There is one particular wall posing on my Facebook account which always seems to make me stop and daydream. It is a post from my friend Debbie, or should I say, it is actually her automatic Nike application which ‘posts’ telling me when she is starting her run and when she has finished. All her friends can then monitor her times and actual distance run. We also have the option of sending her messages as she runs...as if...

Anyhow, I am aware of course for years about such devices/gadgets/gps apps from the fitness world - but it is the integration of this particular application which always makes me think of futuristic scenarios when we can tag other everyday chores and actions around the house. What if the vacuum cleaner has a network connection and broadcasts to the world whenever we clean, “Kevin Curran has started to vacuum the kitchen...Kevin Curran has started in the hallway...Kevin Curran has emptied the vacuum cleaner” or “Kevin Curran has filled the cats dish...Kevin Curran has broken the vase....Kevin Curran has finally taken a bath”...OK, we get the message. I guess what I wanted to bring into this commentary is that data - even innocuous data such as this - even if we do not post it to social networking sites might actually be beneficial. I mean what would you call embedding a sensor in everyday objects? It really is a form or embedded business intelligence. Now that term is overloaded in many ways but such embedded “broadcasting of activity” could if the right analytical tools/processes are applied - perhaps lead to addressing any inefficiencies in our life. Perhaps such data mining might really discover that we run our lives inefficiently. By embedding activity monitoring into our everyday objects, perhaps we can indeed enrich our everyday lives.

So, onto issue 2 of volume 3 and the paper “SYLPH: A Platform for Integrating Heterogeneous Wireless Sensor Networks in Ambient Intelligence Systems” by Alonso, Tapia, and Corchado. The significance that Ambient Intelligence (AmI) has acquired in recent years requires the development of innovative solutions. In this sense, the development of AmI-based systems requires the creation of increasingly complex and flexible applications. The use of context-aware technologies is an essential aspect in these developments in order to perceive stimuli from the context and react upon it autonomously. Here, the authors present SYLPH, a novel platform that defines a method for integrating dynamic and
self-adaptable heterogeneous Wireless Sensor Networks (WSN) which ultimately facilitates the inclusion of context-aware capabilities when developing intelligent ubiquitous systems, where functionalities can communicate in a distributed way.

The paper, “The Role of Augmented Reality Within Ambient Intelligence” by Curran, McFadden, and Devlin seeks to provide an up to date view of the Augmented Reality field and its potential impact in the ambient intelligence arena. Augmented Reality (AR) is a technology which provides the user with a real time 3D enhanced perception of a physical environment with addition virtual elements either virtual scenery, information regarding surroundings, other contextual information and also capable of hiding or replacing real structures. With Augmented Reality applications becoming more advanced the ways the technology can be viably used is increasing. Augmented Reality has been used for gaming several times with varying results. AR systems are seen by some as an important part of the ambient intelligence landscape. This paper therefore presents several types of augmentation applications of AR in the domestic, industrial, scientific, medicinal and military sectors which may benefit future ambient intelligent systems.

Walsh, Barton, O’Flynn, Hayes, and O’Mathuna, and Mohammad in their paper “An Antiwindup Approach to Power Controller Switching in an Ambient Healthcare Network” propose a methodology for improved power controller switching in mobile Body Area Networks operating within the ambient healthcare environment. The work extends Anti-windup and Bumpless transfer results to provide a solution to the ambulatory networking problem that ensures sufficient biometric data can always be regenerated at the base station. The solution thereby guarantees satisfactory quality of service for healthcare providers. Compensation is provided for the nonlinear hardware constraints that are a typical feature of the type of network under consideration and graceful performance degradation in the face of hardware output power saturation is demonstrated, thus conserving network energy in an optimal fashion.

The paper “Investigating Cybercrimes that Occur on Documented P2P Networks” by Scanlon, Hannaway, and Kechadi details how Peer to Peer (P2P) systems can be used or exploited to aid in the execution of a large number of online criminal activity, e.g., copyright infringement, fraud, malware and virus distribution, botnet creation and control. P2P
technology is perhaps most famous for the unauthorised distribution of copyrighted materials since the late 1990’s, with the popularity of file-sharing programs, such as Napster, etc. In 2004, P2P traffic was accounted for 80% of all Internet traffic and in 2005, specifically BitTorrent traffic accounted for over 60% of the world’s P2P bandwidth usage. This paper outlines a methodology for investigating a documented P2P network, BitTorrent, using a sample investigation for reference throughout.

Finally, the paper “Development and Evaluation of a Dataset Generator Tool for Generating Synthetic Log Files Containing Computer Attack Signatures” by O’Shaughnessy and Gray outlines how a key requirement for experimental analysis in the areas of network intrusion and computer forensics is the availability of suitable datasets however, the inherent security and privacy issues surrounding these disciplines have resulted in a lack of available “test-bed” datasets for testing and evaluation purposes. Typically, the datasets required in these cases are from system log files, containing traces of computer misuse. Therefore, there is obvious potential for the use of synthetically generated log files that can accurately reproduce these traces or patterns of misuse. This paper discusses the development, testing and evaluation of a dataset generator tool, designed to produce such datasets, particularly those containing patterns of common computer attacks.

Kevin Curran
Editor-in-Chief
IJACI