The 17th White House Papers
Graduate Research In Informatics at Sussex

Edited by
Jon Robinson

CSRP 571

June 2004

Cognitive Science

Research Papers

Preface

Each year, towards the end of June, postgraduate researchers from Informatics at the University of Sussex get together to discuss their research and (probably more importantly) socialise.

The two-day Isle Of Thorns Annual Graduate Workshop, named after a former conference centre of the University of Sussex, is taking place this year at the Cavendish Hotel for the first time. Each delegate will present a brief overview of their research, gaining valuable research experience as well as the opportunity to take advantage of the interdisciplinary nature of Informatics.

Named after one of the buildings at the original conference centre, the White House Papers was formally the follow-up publication for the workshop. Following the precedent set by last year's workshop, the White House Papers are being published in advance of the conference and are intended to provide a wide snapshot of postgraduate research in Informatics. Intended to be easy reading, the 17th White House Papers consists of typically two-page submissions accompanied by author photographs and short biographies. Due to the breadth of research being carried out in Informatics, much of the emphasis at the workshop and in the papers is to present to an audience whose members come from a large variety of backgrounds. This means that many of the papers serve as a general or non-specialist introduction to the author's work. If readers are interested in the material then they can obtain more information and full publications (in some cases) from the relevant author.

Again following the precedent set last year, all of the papers have been reviewed by members of a Program Committee and authors given the opportunity to amend their papers in response to their reviewer's comments. I would like to take this opportunity to thank the Program Committee for their invaluable contributions and help that I am sure will continue throughout the workshop.

Lastly, it should not be forgotten, however, that the Isle Of Thorns conference and the White House Papers could not be such successes without the contributors themselves.

Jon Robinson
June 2004
Informatics Postgraduate Student Representative
Compiler and Editor

Program Committee

Sallyann Bryant
David Ellis
Jon Robinson
Sampsa Sojakka
Thom Heslop

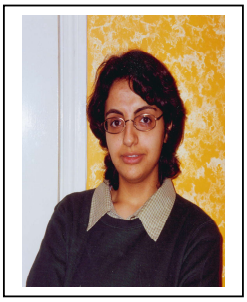
Contents

Biographical Information

Elly Adams

Elly Adams is a former Open University student. In 2000 she began the MRes course and changed to a part-time DPhil in 2001. In 2003 she became a Research Fellow. Her main areas of interest are memory and eyewitness testimony.

Marzieh Asgari-Targhi



Marzieh Asgari-Targhi is a DPhil student at COGS in her second year. Her first degree was in Philosophy at University of London. She then did a Masters in History and Philosophy of Science at the London School of Economics and Political Sciences (University of London). Her research interests lie mainly in analysis of causal reasoning in Artificial Intelligence.

Matthew Bardeen

My current research interest is how the diversity affects the stability of systems, with a focus on ecosystems. To this end I have been studying various systems models such as Daisyworld, Self-Organized Criticality, and Ultrastability. My supervisors are Adrian Thompson and Emmet Spier.

Edgar Bermudez

Edgar Bermudez got his first degree (BSc) in computer Science in the National Autonomous University of Mexico (UNAM) in 2002. In 2003 he did an MRes in Computer Science and Artificial Intelligence at Sussex University and now he is starting a DPhil in the Informatics School of Sussex University. His research interests are active vision and robotics.

Sallyann Bryant

Sallyann Bryant is a DPhil student in the IDEAS laboratory at Sussex. She is particularly interested in eXtreme Programming (XP) and the skills and behaviour involved in pair programming at a single computer terminal. Sal is currently analyzing data collected during a one-week study of commercial eXtreme Programmers.

Martin Coleman

After many years employment in a variety of 'character building' jobs, Martin Coleman finally enrolled at City University (London) in the summer of 1998. Successfully completing a first degree in psychology Martin was then lucky enough to secure a post at the University of Sussex to read for his DPhil. His twin ambitions are to both push back the boundaries of human knowledge whilst simultaneously avoiding the horrors of a 'proper' days work.

David Ellis

David Ellis holds a BSc(Hons) in Computer Science and Artificial Intelligence from the University of Sussex. He is now studying towards a DPhil in the network lab at Sussex University under the supervision of Ian Wakeman.

Amanda Harris

Amanda Harris has a BA in Applied Psychology from the University of Sussex. She is currently in the second year of her DPhil at Sussex and is working as part of the Riddles project in the Department of Informatics. Her research focuses on the influence of motivation on children's ability to engage in effective peer collaboration.

Thom Heslop

After pursuing a long and "colourful" career of various roles (including singer, experimental film distributor and rare record expert) Thom Heslop took his first degree – BSc (Hons) Internet Computing – at London South Bank University, which he gained with distinction. He has since decided that his middle "youth" (ha!) would be best spent frying his brains reading for a DPhil and so is currently in his first year at Sussex, under the supervision of Dr. David Weir.

Li Jian

LI Jian got his bachelor degree in Chongqing University of Posts & Telecommunication, China, and he is the first year of Mphil student in University of Sussex now. His research interesting is JVM and compiler.

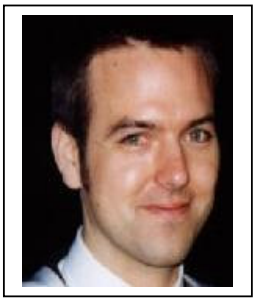
Paul Loader

Paul Loader did his first degree in Philosophy at the University of Kent at Canterbury. After a gap of many years he then went on to do an MSc in Information Technology at Queen Mary, University of London (QMUL), graduating in September 2001. In January 2003 he began his DPhil studies in Philosophy of Cognitive Science.

David Ma

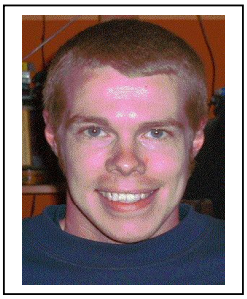
Xingdong Ma got his BEng in Chemical Engineering from Beijing University of Chemical Technology. In the following years, he has completed his MSc in Chemical Engineering from Washington University in St. Louis and MSc in Multimedia Applications and Virtual Environment from University of Sussex. Mr Ma is currently a first year DPhil student in Department of Engineering and Design. His research interests are video streaming and wireless communication.

Mark McLauchlaun



Mark McLauchlan is a DPhil student at Sussex University. He studied German, Economic History and Computer Science at Victoria University in New Zealand before studying a Masters degree in Artificial Intelligence at Edinburgh University. His research interests lie in applying machine learning techniques to problems in Natural Language Processing.

Anthony Morse



Anthony Morse gained a degree in Cognitive Science at the University of Hertfordshire graduating in 1999. He then completed an MSc in Evolutionary and Adaptive Systems at Sussex University where he has now in his final year of a DPhil investigating the development of structure in neural mechanisms.

Obowoware Obi

Obi gained an MSc in Multimedia Applications & Virtual Environments from Sussex in 2002. He is currently in his first year of a D.Phil investigating networking systems.

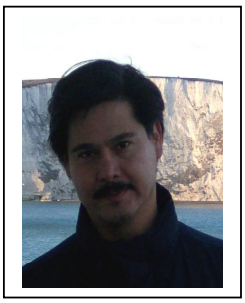
Pasha Parpia

My background is in Physics, having done my undergraduate study at Sussex and a doctorate at Cambridge, in X-ray diffraction studies of defects in single crystals. After several postdoctoral positions working on novel systems for screening breast cancer, and further work in X-ray diffraction, I did a M.Sc. conversion course in Cognitive Science. I have since Lectured in AI at Sussex and at the University of Western Australia, where I was the director of the Cognitive Science Programme. I have since been a Visiting Research Fellow in COGS

Jon Robinson

I originally gained a BSc(Hons) in Computer Science many years ago, and have been in industry for 10 years in a variety of roles. More recently I completed an MSc in Multimedia Applications and Virtual Environments at Sussex in 2002. I am currently in my second year of my D.Phil where I am investigating service composition in Pervasive Computing Networks.

Martin Santos



MSc in Computer Sciences from the University of Colima, Mexico, 1998. Since 1998, lecturer of the School of Telematics at the University of Colima. In 2002 I developed an On-line Testing System: a Simulator of the General Test for Graduate's Bachelor in Arts of the National Evaluation Centre (CENEVAL-EGEL) in Mexico. This work was presented in the II International Congress of Computer Science and Informatics of the ANIEI, Mexico, 2003. From October 2003 DPhil student in Computer Sciences and Artificial Intelligence at Sussex University. My research interests are in the area of cognitive learning processes and teaching – the role of teaching in supporting cognitive learning processes and the implications for the lesson strategy. I am currently working on the design of an experimental lesson strategy that supports students' cognitive learning processes.

Sampsa Sojakka

Sampsa Sojakka came to Sussex from the cold lands of the far north. Using the momentum gathered from studies in physics, he blasted straight through a computer science degree and went on to do a DPhil in evolutionary robotics. Sampsa is studying collective behaviour and synchrony in large scale networks under the supervision of Inman Harvey and Ezequiel Di Paolo.

Ashish Umre

Ashish Umre graduated with a First Class Bachelor of Engineering (B.E.) in Computer Science and Engineering from the University of Madras, India, in 1999. He then came to Sussex in 1999, to pursue Masters of Research (M.Res) in CSAI, and immediately after started his DPhil in CSAI, based at the Networks Research Lab, COGS.

Aybala Yuksel

I obtained a BSc degree in Mathematical Engineering at the Yildiz Technical University in Istanbul. I taught at an Academy for a year, before coming to Sussex to study for an MSc in Internet Technology and Electronic Commerce. My research interest is in the Remote Usability issues and challenges that are inherent when combining low fidelity prototyping within a collaborative online communication environment.

Zaliman Yusoff

Obtained my BSc (Comp Science) and MSc (IT) from Nasional University of Malaysia in 1996 and 1998 respectively. From 1998 to October 2003, I worked as a lecturer at Universiti Tenaga Nasional. In Oct 2003 I registered as a full time DPhil student at Sussex Uni. My main research interest is about emotion (Meta affective) and Intelligent Tutoring System (ITS).

Improving the Reliability of Automobile Memory

Elly Adams
School of Life Sciences
University of Sussex
E.J.Adams@sussex.ac.uk

Introduction

An Eye-witness's memory for vehicles at the scene of an accident or trauma in such cases as child abductions, traffic accidents and any crime involving the use of a 'get-away' vehicle is of crucial importance for many types of forensic investigation. 'Motorfit' (Grantham, 1989), a prototype, devised to assist witnesses in a similar manner to face identification packages, proved problematic on implementation.

This research aims to help bridge the gap between the needs of the police investigators and the lack of scientific literature about automobile memory.

Initial research involving a vehicle marques identification questionnaire test, driving frequency and general memory measures showed that drivers scored higher than non-drivers. Additionally, males scored slightly higher than females in memory accuracy.

Other research involving vehicle speed estimation showed that if estimating in kph, the estimate was lower and less accurate than if the participant was asked to estimate in mph.

Current research includes a 'walk-about' experiment which involves participants walking around a car park and later being asked to identify any vehicles they had seen from a set of photos, similar to those used for face identification by police officers.

Also currently running is an experiment involving participants watching video clips of either a vehicle's journey or the same journey but incorporating an accident. Recall is in two stages after a 'filler' task; free recall, later followed by guided recall similar to the Cognitive Interview.

The research aims to address the following:

1. What do people recall?
2. Can it be predicted who will be more accurate about memory for vehicle?
3. Do certain situations lead to more reliable memory reports?
4. Which methods can be used to improve the reliability of eye-witness reports?
5. How can these methods be best implemented in computer software?

References

Grantham, S. (1989). In Motorfit. Home Office, Police Research Group, UK.

Does the direction of time tell us anything about the difference between causation and correlation?

Marzieh Asgari-Targhi
Department of Informatics
University of Sussex
marzata@sussex.ac.uk

Introduction

One of the main obstacles to building a causal model in AI is to use constraints that are able to differentiate between causation and a mere correlation. First I will examine what is correlation, next I'll talk about what I have come to know as causation, having done some research. Then I will investigate what role the direction of time can play in identifying causal statements from non-causal statements.

What is correlation?

The discovery of correlation began Hundred years ago by Francis Galton, [3], inventor of fingerprinting and cousin of Charles Darwin, set out to prove that talent and virtue run in families. His investigation drove him to consider various ways of measuring how properties of one class of individuals or objects are related to those of another class.

In 1888, he measured the length of a person's forearm and the size of that person's head and asked to what degree can one of these quantities predict the other. He discovered that if you plot one quantity against the other and scale the two axes properly, then the slope of the best-fit line has some mathematical properties. The slope is 1 only when one quantity can predict the other precisely; it is zero whenever the prediction is no better than a random guess, and most remarkably, the slope is the same no matter if you plot X against Y or Y against X.

Galton said, “it is easy to see that co-relation must be the consequence of the variations of the two organs being partly due to common causes”. Therefore for the first time an objective measure of how two variables are ``related" to each other is given and that is based on the data not on human judgment or opinion.

For Galton, then, there was a category broader than causation, namely correlation, of which causation was only the limit.

What is causation?

What patterns of experience would justify calling a connection “causal”? Having looked at the history and philosophy of causation, I think causality has many different facets and elements, and cannot be identified by only one aspect. The elements are as follows:

1. Uncertainty element or probabilistic element of causation.
2. Logical element: Necessary and sufficient elements, i.e, a cause is necessary and sufficient for the effect.
3. Counterfactual element: Causal statements are always described in terms of counterfactual.
4. Explanatory role of causal statements.
5. Its dependency on the direction of time.

There are other explanation that why we use causal terms, such as the agency theory of causation, [4], according to which causality is closely relate to the standpoint from which we (human beings) see the world as agents, but I shall only focus on time.

Does time have any direction?

As I mentioned above causes have definite elements or facets that separates them from

being mere correlation. One of the most important element of causality is that causes have a definite direction in time, i.e if A causes B and A occurs before B, then B does not cause A. Apart from a few speculations in Theoretical physics, [1], it is universally conceded that causes do not operate backwards in time. This understanding that a cause should precede its effect is a temporal expectation in Human discourse. If we consider time as one of the four dimensions of space-time, objects can only travel on one direction in time; from the past, through the present into the future.

Bayesian and decision networks model relationships between variables at a particular point in time, but it's implicit. To consider causal relations, time has been added as an extra variable to their model [2]. That helps to reason about changes over time.

However, The reliance on temporal information has its price; it excludes a priori the analysis of cases in which the temporal order is not well-defined, either because processes overlap in time or because they (appear to) occur instantaneously.

Also, temporal information alone cannot distinguish genuine causation from spurious associations caused by unknown factors- the barometer falls before it rains yet does not cause the rain. The main aim of my research is to find a mechanism that can accommodate for all the aspects of causation that I have talked about not for one or two elements, a holistic causal model perhaps.

Bibliography

[1] J.S. Bell. *Speakable and Unspeakable in Quantum Mechanics; Collected Papers on Quantum Philosophy*, Cambridge University Press. 1987

[2] K. Korb, K. Nicholson, A. *Bayesian Artificial intelligence*. Chapman and Hall CRC, London, 2004.

[3] J. Pearl. Causality, Models, Reasoning, and Inference. Cambridge University Press, 2000.

[4] H. Price. Agency Theory and Causal Asymmetry, Mind, 101, 502--520, (1994).

The value of death: A lesson from Daisyworld

Matthew Bardeen
Department of Informatics
University of Sussex
mdb20@sussex.ac.uk

Death is the endpoint of all living things, and while it is tempting to think of it as an inherently random process, this is far from the truth. Environmental factors, such as lack of food and temperature variations, increase the chance of death in many organisms. This idea is one of the central tenants of Darwin's theory of natural selection. Organisms which are less fit for their environment are replaced by those which are more fit.

In 1978 the Daisyworld model [1] was introduced as a way to lend credence to the Gaia hypothesis, which suggests that organisms have altered conditions on earth to their own liking through localised interactions. Daisyworld is a toy-world and the idea behind it is simple -- localized interactions can affect global dynamics and generate homeostatic behaviour. The model consists of a ``planet", heated by the sun and populated by black and white daisies. The black daisies have a lower albedo (reflectiveness) than the white daisies, thus they absorb a greater amount of solar radiation and raise the local temperature. The growth rate of the daisies is linked to the local temperature. The difference in growth rate causes the area covered by black and white daisies area to vary, thus warming and cooling parts of the planet. This creates a homeostatic response to external forces, such as increasing incoming solar radiation (insulation), and keeps the temperature of the planet relatively constant.

My research extends a 2D version of the original Daisyworld model [2] by adding a variable mortality rate alongside the standard growth rate. In all previous Daisyworld models, the mortality rate of the daisies was assumed to be a constant random value, regardless of temperature. In my model, the mortality rate is assumed to be dependent on the local temperature. Using this I compared the effect of having the constant random mortality rate with that of having the variable mortality rate. The results of my experiments were rather surprising. Even though the variable mortality rate was much higher overall than that of the constant random mortality rate, the daisy systems persisted for longer in many cases and the temperature of the system was less variable.

The reason for these surprising results lies is that with the constant random mortality model, daisies well suited to their local environments could be killed while those that are not are allowed to persist. However with the variable mortality rate, those daisies that are unsuitable for their local environment are more likely to die while those that are suited remain. This effect is most noticeable when mutation rates are high. As the potential difference between parent and offspring increases, the chance for a unsuitable offspring being born also increases. With the variable mortality rate, these offspring die off fairly quickly and open up the cells that they inhabited for re-growth, while under the random constant mortality rate they could persist and serve to destabilize the neighbourhood.

The higher rate of mortality outside the optimum temperature under the variable mortality model yields a higher selection pressure. This provides important feedback to daisy patches and allows a patch to tune albedos to the optimum values for a given local temperature. However, it also means less variation in the albedos -- a fact that helps in some case and hinders in others. In an unperturbed system, this high selection pressure means that the variance in daisy albedo across the planet will tend to some minimum value, determined mainly by the albedo mutation rate. While fine for unchanging systems, a low variance in albedos means that the daisies must mutate in order to persist when faced with

increasing insolation. With a high variance in albedos, it is far more likely that there exists a daisy with an albedo suitable for the increasing temperature. Systems with high mutation rates have a double advantage -- a greater rate of change in response to the environment and more inherent variation.

As the variance in daisy albedo is higher in the constant mortality rate model due to the lower selective pressure, this allows the systems to persist for longer at low mutation rates. With higher high mutation rates, the higher selective pressure of the variable mortality rate model weeds out the unsuitable daisies quicker and leads to those systems persisting for longer.

References

Based on “The value of death: A lesson from Daisyworld” accepted for publication in the Proceedings of Artificial Life IX.

[1] Watson, A. and Lovelock, J., Biological homeostasis of the global environment: The parable of Daisyworld, Tellus, 1983 Vol 35B, pp 286-289

[2] von Bloh, W. and Block, A. and Schellnhuber, H.-J., Self stabilization of the biosphere under global change: A tutorial geophysiological approach, Tellus, 1997, Vol 49B pp 249-262

A robotic approach for active vision

Edgar Bermudez Contreras
Department of Informatics
University of Sussex
ejb21@sussex.ac.uk

Introduction

Vision allows animals to carry out basic tasks employed to survive. From this perspective, object recognition turns out as a primary goal for vision systems, however, not always the vision system *per se* is employed in isolation to carry out the task required, although industrial uses of vision systems are employed in this way). Animals exploit motor capabilities in order to facilitate and fulfil the visual recognition tasks [1][2].

Active recognition or animate vision [3] where no explicit categorical representations of the 3-D world are necessarily required in autonomous agents, can be a solution to different problems in object recognition ([4], [5]) when the camera motion or the agent motion can be useful to discriminate ambiguous object images.

The main aim of my research work is the study of active vision and how autonomous agents employ complex visual information to interact in their environments. Different experiments in robotics and computer vision can be a useful tool in order to explore and to understand the fundamental issues described above.

Vision systems in autonomous agents

In order to study the capabilities of autonomous agents using complex visual information and to find out whether exist advantages in this approach, this work regards the following stages: to build the visual system of the agent, to build the control system and finally to build and test the agent (simulated or embodied) within the environment. So far, my research has mainly focused on the first of these stages.

Due to the importance of the interaction between the autonomous agent and its environment where conditions are potentially changing (illumination, pose, size, etc.), the agent's visual system involved must cope with this invariance dependency in the visual information in order to perform visual tasks.

Different models and paradigms have been implemented in this work to fulfil the feature invariance requirement of the visual system. On the one hand, more engineering based vision systems were explored and on the other hand, more biologically plausible models were studied. Some experiments have been carried out to compare these models and explore their capabilities but the results and the report of them are on going work.

Discussion and future work

One interesting point is the study of the advantages and limitations of using a biologically inspired visual system rather than a more engineering vision system in autonomous and embodied agents. Biologically inspired models offer some invariance capabilities for visual recognition tasks. It is interesting to explore as well, how robust can be an agent employing such visual system to interact within environment and perform basic tasks and to determine the advantages offered by the visual system and those gained from the behavioural strategies emerged from the exploitation of the sensorimotor loop by the agent.

Once the visual system is built and explored, the next step is the study of the interaction between sensors (visual system) and actuators (motors), namely the control system of the agent. Evolutionary strategies can be useful in this stage when the design of this interaction turns out too complex.

The future work of my research is mainly the second and third stages mentioned

previously: the study and exploration of the robot control system and the exploration of the capabilities of the agent interacting with the environment and performing basic visual guided tasks.

References

[1] Carwright, B.A. and Collet, T.S., Landmark learning in bees: Experiments and models, Journal of Comparative Physiology, 1983, Vol 141 pp 521-543

[2] Stamp Dawkins, M. and Woodington, A., Pattern Recognition and active vision in chickens, Nature, 2000

[3] Ballard, Danna H., Animate Vision, Artificial Intelligence, 1991

[4] Spier, Emmet, Behavioural categorisation: Behaviour makes up bad vision, Proceeding of the second symposium enactive perception, 2004

A terminal made for two? Understanding the skill of programming in tandem.

Sallyann Bryant
IDEAS laboratory, University of Sussex, Falmer, UK.
S.Bryant@sussex.ac.uk

Abstract.

Pair programming has been the subject of studies ascertaining its business costs and benefits (Gittins, Hope et al. 2001), providing insight into what it is like (Ambu and Gianneschi 2003) and giving advice about its adoption (Dick and Zarnett 2002). Studies in the psychology of software development have provided insight into the behaviour and knowledge of successful programmers. These two disciplines provide a foundation for assessing the cognitive aspects of pair programming and suggesting an initial categorisation of behaviours to assist in studies. This paper then discusses the early findings from an initial observational study supporting the need for a better understanding of the cognitive aspects of programming in pairs.

1. Introduction

Studies of pair programming have covered many areas and produced a variety of findings, some of which appear contradictory (Bryant 2004). For example, while pair programming has been seen to be enjoyable and productive (Cockburn and Williams 2001), improve the quality of systems (Tessem 2003) and boost the morale of the project team members (Benedicenti and Paranjape 2001), other studies suggest pair programming leads to hoarding code and ganging up on the customer (Noll and Atkinson 2003). Here a classification is given for studies of pair programming behaviours along with initial findings from an observational study.

2 Characterising successful pair programmers

Pair programming provides a useful subject of study as verbalisations are a natural part of the development process and do not have to be specially requested as think aloud protocols or post-hoc explanation. Studies of the characteristics and behaviours of pair programmers could help provide a foundation for their selection, assessment and training. To assist such studies, and ascertain which characteristics are more dominant in successful pair programmers, categories of behaviour have been defined, based on the typical interactions defined by Wake (2002) and modified following a pilot study:

1. A partner asks a question
2. A partner provides an explanation
3. A partner makes a suggestion or counter- suggests an idea
4. The pair change 'driver' in control of the keyboard and mouse
5. The partners confirm or agree with each ther
6. One or both partners look up information
7. A partner reviews or the partner or pair refactor
8. A test is run
9. One partner reminds the other
10. A partner takes a rest
11. Other . . .

These categories were used during a one-week observational study of commercial pair programmers, whose expertise had been assessed by themselves and their managers.

3 Initial findings

3.1 Skills ratings

Initial findings indicate that novice pair programmers are somewhat over-confident of their ability when their self-assessment is compared with that of their manager. In contrast, more experienced pair programmers appear comparatively under-confident. This suggests that pair programming requires more specialist skill and knowledge than initially meets the eye

and that those new to pair programming do not yet consider it very different to working on their own whereas those with more experience are aware of the additional skills required e.g. communicating complex ideas and resolving conflicts of opinion.

3.2 External representations

Although the eXtreme Programming (XP) methodology in use asserts that external representations are not required, in an observational study of 14 one-hour sessions of pair programming a total of eighteen informal external representations were produced. Typically these were highly idiosyncratic and ephemeral, produced only for the task at hand. In informal interviews, comments regarding external representation use were varied. Some developers felt that they were mainly useful for 'helping them think', others used them to communicate with their programming partner while still others used them to communicate outside of their programming pair. A number of experienced pair programmers explained that within a pair the code was adequate to communicate given the intuitive nature of the development environment and the ability to quickly produce a coded demonstration.

4. Conclusion

In line with the conflicting results shown in current studies of XP, initial findings of an observational study of commercial pair programmers indicate that the knowledge, skill and tools required for programming in pairs may be poorly understood and somewhat under-estimated by those who are not experienced in its practice. This suggests that further analysis of the characterising behaviours of expert pair programmers would be instructive with regards to the selection and training needs of novices. It may also assist in considering the validity of providing a remote pair programming environment.

References

Ambu, W and Gianneschi, F (2003), Extreme programming at work, 4th International conference in Extreme Programming and Agile Processes. pp347-350

Benedicenti, L and Paranjape, R (2001). Using extreme programming for knowledge transfer. Proceedings of the 2nd International Conference on eXtreme Programming and Agile Processes in Software Engineering.

Bryant, S (2004). XP: Taking the psychology of programming to the eXtreme. 16th annual workshop of the Psychology of Programming Interest Group, Carlow, Ireland. pp121-132

Cockburn, A and Williams, L (2001). The costs and benefits of pair programming. Extreme Programming Examined. G. Succi and M.Marchesi, Addison Wesley.

Dick, A and Zarnett, B (2002). Paired programming and personality traits. 3rd International conference on eXtreme Programming and Agile Processes in Software Engineering.

Gittins, R., Hope, S et al (2001). Qualitative studies of XP in a medium sized business. 2nd International conference on eXtreme Programming and Flexible Processes in Software Engineering. Villasimius, Sardinia, Italy.

Noll, J. and Atkinson, D (2003). Comparing eXtreme Programming to traditional development for student projects. 4th international conference on eXtreme Programming and agile processes in software engineering. pp.225-233

Tessem, B (2003). Experiences in learning XP practices: A qualitative study. 4th international conference on eXtreme Programming and agile processes in software engineering. pp131-137

Wake, W (2002). Extreme programming explored. NJ, USA, Addison Wesley.

Human Reasoning and the Sunk Cost Effect.

Martin Coleman
Life Sciences (psychology). University of Sussex, Brighton, East Sussex. UK.
mdc20@sussex.ac.uk

The viewpoint that human decision-making and classical rationality are one and the same thing has been under attack since the early nineteenth century (Gigerenzer & Goldstein, 1996). Today the generally accepted view is that, rather than exhibiting perfectly rational decision-making, "people rely on a limited number of heuristic principles which reduce the complex task of assessing probabilities and predicting values to simpler judgmental operations. In general these heuristics are quite useful, but sometimes they lead to severe and systematic errors" (Tversky & Kahneman, 1974, p.1124).

Simon (1956) argued that human minds should, also, be understood within the context of the environment in which they evolved. Simon's theory of bounded rationality states that humans have only a limited cognitive capacity but, that this capacity has evolved to work efficiently within real-world environments. In a test of "bounded rationality" Gigerenzer and Goldstein (1996) compared the performance of "fast and frugal" heuristics to that of "rational" algorithms in making inferences about a real-world environment. The authors concluded that, in order to be successful within real-world situations, decision-making mechanisms did not need to conform to the norms of classical reasoning.

The sunk cost effect is manifested in the greater tendency to continue with an endeavour once a prior investment of time, money or effort has been made (Arkes and Blumer, 1985). The phenomenon has, traditionally, been understood within the framework of heuristics and biases. Sunk cost effects are said to occur due to the over-application of the, generally useful, heuristic "waste not, want not".

In 2002 Kacelnik and Marsh found evidence to suggest that Starlings were subject to sunk cost effects. In conditioning trials birds were found to prefer food rewards associated with high effort to identical food rewards associated with low effort. It seems unlikely that starlings could use "high-level" heuristic such as "waste not, want not" in their decision-making.

To investigate whether sunk cost could also influence human taste preference, 115 participants took part in a between-subject design experiment. The sample consisted of16 males and 99 females (mean age=23.08 years, SD=6.46). The stimulus of a computer-generated treasure hunt was used to vary the amount of effort that individuals had to invest in the finding of chocolate samples. At the end of the treasure hunt participants were found to spend significantly more money on the chocolate associated with the "hard to find" samples than on the chocolate associated with the "easy to find" samples. It was concluded that sunk cost could influence human taste preference.

To investigate whether prior conditioning can moderate the influence of sunk cost, 77 participants took part in a written-scenario based study. The sample consisted of 16 males and 61 females (mean age=23.15years, SD=6.33). Sunk cost was found to exert less influence on participants pre-conditioned to expect failure in investment decisions than on those participants pre-conditioned to expect success or those in a control group. The results suggest that learnt "effort equals reward" associations have a role to play in the manifestation of sunk cost effects.

It appears that the traditional framework of heuristics and biases is inadequate to explain the sunk cost effect. The author believes that "high-level" heuristics and "low-level" conditioning both have a role to play in the phenomenon. Further research is planned to test this hypothesis.

References.

Arkes, H.R. (1991). "Costs and benefits of judgmental errors: Implications for debiasing", Psychological Bulletin, 110, 486-498.

Gigerenzer, G. and Goldstein, D.G. (1996). "Reasoning the fast and frugal way: Models of bounded rationality". Psychological Review, 103, 650-669.

Kacelnik, A. and Marsh, B. (2002). "Cost can increase preference in starlings". Animal Behaviour, 63, 245-250.

Simon, H.A. (1982). "Models of bounded rationality". Cambridge, MA: MIT Press.

Tvesky, A. and Kahneman, D. (1974). "Judgement under uncertainty: Heuristics and biases". Science, 185, 1124-1131.

Next Generation Overlay Networks - Infrastructure for Denial of Service Defence

David Mark Ellis
Network Lab
Department of Informatics
University Of Sussex
davide@sussex.ac.uk

Introduction

We briefly describe a next generation internetwork designed to protect network services from Denial Of Service attacks. Denial Of Service attacks are characterised when one or more attackers starving the resources of a target offering a service (i.e. a web server), therefore not allowing the target to respond to legitimate requests. We are particularly interested in attacks on network bandwidth and where the attackers form a distributed attack base.

Background

Ideas pioneered in MayDay [2] and SOS [5] describe an overlay service, implemented on top of the IP network. An overlay network is a way of constructing a new type of network using an existing infrastructure, such as implementing the IP protocols over the existing telephone network. There are number of advantages in doing this stemming from the fact that you have more control over the nodes.

These networks have ingress points and egress points, points that provide access into and out of the overlay respectively. A client wishing to use the network, must locate an ingress point and authenticate with it. The client may then send data through the network to utilise a resource. When the packet arrives at an egress point, it is sent to the ``real service". It helps prevent Denial Of Service, because ingress nodes are the only parts of the network known to the public. If an ingress node is attacked, clients can use another node. The actual target service is protected because only the egress points are allowed to contact it, this is enforced with a firewall acting as a lightweight authenticator.

While this infrastructure has an inherent preventative property it is not publicly accessible, you must be an authenticated client to use the service. Additionally these services may only support a single target host, making such a system less economically viable.

Infrastructure

By providing a public infrastructure we must allow attackers to use the system. So we must assume that all traffic traversing the system could be attack traffic, and nodes must be given reactive countermeasures to isolate the attack. The system reacts in a similar manner to the pushback algorithms [4][6], where bandwidth constraints are applied to upstream nodes, until the attack begins to stop. Unlike the pushback approach, we do not try to identify an aggregate representing the attack packets. Instead we use a much simpler approach: Each node is responsible for its own traffic, so if it receives a bandwidth restriction message, it will begin to use other outgoing links. Obviously if the node is compromised, it is less likely to respond in the expected way and an issue of reputation and trust arises.

There are a number of economic issues that must be addressed if these kinds of systems are going to be deployed. Namely: who pays for the nodes? We envisage networks of thousands of nodes, supporting possibly hundreds of services.

One way to solve this problem would be for a single organisation to acquire the nodes

and charge other organisations wishing to host their services within the network, much like akamai [1]. This solution assumes that the hosting organisation possesses the capital to set up and maintain such a network, and that there are enough services wishing to be hosted. There may also be issues with "saturation" levels: i.e. what number of services can be successfully maintained in a network of n nodes?

An alternative way to provide the necessary infrastructure is to allow organisations wishing to provide a service to contribute to the network. Organisations could be asked to contribute a small number of nodes to the network, and in return their clients would be able to utilise the thousands of available nodes. To take it one step further, organisations could be offered a usage of the network proportional to their contribution in nodes; or their offering of nodes could subsidise their joining cost. This solution allows the network to scale well, as each new service also brings a number of contributing nodes. A multi-organisation approach however means that mechanisms for managing and controlling nodes is needed.

The multi-organisational approach seems most useful in a real world deployment, so we will investigate it further. In providing this infrastructure, we see two options:

- There is one controller domain, and nodes and their connections are "donated" (like planet lab [7]).
- Each contributor is in control of each of its nodes.

Administration by a single organisation seems to be the easier approach. Many current Denial Of Service prevention schemes in fact note this loss of control over administrative boundaries as a negative property (traceback [3], pushback [6] etc.). In this scenario, each node can be controlled and maintained uniformly. It does mean that the contributing organisation must trust the hosting organisation fully; it also means that the control of the network is ultimately in the hands of the hosting organisation, whereas the latter approach has a more peer to peer like spirit.

In the case that every contributor is control of their own nodes a number of issues arise: Trust, how do we know that a node is going to obey the predefined protocols? We need some metric of trust between nodes, we may decide that nodes are trusted if they belong to the same administrative domain, and other such relations are earned; Software, does every node use the same software? or simply respond to a predefined set of external protocols; Security, in this situation we can't assume that each node is inherently secure, so mechanisms for detecting and isolating a breach across administrative boundaries needs to be well understood. This last point also has a lot to do with trust.

Concluding Remarks

In this paper we have outlined a next generation network for the protection of Distributed Denial Of Service attack. We have described a novel approach based on overlay networks, which provides a solution that is both preventative and reactive to an attack. Several issues have been raised that will form the basis for further investigation, including: the reactive measures; dealing with multiple organisations; trust; and security. Many of these subjects will be investigated further and form the basis for future work in this area.

References

[1] Akamai. http://www.akamai.com.

[2] D ANDERSON. Mayday: Distributed filtering for internet services. http://nms.lcs.mit.edu/papers/mayday-usits2003/paper.html.

[3] Characterizing and tracing packet floods using cisco routers. http://www.cisco.com/warp/public/707/22.html.

[4] John Ioannidis and Steven~M. Bellovin. Implementing pushback: Router-based defense against DdoS attacks. In Proceedings of Network and Distributed System Security Symposium, Catamaran Resort Hotel San Diego, California 6-8 February 2002 1775 Wiehle Ave., Suite 102, Reston, VA 20190, February 2002. The Internet Society.

[5] A. Keromytis, V. Misra, and D. Rubenstein. Sos: Secure overlay services, 2002.

[6] Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxsonm, and Scott Shenker. Controlling high bandwidth aggregates in the network. Technical report, ATT Center for Internet Research at ICSI (ACIRI), 2002.

[7] Planet lab. http://www.planet-lab.org.

The role of learning goals in children's collaborative interactions

Amanda Harris
Ideas Lab, Department of Informatics
a.l.harris@sussex.ac.uk

The use of peer collaboration as a method of learning has become very popular in the UK primary classroom. The National Curriculum has identified 'working with others' as a 'key skill' which incorporates abilities such as being able to engage in group and paired work (National Curriculum Online, 2004). Improvements in children's problem solving skills after collaboration with either an adult or peer have been widely documented (Roschell & Teasley, 1995, Howe et al 1995, Underwood & Underwood, 1999, Azmitia, 1988). However, while some children engage very effectively in group work others consistently fail to work together productively. The individual differences children bring to the collaborative group therefore play an important role in the effectiveness of the learning experience. Among those identified as being influential are gender, ability and peer relationships. However, individual differences in motivation have not been addressed. This is an important area of investigation as children's beliefs about learning and their attitudes to the tasks they are expected to undertake will impact on the goals they adopt and therefore on the behaviour they display (Dweck and Elliot, 1988).

Cognitive theories of motivation identify a goal as providing an insight into the purpose behind behaviour, and as such is a complex cognitive structure constructed within the person-environment interaction (Lemos, 1996). Learning goals are those that provide a cognitive focus, or purpose to behaviour, in situations where competence is of specific relevance. Traditionally, goal theory has emphasised two types of learning goals each associated with distinct behavioural patterns evident in achievement situations. Mastery goals are those that focus on the development of competence through task mastery whereas performance goals focus on the demonstration of competence in relation to others (Dweck and Elliot, 1988). More recently this distinction has been revised and has incorporated approach and avoidance elements to the mastery – performance dichotomy (Elliot and McGregor, 2001). The types of behaviours associated with different learning goals impact on the way in which individuals engage in different tasks and influence learning outcomes; approach goals often being associated with more adaptive patterns of learning (Dweck and Elliot, 1988). Learning goals have been examined in a variety of classroom settings. However, no studies have explored goal related behaviour within a collaborative context. My research seeks to examine the impact of different learning goals on children's engagement in peer collaboration.

The aim of initial studies was to assess the nature of each child's participation in a collaborative task and relate this to their learning goal orientation. Pairs of children were videotaped interacting with a piece of educational software which required them to work together. Collaboration was measured by analysing the language used by individual children with the use of a coding scheme devised for the study. This consisted of 18 codes each falling within one of four broad categories; metacognitive comments, positive regulatory comments, negative regulatory comments and off task comments. Learning goal orientation was measured by a teacher rated questionnaire adapted from the Patterns of Adaptive Learning Scale (Midgley, 2002).

Initial results indicate that learning goal orientation was significantly related to particular types of language falling within the positive regulatory comments category. For example, the more mastery orientated a child the more they engaged in disagreements with their partner whereas the more performance orientated a child the less they involved themselves in this type of interaction. The socio-constructivist

approach to learning argues that in order for development to occur within the course of social interaction, children need to be able to resolve initially different perspectives in order to reach a new and joint understanding of the task at hand. The results of this study indicate that the performance motivated child may find this aspect of collaboration more difficult as they are less likely to vocalise disagreements than are their mastery orientated peers.

Future research will continue to explore the demands of a collaborative task in relation to motivational patterns and learning styles and examine the impact these have on learning outcomes within a collaborative context. While increasing our understanding of the processes involved in peer collaboration, the research will also have implications for the way in which we scaffold and support such interactions.

References:

Azmitia, M. (1988) Peer Interaction and Problem Solving: When are Two Heads Better Than One? Child Development, Vol 59, p87-96.

Dweck, C. S,. & Elliot, E (1988). Goals: An approach to motivation and achievement. Journal of Personality and Social Psychology. Vol 54, p5-12

Elliot, A. J. & McGregor, H. A. (2001) A 2 x 2 Achievement Goal Framework. Journal of Personality and Social Psychology. Vol 80 (3), p501-519.

Howe, C., Tolmie, A. & MacKenzie, M.(1995) Computer support for the collaborative learning of physics concepts. In Computer Supported Collaborative Learning, O'Malley C. (ed) Springer-Verlag, Berlin.

Lemos, M. S. (1996) Student's and teacher's Goals in the Classroom. Learning and Instruction, Vol 6 (2), p151-171.

Midgley, C (2002) (ed) Goals, Goal Structures and Patterns of Adaptive Learning. Lawrence Erlbaum Associates, USA

National Curriculum Online (2004) http://www.nc.uk.net (Accessed on 7/2/2004)

Roschell, J. & Teasley, S. D. (1995)The Construction of Shared Knowledge in Collaborative Problem Solving. In Computer Supported Collaborative Learning, O'Malley C. (ed) Springer-Verlag, Berlin.

Underwood, J & Underwood, G (1999) Task Effects on Co-operative and Collaborative Learning with Computers. In Learning with Computers. Littleton, K & Light, P. (eds) Routledge, London

Building User Mental Models of Pervasive Computing Environments Using External Representations

Thom Heslop

Department of Informatics

University of Sussex

T.T.Heslop@sussex.ac.uk

1. Introduction

With the advent of computer technologies embedded in a variety of devices and the convergence of wireless technologies with the Internet has come the possibility of a *pervasive* computing environment. This environment will provide a wide variety of services within these networks, theoretically allowing the user to tailor their computing environment according to their needs. However this concept of the environment as a computing device presents many challenges to non-technical users, not least in the ability to control and configure it to their wishes. Many services available to users are invisible and so it can be difficult to conceptualise their operation singularly or in conjunction with other services. There is also the challenge of user input for the composition of services: Kim and Gil [1] point to the need for the system to provide guidance to programmers in order to tackle problems of incomplete, inconsistent or ambiguous input in service composition. If we are to allow a non-technical user with little or no programming experience to express their wishes in a natural and intuitive way (natural language input, for example, rather than a programming language) how can the problem of ambiguity in the systems interpretation of the user's input be addressed?

In my research I propose to investigate the following areas: can an external representation of such a system help users to interpret and internalise its behaviour, thus forming a 'correct' mental model of the system and how to use it? How can the user tell that their wishes have been correctly interpreted by the system before they are put into operation? How can the user see how their commands (or *policy*) will affect the state of the system, especially already existing policies?

Piaget, among others, has discussed the importance of experimentation in learning - the user "must displace, connect, combine, take apart and reassemble" [2] in order to learn and understand an object or system. How can we allow users to explore and experiment with the system in a tangible and safe way, helping them to build up a coherent and 'correct' mental model? And finally, at what level of functionality can an external representation actually hinder the creation of useful mental models?

2. Conceptual and Mental Models

As shown in the work of Norman [3] and others [4] the provision of a clear conceptual model of a device / system by its design is imperative for users to understand its function and learn how to make use of it correctly. If there is no clear conceptual model provided by the design then the user is likely to develop their own mental model that, more often than not, tends to be inaccurate. This inevitably leads to fundamental misunderstandings about the uses and operation of the device / system in question. As it is recognised that providing good conceptual models for single-use devices can be problematic so the development of a coherent mental model for a collection of interacting devices offering a wide variety of combinations can be seen as an even more complex and difficult issue. However, the principle of *visibility* could be of help in addressing this problem.

Norman points to the importance of visibility (the visible structure of the system or how the device explains itself) both in gaining an understanding of device / system functions and in the mapping of user actions to the results of that action (showing how the "state of the world" changes). An external or graphical representation of a complex system such as a pervasive computing environment may be a way of providing the visibility

needed for a non-technical user to make sense of it.

3. Proposed System

I am currently working with the NatHab project, which is engaged in exploring systems for service composition using natural language descriptions of *policies* [5]. I propose to develop a parallel system using an interactive graphical representation of the domain environment, dynamically generated from the same ontological source as the aforementioned NL system. This virtual environment will feature graphical representations of all services available to the user at any given time allowing for graphical expressions of semantic expressions – that is the user will be able to see an animated visualization of their policy originally expressed in natural language and how it will affect the system (such as already existing policies). It is intended that this external representation will use the same underlying policy representation language. This system will be used to evaluate how an external representation of the pervasive environment helps the user to create mental models for its use.

It may also be possible to extend the graphical expression so that the user would be able to directly interact with it in order to amend or create policies – in effect a simple Visual Programming Language [6] for the composition of services. Although this is not currently the main focus of the research discussed here, it could provide an interesting additional avenue, time permitting.

4. Research Plan.

In order to develop the system outlined above the following I am currently investigating the following issues as part of a literature review:

a) *The dynamic generation of graphical representations from semantic representations of objects*.

b) *Visual grammars for the representation of the behaviour of graphically represented objects.*

c) *Ontological frameworks that can support this approach.*

d) *How actions and conditions can be graphically represented.*

e) *How a simulation of policies can be constructed from a combination of animations representing the behaviour of each object involved.*

I currently envisage that my research will follow the following stages:

Stage A – Literature review: as well as the issues outlined above I am investigating external representation and the construction of mental models. Other dynamic visualization systems are also being evaluated, such as the ProtoViz system [7] as well as already existing graphical simulations for service composition, such as the "Haystack" information management program [8].

Stage B – Development and implementation of system, based on the findings of the previous stage.

Stage C – Usability trials with users. When the system is operational, it is envisioned that a number of experiments will be carried out in order to investigate the development of mental models around pervasive computing systems as discussed previously.

References

[1] Kim, J., & Gil, Y., "Towards Interactive Composition of Semantic Web Services",

[2] Piaget, J., 1970, "Piaget's Theory" in Mussen, P.H(Ed), *Carmichael's Handbook of Child Psychology,* pp 703 –32 New York: Wiley

[3] Norman, Donald. A. 1988, *The Design Of Everyday Things,* New York: Basic Books

[4] Preece, J., Rogers, Y., Sharp, H. 2002, *Interaction Design,* New Jersey: Wiley & Sons

[5] Weeds, J., Keller, B., Weir, D., Wakeman, I., Rimmer, J., Owen, T., 2004, "Natural Language Expression of User Policies in Pervasive Computing Environments" http://www.cogs.susx.ac.uk/users/juliewe/ontolex04.pdf

[6] Chang, S., 1990, "Principles Of Visual Languages" in Chang, S (ed), *Principles Of Visual Programming Systems,* New Jersey: Prentice Hall

[7] Elvquist, N., 2003, "ProtoViz: A Simple Protocol Security Visualization", http://www.cs.chalmers.se/~elm/courses/security/report.pdf

[8] Huynh, D.F., Quan, D., Karger, D.R., "User Interaction Experience for Semantic Web Information" haystack.lcs.mit.edu/papers/www2003-ui.pdf

Distributed Java Just-in-Time compiler for embedded system

Li Jian
Department of Informatics
University of Sussex
jl58@sussex.ac.uk

Introduction

One of the important features of the Java programming language is its platform independence. A Java program can be executed on any platforms that support Java. However, this characteristic introduces a trade-off in the execution performance, which is especially highlighted in a resource-constrained environment. This paper introduces an alternative way that a Just-In-Time (JIT) compiler can improve the Java execution performance in such an environment.

Approaches of Java byte code execution

Java programs are normally either interpreted or compiled. The prevailing way to execute a Java programme is for it to be interpreted in a resource-constrained environment, since it has a small memory footprint and is easy to implement. However, measurements reveal that, on average, the interpreted virtual machine performance is approximately 10 times slower than compiled native code [1]. This speed differential between interpreted versus compiled code increases when the Java Virtual Machine (JVM) tries to interpret the Java byte code on the fly with limited amount of memory.

A Just-in-Time compiler [2][3][4] is a kind of dynamic compiled virtual machine, which translates the Java byte code on the fly when the procedures satisfy the compilation condition, such as being invoked frequently enough. However, little or no extra memory is available for dynamic code generation is still one of the important issues for this technique. Furthermore, the resource-constrained environments are generally slower than conventional computers and workstations. Therefore, it is not an appropriate way to apply this technique directly in a resource-constrained environment.

Although ahead-of-time compilation [5] achieves the best performance amongst these three approaches, Java programmes also have to suffer from a long start-up time penalty. Here the entire programme is compiled at once, and as a result of this, some advanced optimisation strategies can be applied to the programme. However, this analysis and optimisation also slows the compilation speed and introduces a trade off, in order to improve the final execution performance.

Distributed JIT compiler for resource-constrained environment

In order to improve the performance of the Java Virtual Machine beyond the pure interpreter performance, some kind of static and/or dynamic compilation is required. The following figure shows an outline of the architecture of the distributed JIT. The interpreter module is responsible for executing the Java byte code initially, and the Compiler stub module is responsible for translating the Java byte code into native code via the remote JIT compiler executing on a remote powerful machine. After translation is completed, the stub is also responsible for registering the code to the scheduler to prepare it to be executed next time.

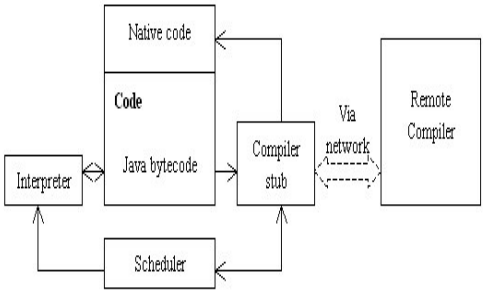


Figure 1: The Architecture of Distributed JIT

In a distributed JIT, two improvements aimed at resource-constrained environment are made. One is on the JIT compiler itself and secondly through compiler procedure improvements. The JIT compiler is separated into two parts, the compilation service worked on the servers and the compiler stub co-operate with the JVM as a client of the former. Thus it will try to request the server to translate a methods matched translation condition into an efficient native version. This should be done automatically and the target machine can execute the Java program as normal even if the connection of target machines is broken. Secondly the compiler procedure can be improved. Usually, traditional JIT compilers work in "user time" whereby it is usually the case that the program is paused and waits for the JIT compilation. The native version of the procedure is immediately executed until the compilation finishes. he execution engine, the interpreter, does not know the native version and continues to execute the interpreted version of code until the native version is successfully registered to the schedule by the compiler stub. Therefore, the benefit of the asynchronous compilation approach avoids the execution pause even when the compilation and transmission take a long time.

Conclusion

This paper introduces an alternative approach to the JIT compiler in a resource-constrained environment. The distributed JIT separates the compilation block and execution engine via a network. This approach takes the advantages of the JIT, compiling the bytecode on-the-fly, and avoids the large memory overhead of traditional JIT's.

References

[1] The CLDC HotSpot Implementation Virtual Machine, Sun Microsystems

[2] M. P. Plezbert, R. K. Cytron. Does "Just in Time" = "Better Late than Never"? *ACM 1997, Principles of Programming Languages*.

[3] M. Chen, K. Olukotun. Targeting Dynamic Compilation for Embedded Environments. *OOPSLA'03*, 26-30 October 2003

[4] IBM's WebSphere Micro Environment: http://www.ibm.com/software/wireless/wme/

[5] gcj, The GNU Compiler for the Java Programming Language, www.gcc.gnu.org/java/

Enactive Causation

Paul Loader
Department of Informatics
University of Sussex
P.Loader@sussex.ac.uk

"I call *cause* that which I push away" (L. Wittgenstein)

Three Presuppositions

Much philosophical writing on 'causation' seems to make one or more of the following assumptions:

(1) The possession of causal concepts predates the use of causal language and is derived from the detached observation of causal phenomena.

(2) Scepticism about causation, if not justified, is at least meaningful.

(3) The conditions under which it is legitimate to assert that 'A caused B' can be rigidly specified.

However, an approach suggested by Wittgenstein (1937/8) seems, at least on one interpretation, to undermine these assumptions.

Wittgenstein's Account

Wittgenstein argues that our causal concepts evolve out of primitive 'causal behaviour' (for want of a better term).

We are to imagine a pre linguistic scenario in which certain types of unreflective behaviour occur. One such behaviour might retrospectively be labelled "*reacting to the cause*". An example would be that of someone responding to a physical threat by adopting a defensive stance. Another (slightly more sophisticated) behaviour might be called "*tracing the cause*". An example of this would be following a piece of string, to see who or what was pulling it at the other end.

Onto these primitive behaviours are later grafted certain ways of speaking which form the beginnings of causal language – for example I might assert "*He's to blame*" or "*She broke it!*". Such utterances can be viewed as quantitative extensions of behaviour rather than as a qualitative leap in the direction of pure conceptualisation. (In the same way it might be said that the statement "My tooth hurts" functions initially as a replacement for crying and pointing rather than as a description of an inner state.) Malcolm (1986), taking up Wittgenstein's position, argues in this respect that primitive causal statements are as much akin to "*expressive behaviour*" as to verifiable statements of fact.

Implications of Wittgenstein's Account

Contrary to (1), then, this description makes no reference to the need for prior conceptualising about causation.

It can also be asserted that there is no place for 'doubt' in this scheme of things. Here a remark of Wittgenstein's seems particularly significant –

"*The basic form of the language game is certainty not uncertainty. For uncertainty could never lead to action*" (p.420)

What is being suggested, we might say, is an 'enactive' account of our primitive causal utterances. Causal language develops not from the detached observation of regularities but out of our actions and reactions in a social setting; it is intimately bound up with our immediate practical concerns. Doubt has no role to play in such a scenario, both because 'the game' would never be able to establish itself on the basis of doubt and because it is not even clear what doubt could *mean* in such circumstances.

This latter point brings us to the question of whether the reality of causation can ever be meaningfully disputed. The answer, contrary

to (2), seems to be 'no'. The enactive scenario is the foundation and pre requisite of our more sophisticated causal theorising – it's a description of what causation ultimately *is*. On such an analysis it makes little sense to talk of doubting the legitimacy of causal statements – one can no more be sceptical about causation than one can about running or eating dinner.

Finally, contrary to (3), on this account attempts to add rigour to our causal concepts by determining the precise implications of "*A caused B*" are misconceived. The circumstances in which causal language developed – unlike, for example, the circumstances in which programming languages develop – are not such as to yield the right sort of precision.

Questions

1) Aside from serving as a foil to philosophical scepticism about causation, can this approach offer anything of value to contemporary cognitive scientists? Is it answering any questions they're interested in?
2) Does part of the argument rely on the blurring of the distinction between 'particular doubts' and 'general scepticism'?
3) Even if statements of fact can be reduced to "expressive behaviour", don't we still have the problem of distinguishing true ones from false ones, and thus of working out what makes some causal statements true and others not?
4) How might this 'enactive' approach relate to other 'enactive' approaches, such as the enactive approach to perception (O'Regan & Noe, 2001) ?

References

Malcolm, N. (1986). *Nothing is Hidden*. Basil Blackwell.

O'Regan, J.Kevin and Noe, Alva (2001*) A sensorimotor account of vision and visual consciousness*. BEHAVIOURAL AND BRAIN SCIENCES (2001) 24 (5).

Wittgenstein, L. (1937/8) *Cause and Effect: Intuitive Awareness* in PHILOSOPHIA Vol.6 Nos 3-4 1976.

IEEE 802.11e QoS Enhancement for Wireless LAN

Xingdong Ma
Department of Engineering and Design
University of Sussex
xm20@sussex.ac.uk

Introduction

During the past few years, there has been an explosion in Wireless LANs (WLANs) development conforming to the IEEE 802.11 standard. They are expected to support the network applications with the same QoS level and the wired Ethernet. IEEE 802.11 group is developing Medium Access Control (MAC) protocols to enable a better mobile user experience and to make more efficient use of the wireless channel.

Original 802.11 MAC

The main purpose of the 802.11 MAC protocol is to provide reliable data service to the user of the MAC, i.e., higher layer protocols, and to control fair access to the shared wireless medium. 802.11 standard specifies two channel access functions [1]: *DCF* (Distributed Coordination Function) and *PCF* (Point Coordination Function). [2]

Distributed Coordination Function

DCF is based on *CSMA/CA* (Carrier Sense Multiple Access with Collision Avoidance). Stations deliver MSDUs (MAC Service Data Units) of arbitrary lengths (up to *2304 bytes*), after detecting that there are no other transmissions in progress on the wireless medium. In CSMA/CA, once a station detects that the medium is free, it begins to decrement its back-off counter. Each station maintains a *CW* (Contention Window) that is used to determine the number of slot times a station has to wait before transmission. The back-off counter only begins to decrease after the medium has been free of a *DIFS* (DCF Interframe Space) period. If the backoff counter expires and the medium is still free, the station begins to transmit. In case of a collision, the station randomly picks a new back-off period from its CW, and attempts to gain control of the medium again. Due to collisions and the binary back-off mechanism, there are no transmit guarantees with DCF.

Point Coordination Function

To support time-bounded services, the IEEE 802.11 standard defines the PCF to let stations have priority access to the wireless medium, coordinated by a *PC* (Point Coordinator). The PCF has higher priority than the DCF, because it may start transmissions after a shorter duration than DIFS, this time space is called *PIFS* (PCF Interframe Space). Time is always divided into repeated periods, called superframes. With PCF, a *CFP* (Contention Free Period) and a *CP* (Contention Period) alternate over time, in which a CFP and the following CF form a superframe. During the CFP, the PCF is used for accessing the medium, while the DCF is used during CP. It is mandatory that a superframe includes a CP of a minimum length that allows at least on MSDU Delivery under DCF. A superframe starts with a *beacon frame* regardless if PCF is active or not. The beacon frame is a management frame that maintains the synchronization of the local timer in the stations and delivers protocol related parameters. The PC, typically collocated with the AP, generates beacon frames at regular beacon frame interval, thus every station knows when the next beacon frame will arrive. Upon being polled, along with data, the polled station acknowledges the successful reception. If the PC does not receive the response from a polled station after waiting for PIFS, it polls the next station, or ends the CFP.

802.11e MAC Enhancements

The current MAC has no means of differentiating traffic streams or source. All data is treated equally in both DCF and PCF [3]. As a result, no consideration can be made for the service requirements of the traffic on the channel. For example, low priority burst traffic may choke out a long-running critical video feed, thereby destroying the user's experience.

The tow new MAC modes, EDCH and HCF, being defined under 802.11e, supports up to *eight* priority *TC* (Traffic Class) that map directly to the protocol priority levels.

Enhanced Distributed Coordination Function (EDCF)

EDCF is DCF with some of the elements of the MAC parameterized per-TC. Each TC starts a backoff after detecting the channel being idle for an AIFS (Arbitration Interframe Space). The AIFS is at least as large as the DIFS and can be chosen individually for each TC. It provides a deterministic priority mechanism between the TCs.

Within a station, the eight TCs have independent transmission queues. These behave as virtual stations with the above mentions parameters determining their ability to transmit. The *TXOP* (Transmit Opportunity) is given to the TC with the highest priority of the colliding TCs. These QoS parameters can be adapted by the AP via the beacon frames.

Enhanced Coordination Function (HCF)

HCF is an extension of the polling idea in PCF. Under HCF, as in PCF, the superframe is divided into the CFP that starts with every beacon, and the CP. During the CP, access is governed by EDCF, however, the HC (Hybrid Coordinator, generally collocated at the AP) can initiate HCP access at any time. During the CFP, the HC issues a QoS CF-Poll to a particular station to give it a TXOP, specifying the start time and maximum duration.

If a station is given a CF-Poll, it is expected to start responding with data within a SIFS (Short Interframe Space). If it does not, the HC can take over the medium after a PIFS and allocate another CF-Poll to another station. This allows very efficient use of the medium during the CFP.

Scheduling

The HC has available over time a snapshot view of the per-TC per-Station Queue length information in the cell, including the AP. This information is sent to the HC by the station via the new QoS control field added to the MAC frame definition.

The minimum consideration includes:

1. Priority of the TC;
2. Required Qos for the TC (low jitter, low latency, etc);
3. Queue lengths per TC;
4. Queue lengths per station;
5. Duration of TXOP available and to be allocated;
6. Past QoS seen by the TC;
7. Proposed Research

The enhancement and evaluation of IEEE 802.11e performance will be implemented on Berkeley NS2 [4]. Real time wireless network emulation will be developed for the research. In NS2 emulation, the real network situation can be simulated while passing the real network packet through the simulated environment. The target of this research is to develop wireless video streaming strategies to adapt to changing wireless medium characters.

References

[1] D, Gu, *et. al.* , "QoS Enhancement in IEEE802.11 Wireless Local Area Networks", IEEE Communications Magazine, June 2003

[2] S. Mangold, *et. al.*, "IEEE 802.11e Wireless LAN for Quality of Service", Proc. European Wireless 2002, February 2002, Florence Italy, http://www.ing.unipi.it/ew2002/

[3] Silicon & Software Systems, "Addressing QoS - IEEE 802.11e" http://www.s3group.com/wireless_systems/wlan_qos/

[4] NS2. http://www.isi.edu/nsnam/ns/

Bootstrapping a better parser

Mark McLauchlan
Department of Informatics
University of Sussex
mrm21@sussex.ac.uk

Introduction

Imagine an interface to Amazon or some other online store that allowed you to tell the computer what you wanted to buy. For example you might say the following --- bearing in mind that this is the future, so we already have flying cars:

I'll buy the car with green jets

The computer transforms the sound waves into a set of words and analyses this sentence to determine what you want. Firstly, it needs to do a syntactic analysis, also called parsing. It must identify that *I* is the subject, *buy* is the main verb and *with green jets* modifies the object *car*. From this the computer works out that *buy* means it's a message for the sales department, and the thing being bought is a car with the optional green jets. Note that it's extremely important to get the syntactic bit right. There is a second possible interpretation where the prepositional phrase *with green jets* modifies the verb, implying that you want to purchase a flying car using green jets as currency. This rather contrived example is intended to show how understanding syntax is a first step towards understanding language, which is the ultimate goal of natural language processing. My research is focused on how we can improve the quality of syntactic interpretation without too much effort.

The scarce data problem

As this example illustrates, the key stumbling block is *ambiguity*. Words can have multiple meanings: *jets* can be verb, for instance. A grammar of English can allow different syntactic interpretations of a sentence, as shown above. With a comprehensive grammar the number of alternative interpretations might run into the thousands or even hundreds of thousands.

How can the computer determine which one is correct? The dominant strand of research in this field assumes that the right parse is the most frequent one. Say the computer has access to a large corpus of purchasing requests that have already been syntactically analysed by humans. We'll call this the *training corpus*. The computer compares this new sentence to similar sentences in the training corpus, and chooses the analysis that best fits the analyses assigned to those sentences. For example, if in the training corpus the phrase *green jets* appears with *car* three times and with *buy* just once, then the computer would (correctly) choose the first analysis for the sentence above.

Unfortunately there are a lot of words in the English language, and most of them appear quite infrequently. Even in an enormous training corpus, most words will only appear once if at all. If we haven't seen a word before, then the computer faces a hard road in deciding between interpretations. Worse, enormous training corpora are very hard to come by since every sentence has to be hand-analysed by human annotators --- a dauntingly boring task.

One way around this is to ignore words altogether and just look at their *category*: verb, noun, adjective and so on. Carroll (1993) has developed such a non-lexicalised parser and the results are surprisingly good. A fair number of potential ambiguities can be resolved just by looking at how nouns and verbs behave *in general* rather than considering the actual words themselves. Unfortunately there are still some stubborn kinds of ambiguity, such as prepositional phrases, that really need lexical information to resolve.

Bootstrapping as a solution

In my research I have built a new parser that does consider words as well as word categories. The problem of training data is solved by a neat trick: I use the output of Carroll's parser to train the new one. This bootstrapping approach allows me to create as much training data as we want, but of course the data isn't as accurate as one might like. With care, we can still improve on the old parser. This new model simply does parse *selection*: it takes the top five candidate parses produced by Carroll's parser and attempts to rerank them so that the best parse is ranked first more often.

There have been a variety of bootstrapping techniques published in the literature. Most involve iteratively reparsing the training corpus, which can be quite time-consuming. I have developed a one-step process that still produces good results. The table below shows the accuracy of my model measured using Carroll's (2001) evaluation measure. The oracle score shows how well we would do if we could magically choose the best analysis from the available candidates. This is the practical upper bound for this task, since the correct parse isn't always in the top five candidates.

Base Parse	Reranking Model	Oracle
76.7	77.7	82.0

The key idea in my technique is to break down a parse and only use the unambiguous pieces for training. For example, the sentence above has a subject-verb relation (I'll buy), the verb-object (buy a car) and a modifier (with green jets). The two analyses differ in how they treat the modifier, but they agree on the rest. Therefore I can ignore the former but keep the latter for training. The assumption is that these unambiguous fragments cover enough of the language to be useful.

This approach opens up several avenues for research that are closed to people working with traditional human-annotated corpora. Firstly we can examine how the parsing performance improves with very large amounts of training data. Secondly, we can train and test the parser on different kinds of language. A parser trained on scientific journals will learn different probabilities to one trained on prose and poetry, for example. A third research area involves combining different parsers trained on this data to produce a single, more accurate parser.

Bibliography

[Carroll, 1993] Carroll, J. (1993). Practical unification-based parsing of natural language. Technical Report 314, University of Cambridge.

Enactive Distributed Associationism: Psychological ALife

Anthony Morse
Department of Informatics (COGS)
University of Sussex
anthonfm@sussex.ac.uk

Introduction

Despite the popularity of associationist theories in psychology and cognitive modelling, and evidence of associative learning in neuroscience, there remains a disparity between the two levels of theorising. This disparity results from the nature of the representational entities involved. In psychological terms, theories and models of memory utilising a spread of activity between symbolic entities can account for a great deal of experimental data (memory, priming, schema, etc.). Furthermore, these theories underpin the majority of cognitive models. Such models however are typically symbolic - localist and do not easily map to the circuitry of real brains.

My research offers an account of how associationist learning between neurones can give rise to psychologically isomorphic behaviour without necessitating representational neurones. This theory, being grounded in data from psychology and neuroscience, is then implemented as an autonomous learning robot and subject to psychological investigation.

Associative Theories in Psychology

Associationism in one form or another underlies psychological descriptions of human memory. Memory, it seems is not only overtly associationist (i.e. we recall facts 'associated' with an event or object), but also covertly associationist (in that behaviour can be shown to be modified in predictable ways without conscious awareness) (Young et al 1999). The phenomena of priming, and schemata in psychology are the dispositions towards selection of facts or behaviour due to stimulation of associated representational entities. In cognitive modelling, almost all models contain at their heart a carefully structured network of such 'representational entities' (usually symbolic).

Associative Theories in Neuroscience

Evidence of associative learning (Hebb, D. 1949) shows that a neurone taking part in causing other neurones to 'fire' gains stronger connections to those neurones and is hence more able to cause them to fire in the future. If these neurones were 'representational', this would account for a great deal of psychological data, however the brain does not necessarily use symbolic neurones and associations between distributed representations do not necessarily give rise to the psychological phenomena.

Autonomous Learning

The theory developed in my research results in a model demonstrating that the mediation of associations by context is sufficient to guarantee specific psychological phenomena between any combination of linearly and physically separable representational entities (distributed or otherwise). This unsupervised learning model is then combined with models of cortical microcircuits, which are shown to greatly enhance its computational power. The model is currently being tested on a robotic platform whereby it learns from its own experience displaying the psychological phenomena previously only demonstrated symbolically.

The models, which display associative learning, are generated based on experience and are thus suitable for use in predicting how different experiences can lead to different behaviours and choices in the future. In a simple example, having bumped into several objects (indicated by bumpers and seen as bad) the robot learns to avoid

bumping into things. By associating its actions with their probable outcomes in various different contexts, the robot implicitly avoids future collisions. And by learning sensory motor contingencies the model is able to deal with any form of sensor or coding without requiring specialisation beyond experience. All of this however requires the potential separation of the appropriate representational forms. This is achieved by viewing the representational entities as transient and separable states constantly in flux. For the times in which they exist, predictable relations will result between them as a result of associationist learning.

Liquid Computation

Recent theories in Liquid Computation and Liquid State Machines (LSM) (Maass et al. 2002) suggest that a key role of cortical columns in the brain is to amplify the differences in, and the dimensionality of, sensory data. The idea is that like the ripples on a pond, 'information' about the disturbances that caused them is preserved. The increase in dimensionality following liquid dynamics results in complex non-linear data becoming linearly separable. This high dimensional liquid state turns out to have exactly the properties required to support the complex representations necessary for psychological investigation.

Cognitive Modelling

The recently developed AutoIAC model (Morse 2003) achieves performance equal to hand designed IAC structures in an ongoing unsupervised learning architecture. This hybrid algorithm combines associative learning with pattern recognition (a specific form of associative learning) such that associations are learnt in, and thus mediated by, specific contexts. The acquisition of context dependent associations generates structures with the same functional performance as previously only achieved by designed models. The models display isomorphic behaviours in the following psychological domains: Associative Memory, Overt & Covert Recognition, Visual Prosopagnosia, Semantic & Repetition Priming, Schema production, Phobia development.

Alife and Robotics:

Following the introduction of a Liquid State Machine transforming the input, the model was implemented on a robotic platform maintaining all of the functionality on which psychological accounts have been based. The robot is seen as enactive as it generates its own world of representational associations. Future research will be directed at establishing the theory and model as a model of psychological learning (ontogenetic development) where it is anticipated that manipulating environments and situations should result in a more diverse range of psychological phenomena being displayed.

Bibliography

Hebb, D., (1949) The Organization of Behaviour. Wiley, New York.

Morse, A.F., (2003) Autonomous Generation of Burton's IAC Cognitive Models. In R. Young (Ed.)(2003) The Proceedings of the European Conference of Cognitive Science

W. Maass, T. Natschläger, and H. Markram., (2002) Computational models for generic cortical microcircuits. In J. Feng (Ed.)(2002) Computational Neuroscience: A Comprehensive Approach. CRC-Press.

Young, A. W., & Burton, A. M. (1999) Simulating face recognition: Implications for modeling cognition. Cognitive Neuropsychology, 16(1), 1-48

Security Issues in Mobile Ad-Hoc Networks: A Survey

Obowoware O Obi
Department of Engineering and Design
University of Sussex
o.o.obi@sussex.ac.uk

Abstract—**In this paper, we present a survey of the security requirements and vulnerabilities in mobile ad-hoc networks. We highlight the challenges involved in safe guarding these networks. We also discuss the latest trend in providing security for ad-hoc networks. Specifically, with regards to providing security, we examine the area of key management for mobile ad-hoc networks.**

I. INTRODUCTION

Mobile ad-hoc networks (MANET) symbolises a system of wireless mobile devices (usually referred to as nodes) that can freely and dynamically self-organise1 into arbitrary and temporary network topologies, allowing people and devices to seamlessly inter-work in areas without any preexisting communication infrastructure [1]. The nodes communicate among one another using wireless radio and operate by following a peer-peer network model. It enables a wide range of powerful applications, from instant conferencing between notebook PC users to emergency and military service that must perform in the harshest conditions.

The unreliability of the wireless links between nodes, constantly changing topology owing to the enrolment and deenrolment of nodes on the network and the lack of incorporation of security features in statically configured wireless routing protocol not meant for the ad-hoc environment all lead to increase vulnerability and exposure to attacks.

Providing security support for mobile ad-hoc networks is particularly more difficult notable because:

- Wireless networks are susceptible to attacks ranging from passive eavesdropping to active interfering; occasional break-ins by adversary may be inevitable in a large time window.
- The limited physical protection for each of the nodes.
- A scalable solution is needed for a large-scale mobile network.
- Mobile users demand anytime and anywhere services.
- The absence of a certification authority.
- The lack of a centralised monitoring or management point.

This, in effect, underscores the need for intrusion detection, prevention, and other related countermeasures. If mobile adhoc networks are to go beyond their current limited use in military systems or where there is complete ownership by one party, then, there is the need to address the above issues.

In terms of the organisation of this work, we present in section 2, the security requirement for ad-hoc network. In section 3, we discuss the security treats and vulnerabilities on ad-hoc networks. In section 4, we give a review of work that has been done in the area of key management in adhoc networks and in section 5, we highlight the direction our research will follow.

II. SECURITY REQUIREMENTS

The basic security requirements of an ad-hoc network is similar to that of a distributed system. The overall problem encompasses the security of the network environment and the security of each individual network node. The security of each individual node is integral due to the nature of ad-hoc networks, which does not allow us to assume that networked devices will always be under the continuous control of authorised users. As a result, the physical security of the node becomes an important issue, leading to the requirement of temper-resistant nodes [2], if comprehensive security is to be provided. In this work we will focus on the network security related issues.

The goal of system security is to have controlled access to resources [3]. Its essential components are; confidentiality, integrity, availability, authentication, and non-repudiation.

Confidentiality provides that only authorized users, entities or processes may access and use system resources and disclose/send or be disclosed to/receive results of system processing, as and at the times authorized. This means that in an ad hoc network this property ensures that data between nodes is not accessible from unauthorised entities and that intermediate and non-trusted nodes do not understand the content of a packet being transmitted. If authentication is taken care of properly, then confidentiality is trivial.

Integrity is the property that assures that system inputs are accurate, complete and carry the right authorization, and system processing is complete and accurate, that is accuracy and completeness are preserved or system resources, processes, and products are modification and tamper-free. Hence, in a network, integrity assures that messages and

packets are not modified in-transit, and that what is received is what was originally sent.

Availability is the attribute of resources, processes, and result of processing of a system being adequate, accessible and usable timely and as prescribed, but not short or in excess of what is required. This is an important survivability engendering property. Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [4].

Authentication is proving that a user or entity is who he/it claims to be. Authentication enables a node to verify the identity of a communicating party or the source of information. This prevents an adversary masquerading a node, thus ensuring the security of sensitive information and the operations of other nodes.

Authorization is determining whether or not a particular user or entity has the right to carry out an activity. Authorisation establishes rules that define what each network node is or is not allowed to do. In many cases it is required to determine which resource or information across the network a node can access.

Non-repudiation is the inability of a user or entity to deny that he/it performed an activity. Non-repudiation ensures that nodes cannot deny sending out and receiving data. This is useful when detecting and isolating compromised nodes. Any node that receives an erroneous information can accuse the sender with proof and, thus, convince other nodes about the compromised node.

Other security needs of ad-hoc networks are, *ordering, timeliness, isolation, lightweight computations, location privacy,yself-stabilisation, byzantine robustness, anonymity, keymanagement, access control, and trust.* For a detailed reading of these, see [5].

III. VULNERABILITIES AND THREATS

Ad-Hoc networks are susceptible to a wide range of attacks by virtue of their wireless nature. Active and passive attacks can be carried out with relative ease. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and nonrepudiation. The wireless link between nodes are highly vulnerable to link attacks, which include: passive eavesdropping, active interfering, leakage of secret information, data tampering, impersonation, message replay, message distortion and denial of service. Eavesdropping might give an adversary access to secret information, violating confidentiality.

The lack of a centralise authority makes it difficult for the security requirements mentioned above to be implemented. Encryption and authentication rely on cryptographic keys, which are difficult to establish with no common administrative control. Key generation, management and distribution schemes exists, but few fit the (unclear) trust model of ad-hoc networks. In contrasts, having a centralise entity could lead to a single point of attack such as denial of service attacks (DoS) and thus, making the network more vulnerable.

Wireless transmission can be intercepted, and an adversary with sufficient transmission power and knowledge of the physical and medium access control layer mechanisms can obstruct its neighbours from gaining access to the wireless medium. Assisted by these “opportunities” that wireless communication offers, malicious nodes can meaningfully alter, discard, forge, inject, and replay control and data traffic, generate floods of spurious messages, and in general, avoid complying with the employed protocols [6]. The impact of such malicious behaviour can be severe, especially because the cooperation of all network nodes provides for the functionality of the absent fixed infrastructure. In particular, as part of the normal operation of the network, nodes are transiently associated with a dynamically changing, over time, subset of their peers; that is, the nodes are within the range of their transceivers, or the ones that provide routing information and implicitly agree to relay their data packets. As a result, a malicious node can obstruct the communication of potentially any node in the network, exactly because it is entitled or even expected to assist in the network operation.

In Addition, freely roaming nodes join and leave MANET sub-domain independently, possibly frequently, and without notice, making it difficult in most cases to have a clear picture of the ad-hoc network membership. In order words, there may be no ground for an a priori classification of a subset of node as trusted to support the network functionality. Trust may only be developed over time, while trust relationships among nodes may also change, when, for example, nodes in an ad hoc network dynamically become affiliated with administrative domains. This is in contrast to other mobile networking paradigms, such as Mobile IP or cellular telephony, where nodes continue to belong to their administrative domain in spite of mobility. Consequently, security solutions with static configuration would not suffice, and the assumption that all nodes can be bootstrapped with the credentials of all other nodes would unrealistic for a wide range of MANET instances.

From a slightly different point of view, it becomes apparent that nodes cannot be easily classified as “internal” or “external”, that is, nodes that belong to

the network or not; i.e, nodes that are expected participate and be dedicated to supporting a certain network operation and those that are not. In other words, the absence of an infrastructure impedes the usual practice of establishing a line of defence, separating nodes into trusted and untrusted. As result, attacks cannot be classified as internal or external either, especially at the network layer. Of course, such a distinction could be made at the application layer, where access to a service or participation to its collaborative support may be allowed only to authorized nodes. In the latter example, an attack from a compromised node within the group, that is, a group node under the control of an adversary, would be consider an internal one.

Most of the currently consider MANET protocols were not originally designed to deal with malicious behaviour or other threats. Thus, they are easy to abuse. Incorrect routing information can be injected by malicious nodes that respond with or advertise nonexistent or stale routes and links. In addition, compromised routes, i.e., routes that are not free of malicious nodes may be repeatedly chosen with the "encouragement" provided by the malicious nodes themselves. The result is that the pair of communicating end-nodes will experience a DoS, and they may have to rely on cycles of time out and new route discovery to find operational routes, with successive query broadcasts imposing additional over-head. or even worse, the end nodes may be easily deceived for some period of time that the data flow is undisputed, while no actual communication takes place. For example, the adversary may drop a route error message, "hiding" a route breakage, or forge network and transport layer acknowledgements.

Finally, mobile or nomadic host have limited computational capabilities, due to constraints stemming from the nature of the envisioned MANET application. Expensive cryptographic operations, especially if they have to be performed for each packet and over each link of the traversed path, make such schemes implausible for the vast majority of mobile devices. Cryptography algorithm may require significant computation delays, which in some cases would range from one to several seconds for low-end devices. These delays, impose for example by the generation or verification of a single digital signature, affect the data rate of secure communication. But, more importantly, mobile devices could become ideal target of DoS attacks due to their limited computational resources. An adversary could generate bogus packets, forcing the device to consume a substantial portion of its resources. Even worse, a malicious node with valid credentials could frequently generate control traffic, such as route queries, at a high rate not only to consume bandwidth, but also to impose cumbersome cryptographic operations on a sizable portion of the network nodes.

IV. KEY MANAGEMENT

Key management is the set of techniques and procedures supporting the establishment and maintenance of keying relationship between authorised parties [7]. It is hardest part of cryptography [8]. Designing secure cryptographic algorithms and protocols isn't easy, keeping the keys secret is much harder. Key management encompasses techniques and procedures supporting:

- Initialisation of system users within a domain;
- Generation, distribution, installation of keying materials;
- Controlling the use of keying materials;
- Update, revocation and destruction of keying materials and;
- Storage, backup/recovery, and archival of keying materials.

Key management plays a fundamental role in cryptography (which is paramount to security) as the basis for securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures. In ad-hoc networks, key management is a challenging issue because there is no centralise entity/entities to provided the services. Thus a way has to be devised to simulate such entity/entities to carry out these task. Some work has already been done in this area. In [9], a key management facility is proposed. The system, as a whole, has a public/private key pair K/k used in the verification and signing of public key certificate of the network nodes. It is assumed that the public key K of the system is known to all nodes and that the nodes trust any certificate signed by the corresponding private key k. The private key k of the system is securely distributed using a (n, t + 1) threshold cryptographic scheme to n arbitrarily chosen nodes called servers, thus providing a good level of fault tolerance. To issue a certificate, each server generates a partial certificate signed with its share of the system's private key. These partial certificates are then forwarded to a combiner which computes the signature from the partial signature. Besides threshold cryptography, the system also employs proactive share update to ensure that an adversary is not able to compromise enough servers over a long time period. This system however assumes the existence of a trusted entity that initially empowers the servers. Also, it follows a hierarchical approach, that is the entire system is partitioned into domains where local servers are deployed [10]. Several characteristics of ad-hoc network make this approach ineffective;

1) High mobility causes frequent route changes, thus contracting the local server in a timely fashion is non-

trivial. Besides the server maybe multi-hops away and may also move. This not only causes complicated dynamic repartitioning of the network, but also stretches the problem of locating and tracking a local server.
2) Multi-hop communication over the error-prone wireless channel exposes the data transmission to high loss rate. This reduces the success ratio and increases the average service latency.
3) Every local server is exposed to a single point of attack. Threshold secret sharing among local servers solves this problem, but aggravates the previous two concerns.

A more recent proposal [10], [11], [12] addressed availability by making all n nodes in the network share the functionality of a centralise entity. Any t + 1 nodes in the local neighbourhood of the requesting node can issue or renew a certificate. Another novelty is that any node not possessing a share can obtain a share from any group of at least t + 1 nodes already possessing a share. However, just like in [9] the first t + 1 nodes must be initialised by a trusted authority. Also while this system address availability and fault tolerance, it compromises the security of the network. In general, the gap between t and n in a secret sharing scheme defines the security of the system. t can be chosen between 1 and n in any secret sharing . As t approaches, thus closing the gap between t and n, the system becomes more secure because an dversary needs to compromises at least t nodes to collapse the system. But if t is too large, the system becomes less available to clients and also less tolerant to fault. When t approaches 1, making the gap larger, the effect is reversed and the system becomes more available and less secure. Kong chose to keep t relatively small to address the availability problem and ended up with a vulnerable system where any adversary need only compromise a small number of nodes in the network to collapse the service.

Another notable scheme that employs threshold cryptography is one proposed by Seung Yi and Robin Kravets [13], [14]. In their scheme, they took in to consideration the heterogeneity of ad-hoc networks. They argued that mobile nodes in many ad-hoc networks will be heterogenous in many respect, especially in term of their security and that any service or framework should take this into account. Seung Yi et al threw more light on their argument by describing a battlefield scenario which comprises of a military unit consisting of infantry soldiers, platoon commander's jeep, company commander's vehicles artillery vehicles, transport vehicles, and even tanks. They stressed the fact that all of these nodes have different strength in terms of their transmission range, ranks, power, capabilities and level of security. They suggested that it will be wise to pick nodes with higher ranks, more power, more capabilities to provide security services for the entire network. They called these nodes mobile certification authorities (MOCA). However, the scheme still relies on the need of a trusted third party for the initialisation stage of the MOCA.

One other scheme worth mentioning is the one proposed by Hubaux et al [15], [16], [17]. In this scheme, every node plays the role of its own centralise entity, similar to the PGP web of trust model but unlike the latter, there is no certificate repository where certificates are stored. Each node is required to store its own certificates. For two parties wanting to authenticate themselves, they must search there certificate repository for a chain of certificates that link both of them. Hubaux equated this to finding an intersection point between the certificate chain carried by each user and proposed a shortcut-hunter algorithm for this purpose. While this fits the description of self-organisation in ad-hoc networks, however,it does not scale beyond a relatively small community of trusted nodes because it would be difficult for each node to maintain a long list of trusted friends, potentially as large as the list containing all the nodes in the whole network.

V. RESEARCH DIRECTION

Given the aforementioned contributions that rely on trusted third parties to initialise the network, are based on a threshold access structure and the static adversary model, our research direction is to complement these efforts. We consider obtaining a security support for mobile ad hoc networks, which is self-initialising, is based on the more realistic general access structure, secure against an adaptive adversary, and allows seamless enrolment and de-enrolment. Threshold structures and static adversaries do not fit well in ad-hoc networks, as the heterogeneity and the dynamic nature as well as the security exposures of the network needs to be taken into account. Our research direction will therefore involve the development and application of verifiable secret sharing, proactive sharing and re-sharing over general access structures, without a dealer, with a bandwidth-efficient verification scheme, allowing enrolment and de-enrolment.

REFERENCES

[1] M. Ilyas, *The HandBook of Wireless Ad-Hoc Networks*, M. Ilyas, Ed. CRC Press, 2003.
[2] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," 1999, http://wwwice. eng.cam.ac.uk/publications/files/tr.1999.2.pdf.
[3] D. Zhou, *Security Issues in Ad Hoc Networks*, ser. The hand Book of Wireless Ad-hoc Networks. CRC Press, 2003, ch. 32, pp. 1–13.
[4] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead, "Survivable Network Systems: An Emerging Discipline," Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213, Tech. Rep., 1997.
[5] M. Mishra and K. M. Nadkarni, *Security in Wireless Ad-Hoc Networks*, ser. The hand book of Wireless Ad-Hoc Networks. CRC press, 2003, ch. 30, pp. 1–51.

[6] P. Papadimitratos and Z. J. Haas, *Securing Mobile Ad-Hoc networks*, ser. The hand Book of Wireless Ad-hoc Networks. CRC Press, 2003, ch. 31, pp. 1–17.
[7] A. J. Menezes, P. C. van Oorschot, and S. Vanstone, *The Hand Book of Applied Cryptography*. CRC Press, 1997.
[8] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Second, Ed. John Wiley & Sons, Inc, 1996.
[9] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE network, special issue on network security*, 1999.
[10] J. Kong, P.Zerfos, H.Luo, S.Lu, and L. Zang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," *IEEE ICNP (International Conference on Network Protocols)*, 2001.
[11] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks," Tech. Rep., 2000.
[12] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing Ad Hoc Wireless Networks," 2002.
[13] S. Yi and R. Kravets, "MOCA : Mobile Certificate Authority for Wireless Ad Hoc Networks," 2002.
[14] ——, "Key Management for Heterogeneous Ad Hoc Wireless Networks," Tech. Rep., 2002.
[15] J.-P. Hubaux, L. Buttyan, and S. . Capkun, "The Quest for Security in Mobile Ad Hoc Networks," *Mobile Ad Hoc Networks Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing, MobiHOC*, 2001.
[16] J.-P. Hubaux, T. Gross, J.-Y. L. Boudec, and M. Vetterli, "Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project," 2001.
[17] S. Capkun, L. Buttya, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE TRANSACTIONS ON MOBILE COMPUTING*, vol. 2, no. 1, 2003, jANUARY-MARCH 2003.

Biological and Astronomical Time

Dr Pasha Parpia
Department of Informatics
University of Sussex
D.Y.Parpia@sussex.ac.uk

There are two platforms that permit the establishment of the scientific notion of time in the human mind. These are (1) the internal human cognitive capacity to experience duration and have an episodic memory, and (2) factors, that may be regarded as external to the cognitive domain such as the cyclic phenomena in the external world.

Virtually all living organisms have "biological clocks" that regulate their behaviour in the temporal domain. Their mechanisms are based on either (1) oscillations, or (2) unidirectional processes, that trigger development and aging (hourglass clocks). The function of the first is based on a genetic transcription-inhibition feedback loop, which is common, in its principle of function, to virtually all living organisms from primates through rodents, fish, frogs, insects to even cyanobacteria (the prokaryote, blue-green algae).

The function of the second, the hourglass clock, is governed by the limited number of cell division cycles that can be performed by individual cells in the body, and this type of clock plays a predominant role in development and ageing. However, they are subject to alterations in their function by environmental factors such as temperature (in cold blooded creatures), nutrients and cytotoxic agents, while the body clock which functions on an oscillatory basis is temperature compensated and is accurate to a few parts in a thousand.

It is interesting to note that the body's circadian rhythm, which when averaged, has the periodicity of the moon around the earth, becomes entrained by the 24 hour cycle of the sun. Entrainment occurs through a dedicated pathway from the eyes to the bodily clock located, in mammals, in the suprachiasmatic nucleus of the hypothalamus.

The astronomical factors that provide the human system with the concept of time are principally those arising from the rotation of the earth on its axis and its revolution around the sun. Knowledge of the regularity of the motion of astronomical objects can be dated back to over 5,000 years ago.

The Scooby Event-Based Middleware for Service Composition in Pervasive Computing Networks.

Jon Robinson
Network Lab
Department of Informatics
University of Sussex
J.R.Robinson@sussex.ac.uk

Introduction

Pervasive computing, or Ubiquitous Computing as it is alternatively known as, was first introduced in concept by Mark Weiser of Xerox Park Laboratories in 1991 through the publication of his seminal paper entitled "The computer for the 21st Century"[1]. In this paper, he envisioned a world where computers would no longer be considered to be obtrusive devices as characterised by desktop and server computers of today, but instead, computers would become invisible and transparent to the average user, and be embedded in a variety of devices. These *smart* devices would permeate throughout this pervasive infrastructure whereby human-computer interactions would become transparent, and oblivious to end-users. At the time, computer technology was not sufficiently advanced to provide a realistic real-world interpretation of his vision. However, due to advances in:- miniaturisation; increased processing and storage; and development of wireless communication protocols (for example Bluetooth [2]), we can start to effectively produce smart devices that are small and powerful enough to provide the infrastructure that Weiser first envisioned.

Now that these smart devices are starting to become main stream (for instance WAP/Java enabled phones, PDA's, Tablet PC's) and cost effective for the general public to own, attention can now be focused on the dynamic composition of services and resulting middleware layer required to power such scenarios as outlined by Weiser.

The focus of my work is the exploration and development of a middleware layer that aids in the composition of dynamic services, based on polices outlined by an individual user. The first stage was to investigate and determine which type of messaging system would suit such an ad-hoc, dynamically changing distributed environment. There are three types variants of Publish/Subscribe systems available at present [4], to which all messaging systems can be attributed to. Topic-based systems come in a variety of forms, of which an example is the Corba Event [10] system that utilise a flat model for representing events. Type-based systems allow for events to be filtered and classified by objects on which operations can be performed. Examples of such systems would include, Java RMI [8], Jini [7] & Trader [9]. The third form of Publish/Subscribe is that of Content-based systems. These allow for an event to be composed out of tuples of information, and transmitted indiscriminately to any listening services. Such examples are Elvin [5], Gryphon [11].

Ideally, in a pervasive environment, information needs to be propagated throughout with the least amount of specific information for identifying the target services. To this end, we can introduce a set of criteria that is required to be satisfied for providing a general form of communication. The notions of *space decoupling*, *time decoupling* and *flow decoupling* [12] can be introduced that allows for the decoupling of location dependant information from the event. Introducing this decoupling, allows the consumer and producer to be independent of each other and not be reliant on any dependencies, by allowing each to be; unaware of the whereabouts of each other; not to be dependant on the linear execution of a service (i.e. can be doing something else once an event has been transmitted); and not be in a blocking state waiting for a reply to occur once an event has been dispatched.

Out of all three variations of the Publish/Subscribe paradigm, only Content-based routing satisfies all three requirements. To this end, the proposed infrastructure we have developed utilises the Elvin [5] event notification system, as the backbone message system.

The Scooby Middleware

The components of our system, can be characterised by the following layers:

Elvin event System → Middleware Layer → Service Composition Language

The middleware layer provides the mechanisms for discovery, service identification, accessing of remote service functionality and synchronisation between services. The novelty of this implementation, is the introduction of binding variables that allow services to search for any matching proxy services based on a given criteria. A combination of late and lazy dynamic binding between these constructs and services are provided at different points within the lifecycle of a users' service. For instance, when first instantiated, bindings are resolved against any matching services available within the infrastructure based on the pre-requisites laid down by the user in their initial composition. As these binding constructs have a number of states, that continually change between, discovery, suspend and connection, they will continually evolve over time to link to better matching services during their lifetimes. Final checks are performed when an invocation request is required, and reflection is used for identifying which method in the target service is required. In addition to allowing for bindings between services, binding variables can also be associated to complex events that can occur over an indefinite amount of time. This is required to allow an event-driven model of a service to be adopted instead of just relying on an RPC mechanism, albeit transported over an event messaging system.

The notion of binding variables forms an important feature of the service composition language that has been developed. For example in the following figure, we have outlined a simple service composition that allows for two bindings between services, to provide a new service that converts documents from one type to another before printing.

```
proxy PDFPrinter {
  bind printer to proxy match { implements : printer & location
: 5a22 }
  bind converter to proxy match { implements : pdf2ps }
    {    location:5a22    }
  { # start of method declarations
    public void print( blob file ) {
      if( file is PDF ) ) file = converter.convert(file)
      printer.print(file)
      }
  } # end of method declarations
} when bindexception{
    reporterror( "error occurred" )
    terminate
    }
```

Figure 1: Example printer composition.

In this example, the *printer* and *converter* binding variables are dynamically bound to services that satisfy the requisites laid down by the user. When accessing a services member method, the dot notation is used to offset against the binding variable.

The Scooby compiler is used to translate this code into Java, which is subsequently linked into the middleware layer, and becomes part of the infrastructure.

Conclusion

In conclusion we have outlined the vision of Pervasive Computing, along with some background on the types of communication systems that would benefit from this paradigm of computing. Additionally, we have introduced our proposed system [6] which provides a solution based on the use of binding variables utilising late and lazy dynamic binding, along with the supporting service composition language in which users can formally specify their policies which is all based on an event notification messaging system.

References

[1] WEISER, M. 1991. The Computer for the 21st Century. Scientific America

[2] Bluetooth Specification. http://www.bluetooth.org/foundry/adopters/document/Bluetooth_Core_Specification_v1.1. Feb 2001

[3] ROBINSON, J, & WAKEMAN, I. 2003. The Scooby Event-Based Pervasive Computing Infrastructure. Ubi Net Sept 2003, Imperial College, London.

[4] ROBINSON, J. 2004. A Survey of Middleware, Discovery & Composition technologies to aid in the goal of distributed service composition in a pervasive environment.
[5] Elvin, http://elvin.dstc.edu.au
[6] ROBINSON, J. 2004. The Scooby Event-based Middleware layer and service composition system.
[7] JINI. 2004. Jini Architecture Specification. http://wwws.sun.com/software/jini/specs/jini1.2html/jini-spec.html. Sun Microsystems, Inc. 2004.
[8] RMI. 2002. Java RMI Specification. ftp://ftp.java.sun.com/docs/j2se1.4/rmi-spec-1.4.pdf. Sun Microsystems, Inc. 2002.
[9] VAUSDEVAN, V. 1998. A reference model for Trader-based distributed systems architectures. Object Services and Consulting Inc, January 1998
[10] CORBA Notification Service. http://www.omg.org/docs/formal/02-08-04.pdf
[11] STROM, R., BANAVAR, F., CHANDRA, T., KAPLAN, M., MILLER, K., MUKHERJEE, B., STURMAN, D., AND WARD, M. 1998. Gryhon: An information flow based approach to message brokering. In International Symposium on Software Realiability Engineering '98 Fast Abstrac, 1998.
[12] EUGSTER, P., FELBER, P., GUERRAOUI, R., AND KERMARREC, A.M. 2001. The many faces of Publish/Subscribe. Technical Report DSC ID:2000104, EPF Lausanne, 2001

Effective Teaching and Cognition

Martin Santos
Department of Informatics
University of Sussex
J.M.Santos-Virgen@sussex.ac.uk

One of the main goals of technology and education concerns the lesson strategy or teaching expertise required to support the lesson learning processes, for example, via e-learning. However while technology is intended to be exploited as a method of pedagogy, how to teach a lesson in relation to students' cognitive learning processes remains unclear.

Research questions

Which teaching events should be implemented in a lesson to support students' cognitive learning processes? What is the relationship between student's cognitive learning processes and teaching events? Which narrative sequence is appropriate for a lesson to support learners' cognition and how can it be presented with the aid of multimedia technology? These findings will be useful for implementations in Intelligent Tutoring Systems (ITS), or Information and Communications Technologies (ICTs), like interactive-tv or audiovisual presentations supported with electronic devices.

Effective Teaching

The importance of effective teaching with technology has been highlighted by several researchers (i.e., Murray 1999, Laurillard 2002, Shute and Towle 2003). However they do not provide evidence for a principled lesson strategy that had proved to be successful, therefore, the question still needs to be sufficiently answered to be applied in schools.

(Laurillard, 2002), have pointed out the necessity of a strategy for effective teaching: "we need cognitive psychology to tell us, in a content-specific way, how a natural environment affords learning. Then, perhaps, we can construct the means of access that will turn an environment [with technology, the university lecture, or other] into one that affords learning."

Several researchers (Guttormsen Schar and Krueger 2000, Najjar 2001, Mayer and Moreno 2002) have proposed principles to use different media technologies to design instructional presentations. However these experiments are usually short (5 minutes) and do not seem to link learners' cognition to a 50 minutes lesson. A description of the teaching process and its relation to multimedia technology is therefore required.

Cognitive Processing and teaching events

Although investigation in education has been carried on since the nineteenth century, contributing with several theories to the understanding of learning processes and therefore to teaching, the problem is complex and it seems that scientific research has not been satisfactory related to the events of teaching.

Gagné (1977) and Glaser (1987) aim to establish an understanding of learning in relation to human cognitive processes. Similar ideas had been presented by Ohlsson (1991) and (Simon, 1989). Gagné (1977) seems to be the first who related selective perception, attention, working memory encoding, transfer, long-term memory storage, retrieval and feedback, to the instructional events for learning. Gagné proposed how to implement successfully teaching, based on the requirements of cognitive processing of the learners.

Gagné's instructional events were designed based on the knowledge during the 70's about how human brain works, and the knowledge about cognitive processes had advanced in the last years and computational technology available for teachers has also improved. Therefore, an updated analysis is required relating the evidence in cognitive science to the events of learning in a class. According to Laurillard (2002), these events of learning also

require more empirical evidence of their global utility for teaching in a real university class.

The events of learning have been termed lesson instructional strategy by some authors (Smith & Ragan, 1999) who include supplantive or generative approaches to the lesson strategy. These strategies refer to the level of independence or scaffolding that should be provided to the learner.

Conclusion

The problem of effective teaching has a long tradition of research. The knowledge about Cognitive Processes has advanced (Anderson, 2000, Eysenck & Keane, 2000). However, there seems to be limited research at present of how these findings of cognitive science can be related to events of teaching.

The problem is complex because theories have been studied in detail with many purposes: to derive technological applications, to theorize deeply a particular concept, to criticise its point of view through the light of another theory. The abundance of theories, criticisms and research complicate this task, may be that is the reason why there not seems to be a strong trend of research focused on integrate learning theories, although these theories were constructed to the same purpose of enriching the knowledge of how to teach effectively.

Research Objectives

Analyse cognitive learning processes related to principles for effective teaching to explain how these events afford learning. Integrate the common teaching events present in successful e-learning implementations proposing a model to understand how to afford learning with technology. Design an experimental lesson strategy that supports students' cognitive learning processes using an appropriate narrative and multimedia technology.

References

Anderson, J. R. (2000). Cognitive psychology and its implications (5th ed.). New York. W. H. Freeman.

Guttormsen Schar, S. G. and Krueger, H. (2000). Using New Learning Technologies with Multimedia. IEEE, Multimedia, July-September 2000, 40-51.

Gagné, R. M. (1977). The Conditions of Learning, New York; Holt Rinehart and Winston.

Glaser, R. (1987). Advances in Instructional Psychology volume 3, Hillsdale NJ. Lawrence Erlbaum Associates.

Laurillard, D. (2002). Rethinking University Teaching. RoutledgeFalmer.

Murray, T., (1999). Authoring Intelligent Tutoring Systems: An Analysis of the State of the Art. International Journal of Artificial Intelligence in Education, 10, 98-129.

Najjar, L. J. (2001). Principles of educational multimedia user interface design. In R. W. Swezey & D. H. Andrews (Eds.), Readings in training and simulation: A 30-year perspective (pp. 146-158). Santa Monica, CA: Human Factors and Ergonomics Society.

Ohlsson, S. (1991). System hacking meets learning theory: Reflections on the goals and standards of research in artificial intelligence and education. Journal of Artificial Intelligence in Education, 2(3), 5-18.

Shute, V.J., and Towle B. (2003). Adaptive E-Learning. Educational Psychologist, 38(2), 105-114. Lawrence Erlbaum Associates, Inc.

Simon, H. A. (1989). The scientist as a problem solver. In D. Klahr and K. Kotovsky (Eds.), Complex information processing: The impact of

Herbert Simon. Hillsdadel, NJ: Erlbaum.
Smith, P., Ragan, T., (1999). Instructional Design. NY. Wiley.

Temporal Coding via Neural Synchrony

Sampsa Sojakka
Centre for Computational Neuroscience and Robotics
Department of Informatics
University of Sussex
sampsas@sussex.ac.uk

Introduction

In a seminal contribution more than 75 years ago Adrian showed that the firing rate of stretch receptor neurons is related to the force being applied to the muscles (Adrian, 1926). As a result, early neural network models interpreted the output of artificial neurons as an abstraction of the firing rate in their biological counterparts. In recent years this view has been challenged due to mounting experimental evidence showing the need to take into account the temporal dimension in neural information processing. In particular, Thorpe et al. have shown that humans and monkeys are able to respond to a visual categorization problem in such a short time interval that there is enough time for only one spike to be generated at every relay station in the visual pathway (Thorpe, Delorme, & Ruellen, 2001). This result clashes with the frequency rate coding hypothesis and points to the existence of computational processes based on the precise timing of spikes in neuronal ensembles.

Several possible such temporal coding mechanisms have been proposed including those based on inter-spike intervals, latency or the synchronized firing of neurons (Shadlen, 2002). Of these, firing synchrony presents the most compelling hypothesis due to wide ranging experimental evidence in its support. This paper will give a brief overview of neural synchrony, its potential uses and how networks can be constructed to take advantage of this property.

Synchrony

Synchronisation is a rather ubiquitous phenomenon in nature. Examples range from the flashing of fireflies to circadian pacemaker cells, lasers and superconducting Josephson junction arrays (Strogatz & Stewart, 1993). Generally speaking synchrony results when homogeneous oscillating units (e.g. neurons) are arranged in a pulse coupled network with certain parameters. When run freely the oscillators in such a network entrain on each others signal and the synchronized state becomes an attractor that slowly envelops all units even if their natural period differs from that of the synchronised state. The degree of synchrony is measured by the phase variables of all oscillators with two oscillators being in synchrony if their phases are identical.

Firing synchrony can be used for computation in a number of ways. It provides a 'many neurons now agree' measure that can be exploited by other neurons in a detection of a particular event (Hopfield & Brody, 2000). This structure is particularly robust to lesions and failure of individual neurons since it is the collective behaviour of the synchronized ensemble that matters. Neural synchrony has also been found to play a crucial role in the activation and cooperation of disparate areas of the brain. Experiments have shown the formation of remote synchronised clusters within the cortex both in the integration of visual information (Singer & Gray, 1995) and the codification of odours in the olfactory system (Laurent & Davidowitz, 1994). Finally, a temporal code provides the network with the capability to detect and generate complex time series data given that the network fulfils certain architectural constraints.

Architectural Requirements

Synchrony is easy to achieve, so much so that for a wide range of parameter values and initial conditions virtually all pulse coupled networks end up in the synchronised state (Strogatz, Mirollo, & Matthews, 1992). Unfortunately such synchronized states form

stable attractors meaning it will be difficult to desynchronise the network after convergence. This is unsatisfactory for the construction of neural networks where convergence usually has a functional role and the inability of the network to escape the attractor will prevent it from resetting. This means that if a network based on synchrony was constructed to, say, produce a particular pattern on a given input, it would always produce that pattern after being once presented with that input.

In order to get around this problem networks utilising synchrony must be constructed in a manner that ensures that the resulting attractors are *unstable* so that a small perturbation (such as noise) is sufficient to make the network leave the attractor and proceed with the next task. This has proven tricky in practice but recent work has shown that pulse coupled networks with heterogeneous nodes, strictly excitatory connections and sufficient delay give rise to unstable attractors that prevail for large network sizes and a wide range of parameters (Timme, Wolf, & Geisel, 2003). Furthermore, such architectures exhibit dynamic formation of synchronised clusters that can be used to encode information in trajectories in state space making them ideal candidates for producing networks with varying degrees of temporal pattern generation (Winfree, 2000).

Current Research

The role of synchrony in the cortex and the capabilities of networks exhibiting unstable attractors are still largely unknown. Despite neurophysiological evidence pointing to its existence, the functional role of neural synchrony remains largely undefined due to experimental difficulties tying large scale cortical phenomenon to information processing at the neural level. My research in this area is twofold. The initial aim is to investigate and map the architectural and topological requirements for networks exhibiting unstable attractors and neural synchrony. The secondary aim is to compare these networks against more conventional designs in time based tasks such as controlling an autonomous robot and produce biologically plausible computational models capable of reproducing the synchronisation behaviour found in the cortex.

References

Adrian, E. D. (1926). The impulses produced by sensory nerve endings. *The Journal of Physiology*,*61*, 49-72.

Hopfield, J. J., & Brody, C. D. (2000). What is a moment? Transient synchrony as a collective mechanism for spatiotemporal integration. *Proc. Natl. Acad. Sci.*, *89*, 1282.

Laurent, G., & Davidowitz, H. (1994). Encoding olfactory information with oscillating neural
assemblies. *Science*, *265*, 1872-1875.

Shadlen, M. N. (2002). *Rate versus temporal coding models*. Encyclopedia of Cognitive Science,
Macmillan.

Singer, W., & Gray, C. M. (1995). Visual feature integration and the temporal correlation hypothesis. *Annual Review of Neuroscience*, *18*, 555-586.

Strogatz, S. H., Mirollo, R. E., & Matthews, P. C. (1992). Coupled nonlinear oscillators below the synchronization threshold: Relaxation by generalized Landau damping. *Physical Review Letters*, *68*, 2730.

Strogatz, S. H., & Stewart, I. (1993). Coupled oscillators and biological synchronization. *ScientificAmerican*, *269*(6), 102-109.

Thorpe, S. J., Delorme, A., & Ruellen, R. V. (2001). Spike-based strategies for rapid processing.
Neural Networks, *14*, 715-725.

Timme, M., Wolf, F., & Geisel, T. (2003). Unstable attractors induce perpetual synchronization
and desynchronization. *Chaos*, *13*, 377-387.

Winfree, A. T. (2000). *The geometry of biological time, second ed.* Springer, New York.

Economics of Cooperation: Information Foraging in Distributed Systems

Ashish Umre
Network Research Lab, Department of Informatics,
University of Sussex, Falmer, Brighton, BN1 9QH, UK
ashishu@cogs.susx.ac.uk

Abstract. The sharing and collective processing of information by individuals in any social system is an attempt to reduce the uncertainty associated with key features of their environments by collecting and storing information. By sampling each of its options regularly, an individual gains from being able to exploit them when they are productive and avoid them otherwise. In this way, collection of information can be thought of as a solution to the uncertainty problem that maximises potential opportunities. However, doing so may entail certain costs because of valuable resources, including time, energy and attention. We explore the cost/benefits of cooperation within the domain of distributed systems, where biologically inspired agents communicate and cooperate with each other using the environment to disseminate information about resources/services.

Biological Basis for Cooperation

To account for the manifest existence of cooperation and related group behaviour, such as Altruism and Restraint in competition, evolutionary theory has acquired two kinds of extension: Genetic kinship theory and reciprocity theory. If the agents are sufficiently closely related, altruism can benefit reproduction of the set, despite loses to the individual altruist. The evolution of the suicidal barbed sting of the honeybee worker could be taken as a paradigm for this line of theory.

Many of the benefits sought by living things are disproportionally available to cooperating populations. The problem lies with the fact that while an individual can benefit from mutual cooperation, each can also do so even better by exploiting the cooperative efforts of others. Over a period of time, the same individuals may interact again, allowing for more complex patterns of strategic interactions. (Dugatkin 1998) argues that there are at least three ways that cooperation can evolve among unrelated individuals: reciprocity, group selection, and by-product mutualism. Though, kin selection is a fourth candidate.

Then again, how advantageous cooperation really is?

The acquisition and use of socially acquired information is commonly assumed to be profitable. But, there could be scenarios where the use of such information either provides no benefit or can actually incur a cost. It is suggested (Luc-Alain Giraldeau, Thomas Valone et. al. 2002) that the level of incompatibility between the acquisition of personal and socially acquired information will directly affect the extent of profitability of the information, when these two sources of information cannot be acquired simultaneously, because of cognitive or physical constraints. Also, a solitary individual's behavioural decisions will be based on cues revealed by its own interactions with the environment.

However, in many cases, for social animals the only socially acquired information available is the behavioural actions of others that expose their decisions, rather than the cues on which the decision was based. In such a situation it is thought that the use of socially acquired information can lead to *informational cascades* that sometimes result in sub-optimal behaviour.

Cost for everything

In any social group, individuals possess various behaviours that define the assortment of the interactions at all sorts of levels, individual, groups, cliques, teams etc. The social foraging theory suggests that, the functional consequence of an individual's foraging behaviour depends on both the individual's own actions and the behaviour of other foragers. There may be conflicts of

interest between signallers and receivers. Where such a conflict exists, the receiver's need to acquire information may favour sensitivity to the cues provided by the behaviour and appearance of the signaller. In turn, this sensitivity may give rise to opportunities for manipulation and exploitation by the signaller. It is understood that exploitative strategies are unlikely to persist in the long run, because they generate selection for a change in receiver responses. However, it is argued, that the evolution of exploitation may prove a recurrent, though, transient phenomenon.

There are costs associated with broadcasting information publicly, as exemplified by the production of "food vocalisations" in many social animals, after locating resources. The issues that come under this context are, dangers of predation, and mass recruitment to a very less profitable resource may lead to starvation.

Other costs within the context of a social system are cost of misinformation (lying), cost of accessing/using the resources and cost of signalling/cooperation. We use foraging games to analyse the economics of Kleptoparasitic[1] behaviour, to predict the ecological circumstances under which the behaviour is maintained.

Information Dissemination Framework

A generic model of distributed applications, with abstractions of costs and benefits is implemented. Agents share information (through the environment, *Stigmergy*) about the location of resources and services for the completion of requests generated by users. We analyses aspects of multi-agent systems, such as, optimal number of agents in the system, throughput of the system, degree of cooperation (which can depend on an implicit factor of relatedness). Demonstration of the use of Nash equilibrium / ESS (Evolutionary Stable Strategy) to show the *"tragedy of the commons"* for certain situations both in the simulations and in real life, e.g. *slash dot effect*. How a certain resource/service gets over exploited because of it being over publicised and may lead to its exhaustion/starvation.

We explore various cooperative/competitive strategies that encompass most aspects of social behaviour. Mixed strategy models showing the possibility of freeloaders or lying. We model trust in the system, reputation, altruism, misinformation, and free riders (Kleptoparasitic behaviour). Demonstrate how game-theoretic models can make novel, quantitative, and testable predictions concerning social foraging theory, within the application domain of distributed systems e.g. P2P networks. The simulation model should eventually be able to help understand some of the contexts in which cooperation emerges, is beneficial or not, and to what extent. Also, how the various costs can be minimised/optimised, by implementing dynamic strategies.

Acknowledgements

This research is supported by, *Future Technologies Group* and *Programmable Networks Lab*, at the British Telecom Research Labs, Adastral Park, UK.

References

(Caraco and Giraldeau 2000) *Social Foraging Theory*, Princeton University Press.

(Luc-Alain Giraldeau, Thomas Valone et. al. 2002) *Potential disadvantages of using socially acquired information*, Phil. Trans. of the Royal Society, London.

(Seeley 1995) *The Wisdom of the Hive – The Social Physiology of Honey Bee Colonies*, Harvard University Press, Cambridge.

(Anderson and Franks 2001) *The Complexity and Hierarchical Structure of tasks in Insect Societies*, Animal Behaviour, 2001. 62:643-651.

(Dugatkin 1998) *Game Theory and Animal Behaviour*, Oxford University Press.

[1] Kleptoparasitism refers to all forms of exploitation of others' food discoveries or captures. It constitutes the information-sharing models in the Social Foraging Theory paradigm.

HOW TO IMPROVE LOW-TECH PROTYPING REMOTELY?

Aybala Yuksel
Department of Informatics
University of Sussex
A.Yuksel@sussex.ac.uk

Introduction

Low-tech prototyping is an emerging area in human-computer interface design. It takes place earlier in the design process. Low-tech prototypes allow designers to see their design in general, without going into more detail [1]. Thus it allows the flexibility in performing drastic changes to low-tech prototypes.

In order to attain more relevant usability data, a development team wants to reach real world users. Contacting users at remote locations introduces challenges, such as transportation costs [2] and resulting issues regarding the problematic configuration of laboratory equipment [3]. Online communication with remote users while doing low-tech prototyping may be an effective way of reducing those challenges.

The primary focus of my research is to investigate the challenges of fusing low-tech prototyping with online communication to allow the designers and users to work in separate locations. They communicate online and remotely with each other. This leads to remote usability issues that will be inherent from such a combination of the two areas. Therefore, in this paper, I will initially discuss Low-tech prototyping followed by what constitutes as online communication. Next, I will summarise the combination of the two and some of the resulting remote usability issues. Finally I will discuss my aims and future plans.

Low-tech Prototyping

A low-tech prototype is also collectively known as a low-fidelity prototype [4]. It is essentially the modelling of the design with low level of details. There already exist a number of techniques that are used in low-tech prototyping such as sketches, storyboards and sitemaps. *Storyboards* [5] are a series of sketches that illustrate a design concept and navigational aspects of a product such as a web site. A *Sitemap* [5] is a hierarchical diagram of sections of a web site. *Sketches* are freehand drawings that show the outline of a design.

Sketching

Designers like to sketch in the early stage of the design process (Sketch Recognisers from the End-User's, the Designer's, and the Programmer Perspective). Even if a design project has less budget and time, because of its easiness and cheapness it is often preferred by designers.

Currently, designers can use paper or electronic based sketching tools to outline a design. One of the advantages for sketching on paper is that it allows designers to sketch freely that can support them within the creative process and allow them to express new ideas simply. Another advantage is that it can allow designers to prototype more effectively by making the process easier and hence, cheaper [6]. Juxtaposed with this method of sketching are the benefits of using a software-based medium (i.e. a sketching tool). Here, software can allow the designer to test their design at any point during the creative design processes. This means users can view the current design and comment on its viability with their expectations, and as a result can increase the flow of communication between user and designer to enhance the effectiveness and productiveness of the creative design process. Moreover, editing functionality within such tools reduces both the time spent on designing, and project costs.

This research aims at investigating such electronic-based sketching tools, for example DENIM [7] with the view to expand on its collaborative nature and explore the resulting

remote usability challenges that would be highlighted from such a fusion.

Online Communication

Online communication is the way in which to exchange information or to convey an idea if the user is located remotely. There are presently, several forms of online communication that can be characterised by *email*, *chat*, *voice conversation* or *conferencing* amongst others. Each form of communication may introduce different issues in the flow of information between design and user. For instance, issues regarding bandwidth consumption [11] that dictates the amount of information that can flow at any single time, and that of latency that can introduce sequencing problems with online communications.

Other issues may arise when using communication tools such as NetMeeting for text or audio based chatting, or web conferencing that requires the user to be knowledgeable of the communication tool or have the ability to learn how to use it. Due to such a faceless form of medium, communication with an unknown (or known) user may sometimes result in potential ambiguities or misunderstandings as nonverbal elements are left out [9].

Remote Usability Evaluation

Traditional usability evaluations are conducted through usability laboratories that are equipped to handle such investigations. Although existing usability evaluation methods are effective, there are factors that can affect the validity of their results. These situations often involve a limited number of users or the reproduction of such results that are difficult or impossible to replicate, which in turn can affect their overall effectiveness [10].

The research area I am interested in exploring is the combination of low-tech prototyping with online communication and the resulting research challenges produced from such a joining. Some of the challenges include a loss of usability data while observing users when applying such evaluations to a remotely situated user. For instance, difficulties in communication may be associated with a lack of face-to-face communication, which may result from the lack of non-verbal elements. However, remote usability evaluation reduces the costs incurred by transportation as there is no need for users to be present at a usability lab or similarly, developers may no longer be required to be present at remote locations. This introduces a new dimension in the effectiveness of usability testing as the user can be observed in their natural work environment.

Another important consideration is that existing tools might not be up to the challenge that remote usability would require from them. For instance the user interface of such a system, and the concepts employed to describe the processes might not be adequate in such a situation. Hence, one of the areas I intend to address are the requirements of what such a scenario would place on the interface design to produce an affective tool.

Future Work

I have briefly introduced the area of research that I am endeavouring to explore. I am presently investigating the issues and challenges that would result from such a combination of low-tech prototyping coupled with a collaborative form of communication. My next step is to clearly identify those issues that are inherent in such a hybrid system, in terms of interface, usability and communication (human or computer based) along with a more in-depth review of existing systems.

References

[1]Wilson Diane, Rauch Thyra, and Paige Joeann, (1992), Low-tech Prototyping , IBM Corporation. Internet WWW page at: < http://www.firelily.com/opinions/low-tech.html>(Accessed: 15/06/04)

[2]Hartson H. Rex, Castillo Jose C. (1998), Remote Evaluation for post-deployment usability improvement. Published in the Proceedings of the Working Conference on Advanced Visual Interface (AVI'98)

[3] Krauss F.S.H. (2003) Methodology for remote usability activities: A case study, IBM System Journal Vol 42 No 4

[4]Paper Prototypes, WWW page at: http://www.deltamethod.net/9PrototypeDesign_Activities_PaperProto.htm (Accessed: 14/06/04)

[5] Mark W. Newman and James A. Landay, "Sitemaps, Storyboards, and Specifications: A Sketch of Web Site Design Practice." In *Designing Interactive Systems, DIS 2000*, New York City, August 2000

[6] Black 1990, Goel 1995, Gross and Do 1996, Newman and Landay 2000, Wagner 1990, Wong1992.

[7] Mark W. Newman, James Lin, Jason I. Hong, and James A. Landay, "DENIM: An Informal Web Site Design Tool Inspired by Observations of Practice." In *Human-Computer Interaction*, 2003.

[8] Usability Methods and Tools, Human Computer Interaction at Viginia Tech, Internet WWW page at: <http://research.cs.vt.edu/usability/projects/remote%20evaln/remote%20evaln.htm>(Accessed: 15/06/04)

[9] Dr. Diane Finley, Communication Issues in the Online Classroom, Department of Psychology The Online Express Prince George's Community Collage Fall 2000)

[10] Castillo Jose C., Hartson, H. Rex, Hix Deborah (1997). Remote Usability Evaluation at a Glance, Virginia Polytechnic Institute and State University, Blacksburg, VA

A Sound Emotionally Affective Framework for Intelligent Tutoring System (ITS)

Mohd Zaliman Yusoff
IDEAS lab, Department of Informatics,
School of Science &Technology,
University of Sussex, UK.
mzy20@sussex.ac.uk

Abstract

This paper is a step towards incorporating emotion in an ITS environment. A sound emotionally affective framework, which integrates emotion appraisal theory and ITS is presented. There are two benefits from this system to students:

1. by maintaining student's positive emotional state or by regulating students' negative emotional state and
2. by suggesting potential learning strategies to students. This proposed model has the potential to not only help students to improve their learning performance but also to improve their emotional state during learning.

Key word: *Intelligent Tutoring System (ITS),, Sound emotionally Affective Framework, Learning*

Despite the fact that emotions play an important role in learning, very few attempts have been made to study emotions in an Intelligent Tutoring System (ITS). Intelligent Tutoring Systems (ITS) are an active area of research, which studies and develops a variety of techniques in understanding the intelligent nature of learning. The integration between emotions and ITS has become more important, with many findings from researchers in education and psychology proving that a sound emotionally affective intelligent system helps students to perform better in mastering their learning. (Fredrickson, 1998, Goleman, 1995).

Therefore, this proposed system is modelled to integrate emotions with an intelligent tutoring system. This integration benefits students from two aspects. First, it is designed to prolong the engagement period between the students and their lesson by maintaining students' positive emotional state or regulating students' negative emotional state. For instance, this proposed system would allow a happy student, who has completed a difficult programming task very well, to freely select his/her next programming task as a means to retain his/her happiness. Likewise, for a sad student, who has given up on a difficult programming task, the system will suggest that the student read an effective coping statement such as "*I don't let my sadness to effect my performance*" repeatedly in order to reduce the affect of his/her sadness. In addition, relaxation activities such as head and eyes movements can also reduce his/her sadness. As a result of these strategies, students will feel better and, this in turn, will lead to prolong their study duration.

Second, this proposed system is anticipated to help students by giving suitable suggestions and strategies to improve their learning performance. These strategies are adapted to the elicited students' emotional state. It is based on the premise that students in positive emotional state are more capable in mastering their lesson (Fredrickson, 1998). For example, this system will suggest to a very angry inferred student, who has given up on his/her difficult programming lesson, to seek for a specific programming example and to proceed with an easier programming lesson before considering redoing the current lesson. On the other hand, for a joyful student, who has completed an easy programming task very well, the system will challenge this student to do a more difficult programming lesson or suggest to the student to seek only for a

generic example in his/her next programming task.

This proposed model is implemented in two phases: 1) the appraisal phase, which propose to infer the students' emotional state and 2) the reaction or regulation phase, which propose to use adaptive strategies and activities, in order to maintain or to regulate the elicited emotion. To strengthen this appraisal phase, Roseman's emotion appraisal model (Roseman, 1984, revised 1996) is referred to. A student's emotional state is inferred based on their reaction to self, others or notes, the control that the students have over the learning material, and the difficulty level of the lesson. For instance, a student is inferred to experience ***Joy*** emotion when he/she has completed a ***difficult*** programming task very well mainly by using his/her ***own knowledge*** with a ***high control*** over the lesson.

The second phase of this model is the reaction or regulation phase. The underpinning strategies used in this phase are to maintain students' positive emotional state or to reduce or regulate students' negative emotional state. Statement such as "***I can make things happen***" is an example of a coping statement used to maintain student happiness. By contrast, "***I saw this problem in another perspective to make it seem more bearable***" statement is used to reduce the anger of students. Apart from coping statements, relaxation activities such as muscle and head exercises will be employed to help students reduce their negative emotional state.

Possible strategies and suggestions are also made to these students in this second phase. To a sad inferred student, the system might suggest to the student to request for an easy programming task or to study more programming examples before proceeding with his/her lesson. On the other hand, the system might suggest to a happy student to do a more difficult programming level and to ask for less help in his/her next lesson. The complete framework for this proposal is as figure 1.

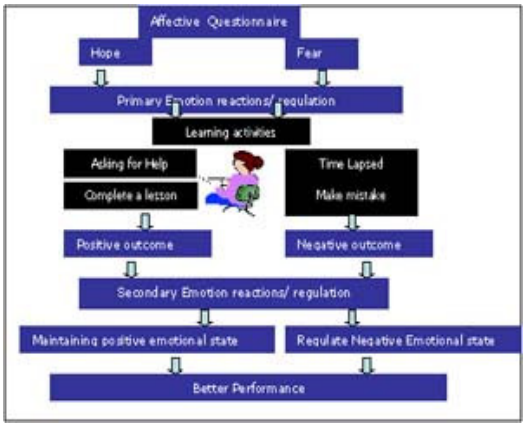


Figure 1: A Sound Emotionally Affective framework

References

1. Brown, J and Burton, R.R (1975), *Multiple Representation of knowledge for tutorial reasoning,* In Bobrow, D.G and Colin A., Editors, Representation and Understanding, page 311-349. Academic Press, New York
2. Goleman, D 1996, Emotional *Intelligence: Why It Can Matter More Than IQ* Bloomsbury Publishing Plc.
3. Fredrickson, L,. B. : *What Good are Positive Emotion ? (1998)*: Review of General Psychology, Vol 2, 300-319.
4. Roseman,J.I., Antoniou,A.A., Jose, E.P, : *Appraisal Determinants of Emotions: Constructing a More Accurate and Comprehensive Theory* : Cognition and Emotion (1996), 10(3), 241-277.