



**Faculty of Technology and Environment**

**School of Computing and Mathematical  
Sciences**

**17<sup>th</sup> Annual Post-graduate  
Research Conference**

**Wednesday 16 & Thursday 17 march 2011  
Held in  
Room 705, Byrom street**

# ANNUAL POSTGRADUATE RESEARCH CONFERENCE

Wednesday 16th March 2011

Opening and Welcome by Professor Madjid Merabti  
(09:15 - 09:30)

(Tea/Coffee from 9.00am)

Session Chair: Abdullahi Arabo Session Rapporteur: Dr Kashif Kifayat

TIME	NAME	YEAR	TITLE
9.30	Rob Hegarty	3 <sup>rd</sup>	Forensic Analysis of Distributed Service Orientated Computing Platforms
9.50	Laura Pla Beltran	1 <sup>st</sup>	Games Interface for Security
10.10	Andrew Hardy	2 <sup>nd</sup>	Communication and Sensing for Energy Management a Data-Centric Approach
10.30	Stewart Blakeway	3 <sup>rd</sup> (PT)	THE IMPLEMENTATION OF COGNITIVE ATTRIBUTES IN A MOBILE AD-HOC NETWORK TO BETTER MEET MISSION OBJECTIVES

Tea/Coffee Break (10.50 - 11.10)

Session Chair: Simon Cooper Session Rapporteur: Dr Paul Fergus

11.10	Brett Lempereur	3 <sup>rd</sup>	Information Flow Monitoring: Policy, Model, and Analysis
11.30	Ahmed Sultan Kozal	1 <sup>st</sup>	MULTIUSER COOPERATIVE SPECTRUM SENSING IN WIRELESS COGNITIVE RADIO NETWORKS
11.50	Mark Evans	3 <sup>rd</sup> (PT)	Policy formation in viable collectives of autonomous agents
12.10	Zaynab Ahmed	2 <sup>nd</sup>	Fast Block-Matching Motion Estimation

Lunch (12.30 - 13.30 - Post Room)

Session Chair: Andrew Hardy

Session Rapporteur: Dr Michael Mackay

13.30	Shamaila Iram	1st	An Integrated Web-based e-Assessment Tool
13.50	Ricardo Duarte	1st	High Performance 3D Embodied Character Animation
14.10	Mazhar Ul Hassan	4th	A COMPOSITE SECURITY SCHEME FOR HOME NETWORK APPLIANCES IN PEER-TO-PEER NETWORKS
14.30	Andrew Attwood	2nd	A MOBILITY ARCHITECTURE FOR AUTONOMIC WIRELESS MESH NETWORKS
14.50	Chunlin Song	3rd	Robust Region-Adaptive Watermarking System
15.10	Nathan Shone	1st	Monitoring within the System-of-Systems Domain

Tea/Coffee Break (15:30 – 15:50)

Session Chair: Brett Lempereur

Session Rapporteur: Dr Bob Askwith

15.50	Faisal Alsheed	2nd	An autonomic Quality of Service (QoS) negotiation mechanism to support Service Level Agreements (SLA) management for cloud-based applications
16.10	Glyn Hughes	3rd (PT)	Supporting Cloud Computing Management through an Object Mapping Declarative Language
16.30	Behnam Bazli	2nd	Using Structure of Ubiquitous computing to utilise security and trusted services
16.50	Emma Higgins	2nd	Developing a methodological geographic information system framework to augment identification of future risk of anomalous dwelling fires

Close 17:10

**Thursday 17<sup>th</sup> March 2011**

**(Tea/Coffee from 9.00am)**

**Session Chair: Andrew Attwood    Session Rapporteur: Dr David Lamb**

<b>TIME</b>	<b>NAME</b>	<b>YEAR</b>	<b>TITLE</b>
9.30	Stephen Tang	4 <sup>th</sup> (PT)	Game Content Model: Ontology for documenting Serious Games Design
9.50	Chelsea Dobbins	1 <sup>st</sup>	CAPTURING AND DISTRIBUTING DIGITAL MEMORIES: ISSUES AND CHALLENGES
10.10	Ibrahim Idowu	1 <sup>st</sup>	Ad-hoc And Wireless Body Area Network
10.30	Michal Kennedy	2 <sup>nd</sup>	System of Systems Secure Composition Concerns

**Tea/Coffee Break (10.50 - 11.10)**

**Session Chair: Chris Dennett    Session Rapporteur: Dr Martin Randles**

11.10	William Hurst	1 <sup>st</sup>	A Framework for Secure Operation in Critical Infrastructures
11.30	Stathis Goudoulakis	1 <sup>st</sup>	Study of Planning and Re-planning Algorithms for Digital Interactive Storytelling
11.50	Hector Ruiz	2 <sup>nd</sup>	The role of Fisher information in primary data space for neighbourhood mapping
12.10	Hermina Duratovic	2 <sup>nd</sup>	Trust of collaborative components in web services

**Lunch (12.50 - 13.50 - Post Room)**

**Session Chair: Mike Kennedy    Session Rapporteur: Dr Dave England**

13.50	Mohamed Ahmed Al. Zawi (presenting remotely)	5 <sup>th</sup> (PT)	Self - Healing Technology Using Artificial Intelligence
14.10	Mohssen Ghaderi	1 <sup>st</sup>	State Management in Large-Scale Distributed Systems
14.30	Abdulraqeb Alselwi	2 <sup>nd</sup>	Cyber security and network intrusion monitoring

14.50	Luke Okelo	4 <sup>th</sup>	Ambient Intelligence In Support Of Spatial Navigation for the Visually Impaired
15.10	Norulzahrah Mohd Zainuolin	2 <sup>nd</sup>	A Model and Implementation for Digital Forensic Investigation of Online Social Networks

Tea/Coffee Break (15:30 - 15.50)

Session Chair Hermina Duratovic

Session Rapporteur Dr Martin Hanneghan

15.50	Shenin Hassan (Presenting remotely)	1 <sup>st</sup>	Learning in the Cloud: Existing model, limitations and challenges
16.10	Haseeb Ur Rahman	4 <sup>th</sup>	Memory Threads: Organizing Human Digital Memories to Organize Social P2P Network
16.30	Naim Mohd Radi	5 <sup>th</sup> (PT)	A measure of the redundancy in the image data
16.50	Chris Carter		Extensible Test bed Architecture and Topological Analysis for the Scalability of Hybrid-P2P Massively Multiplayer Online Games

Close 17:10

## **User-centred and Context-aware Identity Management in Mobile Ad-hoc Networks (UCIM in MANets)**

**Abdullahi Arabo**

[a.arabo@ljmu.ac.uk](mailto:a.arabo@ljmu.ac.uk)

Digital identities are at the heart of many contemporary strategic innovations for crime prevention and detection, internal and external security, business models etc. This requires the disclosure of personal information and the applicability of contextual information as well as allowing users to be in control of their identities. In this presentation, we review some issues of contextual computing, its implications and usage within pervasive environments with our main emphasis on identity management in (MANets) and emergency situations where different systems need to interact in an ad-hoc manner. The use of contextual information in ad-hoc environments can extensively expand the adaptation and usage of such applications. The main focus is on the areas of context-awareness and user-centricity together with its security issues and implications. Context-awareness allows us to make use of partial identities as a way of user identity protection and node identification. User-centricity is aimed at putting users in control of their partial identities, policies and rules for privacy protection. These principles help us to propose an innovative, easy-to-use identity management framework for MANets. The framework makes the flow of partial identities explicit; gives users control over such identities based on their respective situations and contexts, and creates a balance between convenience and privacy. We also provide the overview of our proposed framework, its development and lab results/evaluations, and outline possible future work to improve the framework.

## MEMORY THREADS: ORGANIZING HUMAN DIGITAL MEMORIES TO SUPPORT SOCIAL P2P NETWORKS

Haseeb Ur Rahman

[H.Ur-Rahmam@2008.ljmu.ac.uk](mailto:H.Ur-Rahmam@2008.ljmu.ac.uk)

People collect and store their digital memories in different ways e.g. pictures, text, videos and so on. These memories are collected at different times, places, events and so on, and are invariably remembered based on a reference that relates directly to where or how they were captured. Such references help in recalling these memories, and are generally common among a group of people. Various hardware or software tools, such as Memory for Life systems, are nowadays able to analyze captured digital memories and store information associated with them. The stored information is then used by the system to properly organize the memories on a device and generate meaningful information about a person's life. To share digital memories, there is also a need to organize them in a network in a way that reflects the entity, place, person, object, or similar, that forms part of the memory to be shared. The network should also allow other entities to find or organize digital memories within it.

The information stored with the memory in the form of metadata, should contain the references needed through which people recall those memories. Based on similar references, our work considers how digital memories can be grouped together to form a **memory thread**. In other words, a memory thread is the collection of digital memories having a common reference under common criteria and arranged in a specific order. We use these two types of criteria to form a memory thread *selection criteria* and *arranging/indexing criteria*. The selection criteria selects digital memories which have a common reference point as used by people to recall their memories. The indexing criteria arrange the digital memories in a specific order. It is therefore important that every digital memory should have at least one memory key which can be used as an indexing criterion. For example, the memory thread of a person's life will contain the digital memories that they captured throughout their life. The person in this example is the *selection criterion* and age is the *arranging criterion* used for forming the memory thread.

Based on the idea of memory threads, we will present our work proposing a social P2P network which organizes peers according to the memory threads stored for different entities. A memory thread for an entity within a network groups those peers in a community which have common references associated with their digital memories. The indexing criteria for each thread arrange peers in a specific order, which allows tracing via peers, avoiding unwanted answers during a search of the network. It also allows peers at different locations in the thread to be accessed easily, bringing the most similar peers together in a community so that data can be found easily by searching just a limited number of peers. The communities are formed around the idea of entities for which the memory threads are formed, as distinct from organizing peers according to an interest or data contents they share. The social P2P network also considers the strength of social relationship in order to share digital memories with each other.

We will consider these concepts in our talk, and present initial evaluation results from simulations designed to test the effect of data and connection categorization on searching.

# **Examination of Four Dimensions of eGovernment: Services, Security, Transparency & Trust Why has it not progressed to the degree expected?**

**Shauneen Furlong**

**[SFurlong@territorialcommunications.com](mailto:SFurlong@territorialcommunications.com)**

eGovernment has not progressed to the degree expected. To understand this situation and why it has not advanced as anticipated, it is useful to examine its development through the four dimensions of services, security, transparency and trust.

The primary focus of this research is on the public sector and the new processes of coordination made possible or even necessary by the advent of technology – and the spreading of online activities in particular. It also comprises a more fundamental sharing and reorganizing of power across all sectors (including the public at large) and modernizing existing government structures and processes to improve performance with respect to service delivery and policy-making. The growing set of interdependencies among public, private and civic organizations lies at the heart of these challenges, and it is quite necessary to examine the impacts of digital technologies on government internally (considering roles and relations among politicians, public servants and the public) and externally (across all stakeholders).

In order to be more precise on the scope of e-government adopted for this research, it is useful to turn to one definition adopted by many governments as of late – namely, the continuous innovation in the delivery of services, citizen participation, and governance through the transformation of external and internal relationships by the use of information technology, especially on the Internet. This broad starting point is, in turn, supported by other groups such as the OECD now often referring to e-government as fundamentally about achieving good government (in a modern day context). This perspective underscores the widening canvass of e-government as digital technologies and online activities permeate most all aspects of government activity.

The four main dimensions of e-government examined in this research are: i) online service delivery and the consequences and opportunities for incorporating portals and integrative service mechanisms in government to citizen service relations; ii) security mechanisms and policies tied to online services but also the shift to more seamless governance to combat crime and terrorism via new digital platforms both within and across government organizations; iii) rising pressures for transparency in government (and all institutions) and the implications for public sector management and accountability; and iv) shifting notions and levels of trust as determined by public support, participation and engagement in a more digitally wired and inter-connected polity.

# **The development of an adaptive environment (framework) to assist the teaching, learning, and assessment of geography within Oman secondary education system**

**Batoul AL-Lawati**  
**B.M.AL-Lawati@2009.ljmu.ac.uk**

The radical changes in knowledge and technology based -societies, has required individuals to be knowledgeable about information and communication technologies because of the ubiquitous usage in all aspects of our daily life. Educational institutes thus need to strengthen their ICT curriculum in every subject area. As the level of technology rises, the acquisition of technological skills will cease to be regarded as anything other than essential. Proficiency in the use of technology will become an indispensable skill at almost all levels of work and the criterion will be not whether an individual can use technological equipment but the extent to which an individual can solve problems and enhance procedures using the available technology. Using information technologies in the field of the social studies such as geography contributes to rendering abstract phenomena concepts visualization and increases student's interest in social studies. Geography is a subject that is particularly suitable for teaching through the use of technology, and it offers many opportunities for the development of skills in ICT and other technology areas.

The aim of this research work is to design and develop a framework to support the creation of an adaptive and interactive virtual environment to be used by the instructors and learners. Thorough investigation into various methods and techniques of teaching and learning will be performed. From these initial research findings a framework will be developed in collaboration with educators both in the UK and Oman to ensure a robust development is achieved, that contains all the necessary elements of an interactive virtual environment. A further research aim is to investigate the impact of using such an interactive learning environment from a pedagogical perspective. The findings of this part of the research will inform the most of appropriate teaching and learning methods to incorporate the framework into the secondary school curriculum, the case study will focus on geography curriculum, with particular reference to the GCSE level which will take place in Oman.

# USING NETWORK STRUCTURE TO ENHANCE SECURITY AND TRUST OF UBIQUITOUS COMPUTING SERVICES

**Behnam Bazli**

[B.Bazli@ljmu.ac.uk](mailto:B.Bazli@ljmu.ac.uk)

Developments in Ubiquitous Computing are expected to introduce interactive and programmable living spaces as an integral part of future computing environments. Such a user-oriented environment will require a secure network infrastructure to ensure integrity, interoperability, privacy, fault tolerance and simple development and execution of applications.

Various middleware architectures have been proposed for ubiquitous computing environments as a means of securing the network infrastructure, enabling integrity, privacy and reliability mechanisms as part of the service access interfaces and implementations provided. In a Ubiquitous Computing context, the middleware acts as a cluster of services, providing a distributed layer between applications and the hardware infrastructure to facilitate integration of components and easy deployment within the ubiquitous environment.

Such solutions exist as research projects, but have only been addressed and implemented within small spaces with limited functionality and services. This work is aimed at using small world network infrastructures and properties to propose a middleware to efficiently coordinating the components in large-scale network and smart-building. The solution will use factors such as context awareness, location sensing, the building layout and other metrics and services in order to apply the required security policies.

Unlike random networks, increasing the size of a scale-free network retains its essential characteristics. By considering this, and the properties of small-world networks, a suitable infrastructure will be designed as a middleware solution to accommodate agents, entities, service and application domain and security systems within a user-oriented Ubiquitous Computing environment. Moreover this will be applied to highlight security challenges, as well as ensuring the reliability, privacy, fault tolerance, efficiency and overall effectiveness of the network.

Expanding the network infrastructure would ordinarily require the middleware to support new entities through extensive reprogramming to accommodate the change in network size. By making use of scale-free properties, the proposed infrastructure will allow the middleware to maintain a balance by rebinding to equivalent security services at specific locations within the network as the size of the network changes.

# **Information Flow Monitoring: Policy, Model, and Analysis**

**Brett Lempereur**

**b.lempereur@2006.ljmu.ac.uk**

Live digital forensic techniques that capture a snapshot of operational state at the time of seizure are helpful, but only provide information about current state. The examiner is still required to piece together artefacts from stored information to assert knowledge of historical events, such as an interaction with another computer that occurred a month ago.

There are two approaches to piecing together this historical information. The first approach uses information commonly available on systems, such as file-system metadata and access logs, typically this does not require configuration in advance. While this method is generally applicable, it is not precise and there is no guarantee that the view produced is either complete or accurate. The second approach involves deploying software in advance to produce records for use by a forensic examiner after an incident has occurred. Systems that use hypervisors or specialised hardware to record every action taken on a system for forensic replay are only useful in edge cases. Audit records consider each system in isolation, although techniques exist that allow for the correlation of audit logs across hosts. In addition, attempting to audit every interaction on a system will yield records that are difficult to even store, with a low ratio of useful information to noise.

This talk will present our solution to the problem of obtaining audit records useful for post-hoc forensic analysis of large computer networks, beginning with an outline of our cross-platform information flow model, and then demonstrate how we apply security policies to determine interesting sequences of information flow events. Finally, we show how our system combines and interprets event sequences within and between hosts.

# **Robust Region-Adaptive Watermarking System**

**Chunlin Song**  
**C.L.Song@2004.ljmu.ac.uk**

Digital image watermarking techniques has been drawing the attention of researchers and practitioners as a means of protecting copyrights in digital images. The technique is a subset of information hiding technologies which works by embedding information into a host image without perceptually alters the appearance of the host image. Despite the progress in digital image watermarking technology, the main objectives of the majority of research in this area remains to be the improvement in imperceptibility and robustness of the watermark to attacks.

Watermark attacks are often deliberately applied to a watermarked image in order to remove or destroy any watermark signals in the host data. The purpose of the attack is aimed at disabling the copyright protection system offered by the watermarking technology. Our previous research in the area of watermark attacks found a number of different types of watermark attacks. They can be classified into a number of categories including removal attacks, geometry attacks, cryptographic attacks and protocol attacks. Our research also found that both pixel domain and transform domain watermarking techniques share similar level of sensitivity to these attacks.

The experiment which was conducted to analyse the effects of different attacks to watermarked data provided us with a conclusion that each attack affects high and frequency part of the watermarked image spectrum differently. Furthermore, the finding also showed that the effect of the attack can be alleviated by using watermark image with similar frequency spectrum to that of the host image. The results of this experiment lead to a hypothesis which would be proven by applying a watermark embedding technique which takes into account all of the above phenomena. We call this technique the Region-Adaptive Watermarking.

Region Adaptive Watermarking is a novel watermark embedding technique where the watermark data is embedded on different regions of the host image using a combination of Discrete Wavelet Transform and Singular Value Decomposition techniques. This technique is derived from the earlier hypothesis that the robustness of a watermarking process can be improved by using watermark data which frequency spectrum not too dissimilar to that of the host data. To facilitate this, the technique utilises dual watermarking technologies and embed parts of the watermark images into selected regions in the host image. Our experiment shows that our technique has improved the robustness of the watermark data to image processing attacks as well as geometric attacks, thus validate the earlier hypothesis.

In addition to the improving the robustness of the watermark to attacks, we can also show a novel use the Region-Adaptive Watermarking technique as a means to detect if certain type of attacks have occurred. This is a unique feature of our watermarking algorithm which separates it from other state-of-the-art watermarking techniques. The watermark detection process uses coefficients derived from the Region-Adaptive Watermarking algorithm in a linear classifier. The experiment conducted to validate this feature shows that in average 98% of all watermark attacks can be correctly detected and identified.

## **Ad-hoc and Wireless Body Area Network**

**Ibrahim Idowu**

**I.O.Idowu@2009.ljmu.ac.uk**

In today's age of technological advances and increased demands and changes in our lifestyle, the Internet has become of paramount importance to every individual living in the society. This is the result of technology and its role in our life driven by increased mobility and usability of technology using wireless communications. This has required advances in mobile devices and technologies (including wireless communications for single and multi hop configurations indirectly linked to wired infrastructures) that typically use a base station or access point as the point of attachment. An example of this network is ad-hoc and wireless Body Area Networks. There is real potential to exploit these technologies in a raft of application domains due to the ease in which devices can be dynamically connected using low cost wireless connectivity. Smart devices can be used to join networks, access information and provide services through mobile middleware services at anytime, and anywhere. This provides a vast number of opportunities for business, health care, education, and recreational opportunities that make our day-to-day life a lot flexible through the growing popularity. In this presentation I will be covering some of the research issues on both wireless body area networking and ad hoc network. A summary of the current challenges faced by other researchers, proposed solutions and possible trends of research direction for the future, will also be presented.

# **A measure of the redundancy in the image data**

**Naeem Radi**

**N.Radi@2004.ljmu.ac.uk**

In our attempt to outperform JPEG2000, we introduce a novel hybrid image coding system that uses predictive coding as a front end for wavelet transform. The effectiveness of wavelet transform coding is improved by first performing predictive coding on the original image data which produces prediction error data which is then quantized to produce the quantized prediction error data. Wavelet transform is performed on the quantized prediction error data rather than the original image data since the quantized prediction error data is much more redundant than the original image data. However, wavelet transform coding does only depend on the redundancy of the data in order to perform well but more importantly on having large homogenous regions in the image. This research paper attempts to develop a measure for a type of data redundancy that also incorporates how the data is organized. The new measure helps to decide on the number and sizes of homogenous regions in the original image data or the quantized prediction error data. This measure helps in evaluating the usefulness of introducing the predictive coding stage.

# Monitoring within the System-of-Systems Domain

**Nathan Shone**

[n.shone@2007.ljmu.ac.uk](mailto:n.shone@2007.ljmu.ac.uk)

System-of-Systems is a term which bears relevance in multiple research disciplines. However within the realm of computing it is still in its infancy. The main notion behind System-of-Systems (SoS) is to address issues such as efficiency, flexibility and integration that are arising from the increasing complexity found in modern network infrastructures. The concept of SoS is to integrate complex independent systems, to form a large-scale distributed System-of-Systems. This can reduce complexity for users, pool system resources and achieve greater levels of interoperability.

One of the main problems with SoS is that the increased structural complexity, dynamicity and the uniqueness of each SoS implementation make them largely unpredictable. It is in these situations that careful pro-active monitoring is required, to ensure the validity and integrity of the systems. The unpredictability of SoS makes for a possible security risk, as it is difficult to predict behaviour of dynamic interoperability, which may create unknown vulnerabilities or security risks. Neither the initial response of joining individual systems together, nor the future behaviour of the newly integrated systems can be accurately determined. Sometimes, when integrating systems, security settings need to be changed in order to reach a compromise between security and functionality. Monitoring is essential in these situations to ensure behavioural conformity of systems, in order to maintain a consistent level of security. The high network speeds, real-time functionality, dynamicity, pro-active roles and self-adaptive roles required in monitoring SoS are highly demanding and cannot be sustained by current commercial monitoring solutions. Nor can they be sustained by distributed monitoring approaches such as those provided by the Ganglia, MonALISA and Nagios research projects.

With significant interest in SoS from military, defence, government and research organisations, the implementation of SoS should increase. This interest highlights the need for capable and scalable monitoring solutions to be in place, to ensure the security and integrity of all systems integrated into a SoS architecture. This presentation will look at the background research and current issues relating to SoS monitoring. It will also review the aims and objectives of this research project.

# **A Readiness Study into E-Government Information Systems Migration to Cloud Computing**

**Rabea Kurdi**

[R.Kurdi@2009.ljmu.ac.uk](mailto:R.Kurdi@2009.ljmu.ac.uk)

Under the umbrella of the ICTs world revolution, e-government presents a tremendous impetus to move forward in the 21st century with higher quality, and cost-effective government services as well as providing a better relationship between citizens and government. Moreover, E-government applications are increasingly making use of new technological developments and this trend appears likely to continue at great pace in the coming years. The benefits of e-government services over traditional government services are numerous, which can include increased speed and efficiency, lower costs, 24/7 services, etc. However, many e-government initiatives have not achieved their expected success and benefits. Much research in the area of e-government has been motivated by the aforementioned need for improving e-government initiative success rates. One particular research angle relevant to this study, suggests that such deficiency is related to the lack of application of systemic approaches to the design, introduction and management of e-government systems. This is based on the premise that the design and introduction of any new socio-technical system such as e-government systems can trigger a complex transformative process. Thus the application of principled methods of business process change management are required. Hence, the overall motivation of this research study is to test the hypothesis that the application of modern business process change management methods can lead to improved e-government success rate.

The main aim of this research is to develop a comprehensive framework of associated guidelines and tools to support E-Government Information Systems (EGIS) readiness analysis, with a specific focus on the EGIS migration to a Cloud Computing provisioning model. To this end, the proposed framework aims to provide a method to guide the assessment of EGIS systems migration readiness including assessing the degree of maturity of a considered e-government system. The proposed framework covers four dimensions namely: (i) Technology, (ii) Organisation, (iii) People/Stakeholders, and (iv) Environment and Society. In addition, the proposed framework also presents novel contributions of associated guidelines and tools to help the government leaders to migrate to cloud computing this includes: Top management support, Strategy and vision Alignment, Security and Privacy, Systems Quality, Financial/ fund, Public-Private Partnership (PPP), Capability and Sustainability, and Stakeholders Motivation/Acceptance.

# Forensic Analysis of Distributed Service Orientated Computing Platforms

Robert Hegarty

[R.C.Hegarty@2006.ljmu.ac.uk](mailto:R.C.Hegarty@2006.ljmu.ac.uk)

Cloud computing is an emerging model of computing that offers elastic scalable computing resources to many concurrent users worldwide. It provides resources that are paid for as they are consumed which can be dynamically scaled to suit the demands of the user. This is obviously attractive to companies who wish to consolidate their resources by creating their own elastic resource platforms or outsource to obtain more flexible cost effective computing resources. As cloud computing platforms may be used to carry out illicit activity, computer forensic techniques capable of processing cloud platforms are required. Computer forensics is the practice of analysing computers to determine if they have been used in the commission of a crime or breach of policy. Various techniques are employed to analyse all aspects of a computer and/or network to determine if malicious activity has occurred. One such technique is signature detection, where signatures from known illicit files are searched for to determine their presence on a computer or storage device.

We have identified that the scale and distribution of data present a barrier to the application of existing signature detection techniques. To reduce the scale of the signature sets used to analyse cloud platforms, we have developed a model to determine a suitable signature length for use in the forensic analysis of a large distributed set of files. Our model not only reduces the length of the signatures used for forensic analysis, but it also determines the accuracy of a search using signatures of any given length. This allows us to calculate an appropriate length signature to use in the first round of a two round search technique. Using this approach we negate the requirement to analyse each and every file in a cloud using 128bit MD5 hash values. By reducing the signature length we show that we can reduce the amount of data required to carry out signature detection. This will make feasible a distributed approach to signature detection in large scale distributed platforms.

Through experimentation we validate our model and demonstrate that it is possible to use shorter length signatures to accurately carry out forensic analysis if factors such as the scale of the data undergoing analysis and the scale of the signature set used for the analysis are taken into account. We will present our results and discuss the further challenges our ongoing work is addressing to move toward our vision of enabling forensic analysis of large scale distributed cloud computing platforms.

# **A MODEL AND IMPLEMENTATION FOR DIGITAL FORENSIC INVESTIGATION OF ONLINE SOCIAL NETWORKS**

**Norulzahrah Mohd Zainudin**

**[N.Mohd-Zainudin@2008.ljmu.ac.uk](mailto:N.Mohd-Zainudin@2008.ljmu.ac.uk)**

The growth of online social networks has encouraged new ways of communicating and sharing information and is used regularly by millions of people; it now seems that these networks will be an enduring part of everyday life. The rapid growth of online social networks has also resulted in an increase in their use for significant criminal activities and perpetrators are becoming increasingly sophisticated in their attempt to use technology in order to evade detection and perform criminal acts. Despite the fact that there a number of existing models developed for digital forensic investigation, most have quite similar approaches; some of the models are also generic and fail to focus on the purpose of the investigation. In addition, there is no standard and consistent model, only sets of procedures and tools, thus many digital crime investigations are performed without proper guidelines. Perhaps even more important is the fact that there is no model built specifically for online social networks while in contrast digital crimes related to them are rapidly growing in number.

To address these challenges, we have developed a standard model of digital forensic investigation for online social networks. In this talk we will present our research that incorporates the existing traditional frameworks, allowing us to compile a comprehensive digital forensic investigation model specifically for online social networks. We will consider how these ideas can be developed further, concentrating on an implementation as a prototype that will reflect the forensic investigation process in online social networks based on our proposed model. We will also present our results from experiments using a number of applications to select the significant features that can be applied in implementing our model.

Finally, in order to provide an implementation, we must develop an algorithm to ensure that the objective of systematic investigation is accomplished, using the analysis processes as described in our model. This future work, including methods for carrying out a number of case studies to validate the algorithm, will be discussed. In conjunction with development of the algorithm, we will develop a technique that is capable of automated searching for extracting, filtering and reporting important information in the network. We will discuss how this prototype will be evaluated to ensure the functionality meets the essential requirements of the model.

# **Detection of Whitewashing Attacks in MANET**

**Abbas, Sohail**

**S.Abbas@2008.ljmu.ac.uk**

In multihop networks such as mobile ad hoc networks (MANETs), a node can misbehave by selfishly dropping others' packets to save battery life. This selfishness or misbehaviour can disrupt the whole network functionality and can severely degrade network performance. Cooperation enforcement schemes such as reputation, trust, and credit based schemes have been developed to discourage node misbehaviour. However, these models are vulnerable to whitewashing or identity changing attacks. Whitewashing occurs when a node having poor reputation/trust changes its identity to start afresh and escape from the consequences of its bad actions. This attack can significantly affect the performance of reputation based models as well as other protocols developed for MANETs. We propose a cross-layer approach to detect whitewashers using signal strength values. We use the normal entrance and exit behaviour (from radio ranges) of nodes to distinguish between new legitimate nodes and whitewashers. Simulation results show that our scheme produces more than 90 percent of true positives with low false positive rate in mobile environment. Moreover, the scheme is lightweight that does not cause any extra overhead caused by the periodically broadcasting beacons. It does not make use of trusted monitors, node localizations or any extra hardware, such as directional antennas.

# MANAGING AND SHARING HUMAN LIFE MEMORIES USING P2P

**Azizan Ismail**

[A.B.Ismail1@2006.ijmu.ac.uk](mailto:A.B.Ismail1@2006.ijmu.ac.uk)

People are capturing and storing an ever-increasing amount of personal memories, with new types of information constantly being added such as GPS location data, heart-rate monitor recordings, TV viewing logs and so on. The need to keep, manage and share our personal memories in a digital way has become important through the necessity to remember so many things such as the names of people, places, phone numbers, email addresses and general knowledge, and also to allow us to share our personal experience, improve communication between people, undertake personal reflection and analysis, review conflicts, identify relevant information and recall evidence to mind. Without a digital means to store this knowledge there is a possibility that we might forget or lose important data forever. However, keeping everything may have negative side effects, such as information overload and less effective data searching and browsing. Therefore, technological solutions are needed that can be used for updating and managing the relevant and critical data for future use. The rapidly developing technologies for recording multimedia (such as digital cameras for images and video), ubiquitous sensors and the availability of low-cost-storage can make the accumulation and retention of a lifetime of digital memories possible. Problems relating to the management of personal digital data, the sharing of it with others, the way data should be presented and the methods for allowing understanding of such information and content are becoming increasingly complex.

The aim of our research is to help people manage and use their memories across their entire lifetime. In this project, we developed a prototype allowing the generation of a narration story of an individual based on time-frame based events through the analysis of photo images. Narration for groups of photos based on the event or time frame can make it easier for a user to understand the content of photos without viewing each of them individually. This prototype – called “MyMemories” – makes use of a cluster engine, photo metadata extraction technique, text or voice story summary generator, tagging of related videos, sharing of images (selected images or whole collections), comments from friends, image processing to obtain a personality narration report and correlated stories between two or more people using digital photos. MyMemories also allows users to share all or a selection of their images, as well as the results established by the system, with their trusted friends by using peer to peer groups. We demonstrate our approach using a collection of personal photo images, showing the ability to automatically generate a narration of a selected group of images and produce a narration story of the whole collection. We used JXTA peer to peer networking technology since this provides an open set of peer to peer protocols that enables any devices on a network to communicate, collaborate, and share resources.

In this presentation, I will discuss the challenges associated with digital memories, present the MyMemories system, and discuss the various technologies and techniques developed to make it possible

# **Pre emptive routing protocol**

**Jasim Saeed**

**M.J.Saeed@ljmu.ac.uk**

Over the last twenty years the use of wireless and especially ad hoc wireless communications has seen a phenomenal growth. The performance of the mobile ad hoc networks has been under intense pressure since its inception. A mobile ad hoc network (MANET) is a wireless network temporarily and spontaneously created by mobile stations without requiring any infrastructure or central control. Network managements and communications are typically performed in a distributed manner. Inherently mobile ad hoc wireless networks have to operate within limited resources and if the resources are not used efficiently the performance of the network is severely compromised.

In this presentation a new routing protocol is discussed which pre empts the route failure and allows the nodes to find an alternative path and switch to the new path before the route fails. Existing routing protocols are typically reactive to route failure but by linking our protocol to our MAC layer we can improve performance. Our MAC protocol is based on Signal Strength to Distance (SSD) ratio and Partial Back-off. SSD informs neighbours about the interference range that can cause slowdown, leading neighbours to apply Partial Back-off instead of complete back-off. Simulations were carried out to prove the concept of this pre emptive routing protocol and the results of these simulations will be presented and compared against the existing standard of 802.11.

# A COMPOSITE SECURITY SCHEME FOR HOME NETWORK APPLIANCES IN PEER-TO-PEER NETWORKS

Mazhar UI Hassan

[M.UI-Hassan@2006.ljmu.ac.uk](mailto:M.UI-Hassan@2006.ljmu.ac.uk)

The term peer-to-peer refers to the concept of a network of equals (peers) using appropriate information and communication systems, whereby two or more individuals are able to spontaneously collaborate without necessarily needing central coordination. Peer-to-peer networks have been utilised for a variety of purposes, from file-sharing to Voice-over-IP, and a particularly interesting area of recent application is that of Networked Appliances. A Network Appliance is defined as a dedicated function consumer device with an embedded processor and a network connection. Network Appliances present an exciting opportunity to provide new functionality to appliances used within home networking environments. However, the security for such devices in distributed networks presents many challenges, and remains a largely unresolved issue. This is especially true where peer-to-peer networking is used, due to the lack of centralised control. Considering security, various schemes have been proposed, however research shows various weaknesses within the reported solutions. We propose a novel scheme called the Home Networked Appliances Security Scheme (HNASS) to secure communication among peers utilizing the services of home networked appliances. The key feature of this scheme is that it utilizes a simple but appropriate architecture to protect peers both within and outside the network. At present our work has considered a number of specific security issues, however we believe the scheme could yield a security solution able to evolve into a more generalized standard for protecting such networks.

This talk will consider issues including peer-to-peer networks as they apply to different home appliances. We will look at how these appliances work together, the impact this has on the security of these appliances over P2P networks, and how we can apply our HNASS solution to perform component composition analysis for improving security.

# **Self – Healing Technology Using Artificial Intelligence**

**Mohamed Mousa Al-zawi**

**M.R.Ahmed-Al-Zawi@2005.ljmu.ac.uk**

Self-Management systems is the main objective of Autonomic Computing (AC), so it is needed to increase the running system's reliability, stability, and performance. One of the most important components of AC is self-healing, and it works in a way that the fault will be detected, analyzed, and then repaired. All of these phases are accomplished in the real-time system. In this technology, the system is capable of performing a reconfiguration action in order to recover from a permanent fault. Moreover, self-healing system should have the ability to modify its own behavior in response to changes in the environment. Artificial Intelligence is used to solve the main challenges of self-healing, such as monitoring, interpretation, resolution, and adaptation.

# **MULTIUSER COOPERATIVE SPECTRUM SENSING IN WIRELESS COGNITIVE RADIO NETWORKS**

**Ahmed S. B. Kozal**  
**A.S.Kozal@2010.ljmu.ac.uk**

The explosive growth in wireless services over the past years illustrates the huge and growing demand of the business community, consumers and the government for wireless-based communications.

Due to the development of new applications and wireless technology, most of the spectrum resources have been allocated to support reliability and higher data rate for wireless services.

Even though regulation authorities have expanded some unlicensed spectral bands, the present regulation systems assign fixed frequency bands to specific users or service providers and licenses are required to operate within those bands. However, the allocation of these radio frequencies to specific users does not ensure that these frequencies are utilized most efficiently at all times, as studies that most of the radio frequency spectrum may be inefficiently utilized.

Cognitive radio is a novel approach that aims at improving the utilization of the electromagnetic radio spectrum and easing the congestion of the wireless communication spectrum.

The cognitive radio, built on a software-defined radio, is defined as an intelligent wireless communication system that is aware of its environment and uses the methodology of understanding-by-building to learn from the environment and adapt to statistical variations in the input stimuli, with two primary objectives in mind: highly reliable communication and efficient utilization of the radio spectrum.

In this research, we focus on spectrum sensing and multi-user cooperation as they represent major challenges in cognitive radio. We believe that by combining between these two techniques, many benefits can be gained including improvement of the spectrum utilization.

Cooperative spectrum sensing is proposed to solve the hidden primary problem which is occurring due to fading and shadowing. This research aims to improve the spectrum sensing by studying the cooperative spectrum sensing in both centralized and decentralized mechanisms.

# A MOBILITY ARCHITECTURE FOR AUTONOMIC WIRELESS MESH NETWORKS

**Andrew Attwood**

[A.Attwood@2006.ljmu.ac.uk](mailto:A.Attwood@2006.ljmu.ac.uk)

Mobile mesh networks will become ubiquitous in their use within the future Internet of Things. Both individual devices and device clouds will operate in the fringe Internet, displaying differing levels of mobility through individual and collective mobility patterns. Maintaining device connectivity whilst mobile will provide increased fidelity to the systems and devices that we interact with. Device clouds will be highly dynamic, requiring ad hoc inter-connectivity with other clouds, individual mobile devices and the edge Internet to ensure optimum connectivity and access. Furthermore these clouds could become fragmented during their operation, leading to an inter connectivity requirement between fragments. There may be critical infrastructure components within the distributed system that will require mobility architectures to be fault tolerant. This will require schemes to exhibit dynamic scalable properties, which enable the continued operation of networks whilst sections are asleep or in a failed state due to an attack or node failure.

We propose the Indirection Overlay for MANETs (IoMANETs) mobility framework as a solution. IoMANETs initial design provides a fault tolerant, scalable solution to the Internet of Things mobility problem. IoMANETs achieves this through the application of hard (device) and soft (distributed state) overlay supported indirection. IoMANETs consists of three major components; Mobility Overlay Supporting Indirection and Packet Delivery (MoSIPD), Wireless Mobility Border Protocol (WMBP) and Distributed Application State Management (DASM) This report details our background research and an initial specification of the IoMANETs architecture. Additionally we outline problems with current relative addressing schemes that will need to be resolved if IoMANETs is to be realised. More specifically insuring that the hierarchical wireless topology evolves  $G_0(V,E) \rightarrow G_i(V,E)$ . To meet the predicted capacity and critical infrastructure requirements  $G_{i+1}(V,E)$ , whilst minimising indirection state control overhead and operating within the low power constraints of the individual devices.

# **Fast Block-Matching Motion Estimation**

**Zaynab Ahmed**  
**Z.Ahmed1@2009.ljmu.ac.uk**

Block-matching motion estimation is the most important part for any motion compensated video coding standards such as ISO/IEC MPEG and ITUT. The block-matching algorithms eliminate the temporal redundancy, which is found predominantly in any video sequence. In this case, video frames are divided into equal sized non-overlapping macro blocks and the displacement of the best-matched macro block from the previous frame as the motion vector of the macro block in the current frame within the search window is calculated. During block matching, each target block of the current frame is compared with a previous frame in order to find the best matching block. Block-matching algorithms calculate the best match using the Mean Absolute Difference (MAD) or Sum Absolute Different (SAD). Full search algorithm (FS) provides the best result by matching all possible macro blocks within the search window; however this algorithm suffers from long computational time, which necessitates improvement. To improve motion estimation search time, there has been a tremendous contribution by various researchers and experts for the past two decades to refine block-matching algorithms. A number of fast block matching motion estimation algorithms were considered in different video coding standards such as Three Step Search (TSS), New Three Step Search (NTSS), Simple and Efficient TSS (SESTSS), Four Step Search (4SS), Diamond Search (DS), Cross diamond search, Adaptive Rood Pattern Search (ARPS), and so on.

A novel block-matching motion estimation technique was developed which is called Mean Predictive Block Matching (MPBM) algorithm, based on Adaptive Rood Pattern Search (ARPS) algorithm. The proposed technique utilizes two available motion vectors (MVs) of the neighbouring MBs instead of one as is the case with ARPS. MPBM tries to decrease the computation time between the current macro block and the macro blocks in the reference frame, by stopping the calculation of the sum absolute different between the pixels in the current macro block and the macro blocks in the reference frame when the current uncompleted sum absolute value is greater than the previous calculated one.

Experimental results showed that the proposed technique minimize the search time of the macro block matching, as well as get better resolution for fast block motion estimation in comparison with various standard block matching motion estimation technique .

# **MEDICAL HEALTHCARE PROVISIONING USING WIRELESS SENSOR NETWORKS**

**Arshad Haroon**  
**a.haroon@2006.ljmu.ac.uk**

Advances in healthcare services and the increase in our standard of living has resulted in people living longer as compared to people born before world war two; consequently, the number of individuals suffering from long-term debilitating conditions as they grow older is also increasing. This demand has resulted in greater health and social care systems.

In the last few years, internetworking research has shifted from an exclusive focus on the office to now include the home. A home network interconnects various electronic devices within a home environment using different industry standards such as Digital Living Networked Alliance (DLNA), Open Services Gateway Initiative (OSGi), and Universal Plug and Play (UPnP).

The aim of the project is to build on these developments and develop a new framework; to support networked medical devices and services in environments, such as the home, where we can use sensor technology to improve healthcare provisioning, reduce costs and streamline how and when services are delivered. The scope of this project is to wirelessly incorporate home medical devices, which may be embedded in the environment as well as those embedded within and on a person's body. This will provide the basis for a detailed evaluation of medical devices and services and their impact on healthcare in the home environment.

## **DIGITAL MEMORIES: A SURVEY**

**Chelsea Dobbins**

**[C.M.Dobbins@2006.ljmu.ac.uk](mailto:C.M.Dobbins@2006.ljmu.ac.uk)**

The practise of capturing and uploading digital content for personal use and for sharing with others has become second nature in today's society. From this inherent need to record many aspects of our lives we find that increasing numbers of people share this content online using outlets such as Facebook, Twitter and Flickr. This allows us to digitise episodic memory and experiences in new and novel ways.

Nowadays it is now common practise for individual's to capture, store, use and share most events in their daily lives, digitally, and often using the Internet. As such with the advancement of storage capabilities, the notion of storing everything one accumulates over a lifetime does not seem impossible and is closer to becoming a reality that first expected. However, as the amount of data we accumulate grows it is also at risk of becoming meaningless and unmanageable. As this data amasses daily, meaningful mementos will undoubtedly be lost amongst the hordes of useless information. There is therefore a challenge to be able to add meaningful information to digital memories to provide better structure.

New possibilities will arise that allow content about us, family and friends to be clustered, based on topic, experience, location and time. This will also include information from physiological computing therefore providing a richer understanding about aspects of our health, level of activity and physical wellbeing, including how we made others feel at that time. This presentation focuses on the current research that has been undertaken within this area, including how memories are currently captured and organised and how semantic annotation and clustering can be used to organise these memories. The use of sensors will also be examined to illustrate how more meaningful information can be attached to our memories. In this sense, a memory will contain rich structures and varied information sources that emerge through the semantic clustering of content and other memories and will form part of compositions between other memories about you, your friends and your family.

# **Extensible Test bed Architecture and Topological Analysis for the Scalability of Hybrid-P2P Massively Multiplayer Online Games**

**Chris Carter**  
**C.J.Carter@2007.ljmu.ac.uk**

Massively Multiplayer Online Games (MMOGs) have rapidly become a key game genre in the last decade. Current mainstream architectural approaches utilise Client/Server-Cluster topologies, where scalability and interaction is hampered by a reliance on hardware provisioning as the primary method for scaling and partitioning game world into distinct regions (or shards) is common.

Recent academic research within this domain of shared-space technologies has focused upon the adoption of P2P-based solutions. This architectural shift introduces a myriad of additional problems to be solved; additionally, whilst scalability is inherent, the distribution of state in an efficient manner is non-trivial. Moreover, current research has been conducted within test-bed environments that do not reflect real world MMOG scenarios and network traffic, with an over-reliance on simulation techniques.

This presentation is split into two parts:

- The former describes the development of a novel MMOG test-bed framework (NHUGS), which combines enterprise web technologies with modern 3D game development solutions and socket-based game networking APIs; whilst presenting the case for its adoption amongst the research community.
- The latter presents a novel Hybrid-P2P Architecture (NAHPALM) using semi-structured topologies and spatially-distributed, self-adaptive interest management through the application of capability descriptors as heuristics. The presentation illustrates how this architecture has been developed and evaluated (in conjunction with a Client/Server comparative case) using the NHUGS framework.

The presentation will also cover the Thesis progress, outline of Thesis content and detail remaining tasks and potential future research work.

# TRUST OF COLLABORATIVE COMPONENTS IN WEB SERVICES

**Hermína Duratovic-Field**

[H.duratovic@2009.ljmu.ac.uk](mailto:H.duratovic@2009.ljmu.ac.uk)

Trust is a vast and subjective field that has been researched in areas such as spam, peer to peer networks and web services. However, very little research has been done into web service collaboration and how trust related metrics are propagated down to the component layers. Trust has the same core requirements; its representation, exchange, establishment and enforcement, as well as a unified way of measuring it through reliability, decision and reputation based mechanisms. From the research conducted we have found that there are too few trust management mechanisms that establish the trust of components that are participating in service collaborations, which is its representation. Most of the work associated with management of trust in components looks at trust establishment between components, with the assumption that some kind of “reputation” exists for each component; however this is not the case. In order for a viable solution to exist, the problem of propagating the reputations scores given by the user needs to be solved, and a feasible solution to the problem needs to be given. Firstly this presentation will define trust in terms of Service Oriented Architectures. Furthermore it will look at describing what efforts have been made in representing and establishing trust of components in service collaborations, as well as describing the proposed framework to resolve the weaknesses highlighted in the presentation.

# **Cyber security and Bio-inspired Network Intrusion Monitoring**

**Abdulraqeb Alselwi**  
**A.Alselwi@2006.ljmu.ac.uk**

Wireless broadband networks suffer from having wireless signals travelling in the reception area leading to new security threats that enable intruders to access and cause compromise of the network communication, DoS attack or information 'phishing'. There is a need to look at how networked sensing systems can intelligently monitor communications activity to defend a cyber space from network intrusions. We consider that bio inspired monitoring for developing network monitoring that exploit the wireless network properties as long the lines of DNA use in forensic science.

Human DNA is used as evidence in criminal investigations. We can process recognizable patterns of DNA to recognise specific persons using DNA sequences since people have the same genes and these genes do not have the same sequence since found at splice junctions located in DNA sequence where mRNA remove the non-coding area to form a translation sequence which depends, typically we depend on forensic tools to align mRNA sequence to confirm the evidence. In our research we will consider computer networks exposed to be attacked by external intruder or using wireless access to attack. The Bio-inspiration such as DNA alignment methods help in handling the search for similarity areas in sequence strings, some of these approaches we believe can be useful in detection mechanisms for network intrusion. What is missing in current techniques is a holistic network approach.

The challenges for security protection in a wireless network make it harder to protect a network or discover intrusion in the network. Challenges in wireless make it easier for intruders to hack by exploiting this access point and can use it as a legitimate user to steal information or use DoS attacks to engage in hostile activities. So in wireless networks we can have two external attacks which are passive attack involve unauthorised listening to routing packets and active attack disrupt a wireless network by introducing some DoS attacks and cause jamming to network which that legitimate user can't access to a network also network intrusion detection and firewalls do not provide adequate protection since these are reactive methods. We identify that we should develop pro-active bio-inspired protection.

In this project we are going to look at network sensing to catch and analyse network traffic, to compare it with its system 'bio-inspired' behaviour during the process in order to tackle any potential DoS or hacking and will use 'bio-inspired' patterns which could be using sequence strings and sequence signature that build from processing that encoding of normal behaviour and network traffic activities, and this might go on to help as a bio inspiration DNA and these could be the improvement of sequences in the network traffic behaviour which might be going to exist for tackling any attack and then we are going to use it to compare it with network intrusion detection systems to improve its ability to block the attacks or at least detect it. Also in bio inspiration such as DNA we will try to use a variety of network forensic data such as audit data, real time and local routing information to investigate how these can be used in a bio-inspired protection model.

# **Developing a methodological geographic information system framework to augment identification of future risk of anomalous dwelling fires**

**Emma Higgins**

**E.Higgins@ljmu.ac.uk**

There are currently 63 fire and rescue services in the UK, providing cover for over sixty-one million people. UK fire services attended at total of 722,000 fires in 2008/09 and of these, 49,000 were accidental dwelling fires. Of the 420 fire deaths in 2008/09, over 65 percent occurred in the home. The increased probability of suffering from an injury or becoming a fatality in the home prompted the introduction of the Home Fire Safety Check in 1999. This scheme has proved successful, seeing a reduction of dwelling fires by approximately 50 percent since its introduction. In addition to this, the number of accidental dwelling fire related fatalities has decreased by 54 percent between since 1999. Although there is a general downward trend, the year on year decrease in the number of fatalities associated with accidental dwelling fires is starting to plateau. Another crucial matter is that thirty-eight percent of accidental dwelling fire fatalities occurred in areas typically defined having a lower risk of fire, which highlights a need to research *why* accidental dwelling fires occur, in order to identify the risk of anomalous fires occurring in the future.

This research attempts to identify the causal factors that cause accidental dwelling fires to occur and explore the potential for displaying this risk information graphically. Soft Systems Methodology (SSM) has proven to be a powerful for tackling problematic management situations. SSM is able to handle situations where the overall goals and objectives may be fuzzy or difficult to define. In addition, the development of a geographic information system to augment identification of future risk of anomalous dwelling fires will involve the input of many key stakeholders, all from different backgrounds. The application of SSM helps to manage the differing expectations and views of stakeholders, whilst the implementation of a system is a generator of organisational change.

The hub of this system is the identification of the contributing factors that can increase anomalous dwelling fire risk. It has been suggested that certain lifestyle factors can increase ones risk of becoming victim to fire in the home, however understanding how presence of these factors *interact* will aid fire and rescue services understanding on how to best prevent and manage these situations. Understanding why fire is bias towards one individual rather than another with seemingly similar circumstances could aid fire service prevention activities. Statistical approaches can be applied to data, both historic fire and rescue service data and current lifestyle data, to test relationships between incidence of fire and risk factors identified.

In this presentation, I will discuss how the fields of SSM, statistical analysis and geographic information systems can be merged with a demonstration of how this can be applied, and is being used, in the operational Fire and Rescue Service environment.

**An autonomic Quality of Service (QoS) negotiation mechanism to support Service Level Agreements (SLA) management for cloud-based applications.**

**Faisal Alsrheed**  
**F.S.Alsrheed@2010.ljmu.ac.uk**

Cloud computing has become prevalent in recent years, increasing the need for negotiable Service Level Agreements (SLA) between the cloud service providers and customers.

However, much of the research carried out in negotiation is focused on theoretical aspects of negotiation protocol and strategy; the practical application and actual deployment of automated negotiation mechanisms has lagged far behind. Thus, there is a need for a novel autonomic quality of service (QoS) negotiation mechanism to support Service Level Agreements (SLA) management for cloud-based applications.

This research work is seeking to promote and discover novel methods for the runtime automatic negotiation of quality standards for SLA adoption.

This presentation will provide an overview of cloud computing and autonomic computing. Then, it will demonstrate how the principles of autonomic computing can be applied to provide a novel autonomic QoS negotiation mechanism. We will also show the progress made to date. Finally, in the last slides we will detail the future work to be completed in order to reach our goal.

**Supporting Cloud Computing Management through an  
Object Mapping Declarative Language**

**Glyn Hughes**

**g.d.hughes@ljmu.ac.uk**

Due to the probable vast scale of Cloud Computing systems, management of the numerous physical and virtual components may become unwieldy. Many software packages that have historically been installed on desktops / workstations for years are slowly but surely being converted to Cloud Computing solutions. The problems that are emerging today are only set to worsen as Cloud Computing becomes ever more pervasive. This paper synopsis previous investigatory research concerning these emerging problems. It then continues, to describe the structure and operation of an object mapping declarative language and the object oriented system which employs it. Both are currently under development to support the management of these numerous Cloud Computing components. The ultimate aim is to develop a system that combines the rich capability of an imperative assembly with the concise simplicity of a declarative language.

**Study of Planning and Re-planning Algorithms for Digital  
Interactive Storytelling**

**Efstathios Goudoulakis  
e.goudoulakis@2008.ljmu.ac.uk**

Games for computers and consoles are established as the leading form of interactive digital entertainment. Digital Interactive Storytelling (DIS) is a relatively new field of interactive computer entertainment that aims to create interactive applications capable to generate consistent narratives. Planning systems is the most widely used technique for DIS. Planning involves knowing the state that you're in, the state you want to be in and then finding the sequence of operators that will get you from the current state to the final state. Planning is necessary for the organisation of large-scale activities since decisions about actions to be taken in the future have direct impact on what should be done in the shorter term. But even if a plan is thoroughly tested and well-constructed, its value decays as changing circumstances, resources, information, or objectives render the original course of action inappropriate. When changes occur before or during the execution of a plan, it may be necessary for a new plan to be constructed by either starting from scratch or by revising a previous plan. This is the concept of re-planning.

Since DIS is a quite new field, there is a lack of prototypes of DIS systems available to the public. Also, although planning systems have been used intensively in DIS systems, there have not been much novel solutions for DIS research with respect to planning algorithms. There is a lack of comparison and evaluation of algorithms that can be used in DIS planning systems. There is also an important gap in the use of re-planning methods in existing DIS systems.

The proposed research aims at investigating AI planning and re-planning algorithms currently used in AI and exploit their potential for the field of DIS, to evaluate their suitability for such systems and to develop new algorithms to improve them. To this end, a framework for a multi-agent system using planning and re-planning algorithms for Digital Interactive Storytelling will be specified, designed, implemented and evaluated with appropriate DIS scenarios.

## **The role of Fisher information in primary data space for neighbourhood mapping**

**Héctor Ruiz**

**H.Ruiz@2010.ljmu.ac.uk**

Clustering methods and nearest neighbour classifiers typically compute distances between data points as a measure of similarity, with nearby pairs of points considered more like each other than remote pairs. The distance measure of choice is often Euclidean, implicitly treating all directions in space

as equally relevant. In this presentation we review the application of Fisher information to derive a metric in primary data space. The aim is to provide a natural coordinate space to represent pairwise distances with respect to a probability distribution  $p(c/x)$ , defined by an external label  $c$ , and use it to compute more informative distances.

## **High Performance 3D Embodied Character Animation**

**Ricardo Leandro Parreira Duarte**  
[R.L.Duarte@2010.ljmu.ac.uk](mailto:R.L.Duarte@2010.ljmu.ac.uk)

Facial and Body Animation has been a subject of study for the last three decades. Today, it still represents a big challenge to create an efficient and realistic animated character. A made and a standard was created to achieve the best possible character animation and put together numerous efforts and different implementations, this is the standard on which we will focus, MPEG-4 based body and facial animation.

In this research project we propose to investigate existing techniques in facial animation and enlighten their strengths and weaknesses to attempt the creation of solutions and enhancements of these. We will focus not only in showing where existing solutions fail to give satisfactory results but we will also contribute to the creation of novel approaches for 3D Embodied Character Animation.

We will develop a novel framework which will be used to create realistic character animation, which will be included in a later stage within the Homura Game Engine platform. This framework will involve novel contributions within the MPEG-4 standard, in the following areas; Character modeling and graphical optimization with LOD (level of detail), realistic facial and body animation, expression models and parameterization models to synchronize voice with facial animation and co-articulation. The results achieved in these areas will be combined and applied to embodied conversational agent applications.

In this presentation we will give a walkthrough in the main areas described above. We will also highlight some of the current issues that exist within each area, and we will present some of work we have already undertaken.

## **Games Interface for Security**

**Laura Pla Beltran**  
**L.Pla-Beltran@2010.ljmu.ac.uk**

Information systems' security is an area of great concern in present times. With new technology developments and innovations, new vulnerabilities and risks appear. A number of factors can make computer security difficult to apply, including users, and issues closely related to their views on and use of security, primarily awareness and usability. Security's tools can be very useful if configured correctly, but configuration often poses a great challenge for

users. Most users do not want to spend time configuring security tools or being interrupted from their primary task by security alerts. Security is often disregarded or downplayed.

The widespread acceptance and engaging nature of games suggests other types of software could benefit from applying some of the games interface design principles. Games' interfaces tend to include features such as the deep customizability, difficulty-regulation strategies, fluid human-system interaction, metaphors, challenge, and promote collaboration and creation of communities.

On the other hand, the use of visualisation to monitor and control network traffic and events can be very beneficial. Highly sophisticated network security tools can overlook certain aspects that a human user could detect with a simple glance. By representing the state of the network and related security features in a graphical manner, visualisation can help the user understand and gather a picture of the current network status, and detect any possible anomalies or suspicious behaviour.

This presentation will provide an overview of the aforementioned issues, existing work and a proposed approach, based on the idea of visualizing the security status of a system through a game-based interface the user can interact with. This interface will bridge the gap between the complexity of the network and the requirement of an easy-to-understand model by representing all this complexity by means of a game interface, allowing the user to visualize and understand the home network and systems and, based on this, make the most appropriate security decisions.

## **Learning in the Cloud: Existing models, limitations and challenges**

**Shenin Hassan**

[S.Hassan-Parackal@2010.ljmu.ac.uk](mailto:S.Hassan-Parackal@2010.ljmu.ac.uk)

Cloud computing has gained considerable momentum since its inception and this is clearly evident from the wide range of cloud applications in use today. Cloud computing is being embraced by many types of business and technical domains, with a growing number of traditional applications moving to the cloud. This paradigm shift in computing is set to fulfill the target set by ubiquitous computing, delivering ICT (Information & Communication Technology) products and services at the users' convenience. In its very basic

form, cloud applications are online applications, eliminating the local administrative effort of maintaining the application. From a business perspective, respective organizations can concentrate more on their core domains of business, eliminating the need to spend portion of their effort on maintaining their ICT infrastructure. As the backbone of any business, ICT usage is very critical for all operation and the very survival of the organization depends on how ICT it is utilized so as to stay competitive and updated.

The global education sector is also moving towards cloud-based technologies. A number of research project and discussions are in progress regarding e-learning, and more specifically, cloud-based e-learning. Cloud-based e-learning applications are on the rise, helping the learning community to expand their scope and mode of knowledge. A number of learning applications, for instance: Google docs; Moodle; Learn.com and others provide the learner the new forms of flexibility and convenience during their online learning experience. New models of learning built on cloud-based pedagogy are needed to support these new Learning Management Systems, and help is required to move from traditional learning models to cloud-based learning models. Cloud-based learning frameworks are beginning to emerge (e.g. IBM BlueSky, Learn.com) integrating diverse technologies to address learning and teaching needs.

A comprehensive, cloud-based learning environment which addresses the complete lifecycle of learning is the ultimate goal of practitioners. This research will investigate technologies and practices from within and without the e-learning field and the cloud computing field.

## **AMBIENT INTELLIGENCE IN SUPPORT OF SPATIAL NAVIGATION FOR THE VISUALLY IMPAIRED**

**Luke Okelo**

**[cmplokel2005@ljmu.ac.uk](mailto:cmplokel2005@ljmu.ac.uk)**

Navigation, whether in real or electronic worlds, is a complex human activity. A lot of notable research has been carried out into developing navigation systems for the visually impaired. Though quite useful to blind or partial sighted persons, traditional navigation aids for the visually impaired have not been fully beneficial in that they have not fully promoted independence in the mobility of blind or partial sighted persons, nor have they facilitated their successful navigation within unfamiliar environments. Often, they have been inconvenient to port, and can only be customized manually and with difficulty. In addition to this, they cannot always indicate the user's location accurately.

In many cases, a person whose vision is impaired experiences difficulty in knowing their location and being able to move safely and independently even in familiar environments. This is even more difficult in unfamiliar places e.g. large, public buildings, airports, hotels, hospitals

Our research describes the progress made in the development of an ambient intelligent spatial navigation system for the visually impaired. The purpose of such a navigation system would be to enable blind and visually impaired individuals to navigate easily within familiar but particularly unfamiliar environments in indoor environments e.g. a large buildings etc.

It is envisaged that such a system would integrate discreetly with an Information Services System of local computer networks operating inside of unfamiliar indoor building environments. It would do this via Ambient Intelligent computing principles, using a programming paradigm known as spatial programming to augment real-life interactions with data processing, thereby minimizing explicit interactions from the user to the application. Through ambient intelligence, spatial navigation for the visually impaired can become adaptable to the individual user, navigation technique and environment, and should be able to satisfy current user tasks, capabilities, information availability and location awareness.

## **Policy formation in viable collectives of autonomous agents**

**Mark Evans**

**[cmsmevan@2001.ljmu.ac.uk](mailto:cmsmevan@2001.ljmu.ac.uk)**

The operation of collectives of autonomous agents can in some respects be considered to be an entity that exhibits intelligence. The intelligence exhibited by the wider system is underpinned by the comparatively simple decisions undertaken by each agent in response to localised stimulus, and is an emergent property of the collective. Work undertaken in the field of social insects and swarm intelligence has revealed direct analogies to the above via stigmergic signalling between insects. Such signalling causes colonies of such insects to exhibit behaviour that is to the overall advantage of the colony, yet there appears to be no centralised control or grand plan to coordinate or impose the same – the behaviour just appears to happen. At the colony level, the collective of insects (which may be considered to be directly analogous to a collective of autonomous software agents) operates so as to

continually maximise its benefit and minimise its losses. At this level, the colony (of agents or insects) is considered to be a viable system i.e. capable of survival within its environment. Examination and presentation of the formation of the policy function within viable systems may lead to overcoming the problem of programming a collective of agents to do useful work, without threatening the viability of the wider system, and that has hitherto been elusive; current research attempts to address this particular aspect.

## **System of Systems Secure Composition Concerns**

**Michael Kennedy**  
**M.Kennedy@2006.ljmu.ac.uk**

System of Systems is a relatively new field that is applicable to numerous disciplines. It is concerned with the ability to provide systems that exhibit higher levels of functionality through emergent behaviours with the collaboration and integration of multiple independent systems. The System of System concepts are focused on improving efficiency and providing the means to address complex issues that arise through the increasing complexity in the information technology environment.

The current research taking place is focused on addressing the many issues surrounding these multifaceted developments with the current focus on the creation of frameworks, methods and classification. There are many challenges within the area of System of Systems

research and its related areas; one of the areas of interest is that of the security available within the system of systems. Due to the composition of these complex structures, in that they're created from working independent systems, they are subject to the usual security concerns and threats that affect all systems; however their increased complexity, configuration and operation leads to additional security considerations that systems in isolation rarely have to consider.

We will be exploring and discussing some of the concerns and challenges that are faced when composing a System of Systems relating to security. We will also examine some of the current approaches available for securing a System of Systems, and present a design for a framework that could be used to provide an indication of the security of a System of Systems composition.

## **State Management in Large-Scale Distributed Systems**

**Mohssen Ghaderi**  
**M.Ghaderi@2010.ljmu.ac.uk**

The rapid and somewhat exponential growth of IT over the last two decades has furnished humans with an amazingly versatile tool. Projections are that this rapidly evolving sphere of human activity will gather further speed, complexity and reach. As systems grow the need to manage them also grows in complexity, depth and necessity. There is a need to undertake a critical review of the existing Systems Management technology and ethos with the ultimate aim of proposing a new approach to the discipline by exploring and utilizing new and emerging technologies to deal with large scale distributed system enabling state management and scalability.

Researching and developing new topologies for Systems Management applications not only represent a substantial area of study, it will also have a potentially important market deployment value by paving the way for a new and liberating approach to this increasingly critical domain of Information Technology.

It is proposed that a fundamental review of the current Systems Management technology is undertaken with a view to utilising new/emerging technologies such as

- Peer-to-Peer for deployment, distributed control and state management,
- Distributed Artificial Intelligence for monitoring and management.
- Hierarchical Timed Colour Petri Nets for systems modelling, validation, simulation, and state reachability analysis.

The research will involve the development of a new framework, distributed management system and protocol, based on existing technologies (C/S, Peer-to-Peer, MAS, etc...), and will focus on weaving together separate technologies to pave the way for a new generation of Systems Management tools which are more flat and therefore far more agile and horizontally scalable to deal with state management in large scale distributed system.

## **ZONE BASED FAULT MANAGEMENT ARCHITECTURE FOR WIRELESS SENSOR NETWORKS**

**Muhammad Zahid Khan**

**[M.Zahid-Khan@2008.ijmu.ac.uk](mailto:M.Zahid-Khan@2008.ijmu.ac.uk)**

Wireless Sensor Networks (WSNs) make extensive use of resource-scarce (limited power, low processing and communication) and tiny wireless sensor devices, which are deployed over a large geographical area to provide important environmental information for applications such as security surveillance, structure monitoring, precision agriculture and pervasive health monitoring. Due to their unique characteristics (having dynamic topology, ad-hoc and unattended deployment, huge amount of data generation and traffic flow, limited bandwidth and energy) and tight integration to the physical environment, WSNs pose considerable challenges for network management and make application development non-trivial. In network management of WSNs energy-efficient network self-organization and fault

management have been identified as key challenges in the design and operations of Wireless Sensor Network (WSNs).

The large scale deployment of sensors in remote environments; managing numerous sensor nodes individually is not a good solution. Therefore, network self-organization is an essential requirement for large scale WSNs. Furthermore, sensor nodes in WSNs are expected to operate autonomously for a long period of time and may not be easily approachable for battery replacement and maintenance due to their physical deployment location; hence faults and failures are normal facts in WSNs. Thus, in order to guarantee the network quality of service and performance, it is essential for the WSNs to be able to detect faults, and to perform something akin to healing and recovering from events that might cause faults or misbehaviour in the network. Therefore, a fault management platform is an integral part of a network management system.

To address these challenges, we proposed a Zone-based Fault Management Architecture for WSNs. The proposed architecture is composed of two novel contributions: an energy-efficient network self-organization scheme and a fault management architecture that offers efficient fault detection and recovery mechanisms to make the network fault-tolerant.

Our proposed management architecture utilizes heterogeneous sensor nodes to partition a network into different zones and perform local clustering to organize the network into clusters, hence to significantly reduce clustering cost and overhead. It utilizes temporary cluster-heads to distribute the energy load among high power sensor nodes to balance energy consumption; thus extends a network lifetime. The proposed fault management architecture carries out localized fault detection and recovery through a hierarchy of sensor nodes (Zone manager and Cluster-head nodes).

We are currently conducting a simulation-based evaluation using GTSNetS Simulator to compare the efficacy and performance of our proposed architecture. We will evaluate our management architecture according to different metrics and compare it with a variety of existing approaches such as LEACH-C and BCDP. At present we are working on the Total energy consumption aspect of the proposed architecture during the self-organization process.

## **Novel Simulation Framework for State Management in Large Scale Distributed Systems**

**Christopher Dennett**  
**C.R.Dennett@2006.ljmu.ac.uk**

This PhD project aimed to develop a simulator interface to support a distributed state management framework intended for use in large-scale distributed systems such as distributed network environments or networked multiplayer games.

The simulator interface is a fully-featured Java interface to the popular and extensively developed ns-3 simulator with many visualisation features to enable rapid network debugging and prototyping of network applications using an interface similar to the regular Java network API. The appealing aspects of this as opposed to classical testing is the requirement of a smaller number of machines with the added benefits of being able to introduce error models, test new protocols, and the

prospective ability to simulate ISP topologies using topology generation tools such as RocketFuel.

The state management framework is intended to pave an easy route to multiplayer game creation, respecting bandwidth, fairness and security requirements while providing marshaling, authentication and state propagation through native language features and features provided by external libraries. The development of the framework and usage in various real-world scenarios and test-cases is proposed to illustrate the features of the simulator implementation or interface, most notably the single-machine execution and visualisation aspects, alongside the capability of simulating different network topologies with varying error models.

The contributions from the project include a critical analysis of existing simulation platforms and networking frameworks and libraries, the Java simulator interface to ns-3 with visualisation of packet delivery through the simulated network, the implementation of various use-cases including stress tests with statistics gathering through flow monitoring, trace capturing, and other means. Additional contributions include the design and partial implementation of the distributed networking framework in relation to the simulator development and features.

Achievements include the simulator design and implementation with solutions to the many issues that surround this with discussion, implementation of test-cases and prototypes illustrating functionalities, and design and partial implementation of my own state synchronisation framework targeted towards distributed games and in particular MMOGs.

## **Game Content Model: Ontology for documenting Serious Games Design**

**Stephen Tang**  
**[o.t.tang@ljmu.ac.uk](mailto:o.t.tang@ljmu.ac.uk)**

Computer games are a form of real-time interactive software wrapped in creatively crafted media that offers game-players engaging, goal-directed play. Designing computer games requires adequate experience and great attention to detail to describe the rules, play and aesthetics that compose the interactive experience. For inexperienced game designers, formalised methods such as game design languages and game meta-models can provide a guide and language to produce a game design specification correct by design. This paper introduces a new game content model that can aid game designers document specification of game design

## **Communication and Sensing for Energy Management a Data-Centric Approach**

**Andrew Hardy**  
**A.Hardy@2009.ljmu.ac.uk**

Concerns about climate change, dwindling legacy energy sources and an aging and under-invested power grid has lead to pressing energy management focus from governments, energy producers, distributors and consumers. In 2009 the UK domestic sector was the largest electricity consumer with the domestic and service sector together making up 70% of total consumption. Appliances are a very significant contributor in these sectors and therefore deserve our considered attention.

Existing appliance energy management solutions and technologies focus mainly on two approaches: appliance efficiency and user behavior change, while appliances can continue to squander energy unjustified. In order to consume more responsibly appliances need to collaborate with users, the grid and their operating environment. The ideal communication and sensing solution should enable simple ubiquitous deployment of low cost self-configuring devices. The goal is for devices that

automatically and securely connect and collaborate across multiple media over a common transport. Any solution should benefit multiple stakeholders and foster mixed contributors and flexible participation, whilst acting as an enabler for incentivizations such as new comfort, convenience and safety features in addition to the primary feature of energy management.

The conventional focus of communication network research has been to enable communication between identified network hosts. However, multiplicity of heterogeneous devices, random deployment and wide-area monitoring and data acquisition has been increasing and these make locating data sources and implementing rapid delivery significantly harder for conventionally focused networks. For some time now researchers have been looking at strategies which focus on a named data abstraction rather than a location abstraction. This has led to two contrasting paradigms host-centric networking and data-centric networking.

As a contribution to these energy management goals, we propose a 'multiple layer 2' data-centric network. This includes a data-centric routing protocol, naming scheme and role assignment mechanism for in-network event processing to form an abstraction hierarchy in which device level state is transformed for the purpose domain delivering relevant energy management state to smart appliances and other interested devices. We are currently developing a simulation for our network.

For future work, it is our intention to implement a test inter-network for the operation of our energy management application, routing and role assignment protocol. We plan to include network nodes from multiple media and layer 2 networking standards. In addition to the standard specific nodes we plan to source or implement forwarding gateways between these networks to form our 'multiple media' and 'layer 2' inter-network. Our simulation work will be used to implement a common software framework for our nodes in which the routing protocol will operate. Plug-ins will provide the common framework with device specific access to the communication standard. A suitable common plug-in mechanism will be selected or implemented allowing the development of an individual plug-in for each communication standard

## **An Integrated Web-based e-Assessment Tool**

**Shamaila Iram**

**[S.Iram@2009.ljmu.ac.uk](mailto:S.Iram@2009.ljmu.ac.uk)**

This research work aims to investigate and evaluate ways of enhancing the learning process by the use of technology. This technology offers a pedagogical strategy to assess the students (online) by describing an evaluating strategy of student's assessment. The proposed system is being developed to provide an interactive web based learning environment. Three different types of assessment techniques have introduced in this paper; Diagnostic Assessment, Self-Assessment and Summative Assessment which help the students and the teachers to improve teaching and learning capabilities. UML has been used to describe the proposed system specification while the whole system is implemented using .NET Framework. e-Learning and e-Assessment System with its web based features presents an equal opportunity of education for both; the students in the classroom and the distant students. This is a student-centric system and the student's progress depends upon his/her own learning efforts. The proposed

assessment system presented in this paper is aimed at supporting students in their learning by providing them instant feedback

## **DISE: A Game Technology-based Digital Interactive Storytelling Framework**

**Simon Cooper**  
**s.cooper@2003.ljmu.ac.uk**

This project details the design and implementation of an Interactive Storytelling Framework. Using software engineering methodology and framework development methods, I aim to create a full Interactive Storytelling system involving a story manager, a character engine, an action engine, a planner, a 3D game engine and a story data/world environment editor. The framework is described in detail and specified to meet the requirement of bringing a more dynamic real-time interactive story experience to the medium of computer games. Its core concepts borrow from work done in the fields of narratology, software engineering, computer games technology and artificial intelligence.

My novelties lie in the data design of the story which allows a modular approach to building reusable resources such as actions, objects, characters or whole story 'levels'; a switchable planner implementation, allowing many

planners, heuristics and schedulers that are compatible with PDDL (the "Planning Domain Definition Language") to be easily integrated with minor changes to the main classes; a game engine and framework for web launched or in browser deployment of the finished product; and a user friendly story and world/environment editor so story authors do not need advanced coding syntax knowledge of PDDL or games programming experience to complete a basic story.

The finished computer game is designed to be a real-time 3D first person experience, with the player as a main story character in a world where every context filtered action displayed is executable and the player's choices make a difference to the outcome of the story, whilst still allowing the authors high level constraints to progress the narrative along their desired path(s).

## **THE IMPLEMENTATION OF COGNITIVE ATTRIBUTES IN A MOBILE AD-HOC NETWORK TO BETTER MEET MISSION OBJECTIVES**

STEWART BLAKEWAY

S.BLAKEWAY@2007.LJMU.AC.UK

Mobile Ad-Hoc Networks are known for their versatility, that is the capability of being easily adapted from one application to another, in addition to this they are very easy to deploy in comparison to their infrastructure counterparts. Unfortunately, due to the unpredictability of the topology a MANET it faces challenges not seen in conventional wired/wireless networks. Many have tried (and succeeded in the most part) to incorporate cognitive attributes into a communications network, this allowing the network to be aware of its environment, its objective and giving the network a thought process in order to make informed decisions to aid the application objectives or to prevent the network from catastrophic failures. It is the aim of this research to present a refined conceptual model that allows for cognitive features found in networks of a wired infrastructure into that of a mobile (wireless) ad-hoc network with no predefined infrastructure.

## **A Framework for Secure Operation in Critical Infrastructures**

**William Hurst**  
**w.hurst@2009.ljmu.ac.uk**

Critical Infrastructures can be defined as infrastructures that would have a damaging impact on national security, cause substantial economic loss or have life threatening consequences if destroyed or attacked. One of the key defining factors of a Critical Infrastructure is society's dependence on the services provided by the infrastructure and the loss that would be encountered if the infrastructure was shut down through an attack.

In recent months the need for Critical Infrastructure protection has been highlighted and been at the forefront of many News articles, in particular the events which took place in Bushehr Nuclear power station in Iran where the Stuxnet virus halted operations.

It is clear that infrastructures face significant threat as the growth in the use of SCADA systems and the fact that networks are becoming integrated in some way with public networks, for example the Internet to enable information sharing, making the system more vulnerable to cyber-attacks. In addition the growing use of wireless networks means that infrastructures can be more vulnerable to direct attack than previously.

Critical Infrastructure Protection refers to the preparedness to an attack on a critical infrastructure and the response taken in order to protect the infrastructure. It is essential to evaluate Critical Infrastructure Protection levels and address how security can be improved. For that reason, the aim of this project is to develop intelligent Middleware that provides effective security with operational observation to assess, plan and prevent or mitigate the effects of an attack.