the continuum partners limited

Capital Markets CRC Limited

## Game theory deployed in defense against network foe, SPAM.

**20 August, 2013 (Sydney):** Researchers at the Capital Markets Cooperative Research Centre (CMCRC), the Australian independent academic centre for capital market research, have developed a spam classifier that outperforms the current model employed in email applications using a totally new model based on repetitive game theory.

The new spam classifier, developed by Professor Sanjay Chawla, Fei Wang CMCRC PhD candidate and Wei Liu (a former CMCRC PhD student) at University of Sydney, outsmarts would-be spammers by predicting their future attempts by learning from past attacks.

Professor Sajay Chawla explains "Typical spam filters make more mistakes over time as the spammers work out how to get around the filter. An example of this is spammers using misspelt words in the title. We have anticipated this adversarial behaviour resulting in a more accurate filter that deteriorates at a much slower rate than current filters would. This means the filter doesn't need to be upgraded as often reducing the cost, time and disruption associated with upgrading software."

A version of the research has been published in the prestigious Machine Learning Journal making this knowledge available to the software development industry including companies like Google, other telecommunication companies as well as organisations with a specific security requirement.

Fei Weng says "Modelling the interaction between a classifier and an adversary as a repeated game theory setting is a far more realistic way of getting training data for the classifier because it allows for cause and effect behaviour to be captured. We look for a compromise solution, or equilibrium, where no party wants to deviate from the situation they are in. The classifier is then trained using this equilibrium position. This approach is both more robust and economical that previous methods. We are now investigating ways of integrating sparse learning methods to make the classifier even more robust against adversarial manipulation."

This technique can be applied to many situations wherever there is some motivation for one party to get an advantage over another such as trading and cyber security and has also been used by Fei Wang for analysis of health insurance claims. Game theory is used extensively in economics and politics today to analyse and predict decision-making and is now being applied to new areas like computer science and data mining.

***For copies of the full study and interviews with Prof Sanjay Chawla:***
Kathryn Hartman, The Continuum Partners
khartman@thecontinuumpartners.com +61 419 238 019

**About Sanjay Chawla:**

Sanjay Chawla is the Professor of Pattern and Data Mining at the University of Sydney, Australia. In 2012, he was an Academic Visitor in the Advertising Science group at Yahoo! Labs, Bangalore, India. He served as the Head of School (Department Chair) of the School of Information Technologies from 2008 to 2011. During 2005-06, he served as the Chief Scientist of DTecht, a start up in health insurance surveillance software.
He serves on the editorial board of IEEE TKDE and Data Mining and Knowledge Discovery and has been a member of program committee’s of leading data mining conferences. He has co-authored a textbook: Spatial Databases, A Tour (Prentice Hall, 2003) which has also been translated into Chinese and Russian. Sanjay's recent research emphasis is on outlier detection, imbalanced classification and adversarial learning. His research has been recognized by five best paper awards (most recently in 2012). He received his PhD in Mathematics (1995) from the University of Tennessee, Knoxville.

**About CMCRC:**

The *Capital Markets Cooperative Research Centre* is a world-leading research organisation that provides thought leadership and break-through technology solutions for capital and health markets (www.cmcrc.com). It is funded equally by the Australian Government, an alliance of University partners and industry partners including, regulators, exchanges and market participants across 10 countries. Research is funded from pooled funding and not sponsored by individuals, companies or institutions. To address its prime goal of industry relevance, industry partners have a major role in the research questions the CMCRC addresses. Academics have primary control over the research design and therefore the results.