea unless some sort of cryptographic means is used.

At the other end of the spectrum is the organized crime. A common use of a compromised telephone network is to use it as a screen for covering-up illegal activities such as ring operations, drug selling, money laundry etc. The call begins usually from payphones because they can offer anonymity and they are easy to find and accessible from almost everywhere. Then the call is routed through many private telephone branch exchanges (PBXs) to make it extremely difficult to trace. This "looping" is a very effective way to mislead authorities from tracing them. The technique however, is on the decline with the advent of convenient prepaid mobile phones [Bla00].

Organized crime has its own customer base that demands cheap international calls and will break into PBXs to serve this base. Knowing that the window of opportunity will close eventually they try to maximize their revenue by exploiting quickly and aggressively the compromised PBX [Wes00]. Selling calls to high cost international destinations is the most usual fraud taking place. It is interesting to note that a compromised PBX may be used in order to attack another PBX or even to jump into a data network getting the necessary anonymity and leaving the owner responsible for the act. This anonymity can also be used by various illegal ring operations to conduct their illicit business. The unsuspected administrator who has not properly secured his PBX will face a very unpleasant surprise sooner or later.

Another sensitive point in a company's telephone network consists of the internal phones placed in publicly accessed areas (i.e in the lobby or in the elevator). As a matter of fact there is also a whole category in relevant articles in underground electronic magazines regarding what is called "elevator phreaking". Such phones are easy to access and as an internal part of the network can easily be misused to expose vulnerabilities. Furthermore they are a great access point for all those who mean to cause harm to the network and its infrastructure. A person can easily slip a "bug" or use them just to place a free call. So they have to be both protected and confined in places that not everyone has access to them. In case they are really needed any necessary steps must be taken in order to secure them and make sure that they cannot cause problems. A special case of an internal phone is the operator's console. If not properly administered, it may have the ability to change setup features and operational data. It could for example unblock barred destinations or leverage call abilities on certain phones.

Most administrators use firewalls and check their computer network's health regularly. Unfortunately the telephone network can help breach the firewall protection. All it takes is an unauthorized modem hooked up in an internal line

and presto! Access to Internet is now possible and viruses and trojan horses lurking can now find their way in through an unguarded entry point.

To make things worse, a dialup line connecting the telephone exchange's CPU to the maintainer's modem in order to remotely administer the switch can be misused causing not only telephone problems but also providing a way to enter the computer network. The Maintenance Port [Ava02] as it is called is usually protected with a simple to guess or default password making it easy to defeat. Having access to the switch, the hacker can reprogram it, install backdoors, turn on functions such as DISA and shut down other functions such as call logging. There is a well known technique, called "war dialing" which consists of calling every single number a company owns in order to discover modems and electronic services to abuse. According to a recent survey [BW07] regarding information security controls, "testing and review procedures including a "war dial" of inbound phone lines to identify active modems" ranked last in a list of 80 controls. In other words, the identification and tracking of modem connections was incomplete, of low quality and not rationalized, pausing a significant risk that shouldn't be neglected.

When a PBX is linked to an organization's IT network, a poorly protected maintenance port can offer an open and undefended "back door" into such critical assets as customer databases and business applications [Pol05]. Imagine a fraudster, having the ability to intercept credit card numbers as the unsuspected client presses the keys in his phone [Bla00]. There are many cases where a perfectly well designed computer network is brought down due to errors and omissions in the telephone network. It is rather oxymoron to invest into computer security but to forget to invest into telephone security. Total security can only be achieved with combined efforts and supplies between IT and telecom world.

Apart from fraud and interception, another hit in our infrastructure can come from what is called "denial of service" which is caused either intentionally or unintentionally and severely harms the integrity of our network especially if we don't have alternative routes or backup lines for our connections. In simple words, we cannot use our telephone to place or receive calls since it is no more operating. A company short on ethics could hire somebody to sabotage the telephone exchange of their competitor making it impossible to do business, causing huge losses. Finally, a disgruntled former employee could have installed a backdoor to completely halt the telephone exchange a few days after leaving the company.

Finally, regarding the modus operandi of a hacker and the sequence of actions attacking a PBX would be the following:

a) Pick up the target (either a specific one or a random one)
b) Do a thorough search in the yellow pages and in the internet for documented lines (directory of phones, direct dial in lines, etc.)
c) Proceed to war dialing, dialing all of the numbers in the specific numbering plan. This step is usually performed with automated tools but can be accomplished with manual dialing too.
d) Judging by the tone and the pattern of the ring tone it might be possible to determine the type of the PBX. Most of the times, the music on hold theme is a clear indication of the PBX manufacturer.
e) If a modem is found then its prompt can help evaluate the type of the equipment connected. It might be a server, the PBX maintenance port, or an employee's PC. The hacker will proceed relevantly.
f) Should the PBX maintenance modem is found, then the default passwords would be the first ones to try. Otherwise guessing can have some success, while social engineering would probably also work.
g) If a service is found (DISA, Voice Mail, IVR) then it can also reveal information about the type of the PBX. Furthermore, each type has documented features and problems that the hacker might try to exploit.
h) Daring enough hackers could also physically present themselves to the PBX site, posing as technicians and asking to visit the PBX itself in order to proceed to "maintenance" works.

The previous steps can be assisted by social engineering tricks where the hacker will manipulate the human element in order to divulge valuable information as already mentioned before.

3 The problem in hand

Checking the proper operation and ensuring the safety of PBX as well as protection against unauthorized use and access is usually left to the owner. This has of course tremendous effects since due to economic and technical difficulties, in essence it is impossible to guarantee that the proper measures are taken. Avaya's PBX user manual states that it is impossible to guarantee 100% security since the owner has the final word in setup and administration of the switch and as so every unauthorized use claims are charged to the owner. Finally, FCC and courts both agree that the owner bears the responsibility for misuse of his system and not the manufacturer.

It is frightening to imagine not being able to call a hospital in an emergency. Furthermore, national economy could suffer great losses if a targeted attack

was to render useless industry's telecommunication lines. In any case, it is apparent that in the modern demanding business environment a company or organization can't survive without telephone service. Even worse, consequences after a multimillion fraud starting from its own telephone exchange would lead to financial and business disaster.

While data communications have long before begun to utilize every possible means of protection, enjoying a vivid research and development sector, PBX arena has not caught up. As a matter of fact, due to the much higher life expectancy and rigidity of PBXs it is common to find still operating more than 20 years old equipment. It is clear that a combined and targeted action has to be taken.

4 Countermeasures

It might seem so far that we are left unable to defend our selves against the evil. This is not the case. Multithreaded actions can be taken to mitigate the security risks There are many simple steps a savvy administrator can take to shield the PBX [And04, NIS01], starting from proper education of the users and himself in order to increase the awareness of the system's security features and vulnerabilities. Conferences and production of educational material would be very productive in this step. Properly communicated security policies should follow. Technical measures such as frequent system passwords changing, barring of premium rate calls, careful assignment of station privileges etc. can only be effective as soon as the users are educated. Manuals, directories and other internal documents should be treated as confidential. Call logging should always be enabled and checked for unusual activity and strange call patterns. Furthermore, call forwarding to external destinations should not be allowed. Especially regarding maintenance port, every serial port connection should be traced to its destination. The modem should be switched on only when the maintainer needs to perform some action and with a well defined time schedule. Dangerous features such as DISA and voicemail deserve also special attention. It is better to be disabled or even removed if they are of no use. Otherwise, in collaboration of the manufacturer, every suggested measure, patch and upgrade should be applied.

The physical infrastructure and especially the expensive one should be protected with proper security measures, be kept in a controlled environment not easily accessible to everyone, and be well hidden from people that don't need to know where it is. In many companies, everyone is invited to have a look at their expensive PBX (Private Branch Exchange), which is waiting behind an open door. Just follow the signs that lead to the place. As a matter of fact many companies tend to advertise their "treasures" by signs and labels making it

easier for the determined one to find. Modern telephone exchanges use expensive and easily removed and carried equipment (i.e. exchange cards) so a couple of minutes would be enough for an incident to take place causing apart from the economic damage also an outage. Furthermore protection from unauthorized access is a must because access to the premises means complete access to our network. A "bug" or other intercept device could be planted there, at the heart of our network.

Specialized experts with manufacturers' help should perform frequent actual security audits including penetration testing and social engineering in order to evaluate the level of security. Problems found in the security audit should be patched immediately.

For those who can bear the costs, hardware solutions such as PBX firewalls should be investigated in order to provide a more thorough defense suite. PBX firewalls are the exact analogy of computer firewalls, filtering in real time incoming and outgoing traffic to detect abnormal usage, high cost and duration calls, data calls etc. Hardware could also be supported by specific software code to ensure safe and risk free PBX management and operation.

Another usually forgotten aspect is the protection against environmental elements and disasters. A fire could burn our infrastructure endangering also human lives. A flood could prove extremely harmful for the sensitive and expensive equipment while a water pipe leak can cause a severe damage and a complete collapse of the network which will not be easy to deal with. It is of great importance to take all the appropriate measures to guard against such incidents. In case of a natural disaster, such as an earthquake, there should always be provision for disaster recovery and business continuity procedures that will ensure that the basic communication needs will be restored the soonest possible.

Besides technical means, common sense and tidiness can help a lot. . It is of paramount importance to operate on a set of standard operating procedures. Equipment, patching and connections should be well documented not only to help technicians in their job to easily expand and service the network but also to make it possible to easily identify and remove any "external" elements, such as "bugs". Moreover, in case of a disaster as stated in the previous paragraph, proper labeling and documentation could speed up the repair time.

Protecting our equipment is not enough. As we will see, our trash needs also protection and proper ways of disposal. Hackers or other persons trying to get access to our network often use the so called "dumpster diving" technique which can give them valuable information about our security protocols, anti hacking measures, the topology of our network and possible soft spots in security or in the infrastructure, or even worse give them access codes and usernames which can lead them directly into our network. The technique is carried out by just inspecting our trash hoping to find valuable data. It is thus of great importance

to destroy all sensitive data before disposal and not just leave them in the dumpster as an easy prey for anyone to find.

5 Other Issues

So far we examined technical threats. However, it is not always necessary to be technically savvy to abuse a telephone network. A very common technique for accessing it is the use of Social Engineering; people who pretend to be someone else use their persuasion to extract valuable information for the network itself or information that can be helpful for infiltrating it. There are two good examples here, one is the use of Social Engineering by a person that impersonates a false ID via the phone and extracts information from a secretary, a username and a password to login to the network and the other is a person that gives false information and impersonates a network technician in order to extract information about the whereabouts of the PBX and take the secretaries approval to access it, and from there to have full access to the network. Further examples can be found in [MS02]. Education and properly enforced security procedures and policies can help mitigate the danger.

6 Conclusions

Closing our analysis we will move from threats coming from outside to threats that originate form the inside. Insiders can prove to be a very difficult enemy hard to deal with. They can prove a valuable ally for a hacker, providing him with passwords and information about the infrastructure. They could also simply give him permission to enter a company and poke around the equipment. Finally insiders could act by themselves exploiting our assets, planting "bugs" etc. For example, an employee, contractor or even a cleaner could forward a seldom-used extension to an overseas number and make international calls by calling a local rate number in the office. Needless to say who is actually paying for the call.

With the advent of new telecommunication technologies which are based around open communications via the Internet Protocol (VoIP) the situation will get even more complicated. The introduction of these technologies means that IT and telecoms managers need now to become even more alerted to prevent new and existing threats that are typically associated with data networks, now impacting voice networks. Conventional PBXs typically use proprietary protocols and specialized software and have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers are multiplied [WK05]. Without

diligent attention, telecoms systems are in grave danger of becoming the weak link in the network and utterly defenseless against targeted attacks. This paper does not address security issues that affect voice over IP systems. It is estimated though that due to the robust operation of existing classical or hybrid PBXs (many of them are up and working for more than 20 years without significant problems) they will still consist the greatest part of private owned telephony equipment and as such need to be addressed separately and concisely.

PBX fraud has been allowed to flourish due to ignorance and naivety. Telephony security has remained a poor second place to IT security [Bla00]. Hopefully this simple taxonomy of dangers and threats and the proposed security program will help to better understand the dangers and the problems and will always be a good quick reference guide for both users and administrators.

References

[And04] Iosif Androulidakis. PBX security. In *2nd Pan-Hellenic Conference on Electronic Crime*, 23-26/11/2004.

[Ava02] Avaya. *Avaya Products Security Handbook*, chapter 2. Nov 2002. Issue 8.

[AW01] Archer and White. *Voice and Data Security*. Sams Publishing, Indianapolis, 2001.

[Bla00] Vincent Blake. PABX Security, Information Security Technical report. 5(2):34–42, 2000.

[BW07] Wade H. Baker and Linda Wallace. Is information security under control? *IEEE Security & Privacy*, 5(1):36–44, 2007.

[Den98] Dorothy E. Denning. *Information warfare and security*. Addison-Wesley Professional, 1st edition, 1998.

[MS02] Kevin D. Mitnick and William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing, Inc., 2002.

[NIS01] NIST. PBX vulnerability analysis. special publication 800-24, 2001.

[Pol05] Craig Pollard. Telecom fraud: the cost of doing nothing just went up, White paper. Insight Consulting, Feb 2005.

[Wes00] David West. De- Mystifying Telecom Fraud. Telecom Business, July 2000.

[Wik07] Wikipedia. PBX, March 2007. http://en.wikipedia.org/wiki/Pbx.

[WK05] T.J. Walsh and D.R. Kuhn. Challenges in securing voice over IP. *IEEE Security & Privacy*, 3(3):44–49, May-June 2005.