Jährliches Magazin der tunesischen wissenschaftlichen Gesellschaft e.V. | Ausgabe 2009

TUNESISCHE WISSENSCHAFTLICHE GESELLSCHAFT

twg

2009 Zeitschrift

in Zusammenarbeit mit der TAG Tunesische Akademiker Gesellschaft e.V.

Izis... das neue Autokonzept der tunesischen Firma Wallys

Das WEP-Verschlüsselungsprotokoll... kann man dem noch vertrauen?

MIMO technology: the next-generation wireless

IMPRESSUM

Die twg-Zeitschrift bietet einen Überblick über die verschiedenen Aktivitätsbereiche und Interessengebiete der Vereinsmitglieder und –freunde.

Außerdem befassen sich die enthaltenen Beiträge mit Themen, die im Alltag der Akademiker in Deutschland von großer Bedeutung sind, seien es über Studium, Berufsleben oder noch neue wissenschaftliche und technologische Forschungsarbeiten bzw. Erkenntnisse.

Design und Layout: Amine Fahem
PDF-Version
Ausgabe Oktober 2009

Tunesische wissenschaftliche Gesellschaft
c/o UStA der Universität Karlsruhe (TH)
Adenauerring 7

Editorial

LIEBE LESER/INNEN,

es ist uns eine große Freude, die twg-Zeitschrift für das Jahr 2009, dieses Mal in einem neuen Aussehen, auszugeben.

Wie Sie dies der Zeitschrift entnehmen können, haben viele tunesische Akademiker in Deutschland beim Erstellen der Inhalte aktiv mitgewirkt. Hierbei wurde eine bunte Mischung an wissenschaftlichen Artikeln erzielt.

Wir bedanken uns an dieser Stelle ganz herzlich bei allen beteiligten Verfassern für die Zeit, die sie investiert haben, und die dabei entstandenen hochkarätigen Beiträge.

Unserer besonderer Dank gilt unserem Partnerverein der TAG in München für die ergiebige Zusammenarbeit und die stete Beteiligung bei der Artikelsammelaktion. Wir hoffen, dass diese Ausgabe der Anfang einer verstärkten Zusammenarbeit zwischen unseren Vereinen bzw. unseren engagierten Mitgliedern ist.

Vielen Dank, dass Sie sich für die twg e.V. interessieren und Ihnen noch viel Spaß beim Lesen!

Adnene Gharbi
Vorstandsvorsitzender der twg e.V.
&
Amine Fahem
Schriftführer der twg e.V.

Für mehr Informationen:

http://www.t-w-g.org | Tunesische wissenschaftliche Gesellschaft e.V.

http://www.tag-munich.de | Tunesische Akademiker Gesellschaft e.V.

Inhaltsverzeichnis

5 Izis... das neue Autokonzept der tunesischen Firma Wallys

6 More economically viable Wind Turbines

8 NCTUns Der Netzwerzksimulator

10 MIMO technology for next-generation wireless Systems

12 Einführung in die Informationsvisualisierung

14 Schwachstellen des WLAN Verschlüsselungsprotokolls WEP

18 System for Body and Mind Monitoring in coaching Process

22 OFET Organic Field-Effect Transistor

23 I am a PC... and I love this Company!

25 Ferienakademie 2008

Izis...

das neue Autokonzept der tunesischen Firma Wallys

Nach 18 Monaten Entwicklung in einer Garage in La Marsa, hat "Zied Guiga", Absolvent an der Uni Lausanne sein Schmuckstück auf dem Pariser „Salon Mondial de l'Automobile" präsentiert. Das Auto ist ein kleiner Geländewagen. Die große Neuheit dieses Auto ist, dass es aus in Tunesien gefertigten Teilen besteht, außer dem Motor, der aus der französischen Firma PSA stammt. Dies ermöglicht die einfache Reparatur und das Erwerben von Ersatzteilen.

Der Izis wird von einem 1,4 L Motor (75 PS) angetrieben, hat einen Vorderantrieb und kann Steigungen von bis zu 39 Grad bewältigen.

Eine elektrische Version ist geplant. Die Reichweite würde dann 90 Km betragen.

Das Auto wurde in Frankreich getestet und hat die vielen Crashtests bestanden. In Februar 2008 wurde es für die europäischen Straßen genehmigt.

Dank einer einfachen Entwicklung, konnten die Preise klein gehalten werden. Der Izis kostet steuerfrei rund die 10.000 Euro (18.000 TND) und hat viele Interessierte in Europa besonders England und in Süd Amerika.

Das erste Auto wird voraussichtlich in Mai 2009 auf den europäischen Markt kommen. Für dieses Jahr werden zwischen 200 und 900 Exemplare produziert. Des Weiteren ist eine „Low-Cost" vier Sitzer-Version im Programm und wird 2010 in Tunesien vermarktet.

Anis Ayadi
Cand. Dipl.-Ing.
Karlsruher Institut für Technologie (KIT)

Technische Daten

Länge	3,34m
Breite	1,68m
Gewicht leer	920 Kg
max. Gewicht	1350 Kg
Hubraum	1,4 L Benzin
Leistung	55Kw (75 PS)
Getriebe	5 Gänge
Bremsen	Scheiben Vorne / Trommel Hinten
Max. Geschwindigkeit	140 Km/h

More economically viable
Wind Turbines

Nowadays the global energy resources and their impact on the environment are the main subject of a hot debate, which is taking place especially in the industrial countries on the national and international level as well. Hereby is the main concern of the involved Industry about the cost reduction in manufacturing and operating costs and increasing of the efficiency. Additionally other parties focus more on the environmental damage, which should be minimized.

One of the favourable technologies, especially with respect to the environment, is the use of wind turbines.

The aerodynamic is a main part in the design of the wind turbines because it's the whole, which allows the translation of the raw wind energy to a controlled rotation of the rotator following the physical laws and as a result the generation of electric power. So if we want to improve the wind turbines, we have first of all to improve its aerodynamics and to do that, we have to optimize the rotor blades.

Wind turbines rotor blades look a lot like the wings of an aircraft. However they have a thick profile in the innermost part of the blade. Choosing profiles for rotor blades involves a number of compromises including reliable lift (*) and stall (**) characteristics and the profile's ability to perform well even if there is some dirt on the surface. Rotor blades for large wind turbines are always twisted in order to achieve an optimal angle of attack throughout the length of the blade. And the most modern ones are made of glass fibre reinforced plastics (GRP).

Concerning the number of blades, there are three concepts, which are: the Danish three-bladed Concept, two-bladed Concept and one-bladed Concept.

However the Danish Concept is the most successful due to the similarity of the dynamic proprieties to a disc, the high energy output, its stability, the less noise than the other designs and the better looking.

Generally, it is an advantage to have a tall tower (***) in areas with high terrain roughness, since the wind speeds increases further away from the ground.

Towers for large wind turbines may be either tubular steel towers, lattice towers, or concrete towers. Most large wind turbines are delivered with tubular steel towers. Despite the good looking of the tubular steel towers, the lattice towers can be more adequate, because they offer the same stiffness for the half price and amount of used steel. Otherwise they have the advantage of giving less wind shade than a massive tower.

In case of stronger winds it is necessary to waste part of the excess energy of the wind in order to avoid damaging the wind turbine. All wind turbines are therefore designed with power control systems. There are two different ways of doing this safely in modern wind turbines, which are:

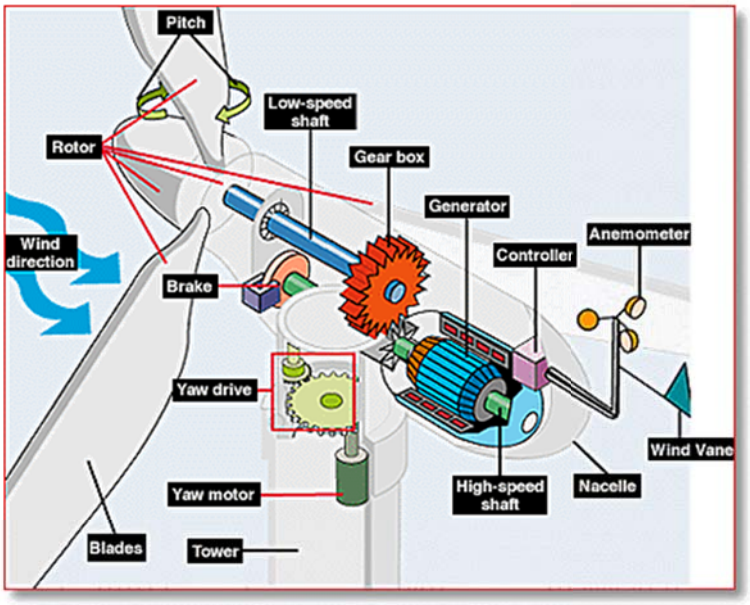
- **Pitch Controlled Wind Turbines:** The turbine's electronic controller checks the power output of the turbine several times per second. When the power output becomes too high, it sends an order to the blade pitch mechanism, which immediately pitches the rotor blades slightly out of the wind. Conversely, the blades are turned back into the wind whenever the wind drops again.

More economically viable Wind Turbines

• **Stall Controlled Wind Turbines:**
Its principle is to avoid the overloading of the generator using the stall phenomenon. However there are two types of stall controlled wind turbines, which are the passive one and the active one. One of the advantages of active stall is that one can control the power output more accurately than with passive stall. Another advantage is that the machine can be run almost exactly at rated power at all high wind speeds. A normal passive stall controlled wind turbine will usually have a drop in the electrical power output for higher wind speeds.

Through our research we could figure out that the most efficient wind turbine must have 3 twisted rotor blades made of glass fibre reinforced plastics (GRP), which look like the wings of an aircraft. Although it has to have an active stall controlling system and a lattice tower.

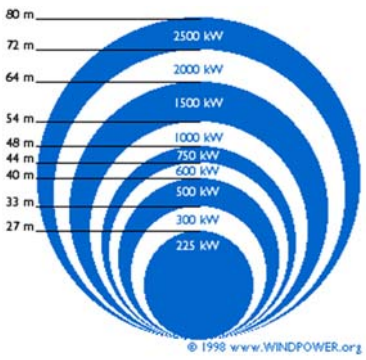
Despite the importance of the aerodynamics in designing a wind turbine, it is still only one part, which requires all the other parts like gearbox, generator and sensors (as illustrated below). And to achieve an optimization, the good coordination with all the other parts and engineers is compulsory. In addition to the technical problems, there are other parameters, which are also important like the budget, environment, the agreement and awareness of the people.



The wind turbine yaw mechanism is used to turn the wind turbine rotor against the wind with the help of electric engines and gearboxes

(*)The reason why an aeroplane can fly is that the air sliding along the upper surface of the wing will move faster than on the lower surface. That means that the pressure will be lowest on the upper surface. This creates the lift, which is perpendicular to the direction of the wind.

(**)Is the phenomenon when the lift from the low pressure on the upper surface of the wing disappears because the air flowing on the upper side stops sticking on the surface of the wing and instead it whirls around in an irregular vortex (=turbulence). Aerodynamics of Wind Turbines: Stall.



Yassine Sellami
Cand. Dipl.-Ing. Maschinenbau
Karlsruhe Institut of Technology (KIT)

NCTUns

Der Netzwerksimulator

NCTUns ist ein offener Netzwerksimulator und Emulator. Er ist der Nachfolger des „Harvard Network Simulators“ und wird von den Forschern der „National Chiao Tung University“ (NCTU) entwickelt.
Für die Beschreibung der Topologie wird die Sprache TCL eingesetzt. Die NCTUns Simulationsmodule werden aber in C++ geschrieben.
Die Technik der Ereignisverwaltung bei diesem Simulator ist eine Mischung aus der diskreten Ereignisverwaltung und der Kernel-Reentering-Technik, so dass Protokollimplementierungen und Applikationen aus der realen Welt benutzt werden können: bei der Kernel-Reentering-Technik erhält jeder simulierte Knoten ein Tunnel-Interface. Die simulierten Verbindungen auf Schicht 2 werden abgebildet. Die Tunnel-Interfaces der Knoten, die in der Simulation verbunden sind, werden auch auf Benutzerebene verbunden. Zur Kommunikation benutzen die Tunnel-Interfaces die TCP/IP-Implementierung im Linux-Kernel. Neue TCP/IP-Module müssen nicht für die Simulation geschrieben werden und so können echte Applikationen in der Simulation integriert werden.

Bei NCTUns interagieren Prozesse der Benutzerebene (User-Level Processes), ein Betriebsystemkernel und eine NCTUns Simulationsmaschine (auch auf der Benutzerebene), um eine Simulation durchzuführen [WHLC+07].

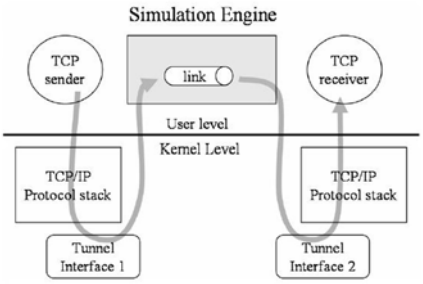


Abb.1: Karnel Reentring [WHLC+07]

Der NCTUns-Simulator besteht aus:
• einer Simulationsmaschine: Die NCTUns-Simulationsmaschine bietet zahlreiche API-Funktionen, die den Entwurf neuer Protokollmodule ermöglichen. Die Simulationsmaschine kann als ein kleiner Betriebsystem-Kernel betrachtet werden. Die ist für elementare Aufgaben wie z.B. Ereignisverwaltung, Zeitverwaltung und Paketmanipulation zuständig. Ihre APIs spielen dieselbe Rolle wie die Systemaufrufe bei einem Unix-Kernel.
• Protokollmodulen: Ein Modul stellt eine Ebene in dem Protokollstack dar. Z.B. implementiert der ARP-Modul (Address Resolution Protocol) das ARP-Protokoll. Module können zusammengefügt werden, um ein Protokollstack zu bilden. Module können zu einem existierenden Protokollstack hinzugefügt werden. Existierende Module können auch ersetzt werden.
• einer GUI (Graphical User Interface): Die GUI erlaubt dem Benutzer, eigene Topologien zu erstellen, die Simulationsknoten einzustellen (Zugehörigkeit zu einem Subnetz, Mac-Adresse, IP-Adresse...), die Simulation durchzuführen und anschließend die Paketanimation abzuspielen. Die GUI ist eine Schnittstelle zwischen dem Benutzer und der Simulationsmaschine. Die GUI ist nur ein Client, die als Server, die Simulationsmaschine hat. Man kann auch ohne die GUI eine

Literatur:

[WHLC+07] : Prof. Shie-Yuan Wang, Chih-Hua Huang, Chih-Che Lin, Chih-Liang Chou und Kuo-Chiang Liao: The Protocol Developer Manual for the NCTUns 4.0 Network Simulator and Emulator, 2007.

NCTUns

Der Netzwerksimulator

tion direkt an der Simulationsmaschine durchführen. Die Simulationsmaschine und die GUI können physikalisch getrennt sein. Sie müssen nicht auf demselben Rechner installiert werden: Ein „Job-Dispatcher“ wurde implementiert, um die GUI und die Simulationsmaschine zu verbinden. Der Job-Dispatcher muss an der Simulationsmaschinenseite ausgeführt werden. Neben dem Job-Dispatcher muss auch simulationsmaschinenseitig der Koordinator ausgeführt werden. Er stellt sicher, ob die Simulationsmaschine für neue Simulationsaufgaben bereit ist oder noch mit anderen Simulationsaufgaben beschäftigt ist. Als Ausgabe erzeugt die GUI verschiedene Dateien, die zusammen das Simulationsszenario beschreiben. Unter anderem wird von der GUI eine Tcl-Datei erzeugt. Die Tcl-Datei enthält die Beschreibung der Topologie des simulierten Netzes.

NCTUns unterstützt unter anderem die Schicht 2-Protokolle Ethernet und 802.11 (Infrastruktur- und Ad-hoc-Modus). Der Simulator enthält auch fertige Simulationsmodule für Switches, Access Points, GSM-Antennen, mobile und nicht mobile Stationen und viele andere Netzwerkgeräte.

Damit ein echtes Gerät von NCTUns emuliert wird, muss die Routing-Tabelle auf diesem Gerät angepasst werden, was von allen gängigen Betriebssystemen unterstützt wird. Unter Emulation ist die Integration von echten Geräten bzw. Applikationen in der Simulation zu verstehen. Jedes Gerät in der Simulation bekommt eine eigene IP-Adresse. Die emulierten Geräte haben eine IP-Adresse in der realen Welt und eine Simulationsadresse. Während der Simulation müssen die Geräte mit der Simulationsadresse angesprochen werden, sonst würden die Pakete nicht über den Simulationsrechner geschickt werden.

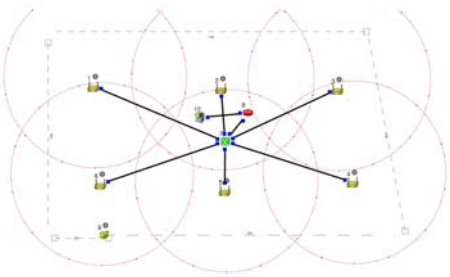


Abb.2: Topologie eines in NCTUns simulierten WLAN-Netzes

Mit NCTUns kann man verschiedene Netze modellieren und die Applikationen unter realitätsnahen Bedingungen testen. Störungen, Interferenzen und Paketverluste können simuliert werden. Auch Paketverluste wegen Mauerdurchgang des Signals können moduliert werden. Manche Faktoren bleiben aber bei der Simulation unberücksichtigt wie z.B. die Reflexion des Signals.

Bei NCTUns wird es aber erst ab der Schicht 3 emuliert, die Physikalischen Verbindungen zwischen Geräten sind alle virtuell. Deswegen eignet sich NCTUns schlecht, wenn man das Verhalten realer Geräte auch Schicht 2 simulieren will. NCTUns ist aber ein praktisches Tool, um neue Protokollimplementierungen zu testen oder um das Verhalten realer Applikationen ab der Schicht 3 zu ermitteln.

Fedi El Arbi
Dipl.-Inf.
Karlsruher Institut für Technologie (KIT)

MIMO technology

for next-generation wireless Systems:

Key Success Factors and Challenges

Most actual communication systems use a SISO (single input single output) configuration with one transmitter and one receiver and information sent over a single channel. MIMO (multiple input multiple output) transmission transmits information over multiple channels, but only occupies the bandwidth of a single channel, and the day when these multiple antenna systems will be implemented in real-word is nearing. Moving from SISO towards MIMO is an evolutional step that is comparable to the transition from analogue to digital transmission of data. This technology can now be used in a wide range of commercial communications devices including mobile phones, PDAs, and laptops. MIMO is also planned to be used in the next 3GPP Mobile radio telephone standards such as the Long Term Evolution (LTE) standard (potential follower of UMTS).

The typical MIMO configuration for cellular network is so that both the base stations as well as the mobile stations are equipped with multiple antennas.

Many commercial wireless LAN (WLAN) devices today employ a 3 × 2 configuration of three transmitters and two receivers for each user. In the future, advanced MIMO techniques, i.e. multi-user MIMO (MU-MIMO), could be also introduced.

Because multiple data streams are transmitted in parallel from different antennas there is a linear increase in capacity with every pair of antennas added to the system. An important fact to note is that unlike traditional means of increasing capacity,

MIMO technology
for next-generation wireless Systems:
Key Success Factors and Challenges

MIMO systems do not increase bandwidth in order to increase throughput. They simply exploit the spatial dimension by increasing the number of unique spatial paths between the transmitter and receiver. In addition, since the channel paths are in general not strongly correlated, MIMO can be used to combat the change of the SISO channel gain over the time due to the Multi-path phenomena (or fading). Such an effect is called diversity which exploits the independent fading in the multiple antenna links to enhance signal diversity.

Along with the benefits of increased bandwidth, multi-signal transmission and re¬ception adds more layers of complexity. For instance, the transmitters must be aligned in time and phase and have a high degree of isolation from each other. Besides new (complex) signal processing algorithms, coding concepts are necessary to exploit the potential of MIMO systems. This presents a number of challenges when moving from SISO to MIMO based systems.

Amine Mezghani
Cand. Dr.-Ing. Elektrotechnik
TU München

Einführung in die Informationsvisualisierung

Der stets sinkende Preis der leistungsfähigen Computergrafik-Hardware führte zu enormen Fortschritten im Bereich wissenschaftlicher Visualisierung. Beginn der 90er Jahre entstand die Idee, die Verfahren der wissenschaftlichen Visualisierung für die Visualisierung abstrakter Daten einzusetzen. Somit ist ein neues Gebiet der Informatik nämlich Informationsvisualisierung entstanden.

Unter Informationsvisualisierung versteht man eine Reihe von Methoden und Werkzeugen zur grafischen Darstellung von großen Datenbeständen.

Der Xerox PARC User Interface Research Group definiert die Informationsvisualisierung als die computergestützte Aufbereitung und die visuelle Repräsentation abstrakter Informationen mit dem Ziel, den kognitiven Zugang zu elektronisch gespeicherten Daten zu erleichtern.

„Information Visualization is the use of computer-supported interactive visual representation of abstract data to amplify cognition." -Xerox PARC User Interface Research Group.

Man unterteilt Visualisierungen nach ihren Anwendungsgebieten grundsätzlich in zwei Kategorien:

- Visualisierung zur Repräsentation von Informationen (z.B. Simulationsergebnisse).

- Visualisierung zur Datenexploration (z.B. Suchmaschinenergebnisse).

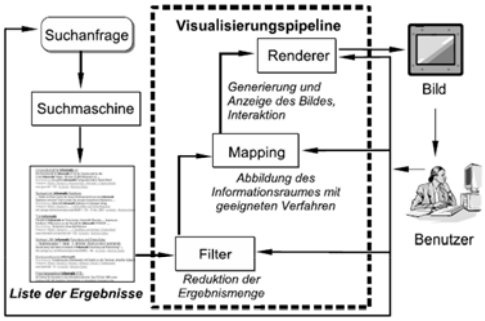


Abb. 1: Zyklus des Visualisierungsprozesses [1]

Laut [1] unterteilt sich der Visualisierungspipeline (siehe Abbildung 1) in 3 Stufen:

- Filtering: Aufbereitung und Reduktion der Daten
- Mapping: Abbildung der Daten auf geometrische Objekte
- Rendering: Generierung und Anzeige des Bildes

Mit der Filterungsstufe werden die abstrakten Daten durch verschiedene Filtermechanismen aufbereitet und gegebenenfalls einer Reduktion unterzogen.

In der Mapping-Stufe wird die Visualisierungstechnik eingesetzt, indem die gefilterten Daten auf abstrakte geometrische Objekte (z.B. Kreise, Linie, Kugel) und ihre Attribute (z.B. Position, Farbe, Größe) abgebildet werden.

Bei der Rendering-Stufe wird das tatsächliche anzuzeigende Bild generiert und die notwendige Interaktion bereitgestellt.

Literatur:

[1]: Martha Argentina Barberana Najarro, "Dissertation: Visualisierung von Informationsräumen", Juni 2003

Einführung in die Informationsvisualisierung

Der Benutzer kann jederzeit über eine Benutzeroberfläche die drei Stufen beeinflussen, um ein besseres Ergebnis zu erzielen. Er kann zum Beispiel die verwendete Visualisierungstechnik in der Mapping-Stufe ändern oder auch bessere Filtermechanismen einsetzen.

Seit Anfang der 90er Jahre wurden verschiedene Techniken zur Visualisierung von Informationen entwickelt.

Mit Einführung von VRML (Virtual Reality Modeling Language) und SVG (Shared Vector Graphic) hat sich die Webvisualisierung in letzter Zeit sehr durchgesetzt.

Abbildung 2 stellt die Entwicklung der verschiedenen Techniken (oberhalb der Zeitachse) und Werkzeugen (unterhalb der Zeitachse) über eine Zeitachse dar.

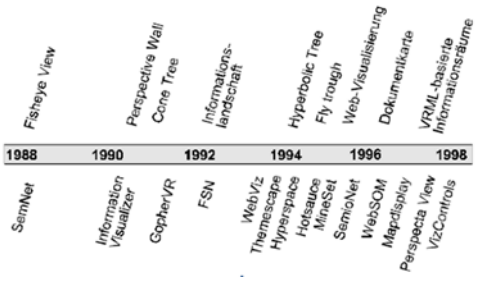


Abb. 2: Entwicklung der Visualisierungstechniken und Werkzeuge [2]

Durch den Einsatz einer geeigneten Technik erhält der Benutzer zuerst einen gesamten Überblick über die Struktur der visualisierten Daten.

Foued Jrad
Dipl. -Ing. -Electrotechnik
Karlsruher Institut für Technologie (KIT)

[2]: Rolf Däßler, "Informationsvisualisierung Stand, Kritik und Perspektiven",Fachhochschule Postdam, 1999

Schwachstellen
des WLAN Verschlüsselungsprotokolls WEP

WEP steht für „Wired Equivalent Privacy“ und ist das von IEEE802.11 ursprünglich vorgesehene Verschlüsselungsprotokoll für WLAN-Netzwerke. Er gewährt dem drahtlosen Netz Schutz gegen Angriffe, indem die Pakete verschlüsselt werden.

WEP hat folgende Vorteile:
- Es ist schwer, den WEP-Schlüssel mit Brute Force Angriffen herauszukriegen, weil der Schlüssel genügend lang ist (40 oder 104 Bit).
- WEP ist selbstsynchronisierend.
- WEP ist effizient und Ressourcenschonend.

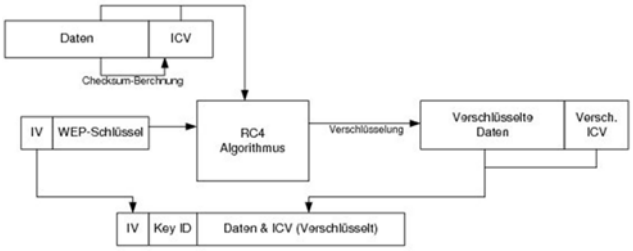


Abbildung1: WEP-Funktionsweise [EdAr03]

Die grundlegenden Funktionalitäten bei einem WLAN-Sicherungsprotokoll sind:

- Authentifikation
- Zugriffskontrolle
- Replay-Schutz
- Schutz gegen Nachrichtenänderung
- Vertraulichkeit

WEP ist bei jedem dieser Gebiete an seine Grenzen gestoßen.

1) Authentifikation

Die Grundanforderungen für die Authentifikation in einem WLAN-Netz sind:

1. Robuste Mechanismen, die nicht „gespooft“ werden können
2. Gegenseitige Authentifikation zwischen dem AP und den mobilen Geräten
3. Von dem Verschlüsselungsschlüssel unabhängige Schlüssel

WEP versagt bei jedem dieser Punkten: Die WEP-Authentifikation basiert auf ein Challenge-Response Verfahren, bei dem der Verschlüsselungsschlüssel benutzt wird, was die Regel 3) verletzt. Bei WEP ist die Authentifikation ein unidirektionales Verfahren: das mobile Gerät kann den AP nicht authentifizieren, was die Regel 2) verletzt.

Abbildung2: Authentifikation im IEEE 802.11[EdAr03]

Außerdem sendet der AP während der Authentifikation einen zufälligen Text. Das mobile Gerät entschlüsselt den Text und sendet ihn unverschlüsselt zurück. WEP benutzt für die Verschlüsselung den RC4-Algorithmus, der auf XOR-Operationen basiert. Ein außen stehender Traffic-Beobachter kann den Challenge-Text unverschlüsselt und verschlüsselt einfangen. Berechnet ein Angreifer **C = P XOR R**, wobei **P** der unverschlüsselte Text ist und **R** der Verschlüsselte, bekommt er eine Kopie von der vom RC4-Algorithmus zufällig generierte Sequenz **C**. Eine Eigenschaft von XOR ist: **P XOR R = C** => **C XOR R = P** und **P XOR R = C** => **C XOR P = R** was dazu führt, dass der Angreifer nun für einen vorgegebenen IV-Wert Daten entschlüsseln und

Literatur:

[EdAr03]: Jon Edney und William A. Arbaugh. Real 802.11 Security. Addison-Wesley, 2003.

Schwachstellen des WLAN Verschlüsselungsprotokolls WEP

vorgegebenen IV-Wert Daten entschlüsseln und verschlüsseln kann. Der Angreifer kann jetzt eine Authenticate-Request an den AP senden, auf den Challenge-Text warten, den mit der vorberechneten Sequenz **C** "XORen" und das Ergebnis mit dem vorher angefangenen IV an den AP zurückschicken. Um das Ergebnis zu überprüfen benutzt der AP den vom Angreifer gewählten AP und generiert die selbe RC4-Sequenz **C**, was dazu führt, dass der Angreifer authentifiziert wird, ohne dass er den WEP-Schlüssel kennen muss.

Ohne den WEP-Schlüssel zu knacken kann der Angreifer mit den anderen Knoten im Netz nicht kommunizieren. Die WEP-Authentifikation bietet aber einem Angreifer mehrere Paare von verschlüsselten Nachrichten und den dazu gehö- rigen verschlüsselten Nachrichten, was der WEP-Schlüssel gefährdet.

2) Zugriffskontrolle:

Die Zugriffskontrolle ist der Prozess, dass einem Gerät die Erlaubnis erteilt, mit dem Netz zu kommunizieren, was mit der Authentifikation nicht zu verwechseln ist. Bei der Authentifikation wird nur die Identität des Gerätes erfahren. Das Gerät erhält aber keine Erlaubnis, auf das Netz zuzugreifen.

Der IEEE802.11-Standard definiert nicht, wie die Zugriffskontrolle implementiert werden soll. In der Regel wird der Zugriff auf das Netz kontrolliert, indem eine Liste von den gültigen MAC-Adressen im AP gespeichert wird. MAC-Adressen können aber geändert werden, deswegen gilt dieses Verfahren als unzuverlässig. Der WEP-Schlüssel ist eigentlich die einzige Verteidigungslinie, die das IEEE802.11 bietet.

3) Replay-Schutz:

WEP hat keinen Replay-Schutz. Das heißt, dass man ein altes eingefangenes Paket an den AP schicken kann, ohne dass der AP erfährt, dass das Paket alt ist. So kann man neue Requests mit alten Responses beantworten. Replay-Schutz wurde im WEP einfach nicht vorgesehen.

4) Schutz gegen Nachrichtenänderung:

Die Arbeit von Borisov et al. [BoGW01] stellt eine Bitumkehrungsmethode vor, in der schrittweise manche Teile des verschlüsselten Textes geändert werden können. Die Arbeit nutzt aus, dass die Position des IP-Headers nach der Verschlüsselung bekannt ist, weil WEP die Positionen von den Bytes nicht vertauscht. Der IP-Header hat ein Checksum-Feld. Ein Bit in dem IP-Header zu ändern, führt zu einem Fehlschlag der Checksum-Überprüfung. Wenn man aber auch die Checksum ändert, könnte die Checksum zum Header angepasst werden und das geänderte Paket wird vom Empfänger akzeptiert.

WEP benutzt auch ICV für die Nachrichtenüberprüfung. Wenn man Stellen in dem verschlüsselten Text ändert, wird der ICV nicht zu dem Klartext passen. Die Logik von WEP ist: der ICV ist verschlüsselt also man kann ihn nicht ändern. Die Arbeit von Borisov und Ian beweist dass es möglich ist, trotz der Verschlüsselung, den ICV-Wert anzupassen. Die CRC-Methode, mit der der ICV berechnet wird, ist eine lineare Methode. Es wurde gezeigt, dass es unter dieser Methode möglich ist, zu wissen, welche ICV-Bits zu ändern sind, wenn

[BoGW01] Nikita Borisov, Ian Goldberg und David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11 http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, 2001

Schwachstellen
des WLAN Verschlüsselungsprotokolls WEP

man ein Bit der Nachricht ändern will. Wenn man eine Nachricht ändern will, muss man nur die Stellen im ICV ändern, die nicht mehr passend sind. Der ICV ist also zwar verschlüsselt, diese Verschlüsselung macht ihn aber nicht viel stärker als einen normalen unverschlüsselten CRC.

5) Vertraulichkeit:
In einer im Oktober 2000 veröffentlichten Arbeit [Walk00] hat Walker potentielle Schwachstellen in WEP vorgestellt. Um Angriffe zu vermeiden, muss theoretisch jedes Paket einen eigenen einmaligen IV haben, was unmöglich ist, da der IV nur 24 Bit lang ist. Man könnte denken, dass eine zufällige Generierung von IVs eine IV-Wiederbenutzung (auch IV-Kollision genannt) in einer kurzen Zeit unwahrscheinlich macht, was aber nicht stimmt. Mit einer zufälligen Generierung bestehen hohe Chancen dass der IV schnell wieder benutzt wird. Dieses Phänomen ist in der Mathematik unter dem Namen „Geburtstagsparadoxon“ bekannt: Die Wahrscheinlichkeit, dass eine Person an dem selben Tag geboren ist, wie ich beträgt 1/365. Ich habe aber 50% Chancen, dass einer aus 25 Leuten seinen Geburtstag am selben Tag wie ich feiert! Die beste Methode, IVs zu generieren, ist also einfach mit jedem Paket den IV-Wert um 1 zu erhöhen. Eine IV-Kollision tritt also nach 224 Pakete auf. IEEE801.11b-Netze sind in der Lage, Pakete pro Sekunde zu übermitteln. À 500 Paket pro Sekunde wird ein IV nach höchstens sieben Stunden wieder benutzt. IV-Konflikte verursachen ernste Sicherheitsprobleme: wenn man die zu einem IV gehörige RC4-Sequenz kennt, kann man jedes Paket, dass den selben IV benutzt entschlüsseln. Um jede beliebige Nachricht zu entschlüsseln, muss man alle mögliche Sequenzen haben, was nur 23 GBytes erfordert. Man muss aber alle Sequenzen berechnen (wie bei 2.1 gezeigt wurde), was nicht leicht ist. Angenommen man hat 2 Nachrichten, die mit demselben (IV, WEP-Schlüssel) Paar verschlüsselt sind. Seien **C1** und **C2** die unverschlüsselten Nachrichten, **P1** und **P2** die Verschlüsselten und Ks der Key Stream. **C1 = P1 XOR Ks** und **C2 = P2 XOR Ks**. Also **C1 XOR C2 = (P1 XOR Ks) XOR (P2 XOR Ks) = P1 XOR P2 XOR Ks XOR Ks = P1 XOR P2**. Man hat jetzt einen Text, der das Ergebnis von der Operation XOR der beiden unverschlüsselten Texte ist. Der Wert von manchen Stellen in dem Klartext ist bekannt, wie z.B. manchen Stellen in den Headern. Der Wert von anderen Stellen ist nicht bekannt, es ist aber bekannt, welche Werte sie haben können, wie z.B. die IP-Adressen-Felder, die nur bestimmte Werte in einem Netz haben können. Wenn man genug Pakete sammelt, bei denen einen IV-Konflikt auftritt, könnte man den Werten einige Teile der RC4-Sequenz erraten und Schritt für Schritt die ganze Sequenz.

Literatur:

[Walk00]: J. Walker. Unsafe at any key size:
an analysis of the WEP encapsulation, 2000

Schwachstellen des WLAN Verschlüsselungsprotokolls WEP

Das kryptographische Hauptproblem liegt aber nicht daran, dass die IVs relativ schnell wiederbenutzt werden, sondern an ihrer Rolle in der Erzeugung einer Klasse von RC4-schwachen Schlüsseln. Es wurde in der Arbeit von Fluhrer et al. [FlMS01] gezeigt, dass bei manchen Schlüsseln, die man als schwach bezeichnet, eine große Anzahl von Bits in den ersten Bytes der RC4-Sequenz nur von wenigen Bits in dem WEP-Schlüssel abhängig sind. Das heißt, manche Bits im Schlüssel wirken auf die Verschlüsselung mehr als die Anderen. Manche Bits haben gar keine Wirkung auf die Verschlüsselung, was die Anzahl der effektiven Bits reduziert, was wiederum einen Angriff auf den Schlüssel vereinfacht. Was noch alles schlimmer macht, ist dass manche Stellen in dem verschlüsselten Text einfach zu erraten sind. Das LLC-Header beginnt z.B. immer mit dem Hexadezimalen Wert „AA“. Wenn man den unverschlüsselten Text kennt, kann man die RC4-Sequenz ableiten und nachher den WEP-Schlüssel. Um diese Schwäche zu beseitigen, wäre es ausreichend, die ersten ein paar generierten R-Werte zu verwerfen, was WEP nicht macht. WEP fördert sogar die Generierung von schwachen Schlüsseln mit dem Hinzufügen von IVs: sogar wenn der WEP-Schlüssel nicht schwach ist, ein schwacher Schlüssel kann beim Hinzufügen von manchen IVs generiert werden.

Zusammenfassung:

WEP war der erste Versuch, Verschlüsselungsprotokolle für WLANs zu entwerfen. WEP hat aber viele Sicherheitslücken, die dazu geführt haben, dass Angriff-Tools entwickelt wurden, mit denen es mittlerweile möglich ist, in weniger als einer Minute den WEP-Schlüssel zu knacken.

Nachdem WEP völlig gebrochen wurde, war es nötig, nach neuen Sicherheitsmechanismen zu suchen. WPA und WPA2 sind viel sicherer und bei denen wurden so gut wie alle Sicherheitslücken von WEP gedeckt, und damit sind sie für Business-Anwendungen reif. Total sicher sind sie aber nicht, DoS-Attacken sind immer noch möglich und Schwache Schlüssel sind mit Wörterbuch-Angriffen schnell zu erraten.

Fedi El Arbi
Dipl.-Inf.
Karlsruher Institut für Technologie (KIT)

[FlMS01]: Scott Fluhrer, Itsik Mantin und Adi Shamir.
Weaknesses in the Key Scheduling Algorithm of RC4.
Lecture Notes in Computer Science Band 2259, 2001.

System for
Body and Mind Monitoring
in coaching Process

Abstract — In order to investigate the correlation between stress and cognitive performance, a mobile Body & Mind Monitoring System was implemented. This system has a modular design and contains different modules allowing a long time and noninvasive monitoring of physiological parameters of a test person in his every day life, for instance ECG, GSR, PPG, respiration and physical activity. The functionality of the created set-up was validated and clinical studies can now be conducted.

I. INTRODUCTION

This research work aims the implementation of a mobile monitoring system which is used in the framework of the Hiper.Campus project in order to investigate correlations of emotional activation (mainly stress), physical activity and cognitive abilities. This system is then used in several studies to identify physiological relevant parameters for the detection of daily-life stress situations. These parameters will deliver the basis for the development of individual support-systems which can be used by students and researchers of our university to enhance their well-being and cognitive ability. Several methods of ambulatory monitoring, which provide the recording of subjective and physiological aspects as well as options for feedback, should be applied.

In order to identify valid parameters for stress-detection, it is necessary to realise a measurement set-up able to acquire these simultaneously in everyday life environment. Therefore we implemented a mobile Body & Mind Monitoring System, registering signals such as Electrocardiogram (ECG), Photoplethysmogram (PPG), Galvanic Skin Response (GSR), respiration and physical activity.

The system is used in two studies. The first study should allow us to examine, by means of psycho-physiological monitoring in natural settings, if certain

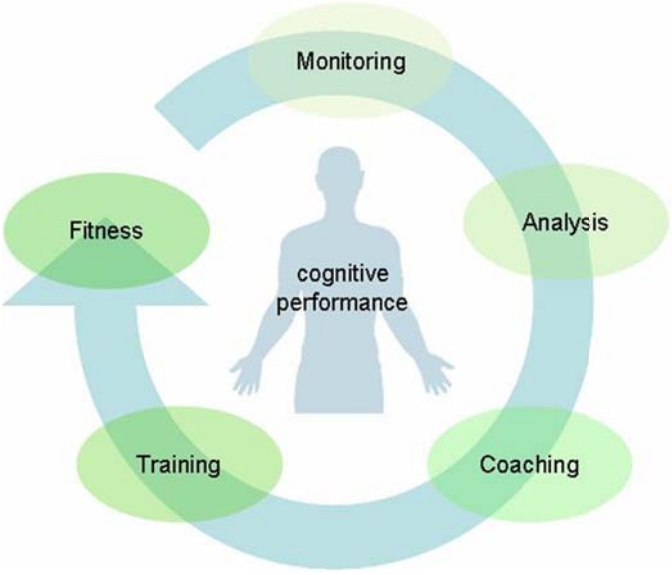


Fig. 1 underlying coaching concept towards an improved cognitive performance with technical support of the Body & Mind Monitoring System

System for Body and Mind Monitoring in coaching Process

methods for stress-reduction and enhancement of physical activity can contribute to an improvement of cognitive functioning. In another study, we want to acquire setting-items, mood-ratings, study-times, learning-outcomes and psycho-physiological parameters of emotional activation and physical activity over the run of the day in order to explore further factors like circadian rhythmic, presence of other persons, etc. and their potential influences on learning processes. The results of the drafted studies should help to develop an individual coaching-system for self-regulated learning. Within the realisation of the research project, sophisticated concepts of cognitive science and affective neuroscience as well as new technological developments are to be generated.

II. METHODS AND MATERIALS

The first step related to the presented roadmap is to implement the Body & Mind Monitoring System. This system comprises a hardware set-up, which has a variety of sensors. These sensors allow a long-time non-invasive monitoring of some physiological parameters such as ECG, PPG, GSR and respiration. These could be relevant for the determination of the stress level of the test person. Furthermore a 3D acceleration sensor-node is used to simultaneously collect information about the activity of that person. The measured signals are then collected by a notebook or PC through a signal acquisition card and are subsequently online post processed and saved by a LabVIEW application.

In addition, two mini card guides were added to the lab system. These are used for a plug-in module, which can directly collect the physio-logical data and either send them via Bluetooth to a terminal or save them locally on a memory card. In this way, we can even use the developed moni- toring system in mobile test scenarios.

In the following sections, the different plug-in sensor modules will be described in more details.

A. ECG-sensor

To detect ECG-Signal, we are using the two-lead method. For instance, we measure the skin potential in the left arm, in the right arm and in a

Literatur:

[1] Mohit Kumar, Matthias Weippert, Reinhard Vilbrandt, Steffi Kreuzfeld, and Regina Stoll, “Fuzzy Evaluation of Heart Rate Signals for Mental Stress Assessment”, IEEE transactions on Fuzzy systems, vol. 15, no. 5, October 2007.

[2] Lizawati Salahuddin and Desok Kim, “Detection of Acute Stress by Heart Rate Variability Using a Prototype Mobile ECG sensor”, International Conference on Hybrid Information Technology (ICHIT'06), 2006.

[3] H. M. Seong, J. S. Lee, T. M. Shin, W. S. Kim, Y. R. Yoon and Y. R. Yoon, “The Analysis of Mental Stress using Time-Frequency Distribution of Heart Rate Variability Signal”, Proceedings of the 26th Annual International Conference of the IEEE EMBS, San Francisco, USA, September 2004.

[4] Lizawati Salahuddin, Jaegeol Cho, Myeong Gi Jeong, and Desok Kim, “Ultra Short Term Analysis of Heart Rate Variability for Monitoring Mental Stress in Mobile Settings”, Proceedings of the 29th Annual International Conference of the IEEE EMBS, Lyon, France, August 2007.

System for Body and Mind Monitoring in coaching Process

reference position on the body surface by means of gel electrodes. After signal conditioning (band pass filtering) and processing (detection of QRS complex), we can determine the HRV (Heart Rate Variability), which is considered to be a meaningful parameter in quantizing the stress level [1], [2], [3], [4].

B. Photoplethysmograph

A finger clip transmission photoplethysmograph is used to register the PPG. In fact, a current source delivers around 18 mA to the IR-Led of the sensor and a very simple voltage divider circuit allows detecting the signal of the photodiode. This latter correlates with the amount of blood in the finger and thus reflects the pulse wave in the blood vessels.

The PPG signal, in combination with the ECG signal, can be used to determine the PTT (Pulse Transit Time), which represents the time needed by a pulse wave to exit the heart and reach the PPG measurement site (in our case the finger) [5]. PTT could also be a meaningful parameter in quantizing the stress level [6].

C. GSR-sensor

There are several standard methods to measure GSR (Galvanic Skin Response) or skin impedance, which some psycho-physiologists consider as an indicator for stress [7]. For our lab-system, we selected the DC constant current concept, since it has a limited polarisation effect on the electrodes [8]. There we have a constant DC current source, which applies, by means of gel electrodes, a limited current (10µA) to the skin. The measured voltage difference between the two electrodes is then proportional to the skin impedance. The electrodes are attached to the palm of one's hand; that is we are adopting a thenar and hypothenar elevation [8].

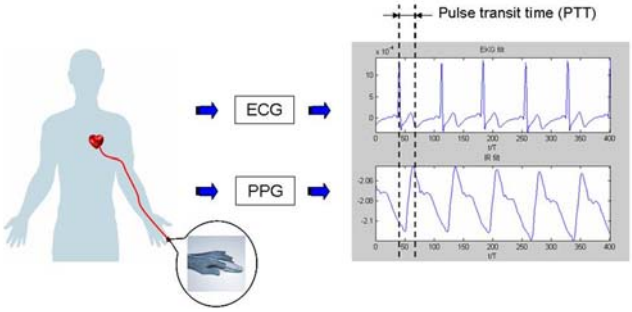


Fig. 2 Extraction method of PTT

Literatur:

[5] P. Vollmer, P. Boll, W. Stork, N. Lutter, A. Wagner, U. Großmann and J. Ottenbacher, "Entwicklung eines mobilen, kontinuier- lichen und nicht-invasiven Blutdruckmessgerätes mit Bluetooth Datenübertragung", Illmenau: BMT, 2004.

[6] R. L-C. Pan, B. Chen and J. K-J. Li, "noninvasive monitoring of autonomic cardiovascular control during stress", Bioengineering Conference, Proceedings of the 1993 IEEE Nineteenth Annual Northeast, Page(s):187 – 188, March 1993.

[7] Nutan D Ahuja, Amit K Agarwal, Ninad M Mahajan, Naresh H Mehta and Hatim N Kapadia, "GSR and HRV: Its Application in Clinical Diagnosis", Proceedings of the 16th IEEE Symposium on Computer-Based Medical Systems (CBMS'03), 2003.

System for Body and Mind Monitoring in coaching Process

D. Respiration-sensor

Another physiological parameter, which our system records, is the respiration rate for chest- and abdomen-breathing. For that purpose, we make use of a respiration effort sensor, which contains a piezoelectric crystal that converts chest or abdominal respiration movement to a small analog voltage. In this way, we can detect the respiration waveforms and thus calculate the respiration rate.

E. 3D acceleration-sensor

The 3D acceleration sensor is used to provide context information for the Body & Mind Monitoring System during stationary and ambulatory measurement scenarios [9]. In fact, we can for example control the excessive movement of one's leg, which reflects being in a stress situation, during a stationary test. And for an ambulatory test, the context information is very important to know whether a registered unusual physiological reaction is due to a physical effort or to a stress situation.

Fig. 3 current Body & Mind Monitoring System

III. RESULTS AND OUTLOOK

The first version of the hard- and software set-up of the Body & Mind Monitoring System has been already implemented and first measurements have shown a reliable monitoring functionality of the system. The next step is to carry out the planned studies, which should allow checking the correlation of emotional activation (mainly stress), physical activity and cognitive abilities.

Dipl. Ing. Adnene Gharbi
Cand. Dr. Ing. Electrotechnik
TH Karlsruhe

This work was conducted at ITIV (Institute for Information Processing Technology), University of Karlsruhe (TH), Germany in cooperation with the House of Competence (HoC) at the Karlsruhe Institute of Technology (KIT)

Literatur:

[8] W. Boucsein, "elektrodermale Aktivität", Berlin: Springer-Verlag, 1988, pp. 89-114

[9] L. Jatobá, U. Großmann, J. Ottenbacher, S. Härtel, B. von Haaren, W. Stork, K.D. Müller-Glaser and K. Bös, "Obtaining Energy Expenditure and Physical Activity from Acceleration Signals for Context-aware Evaluation of Cardiovascular Parameters", Venezuela: CLAIB, 2007.

OFET

The Organic Field-Effect Transistor

Since Bardeen, Schockley, and Brattain invented the world's first transistor in 1947, field-effect transistors (FETs) have dominated the mainstream microelectronics industry. The production processes require sophisticated photolithographic patterning, as well as high-temperatures and high-vacuum; hence the production costs are quite high.

Recent developments in the conducting (conjugated) polymer technology, however, offer quite different application opportunities, bringing a new vision to electronics. Since the late 1970s conjugated polymers have been a focus for the worldwide research as they combine the non-insulating electrical properties of a delocalized π-electron system with the material strength of polymers. Schottky diodes, light-emitting diodes, photodiodes, chemical sensors and organic field-effect transistors (OFETs) have been constructed.

OFETs which are made of conjugated polymers present several potential advantages. First, the deposition techniques for semiconductor films allow large areas to be coated. Many conjugated polymers can be synthesized in a way that they are soluble in organic solvents, so that they can be processed by spin-coating, casting or by various printing methods. Therefore a high-temperature processing is not necessary for producing films. Second advantage is that polymers are mechanically tough and flexible, therefore compatible with plastic substrates. This offers the possibility to realise foldable, flexible products with extremely light-weight. Since the report of the first solution-processed organic field-effect transistor in 1986, there has been great progress in both the materials' performance and development of new fabrication techniques. OFETs have already been demonstrated in applications like organic solar cells,

sensors, memory devices, flexible displays and radio frequency identification tags (RF-IDs).

Research in the field of OFETs has been conducted in an interdisciplinary level on many different disciplines, which have to work parallel in good collaboration. Organic chemists work on the synthesis of high-mobility, high-purity, and high-stability semiconductors. Electronic engineers are trying to improve circuitry that can be realized by OFETs. Physicists are working on the physical model of OFETs, whereas material scientists are looking for new materials and investigating the interface related issues in OFETs.

Zied Fahem
Cand. Dr.-Ing. Elektrotechnik
Universität Hamburg-Harburg

I am a PC...
and I love this Company!

„I am a PC… and I love this Company!“, C'est avec cette phrase désormais mythique que Steve Ballmer a commencé le Microsoft Company Meeting 2008. Cet évènement a été d'autant plus important et symbolique qu'il a coïncidé avec le 25ème anniversaire de la filiale Microsoft France.
Mais faisons un petit retour en arrière. 6 mois pour être exact. Mon aventure chez Microsoft a commencé en Avril dernier. Après quelques péripéties qui me font sourire maintenant que j'y pense, j'ai finalement réussi à intégrer la division « Services Premier » en tant que stagiaire Technical Account Manager - Responsable Technique de Compte pour les anglophobes. Mais que fait un TAM au juste ?

Il faut savoir que l'activité de Microsoft ne se limite pas aux logiciels. La stratégie Microsoft, c'est Software + Services et le contrat Premier, réservé aux grandes entreprises, consiste à accompagner les clients afin de les aider à exploiter au mieux les fonctionnalités offertes par les différentes technologies mises à leur disposition. Ceci inclut bien entendu le support technique mais aussi des audits, du conseil, de l'assistance au déploiement d'architecture et la mise en place de processus assurant un meilleur fonctionnement du département IT. La vente de licences ne suffit pas à avoir des clients très satisfaits et la satisfaction du client est la priorité de tout Microsoftee. Et c'est là qu'intervient le TAM. Le TAM accompagne le client au jour le jour, répond à ses questions, le conseille sur la façon de tirer le maximum de profit des technologies composant son architecture et lui présente les produits susceptibles de l'intéresser. Il organise des workshops, des ateliers et des journées de transfert d'expertise. Il est également présent lorsque le client fait face à des situations de crise et se charge de trouver les ressources techniques les plus adaptées et les plus à même de résoudre les problèmes rencontrés.

En tant que stagiaire, j'ai eu l'occasion de découvrir ce métier qui allie expertise technique, tâches managériales et gestion de la relation client. Nous étions 5 stagiaires à répondre aux questions techniques des clients transférées par les TAM et j'avais pour mission, en plus du traitement des questions, de coordonner cette activité et de faire en sorte que les TAM aient toujours une réponse, fût-elle négative.

Je devais également m'occuper des contrats internes permettant aux clients en cours de renouvellement de contrat ou aux éventuels futurs clients de bénéficier des services et du support Microsoft.

Mais la tâche la plus importante a été celle de CritSit Manager. Les incidents techniques rencontrés chez les clients sont classés par sévérité de D à A suivant leur criticité et leur impact sur la production. Les incidents de sévérité A ainsi que les désastres (sévérité 1) portent le doux nom de CritSit. Lorsqu'un client fait face à une CritSit, le TAM doit réagir en moins d'une heure. Si ni lui ni son backup ne sont disponibles, le CritSit Manager intervient pour débloquer la situation au plus vite. Il intervient également lorsqu'une CritSit a lieu dans un pays où les heures ouvrées n'ont pas encore commencé en vue d'assurer un support en 24x7 au niveau mondial. Le CritSit Manager intervient également pour soutenir le TAM

I am a PC...
and I love this Company!

au cas où la crise prendrait de l'ampleur et que la situation commencerait à devenir ingérable.

J'ai également eu la possibilité de participer à des projets humanitaires financés par Microsoft et visant à aider des ONG à améliorer le quotidien des plus démunis. Car en somme, les nouvelles technologies doivent aussi êtres employées à changer le présent des défavorisés et à leur offrir un futur rempli d'espoir.

J'ai énormément appris de ce stage sur le plan managérial et technique. Les formations et le fait de côtoyer des ingénieurs très compétents mais surtout avenants et serviables y sont pour beaucoup.

Il est vrai qu'en pensant à Microsoft, aux milliards de dollars de chiffre d'affaires et aux dizaines de milliers d'employés, on peut penser à une structure rigide, hiérarchisée, voire inhumaine. Il n'en est rien ! Quelque soit la fonction occupée ou le pays, les Microsoftee sont accessibles et il est facile de lancer une discussion avec un Manager en Allemagne, un TAM aux US ou un CritSit Manager à Dubaï. Je pense que c'est ce côté humain qui m'a le plus impressionné durant ce stage. Déjeuner à la même table qu'un TAM, participer à un tournoi de foot avec un Manager ou discuter avec le Directeur de division lors d'une soirée ou d'un dîner sans sentir le poids de la hiérarchie ne fait qu'accentuer le sentiment d'appartenance et d'unité et facilite beaucoup l'intégration. Bien sûr, l'obligation de résultats est omniprésente et les objectifs à atteindre sont très élevés en termes de chiffre d'affaires réalisé, mais ceci n'est que la réalité du monde libéral dans lequel nous vivons. Mais chez Microsoft, faire des bénéfices aux dépens du client ou des partenaires est contraire à la stratégie du groupe, qui s'inscrit dans l'innovation mais surtout dans la continuité et la confiance mutuelle, et ce afin de garantir la pérennité de l'entreprise.

C'est ce qui a été réalisé en France depuis 25 ans, et c'est ce que Microsoft s'engage à réaliser pour les 25 prochaines années et au-delà.

Néjib Kchouk
Technical Account Manager trainee
Microsoft France

Ferienakademie 2008

Ein wissenschaftliches Förderungsseminar in Sarntal, Italien

„Toll war's", „die beste Sache, die mir je in meiner Studienzeit passiert ist", "schade, dass die zwei Wochen um sind", „absolut empfehlenswert!": solche und andere Kommentare konnte man gegen Ende des Kurses öfter hören. Und dabei war unser Kurs einer mit eher längeren Vorträgen und hatte doch einige Vorbereitungszeit gekostet. Trotzdem waren sich am Ende alle einig: *„der Aufwand hat sich gelohnt"*.

Insgesamt waren wir 16 Leute im Kurs 7: Professor Rigoll (TU München), Professor Yang (Universität Stuttgart) und Professor Kellermann (Friedrich-Alexander-Universität Erlangen-Nürnberg), sowie 13 Studierende.
Die Mischung verschiedener Unis und Semester machte den Kurs zu einem besonderen Erlebnis.

Unser gemeinsames Thema „Natürliche akustische Mensch Maschine Interaktion" prägte den Kurs. Unter diesem Begriff versteht man die Methoden der Verarbeitung des Sprachsignals angefangen von der akustischen elektronischen Verarbeitung des Signals am Eingang (Mikrophon) und am Ausgang (Lautsprecher) des Systems. Zu den grundlegenden Aufgaben gehörten grundsätzlich die Entzerrung und die Enthallung des Signals, sowie die Echo-Kompensation. Akustische Lokalisierung und Ausrüstung von „Smart conference-rooms" prägten die Forschung der Kollegen aus Erlangen. Die 2 Studenten aus Stuttgart haben sich intensiv mit dem paralinguistischen Teil der Sprachverarbeitung auseinander gesetzt. Dazu zählen die „Merkmalsselektion" der wesentlichen Eigenschaften der menschlichen Stimme sowie die „Emotionserkennung" im Sprachsignal. Unsere Mannschaft (TU München) hat sich auch durch das Forschungsthema „Spracherkennung" ausgezeichnet. Ich habe in diesem Rahmen „die statistischen Methoden der Spracherkennung" eingeführt und meine Kollegen haben mit deren Adaptation und Implementierung das Seminar abgeschlossen.

Die Diskussionen, zusätzlichen Erläuterungen und Nachfragen führten so zu Vortragszeiten bis zu drei Stunden. Der in Pausen servierte Kaffee und Kuchen schmeckte jedes Mal so gut, dass wir gerne manchmal eine zweite Pause gemacht hätten. Doch nicht nur Kaffee und Kuchen waren sehr gut, auch die Unterkunft war ausgezeichnet. Der Blick von unseren angenehmen Doppelzimmern im Gasthof Rabenstein auf das *„Sarntal"* war bei dem schönen Wetter begeisternd, und das Essen konnte kaum besser sein.

Uns allen hat die Ferienakademie einen Riesenspaß gemacht. Der enge Kontakt zu Dozenten und Professoren, zu anderen Teilnehmern, anderen Fachdisziplinen, in Verbindung mit einem interessanten Thema und dem schönen Sarntal lassen nur einen Schluss zu: *„Wer nicht an der Ferienakademie teilnimmt ist einfach selber Schuld."*

Othmane Khelil
Cand. Dipl.-Ing. Elektrotechnik
TU München

Tunesische Akademiker Gesellschaft

www.tag-munich.de

- **Gründungsdatum: 1999**
- **Sitz: München**
- **Anzahl der Mitglieder: ca. 130**
- **Tätigkeitsbereich: Bundesweit**

Arbeitsgruppen

Öffentlichkeitsarbeit

Technik & Studium

Kultur

Sport

Studierende während des Studiums unterstützen

Kontakte zwischen den Akademikern fördern und Netzwerke ausbauen

Kontakte zwischen Unternehmen und Akademikern knüpfen

Integration der tunesischen Studierenden in die deutsche Gesellschaft

Highlights

Karriereforum

Mai 2008

10 Firmen

300 Besucher

Orientalische Party

November 2008

Grillfest

Juni, Dezember 2008

Karriereforum 2009

Am 06. Juni an der Hochschule München

Mitgliedschaft: 10€ für Studenten und 15€ für Absolventen

Vorteile:

- Kontakte knüpfen und Weiterbildung
- Fachliche Betreuung während des Studiums
- Vergünstigungen für Veranstaltungen

(Seminare, Workshops, Ausflüge, Partys, Grill...)

Tunesische Wissenschaftliche Gesellschaft e.V.

gegründet 1992

AUSTAUSCH...

KOMPETENZ...

EXZELLENZ

www.t-w-g.org