



**MACQUARIE UNIVERSITY
DEPARTMENT OF COMPUTING
TECHNICAL REPORTS**

**Computing Postgraduate (Research)
Mini Conference 2006
Research Students in Computing**

Department of Computing
Division of Information and
Communication Sciences
Macquarie University
NSW 2109 Australia

Report No. C/TR06-02
June 2006

FOREWORD

The University requires the progress of each Postgraduate (Research) student in the PhD and Masters programs to be formally reviewed every year. To complement the formal University review process, the Department of Computing holds an annual mini-conference for Postgraduate (Research) students. The mini-conference gives the students an opportunity (1) to present their research work to their peers and academic staff, (2) to assess their own progress and research directions, and (3) to discuss all aspects of their program with a panel of academic staff who are not involved in their supervision.

This year's mini-conference was held between 19-23 June 2006. This technical report demonstrates the range and depth of the research projects undertaken by Computing Postgraduate (Research) students.

Thanks are due to Lee Flax for the organisation of the mini-conference itself, Computing Technical Support for the arrangement of the equipment used in the presentations, Melina Chan for compiling the conference materials, Lisa Chanell for organising the catering, and all the academic staff who participated as panel members, and as members of the audience.

But most particularly I'd like to thank the Postgraduate (Research) students whose excellent research work continues to make these events a success.

Annabelle McIver
Director of Postgraduate Research
Department of Computing
Division of Information and Communication Sciences
Macquarie University

**COMPUTING POSTGRADUATE (RESEARCH) MINI-CONFERENCE
19 -23 JUNE 2006, MACQUARIE UNIVERSITY, AUSTRALIA**

Schedule of Presentations

19 June 2006 (Monday)

9.00 am – 10:15 am (in E6A102)

TALK SESSION: 3

GROUP: CLT

AKHMATOVA Elena
PIZZATO Luiz Augusto Sangoi
PROST Jean-Philippe

10.15-10.45 am *Morning Tea (provided in the tearoom E6A302)*

10.45 am – 12:25 pm (in E6A102)

TALK SESSION: 3

GROUP: CLT

ZWARTS Simon
POWLEY Brett
VIETHEN Henriette
WAN Stephen

12.25 – 1.30 pm *Lunch break*

1.30 pm – 2.45 pm (in E6A102)

TALK SESSION: 3

GROUP: CLT

ASADUZZAMAN MM
YAGHI Jim
LONG Vanessa

3.00 pm – 4.45 pm (in E6A102)

TALK SESSION: 6

GROUP: ISVR

GAO Yifan
HO Wai Han Sharon
ZENG Zhao

19 June 2006 (Monday)

3.00 pm – 4.15 pm (in E6A357)
TALK SESSION: 5
GROUP: ISG

HEZART Armin
MA Ji

4.15 - 4.45 pm *Afternoon Tea (provided in the tearoom E6A302)*

4.45 pm – 6.00 pm (in E6A357)
TALK SESSION: 5
GROUP: ISG

ZHANG Keping
MAGHAYDAH Moad
ORGUN Bhavna

20 June 2006 (Tuesday)

11.00 am – 12:40 pm (in E6A357)
TALK SESSION: 4
GROUP: ACAC

LEE Joanne
TARTARY Christophe
WANG Peishun
BALASURIYA Sanka

12.40 – 1.45 pm *Lunch break*

1.45 pm – 3.00 pm (in E6A357)
TALK SESSION: 4
GROUP: ACAC

SUTANTYO Daniel
GUPTA Gaurav
MATUSIEWICZ Krystian

3.00 -3.30 pm *Afternoon Tea (provided in the tearoom E6A302)*

3.30 pm – 4.45 pm (in E6A357)
TALK SESSION: 4
GROUP: ACAC

McDONALD Cameron
CHO Joo Yeon
SEDAGHAT Soroush

20 June 2006 (Tuesday)

3.30 pm – 4.20 pm (in E6A102)
TALK SESSION: 2
GROUP: PLRG

MILLER Gillian
ROBERTS Matthew

22 June 2006 (Thursday)

9.00 am – 9.50 am (in E6A102)
TALK SESSION: 1
GROUP: INSS

BALAKRISHNAN Venkatesan
NAGARAJAN Aarthi

11.00 am – 12:15 pm (in E6A102)
TALK SESSION: 7
GROUP: U

PALYAGAR Bhavani
ALKAHWATI Majid
SUN Hai Yang

12.15 – 12.45 pm *Lunch break*

12.45 pm – 2.00 pm (in E6A102)
TALK SESSION: 7
GROUP: U

FALLAH-MOSHFEGHI SHADSARI Kourosh
BOWER Matthew

23 June 2006 (Friday)

10.30 am – 11.55 am (in E6A357)
TALK SESSION: 8
GROUP: ACAC

YE Qingsong
EL-MAHASSNI Edwin

COMPUTING POSTGRADUATE (RESEARCH) MINI-CONFERENCE 2006

Abstracts of Presentations

19 June 2006

TALK SESSION: 3 9.00 am – 10:15 am (in E6A102)

Textual Entailment

AKHMATOVA Elena

Supervisor: Dr Diego Molla-Aliod

Associate Supervisor: Prof Robert Dale

Abstract:

Natural Language Processing community found courage to approach the task of Textual Entailment only recently, with the first workshop being held in 2005. The task here is to find out if the meaning of one text snippet is entailed from the meaning of another one. The entailment holds in many cases even if text snippets are different in their syntactic structure and wording. This makes this task to be very challenging. The task has attracted attention of many research groups. Approaches to it vary from working with the logical form representation of text up to machine learning approaches. While the logical form representation of text seemed to be an attractive approach, the empirical results, including my own past results, are not that good. Involving machine learning for the task on the other hand seemed to be empirically promising. I intend to demonstrate that in the current presentation. With the help of an alignment technique I propose to extract features indicating presence or absence of entailment. The features extracted from the human-assessed text pairs can be used to build a decision tree for entailment. This approach is challenging from the very beginning, as there are no standard alignment techniques or features for entailment by now.

Improving QA with a better IR

PIZZATO Luiz Augusto Sangoi

Supervisor: Dr Diego Molla-Aliod

Associate Supervisor: Dr Rolf Schwitter and Cecile Paris(CSIRO)

Abstract:

Question Answering (QA) tackles the problem of answering natural language questions using textual documents. Since many Natural Language Processing (NLP) techniques are used when questions/documents/answers are processed, state-of-the-art QA systems tend to not to be as fast as it is required for commercial applications. One way of speeding QA is by including some preprocessed language information on required techniques such as Information Retrieval (IR). In my talk I'll address some methods of including language information on the IR stage for a QA system.

TALK SESSION: 3 10.45 am – 12:25 pm (in E6A102)

Handling Non-Monotonic Relations in Constraint-Oriented Language Processing

PROST Jean-Philippe

Supervisor: Dr Diego Molla-Aliod

Associate Supervisor: Dr Mark Dras

Abstract:

In Constraint-oriented language processing the conditions of well-formedness of a string are specified as a constraint system. Each constraint in the system models a condition, which may be satisfied by a well-formed input. In such a framework, parsing an input string is then a Constraint Satisfaction Problem.

In this talk we will focus on discussing the question that arised as we observed the same drawback in all existing constraint-oriented parsing strategies. We will then present an overview of the strategy we have designed and implemented, in order to overcome this issue.

Structural Characteristic in Statistical Machine Translation

ZWARTS Simon

Supervisor: Dr Mark Dras

Abstract:

In Statistical Machine Translation most approaches do not use any syntactical information of the Language. In my research project I am investigating the effect of syntactical information on Statistical Machine Translation. I want to investigate to different approaches.

First I like to see the effect of syntactically motivated reordering of the source language. Research in this area suggest overall Translation Quality can be improved.

Secondly I like to use syntactical information in the decoder itself. I want to have a look at confidence levels which is usually supplied with the syntax tool. And I want to have a look at local information, since it is not always necessary to have the syntax spanning complete sentences.

'What are they saying about me?' – finding meaning in citing sentences

POWLEY Brett

Supervisor: Prof Robert Dale

Abstract:

Citations are a feature of academic literature. Writers cite other researchers' works which are related in some way to their discussion. Citations and the sentences containing them potentially tell us interesting things the cited and citing documents, the relationship between the research reported in them, the relationship between the researchers, and many other things.

My talk will describe my research in applying natural language processing techniques to analyzing the meaning of citing sentences. I will give an overview of some of the features of citations and the problems involved in extracting them from research papers. I will then focus a specific application of my research: using citing sentences

to automatically generate a review of a document, based on what other authors say about that document.

Algorithms for Generating Referring Expressions: Do They Do What People Do?

VIETHEN Henriette

Supervisor: Prof Robert Dale

Associate Supervisor: Dr Rolf Schwitter

Abstract:

The natural language generation literature provides many algorithms for the generation of referring expressions. In this presentation, I report on an exploration of whether these algorithms actually produce the kinds of expressions that people produce. I compare the output of three existing algorithms against a data set consisting of human-generated referring expressions, and identify a number of significant differences between what people do and what these algorithms do. On the basis of these observations, I suggest some ways forward that attempt to address these differences

Statistical Sentence Generation: Modelling Grammar and Verisimilitude

WAN Stephen

Supervisor: Prof Robert Dale

Associate Supervisor: Dr Mark Dras

Abstract:

Many professions today require the ability to sift through large volumes of textual documents in order to glean relevant information required for some research-like task. Effective summarisation technology will help the user in avoiding documents which will not be useful in such a scenario. However, current summarisation methods merely provide a gist of the document, largely by presenting an unconnected list of extracted sentences which are deemed as important. Moving beyond the state-of-the-art, this will present an approach for generating a more readable coherent abstract-like summary. The approach utilises statistical techniques for generating grammatically correct sentences that paraphrase the content of the original text. Our techniques are domain independent with a reduced reliance on hand-crafted linguistic resources.

TALK SESSION: 3 1.30 pm – 2.45 pm (in E6A102)

Web Based Question Answering in the Biomedical Domain

ASADUZZAMAN MM

Supervisor: Dr Rolf Schwitter

Associate Supervisor: Dr Diego Molla-Aliod

Abstract:

Question answering (QA) in the biomedical domain is a new research area. As a restricted domain, the biomedical domain has a lot of knowledge sources and ontologies that can be leveraged in an effective way to answer clinical questions. In my talk, I will focus on what the state-of-the-art is in QA in the biomedical domain and what my research contribution is.

QA systems try to find concrete answers to user question rather than a collection of documents. It is a common practice that family physicians use the Web to obtain answers to clinical questions. However, the current search engines can retrieve only entire documents rather than concrete answers to questions. It has been shown that it takes about 5 minutes for a physician to obtain an adequate answer via the Web, but the physicians don't spend more than 2 minutes on average for seeking an answer to a question. As a result most clinical questions remained unanswered.

The challenge for biomedical QA systems are: analysis of questions, selection of knowledge sources, acquisition of knowledge, appropriate system interface and evaluation of QA systems. I will address different approaches in analysing clinical questions and the text snippets that contain the answers. Finally, I would like to address my next steps in the development of a QA system for the biomedical domain.

Natural Language Generation for Incremental Explanation of Logic Proofs

YAGHI Jim

Supervisor: Dr Rolf Schwitter

Abstract:

This project was inspired by the popular logic textbook "Language Proof and Logic" by Barwise and Ethemendy. The goal is to create a tool that allows students of the text book to explore in English language the explanation of difficult logic proofs. The formal language of First Order Logic uses special notation and is bound by a certain grammar that can be difficult to interpret. Translating directly from logic to natural language does not make proofs more understandable. A series of different planning activities need to be undertaken to ensure that the resulting text sounds natural and is comprehensible. I will discuss the difficulties in proof explanation, some of the previous research that has been done in the area, and explain how we plan to tackle this problem.

Table Interpretation

LONG Vanessa

Supervisor: Dr Steve Cassidy

Associate Supervisor: Prof Robert Dale

Abstract:

Table processing is an important part of document processing. There are two major tasks in processing tabular data: (1) to find and extract tables from documents, and (2) to unearth the semantics embedded in the extracted tables.

Focusing on the second task, this talk introduces a theoretical framework for extracting semantics from tabular data. The framework includes a knowledge representation scheme, and a programming model providing support to solving problems that don't have deterministic solutions.

The framework also supports the usage of linguistic information and domain knowledge in table interpretation.

TALK SESSION: 6 3.00 pm – 4.45 pm (in E6A102)

Interactive System Design for Virtual Face Sculpting

GAO Yifan

Supervisor: Dr Manolya Kavakli

Associate Supervisor: Dr Scott McCallum

Abstract:

Facial recognition systems, one of the fastest growing biometric technologies today, require the development of new quality assurance and assessment procedures on their performances for national and personal security. There is one barrier to experimental validation and comparison of 3D face recognition, which is the lack of appropriate face database as stated by Bowyer et al. (2004). A challenging aspect in the development of a face database is to provide an intuitive way for users to enter a facial model. Therefore, the significant point of this research project is the exploration of a new methodology to integrate 2D and 3D face data for modeling the generic face of an individual. The experimental and theoretical work in this project is expected to lead to useful discoveries not only in facial identification but also in the implementation of intelligent facial modeling user interfaces.

Face Recognition

HO Wai Han Sharon

Supervisor: Dr Paul Watters

Associate Supervisor: A/Prof Dominic Verity

Abstract:

My presentation will briefly describe the current practice in face recognition evaluation and its issues, then my proposed methodology and metric, and how we can estimate the performance of recognition under different system requirements.

A novel face hashing method with feature fusion

ZENG Zhao

Supervisor: Dr Paul Watters

Abstract:

We present a novel approach to generating cryptographic keys from biometric face data such that their privacy and biometric template can be protected using recently introduced helper data schema (HDS). Our method includes three components, feature extraction, feature discretization and key generation. During feature extraction stage, the global features (PCA-transformed) and local features (Gabor wavelet-transformed) of face images are used to produce new fused features sets in the complex feature space in order to achieve a desirable performance. Then in the feature discretization stage, a discretization process is introduced to generate a stable binary string from the fused feature vectors. Finally, the stable binary string will be protected by Helper Data Schema (HDS) and used as the input parameter of cryptographic key generating algorithms to produce renewable biometric crypto key.

TALK SESSION: 5 3.00 pm – 4.15 pm (in E6A357)

Defeasible Argumentation Systems

HEZART Armin

Supervisor: Dr Abhaya Nayak

Associate Supervisor: A/Prof Mehmet Orgun

Abstract:

An Argument is simply a reason for supporting a claim. Yet, the result of an argument, the claim, is by no means final viz. an argument is defeasible. An argument that was initially accepted may be contradicted and dismissed. The process of presenting arguments and counter-arguments in turn is known as dialectic argumentation. Defeasible argumentation systems are theories that mirror and formalize the dialectic argumentation reasoning.

Argumentation systems already have a number of applications in Artificial Intelligence. Legal reasoning, automated negotiation, and the recommender systems are just some examples of applications of argumentation systems.

Formal Theories of Trust for Secure Systems

MA Ji

Supervisor: A/Prof Mehmet Orgun

Associate Supervisor: Dr Lee Flax

Abstract:

This project focuses on the study of formal theories of trust for secure systems. It involves the development of prototype secure systems in selected target applications. A theory of trust for a given system describes trust of agents in the system. Such theories provide a foundation for reasoning about agent beliefs as well as security properties that systems may satisfy. However, trust changes dynamically. When agents lose their trust or gain new trust in a dynamic environment, the theory based on the initial trust of agents needs to be revised, otherwise it may no longer be used for any security purpose. There is a need to provide formal methods for modelling trust of agent in the security mechanisms of a system. But there is a lack of such formal methods and techniques for dynamic theories of trust. The motivation of our work is to provide a formal approach for (design) obtaining and managing evolving theories of trust for agent-based systems. This project contains four tasks: (1) A deep study of the concept of trust and trust relations. (2): Developing methods and technique for constructing a theory of trust for a given system. (3) Developing a formal approach to revising a theory of trust, and providing a framework for managing theories of trust in dynamic environments; (4) Applying the methods and technique we develop in this project to selected applications.

TALK SESSION: 5 4.45 pm – 6.00 pm (in E6A357)

Visual Cluster Analysis in Data Mining

ZHANG Keping

Supervisor: A/Prof Mehmet Orgun

Associate Supervisor: Dr Annabelle McIver and Dr Kang Zhang(External)

Abstract:

Clustering is an important technique that has been widely used in data mining. Many clustering algorithms have been proposed. However, in practice, using those clustering algorithms to deal with high dimensional and huge datasets sometimes is not feasible. This is mainly due to their non-linear computational complexity and their drawbacks on handling large datasets with arbitrarily shaped data distributions. On the other hand, the numerical feedback of clustering algorithms is difficult for the users to have an intuitive overview of the dataset that they deal with. Visual presentation is powerful in revealing trends, highlighting outliers, showing clusters, and exposing gaps in data mining. Thus, combining visualization techniques and user domain knowledge into clustering analysis process can enhance the efficiency of clustering. Whereas most existing visualization techniques used in clustering are exploration oriented, inevitably, they are mainly stochastic and subjective in nature.

We developed an approach called HOV3 (*Hypothesis Oriented Verification and Validation by Visualization*), which projects the data distribution based on given hypotheses by visualization in 2D space. Our approach adopts the user quantitative domain knowledge as measures/hypotheses either in the cluster discovery or cluster validation processes to reveal the gaps of data distribution to the measures. In addition HOV3 enables users to adjust their hypotheses iteratively in order to obtain an optimized view. As a result, HOV3 provides users an efficient and effective visual method to detect and validate cluster information.

XML Management Systems

MAGHAYDAH Moad

Supervisor: A/Prof Mehmet Orgun

Associate Supervisor: Dr Abhaya Nayak

Abstract:

As the need to support variant operations on XML data such as insertions and concurrent access, has increased, the Dewey based labeling method for XML documents is increasingly considered to be most suitable for labeling XML nodes. In this paper, I present in brief the XML Management Systems (requirements and features). Furthermore, I present two labeling techniques based on Dewey identifiers for XML data management systems (XMLMS). The first technique XMASK improves the performance by dealing with integer numbers while the second technique, which I call PoD (Prefixing on Demand), minimizes the label length for general XML documents and it supports insertion without relabeling any existing node by providing an insertion hook.

DASMAS – Dialogue based automation of semantic interoperability in multi agent systems

ORGUN Bhavna

Supervisor: Dr Mark Dras

Associate Supervisor: Dr Steve Cassidy

Abstract:

This talk presents our ongoing effort on developing a dialogue based framework for resolving semantic interoperability in multi agent systems. Our approach is characterized by: (1) multi agent systems that have real world heterogeneous ontologies; (2) the resolution of semantic differences at run-time through an adapted ontology negotiation protocol (ONP); and (3) the use of the Word Net lexicon in the resolution process.

~~~~~  
**20 June 2006 (Tuesday)**

**TALK SESSION: 4 11.00 am – 12:40 pm (in E6A357)**

***Distributed Algorithms in Extremely Mobile Networks***

**LEE Joanne**

Supervisor: A/Prof Bernard Mans

Associate Supervisor: Dr Mark Dras

Abstract:

A MANET (Mobile Ad hoc NETwork) consists of mobile nodes that communicate wirelessly in an infrastructureless domain, where the nodes employ multi-hop routing (i.e. use other nodes as relays) to deliver packets to destinations that lie outside of their transmission ranges. Current MANET routing protocols always assume an end-to-end path exists for any source-destination pair (i.e. the network topology forms a connected graph). However, for important applications such as search-and-rescue operations, this assumption does not always hold true; these scenarios are characterised by nodes with high mobility, leading to frequent link breakages between nodes and possibly to network partitioning.

Several challenges arise when designing routing protocols for these "extremely mobile" networks, including the limitations of high power consumption, low bandwidth, interference, limited computational ability and high error rates. One particular challenge is how to accurately model the underlying mobility of the nodes. Some initial approaches in algorithm design have used simple mobility models; however, this limits the ability of these algorithms to route effectively in the more challenging, real-life scenarios.

In this talk I will discuss the work achieved during my first year of the PhD. I will explore the challenges involved in modelling node mobility and designing routing algorithms for extremely mobile networks, and present my proposed routing algorithm taxonomy.

### ***Authentication for Multicast Communication***

**TARTARY Christophe**

Supervisor: Dr Huaxiong Wang

Associate Supervisor: Prof Josef Pieprzyk

#### Abstract:

Multicast protocols enable data to be transmitted from one sender to many receivers via a communication network such as the Internet. The applications are as various as pay-TV, online games and military defence systems for instance. The sensitivity of transferred information requires a non-repudiable proof of the sender's identity. Several parameters have to be taken into account such as the size of data packets transiting into the network as well as the time spent by the sender and the receivers to process information. To be of practical interest these constructions have to be proved secure against adversaries since most of these protocols will be used over insecure networks such as the Internet. A central point is the determination of practical good balances between efficiency of computations and security of transmission. In this presentation, I will introduce a few provably secure techniques which enable content authentication over such malicious channels.

### ***Private Information Retrieval***

**WANG Peishun**

Supervisor: Dr Huaxiong Wang

Associate Supervisor: Prof Josef Pieprzyk

#### Abstract:

A Private Information Retrieval (PIR) protocol allows a user to retrieve a data item of his choice from a database while hiding the identity of the item from the database server. To date, PIR has received significant attention in the literature, but a number of practically important limitations remain: queries are limited to returning small items (typically single bits), query response time is too long, and data must be retrieved by address as opposed to by keyword search. All these make PIR schemes impractical in the real world.

Because most PIR protocols have very high computation complexities to retrieve a small item (requiring the computation for each bit of the entire database in order to retrieve a single bit), this results in impractical query response time. To remove this restriction, several protocols were proposed. Unfortunately, these secure coprocessor-based protocols known today still required heavy periodical preprocessing computation. I tackled this problem and developed a new scheme.

Most PIR schemes assumed that the user knows the physical address of the sought item. This is usually not the case in most databases in practical use. Instead, the user typically holds a keyword (for example, the name of a specific company traded in the stock market). To solve this problem, PIR by Keywords was studied. I have been focusing on this case, and proposed a scheme of keyword search on encrypted data.

### ***Character Sums and Recurrence Sequences***

**BALASURIYA Sanka**

Supervisor: Prof Igor Shparlinski

#### Abstract:

This talk will mainly be concerned with the progress and the general direction of the intended research. The character sums and their bounds which play an important part in this research will be discussed.

The recursive sequence  $a_n = na_{n-1} + 1$ ,  $n=1, 2 \dots$  with the initial term,  $a_1=0$  and some of its properties too will be discussed. The bounds of some character sums involving this sequence will also be discussed.

### **TALK SESSION: 4 1.45 pm – 3.00 pm (in E6A357)**

#### ***Smooth numbers and character sums***

**SUTANTYO Daniel**

Supervisor: Prof Igor Shparlinski

Associate Supervisor: Dr Christophe Doche

#### Abstract:

Factorisation and primality testing are the two major areas where we see numerous applications of number theoretic methods, and one topic which has found an increasing amount of use in recent years is the study of smooth numbers. Smooth numbers are composite numbers which has only small prime numbers, and in the talk I will give a brief introduction to what they are and give an outline on how it can be applied to produce some results.

#### ***Digital watermarking of multimedia objects***

**GUPTA Gaurav**

Supervisor: Prof Josef Pieprzyk

Associate Supervisor: Dr Huaxiong Wang

#### Abstract:

This presentation illustrates the work done by me, in my research, since the last mini PG conference in September, 2005.

The major issues and topics discussed in the presentation are:

1. introduction to digital watermarking
2. research objective
3. text watermarking
4. software watermarking – possible attacks
5. software watermarking – proposal
6. Future work

#### ***Cryptanalysis of short variants of SHA-256-XOR***

**MATUSIEWICZ Krystian**

Supervisor: Prof Josef Pieprzyk

#### Abstract:

In this presentation, cryptographic hash functions are briefly introduced and some of their real-life applications are presented. A short overview of recent attacks on

dedicated hash functions is followed by the results of our studies on the security of SHA-256 variants. We outline a general method of finding low weight differential characteristics suitable for attacking SHA-256-XOR and discuss the potential and limitations of this method.

**TALK SESSION: 4 3.30 pm – 4.45 pm (in E6A357)**

***The AES SBox***

**McDONALD Cameron**

Supervisor: Prof Josef Pieprzyk

Abstract:

AES is one of the most highly used block ciphers. It has been approved by the NIST as a standard for US Government sensitive information, including SECRET and TOP SECRET information. The design of AES provides a high level of security and resists the classical methods of attack, including Linear and Differential cryptanalysis. The security of AES against the new algebraic attacks is not well known. One of the components that provides AES with its security is the non-linear SBox, a substitution layer based on a lookup table. The talk will focus on the structure of this SBox and explain the different methods that lead to different algebraic representations. An introduction will also be given on creating approximations to the SBox that hold with significantly high probability.

***Distinguishing attack on NLS***

**CHO Joo Yeon**

Supervisor: Prof Josef Pieprzyk

Abstract:

NLS is one of the stream ciphers submitted to the eSTREAM project. We present a distinguishing attack on NLS by Crossword Puzzle (CP) attack method which is newly introduced in this paper. We build the distinguisher by using linear approximations of both the non-linear feedback shift register (NFSR) and the nonlinear filter function (NLF). Since the bias of the distinguisher depends on the  $K_{\text{const}}$  value, which is a key-dependent word, we present the graph showing how the bias of distinguisher vary with  $K_{\text{const}}$ . In result, we estimate the average bias to be around  $O(2^{-30})$ . Therefore, we claim that NLS is distinguishable from truly random cipher after observing  $O(2^{60})$  keystream words on the average. The experiments also show that our distinguishing attack is successful on 90.3% of  $K_{\text{const}}$  among  $2^{32}$  possible values.

***Development of a Privacy Non-invasive User Identification System With Added Dimension of Longevity and Universality to Cover All Types of People Interacting With e-Government Systems***

**SEDAGHAT Soroush**

Supervisor: Prof Josef Pieprzyk

Abstract:

eGovernment is the use of the information and communication technologies in all feasible areas of public administration, where it makes sense, combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies. eGovernment covers administrative procedures, legislations and available services in electronic form to enable co-operation between actors in eGovernment (citizens, business and government itself).

Literature survey associated with the security of eGovernment systems and services has shown that among various challenges, clients identity management is a key security issue because proof of citizens identity that is non-repudiative is a requisite for any eGovernment services, and so far no standard authentication system is developed, accepted and widely used by citizens.

The existing user identification protocols, for example the proposed biometric solutions, do not apply to all citizens uniformly. For example, facial recognition systems do not automatically remain up-to-date as the citizens' age will change by time. On the other hand, the current identity management solutions lack longevity characteristic, which could be regraded as an element of trust. That is they do not have a history of use attached to them, which otherwise it would endanger their security. These are major concerns for Governments, which try to cut costs of continuous system updates and more importantly they are looking for universal authentication methods that cover all types of people uniformly.

Development of Smartcard technology with embedded biometric has tried to offer a solution to cover majority of citizens but because of privacy concerns and possibility of forging biometric such as fingerprints by intruders, they have not gain support of citizens. Additionally Smartcard technology lacks interoperability with different hardware and application software because there are no global standards defining all aspects of their operation.

The ultimate goal of this PhD study is to develop an appropriate client identity management system that covers all citizens uniformly; its intricacies are invisible to ordinary users, simple and user-friendly and reliable and trustworthy with added dimension of longevity. More importantly it is privacy non-invasive and cost effective in order to win citizens and governments' confidence.

## **TALK SESSION: 2 3.30 pm – 4.20 pm (in E6A102)**

### ***A Specification Framework for Enhanced Modeling of Semi-Structured Information Domains***

**MILLER Gillian**

Supervisor: A/Prof Dominic Verity

Associate Supervisor: Prof Michael Johnson

#### **Abstract:**

The aim of my research is to come up with a framework to allow for enhanced data modeling and constraint specification by information systems practitioners. The research is motivated by practical application, but at the same time should have theoretical underpinnings. As part of the framework I have proposed an abstract language for expressive specification of invariants and data structural constraints. Features of the language include a rich set of encapsulated constraint primitives, concept classification and commuting constraints together with a powerful navigation based path language. The result is a small elegant system which allows for the concise representation of commonly occurring constraint patterns. In the talk I will discuss recent work in progress. Firstly I am developing a concrete XML specification language and supporting modeling environment. Secondly I am interested in the formal aspects of the system. For example we would like to reason about the specification to see whether the specification is consistent and can admit a model. By capturing the essential aspects of the system in a small logical formalism, we can

see that our system is more expressive than the current semantic web ontology languages, but is deliberately less expressive than extensions of first order logic.

***The Semantics of the Pure Pattern Calculus***

**ROBERTS Matthew**

Supervisor: A/Prof Dominic Verity

Abstract:

In this talk, we explore the details and subtleties of the semantics of the Pure Pattern Calculus. The Pure Pattern Calculus is an alternative the lambda calculus and while they share many attributes, they differ in significant and interesting ways. We will approach the semantics by first presenting an incorrect naive semantics and then converging on the correct solution by looking at each problem with the naive semantics.

-----  
**22 June 2006 (Thursday)**

**TALK SESSION: 1 9.00 am – 9.50 am (in E6A102)**

***Security Framework for Wireless Mobile Ad hoc Networks***

**BALAKRISHNAN Venkatesan**

Supervisor: Prof Vijay Varadharajan

Associate Supervisor: Prof Hoang Doan(UTS) and A/Prof Yi Mu(UOW)

Abstract:

Mobile ad hoc networks (MANET) operate without an infrastructure and enable a node to communicate beyond the wireless transmission range via multiple hops. In spite of the advantages, they suffer from a range of issues, the one of them being security. Security is particularly difficult to achieve due to various factors such as -- promiscuous medium, dynamic topology, sporadic connectivity and absence of centralized authority. There have been several researches to secure ad hoc networks. Most of these approaches target to secure the communication due to the self-organized nature of the ad hoc networks. These approaches can be broadly categorized into two groups: one is concerned with the prevention and relies on the cryptographic techniques; other concentrates the detection-response and depends on the monitoring techniques. The former is static and fails to handle selective misbehaviors. The latter falls short due to lack of provision for authentication and integrity.

The presentation introduces our proposed reputation-based trust model known as 'Secure MANET Routing under Trust Intrigue (SMRTI)' for engineering trust-aware mobile ad hoc systems. SMRTI adds strength to secure routing approaches thereby enhancing the security of the communications. We explicitly identify three perspectives (direct, observed and recommended) to capture other node's behaviours or actions and attribute it as experiences. For every experience or captured behavior within a perspective, we evaluate the opinion with respect to the nature of the behavior and the type of the context. We utilize the observed perspective to differentiate and isolate the adjacent colluding attacks. One of the strengths of SMRTI is the exclusion of supplementary message exchanges to gather other node's recommendations. Sequentially, the novelty of recommendation capture eliminates the likelihood of bias that may arise from the recommender's subjective internal ratings. As a result, the model overcomes the honest elicitation and free-riding problems. In addition, we also address the uncertainty introduced in the

relationships when nodes move apart and abstain from communication for a long time. We explain the model using source-initiated on-demand routing protocols and validate the model through simulation results.

***Techniques for the Design of Trust Enhanced Secure Applications***

**NAGARAJAN Aarthi**

Supervisor: Prof Vijay Varadharajan

Abstract:

Web services are increasingly being used in daily life for electronic commerce. These services can range from simple requests to complex business processes, but there is still a major concern about the trustworthiness of these services. Although there are standards for providing confidentiality, integrity and authentication of web services, there are no standard techniques available for reasoning the trust levels of such services. This research aims to provide a Trust enhanced Secure Model (TeSM) that will provide means for specifying and managing trust for web based applications.

This talk will address why the present Web Services Trust specification is inadequate and how Trusted Computing technology can become an essential component of the TeSM framework.

**TALK SESSION: 7 11.00 am – 12:15 pm (in E6A102)**

***A Framework for Validating Requirements Engineering Process Improvement***

**PALYAGAR Bhavani**

Supervisor: Dr Frank Moisiadis

Abstract:

Improving Software Development Life Cycle (SDLC) processes in software development organizations has become a necessity for providing maximum value to customers. Requirements Engineering (RE) processes form a critical phase of the SDLC. There are many types of RE processes identified by research and in practice. Each RE process has its own characteristics, based on its goals, that makes an RE process unique. Thus, software industry has adopted different assessment for different RE processes.

Often RE process improvement is identified as a key exercise to maximize the SDLC process improvement benefits. When RE processes are assessed for their deficiency and are improved, based on well-defined measures, improvement benefits can usually be guaranteed. Such benefits directly enhance the value of customers' business that uses the software systems. As a result, the returns the organizations provide to customers is continuously enhanced.

Research in RE process improvement has examined the relationship between RE process quality and software quality with little attention to measurement. With the industry, often RE process improvement has been argued to have both positive and negative effects based on somewhat ambiguous results, reflecting a lack of RE process measurement. This thesis presents a conceptual measurement-based framework for validating process improvement of an RE process. The distinguishing characteristics of the framework are the adaptation of measures from general engineering, and its simplicity in order to assist the SDLC staff to measure RE

process problems, and then address them by providing improvement pinpointed against the identified and measured problems.

The conceptual framework utilises a standard decision matrix from the literature that connects the quality of RE processes to the quality of requirements with cause-effect relationships. In addition, the framework establishes relationships with other SDLC processes that impact RE processes such that certain RE process problems can be traced to other SDLC processes such as Change Management (CM) and Risk Management (RM).

The conceptual framework has been evaluated using case studies involving some large-scale software development projects in more than one organization. The results of the empirical study and subsequent application of the framework to 'real life' RE indicate that the framework can measure the RE process, and if found to be deficient, improve the RE process and establish proof of benefits of such improvement. Further, the application of this framework can ensure that RE process improvement will have a positive effect on the SDLC to the extent of minimizing cost and schedule overruns that are effected by requirements related rework.

This research therefore provides an important basis and foundation for generalizing RE process measurement and improvement.

### ***Monitoring and management Business collaboration base on service level agreement***

**ALKAHWATI Majid**

Supervisor: A/Prof Jian Yang

#### Abstract:

Businesses establish relationship between them to exchange the service through the internet/intranet where some business request service and other provide the service. They specify the roles of each party playing, what is the format of the messages exchange to provide the service and what is the more important which are the temporal and order constraint for the sequencing of the messages.

Businesses exchange the services need to agree on the service to provide by one business to other before they exchange it. This agreement must to be specified and both businesses sign it.

Agreement defined set of activities, roles, and responsibilities to be taken by different parties to satisfy the terms and conditions in the agreement. Agreement build a new business relationship between contractual partners and provides a guarantee to all contractual partners according to the clauses of the signed contract and relevant laws.

Checking the service provided quality is part of the agreement fulfillment. To monitor the agreement fulfillment we need to compare two qualities, the promised quality, which is specified on the agreement, and the actual service quality. To collect the data from the service exchange, we may use some formulas to calculate the quality from this data collected.

To achieve the interaction between the parties and fulfill the agreement between them we need to address two issues, first, the agreement consist of a set of actions to fulfill this agreement, we need to execute these actions in order, which is mean we execute the first action then we move to the second action to execute it and so on.

Second we check each action's behavior with the rules specified in the agreement and check the provided service quality with the quality specified in the contract.

To monitor the service exchange and to prevent any agreement violation, we need to execute the actions sequentially and check each action's quality, to provide agreed service quality.

We define the Exchange Message Rules (EMR) to be followed when parties exchange messages between them during the service providing. These rules are part of the agreement, the involve parties set these rules. To check the behavior of the message send across the parties (every message send across the involve parties is action of the agreement), we check the characteristics of this message with EMR. The message (action) behavior can change the provided service quality or even this behavior may violate the agreement.

The rules can define as templates and the parties fill the field of these templates and set them as rules in the agreement

### ***A Framework for Managing Consistent Business Transaction***

**SUN Hai Yang**

Supervisor: A/Prof Jian Yang

#### Abstract:

The business transaction is a business process orchestrating and choreographing the loosely coupled web service into one logical unit to achieve one business objective among the Business-to-Business Integration (B2Bi) and Enterprise Application Integration (EAI). Such the business transaction requires transactional support by coordinating distributed autonomous business functionality and guaranteeing the reliable and consistent seamless join of these web services. Solutions to satisfy the database transaction requirements have been proved not to flexible enough to manage consistent business transaction, even the transactional workflow. In order to comprehensively improve existing mechanism and solution for solving transactional issues, my research is to provide a completely business transaction-oriented framework.

Firstly, a scenario in the automotive-dealer industry will be analyzed as a transaction model. Secondly, a Level-based Business Transaction Consistency (**L-BTC**) is constructed. The L-BTC is composite of the three specifics-oriented consistencies, status-oriented consistency, behavior-oriented consistency and business-oriented consistency. There are also another five sub-consistency classifications, physical consistency, abstract consistency, logical consistency, directional consistency and business roles consistency on the basis of five sub-states of the whole business transaction. Thirdly, several business transaction management requirements will be disclosed from the sophisticated transactional model. Each requirement is satisfied to maintain the transaction executing consistently (**B-BTMRs**)<sup>1</sup> or dealing with the inconsistent issues during the execution of the business transaction (**A-BTMRs**)<sup>2</sup>. Finally mechanisms relevant to satisfy each requirement will be imbedded in the framework combined with the proprieties of transactional workflow and web service protocol like WS-C. The application of the Petri net theory will be bound into the framework to achieve the quantitative definition of the business transaction model and construct the transactional mechanism. WS-Coordination as the protocol in SOA coordinating other protocol like WS-Tx to achieve the transactional requirement will be used to direct the framework available under the web service environment.

**(B-BTMRs)**<sup>1</sup>: Basic-Business Transaction Management Requirements to enforce business transaction consistency

**(A-BTMRs)**<sup>2</sup>: Advanced-Business Transaction Management Requirements to deal with inconsistency

**TALK SESSION: 7 12.45 pm – 2.00 pm (in E6A102)**

***Digital Image Watermarking for Copyright Protection***

FALLAH-MOSHFEGHI Kourosh

Supervisor: Dr Len Hamey

Associate Supervisor: Prof Josef Pieprzyk

Abstract:

Copyright protection is a key issue in the current media market's digital reformation. In this presentation I discuss available methods for copyright protection of multimedia documents, focusing on digital image watermarking. Conceptually, watermarking is imperceptible embedding of auxiliary digital information within digital content and its on demand later retrieval. This information can be used for a variety of purposes, especially owner identification in the case of copyright infringement.

Like any other security method, the usefulness of a watermarking algorithm is judged by its robustness to possible attacks. Of particular interest in my work are synchronization attacks that pose a major threat to current algorithms. I discuss this class of attacks and the proposed countermeasures against them. I'll show that interpolation operation that usually accompanies geometrical transformations can significantly affect the performance of watermarking algorithm, even in the case of perfect resynchronization. I'll also propose possible countermeasures to deal with this problem.

***Online Approaches to Developing Computing Students' Expertise***

**BOWER Matthew**

Supervisor: Prof Michael Johnson

Abstract:

While there are some aspects of teaching and learning programming that transfer from the face-to-face environment to the online environment, there are several crucial differences. This research is investigating the ways in which the affordances of online technologies can be leveraged to accelerate the development of computing students towards expert behaviour. This presentation will outline the design-based research approach being adopted, and the interim results regarding how task type, activity specification and interface design can affect the types of collaborations that occur and thus the effectiveness with which student mental models are developed.

~~~~~  
23 June 2006 (Friday)

TALK SESSION: 8 10.30 am – 11.55 am (in E6A357)

Enhancing Privacy in Public Information Retrieval

YE Qingsong

Supervisor: Dr Huaxiong Wang

Associate Supervisor: A/Prof Mehmet Orgun

Abstract:

In recent years, research on protecting database privacy has received considerable attention from both academia and industry. Oblivious transfer (OT) is a cryptographic technique that has been used in various applications to protect database privacy. In

this talk, I will present our recent result on distributed OT . Our approach is based on a combination of secret sharing scheme and Homomorphic encryption functions, which provide information semantic security and require no private key for encrypted data computation. With our improved distributed OT , we also extend our solution to the problem of privacy-preserving set intersection in a distributed scenario that potentially has many applications for online collaboration.

Distribution Properties of Some Pseudorandom Number Generators

EL-MAHASSNI Edwin

Supervisor: Prof Igor Shparlinski

Abstract:

The purpose of this talk is to give an outline and some background information on some well-known pseudorandom number generators. More importantly, we provide some new results on their distribution and, as such, how these might prove useful in cryptographic and for Quasi-Monte Carlo methods. Lastly, we describe some open problems/future work in this area.

~~~~~ ***End of presentations on 23 June 2006*** ~~~~~