Teaching activities in Tunisia for 2010

The IFIP-TC6 teaching activities for 2009 - 2010 will take place in Tunis (Tunisia) at the ***Ecole Supérieure Privée d'Ingénierie et de Technologies (ESPRIT)***, during December 1-3, 2010.

"IFIP-TC6 School in Networking Trends"

Co-chairs:

- **Dr. Farouk Kamoun** Professor Emeritus member of CRISTAL Research Lab ENSI. Head of R&D ESPRIT School of Engineering. Tunis, Tunisia
- **Prof. Ana Pont Sanjuán**. IFIP Working Group 6.9 Chair.

Objectives:

- Give the students an overview about recent topics on communication technologies, virtualization, Network Security Monitoring, Opportunistic Networks.
- Increase their abilities for designing, implementing and maintaining communication networks.

Addressed:

- Master and PhD students.
- A maximum of 25 students is highly recommended.

Course Organization:

- The course is organized in 3 independent modules. Each module consists on 6 hours teaching.
- Teaching Language will be English.
- No fees will be applied.

Module	Title	Hours	Speaker	Schedule
M1	Virtualization	6	Dr. Orhan Gemikonakli	Dec. 1
M2	Opportunistic Networks	6	Dr. Rodrigo Santos	Dec. 2
M3	Network Security Monitoring	6	Dr. Siraj Shaikh	Dec. 3

Virtualization

ORHAN GEMIKONAKLI, obtained his first degree in Electrical Engineering from Eastern Mediterranean University in Cyprus, in 1984. He then continued his studies at King's College, University of London where he obtained his MSc in Digital Electronics, Computers and Communications, and PhD in Telecommunications in 1985 and 1990 respectively. His PhD work was on the analytical modelling and performance evaluation of two-link satellite and terrestrial digital communication systems in Gaussian/non-Gaussian impulsive noise as well as various interferences and system imperfections. Spectrally efficient modulation schemes were considered in this study. He worked at King's College as a post-doctoral Research Associate evaluating the performance of Trellis Coded Modulation Systems, for a couple of years before moving in 1990 to Middlesex University, London as a Lecturer. After working there as a Senior Lecturer, Principal Lecturer, and Academic Group Chair (Acting) for seventeen years, he is now the Head of Department, Computer Communications at this Institution. Throughout his academic career, Gemikonakli developed successful PG programmes in Telematics, Computer Networks, Network Management, Network Security, and Telecommunication Engineering. He taught telecommunication, signal processing, computer networks, programming, network security, operating systems, and modelling and simulation at UG and PG levels as well as supervising PhD students. Gemikonakli was involved in various European technology transfer projects. He is a member of the IET, and a Chartered Engineer. His main research interest is in network security, and performability modelling of complex systems. Gemikonakli published more than 70 research papers in refereed journals and conference proceedings. He serves on various Conference Programme Committees, and advisory boards of scientific journals. His e-mail address is: o.gemikonakli@mdx.ac.uk and his Web-page can be found at : http://www.mdx.ac.uk/aboutus/staffdirectory/Orhan_Gemikonakli.aspx.

Tutorial:

Business environments have undergone huge transformations over the past two decades, mainly moving from paper based processes to electronic ones. Additionally, the exponential increase in the worldwide use of the Internet accelerated this transformation. Nowadays, companies want to communicate with customers and partners in real time, using the Internet. The effects of all of these concerns lead the companies to deploy new servers and storage equipments in their systems. As they wanted to be one step further from their competitors, they deployed new IT applications giving rise to the deployment of more servers and or as they run out of space they added more storage. It is difficult to say that this is done in a strategic way in the light of appropriately developed business plans. "In many cases this has led to what is often referred to as "server sprawl", resulting in low server utilization and high system management costs".
These additions inevitably brought many consequences such as the cost of cooling and supplying power to the systems, extra space required, maintenance cost and so on. Furthermore, it has soon become clear that many new servers deployed are unnecessarily under utilized. Further to these, the complex structures created as a result meant further difficulties in managing and modifying these systems.
Server virtualization manifests itself as a possible solution to these problems. Server virtualization can be defined as a method of running multiple independent virtual operating systems on a single physical computer. Various virtualization strategies have already started to take place in modern computer network infrastructures. While vendors providing server and memory virtualization invest increasingly more into the development of such systems, companies as well as network managers had an increased awareness that they can more efficiently invest into and manage network systems while meeting agreed server level agreements.
Storage virtualisation has similar benefits too. In addition to server and storage virtualization, desktop and network virtualisation are becoming increasingly more important.
Virtualisation brings its challenges too, from management to security. Finally, it is important to evaluate the performance of planned virtualised systems. This is possible through analytical modelling and simulation.

To address the above the module will cover the following topics over 6 hours:

1. Storage and Server Virtualization
2. Virtualization & Data Centre Storage
3. Future Storage Solutions
4. Desktop Virtualisation
5. Network Virtualisation
6. Virtualization Security
7. Performance Evaluation of Virtualised Servers
8. Modelling and Simulation of Virtualised Servers

Opportunistic Networks

Dr. RODRIGO SANTOS, received his Engineering degree in 1997 from Universidad Nacional del Sur and got his Ph.D degree in Engineering in 2001. He has become a Researcher for The National Research Council in Argentina in 2005 and in the same year became Assistant Professor at the Department of Electrical Engineering and Computers at Universidad Nacional del Sur. He has been involved in European Projects at Retis Lab at Scuola Superiore Sant'Anna di Pisa in 2003, 2005 and 2007. He has been a visiting professor at Universidad Nacional de San Agustín in Arequipa, Perú; Universidad Argentina de la Empresa at Buenos Aires, Argentina and at Retis Lab Scuola Superiore Sant'Anna di Pisa. His research interests are mainly related to real-time systems: QoS, Multimedia, Operating Systems and Communications. He has published his research's results in international indexed Journals and proceedings of Conferences. He is a member of several Technical Committes for conferences in the area of real-time systems and also a reviewer for several journals. He is the Executive Secretary for the Latin American Center of Studies in Informatics and A member of the Working Group 6.9 of IFIP. He is also an IEEE member.

systems and ambient intelligent systems. He has been involved in several ESPRIT projects and is still involved in several projects funded by the Spanish Comisión Interministerial de Ciencia y Tecnología (CICyT) and Agencia Española de Cooperación Internacional y Desarrollo (AECID). He acted as advisor of the COOB'92, the Olympic Games of Barcelona 1992 organizing society for the performance of the computer and communication infrastructure. He has acted as project reviewer and evaluator for national and international agencies. He is Vice-president of the International Federation of Information Processing (IFIP).

Tutorial:

Opportunistic Networks (oppnets) is a rather new concept borned around 6 years ago. The key idea behind this kind of networks is to use mobile devices to build a network to transfer data from a source node to a destination one without knowing the path or route to follow. Moreover, the message has no guarantee of reaching destiny. The whole thing relays on a best effort policy but nevertheless results quite effective. An oppnet can be seen as a subset of a Delay-Tolerant Network where communication opportunities are intermittent, so an end-to-end path between the source and the destination may never exist.

A source node passes its message to a nearby node following a gossip fashion. Nodes move around and while being near to others pass the messages they have to them and at some point the destiny node is reached. The basic characteristic is that the nodes may enter and leave the oppnet at any time, they can move and take with them the messages. All these things are done without the interaction of people. Usual elements to become part of an oppnet are cell phones, PADs, netbooks, or any electronic device with communication capacity. The oppnet may be based on any kind of communication technology, WI-FI, Bluetooth, RFID, etc.

The oppnets are part of what has been known as ubiquitous computing and later as pervasive computing. Basically these concepts are related to the use of computing devices in everyday activities without explicit knowledge of the user of its existence. Oppnets appear then to link these devices in a friendly an easy way to help people. They differ from traditional network standards in that the size and structure of the network is unknown. Actually, the oppnet starts with a seed oppnet of one or just a few nodes and grows dynamically with the incorporation of friendly devices. The growth of the network is guided from the application layer that requires information to be retrieved/sent from/to other nodes. In this aspect it is essentially different to the previous approach of Mobile ad-hoc Networks (MANET). In Manets, each device is a"router" that has to keep in someway information about the possible paths to reach a specific destination. In a certain way, a device entering a MANET assumes a compromise for routing messages according to a certain transport and routing protocol. In oppnets instead, devices act as vectors propagating the information as they move. The main thing in oppnets is related to the application layer and not to the transport layer and there is no constraint on the underlying communication standard.

Oppnets bring new problems in their implementation as privacy and security are two main issues that are still not resolved.

They may turn to be an incredible tool to monitor different variables and as an alternative communication path when the main lines are dropped after an incident like an earthquake or hurricane. They can also be used in traffic jams, crowd management,

environmental monitoring, etc. The devices should be prepared to hold information and pass it at the proper moment to other friendly devices. In this message passing, like a gossip chain, information can travel across the city and reach the destination nodes. Obviously, this implies that people, cars, buses, trains, etc, act like vectors carrying the data and in this way the privacy of a person may be violated by revealing the geographical position in a certain instant. People may want to share a public profile in such a way that while moving around the city can collect information on different subjects like shop offers, traffic delays, entertainment activities, etc. By making a public profile of interests, the person may reveal sensible data that

may be used maliciously. These aspects are still to be solved.

In this tutorial the main aspects related to oppnets are presented. The routing alternatives with their pros and cons, selection of devices, applications and their prospective use today, implementation details, etc. As the concept of oppnets is rather new, there still are many open subjects to study and improve.

The tutorial will cover the following topics

1. **General concepts**
   - a) Opportunistic Networks and Mobile Peer-to-Peer Networks
   - b) Communication
   - c) Data Dissemination.
   - d) Privacy Preserving Techniques
   - e) Incentive Schemes
   - f) Proximity Based Services

2. **Layers**
   - a) Network Layer.
     - i. Forwarding-based approach
     - ii. Flooding-based approach
   - b) Transport Layer
   - c) Bundle Layer
   - d) Application Layer

3. **Applications**
   - a) Environmental monitoring, wireless sensor networks.
   - b) Emergency handling and response
   - c) Social communication. Shopping opportunities, micro-blogging, etc.
   - d) File sharing.

Network Security Monitoring

Dr. SIRAJ AHMED SHAIKH, is a Senior Lecturer at the Department of Computing and the Digital Environment, part of the Faculty of Engineering and Computing at Coventry University, UK, since 2009. He is also a member of the Digital Security and Forensics (SaFe) Research Group at Coventry University. He has worked in the area of information and network security for over ten years. He has been involved in research, development and evaluation of large-scale distributed secure systems for identity management, communication networks, livestock and biosecurity, and national security. His doctoral and post-doctoral research involved design and verification of security and safety-critical systems. He has over forty-five peer-reviewed research publications in international journals and conferences. He holds a PhD in Computer Security, MSc in Computer Networking, MA in Higher and Professional Education, and BSc (Honours) in Computing. He has served on the Program Committee (PC) for several conferences and has been the PC Co-chair for the 3rd and 4th International Workshop on Foundations and Techniques for Open Source Software Certification (OpenCert) in 2009 and 2010 respectively. In 2010, he served as a Policy Fellow to the Department of Environment, Food and Rural Affairs (Defra) of Her Majesty's Government (HMG), advising on secure storage and transmission of data from field-based rapid diagnostics devices. The fellowship was funded by Engineering and Physical Sciences Research Council (EPSRC) of UK. He is currently working with the transport and logistics sector in the UK investigating efficient and reliable supply chain networks for consignment delivery. The project consortium is led by Ricardo and Unipart Group, and is funded by Technology Strategy Board (TSB) and EPSRC of UK. From 2007 to 2009, he worked as a Research Fellow at Cranfield University, at the Defence Academy of the United Kingdom, and from 2006 to 2007 as a Postdoctoral Research Fellow at the International Institute of Software Technology of the United Nations University, Macau SAR China. Prior to academia he worked in the industry developing smart-card based access control systems for use by HMG. He is a Chartered Member of the British Computer Society (BCS) and Membership Secretary at the Wiltshire Branch of the BCS. He is also the Secretary for the International Federation for Information Processing (IFIP) Working Group 11.4 on Network Security and a leading member of the Working Group 6.9 on Communications Systems for Developing Countries. As part of his UNU and WG 6.9 commitments, Siraj has been invited to deliver tutorials in South Africa, Mozambique, Jordan and Pakistan. His paper titled "A Deployment Value Model for Intrusion Detection Sensors" won the Best Paper Award at the 3rd International Conference on Information Security and Assurance (ISA 2009), held in Seoul, Korea in 2009.

Tutorial:

The description presented here is a summary for a six hour class room-based tutorial. Supplementary to lecture material, handouts and directed reading will be provided to assist the audience in getting a broader view of the field. The content is a mixture of established knowledge, recent research and practical experience so it provides a well-rounded view.
The course is designed to be accessible to an audience diverse in their interests: those willing to acquire skills for technical and operational environments, those interested in strategic and risk management, and even those willing to pursue further research and scan horizons for technology in this area, will all benefit.

The delivery is broken down into three sessions of two hours each.

Session 1 (Motivation)

This session will introduce the course by motivating the need for security monitoring for modern computer networks. The challenges of network, traffic and temporal scale will be the main focus. It will offer perspectives in the cyber warfare and defence context.

Session 2 (Sensors)

To detect and respond to traffic activity, reliable and complete access to network traffic is imperative. This session sets out the different options available for such effective access. This provides for a basis to understand what types of data can be collected and used for identifying activity of interest. A broader definition for sensors is then introduced with a variety of characteristics (such as location, response and costs) discussed.

Sensor 3 (Placement and value models)

Once characterised, a better understanding of sensor placement can be achieved. This session builds on the previous two and lays down a risk-based model for calculating sensor deployment value and analysis. A case study will be used to effectively illustrate subtleties in placement problems.