Editorial Preface

Is this the Year of Near Field Communications

Kevin Curran, University of Ulster, UK

Near Field Communication (NFC) is a technology that enables a device to communicate with another at a maximum distance of around 20cm or less. Currently, mobile phone manufacturers, financial organisations and mobile network providers are attempting to apply this technology to Smartphones and other handheld devices because of the opportunity to enable the consumer to use commercial services more easily.

As more phone manufacturers start to include NFC chips in their mobiles, the need for applications will increase. Already marketers are looking at the possibilities of using the NFC interface alongside their traditional marketing methods such as posters. Information could also be passed to the NFC device, allowing the user to gain more information about a product or service, so this would be an efficient means of advertising. For example, it would be possible to transmit a URL to the target device so that the user would then be able to navigate to a website to get further information about a product or service in which they are interested. This is where having NFC enabled on a smartphone could prove to be very useful for consumers, enabling them to find out the best price for a product before committing to the purchase. There are many uses for NFC. They can also be used to transfer tokens at airports, which would eliminate the need for boarding cards. The passenger would check-in using their mobile and then re-confirm by swiping their phone again at the departure gate. There is also the possibility of them being able to store biometric information, which is becoming more widely developed for security.

NFC devices can be used in conjunction with image display devices like digital photo frames for displaying images very quickly. All the user needs to do is touch the photo frame with the image ready to be sent, then the connection is established and the image is sent over Bluetooth. NFC is backward compatible with RFID therefore it is perfectly feasible to use an NFC enabled device as an RFID key. This can be used with traditional RFID access control systems as a replacement for the key fobs and cards currently used. Wireless car keys using NFC are being developed by BMW with personalised settings stored into each key. They have developed an NFC car key system which will link into the cars current navigation system which already allows for hotel reservation, and train ticket booking. Using NFC the tickets and reservations can now be stored on the NFC card which can then in turn be used to gain access to the hotel room or validate the ticket with the conductor. Applications for smartphones are starting to appear that allow the user to create their own NFC tags; an application that was developed and is being distributed for free is NXP TagWriter for the Android smartphone. The application uses the NFC enabled phone to send a signal to write contact details, URLs and SMS messages onto an NFC enabled tag which can be on items like business cards up to posters.

NFC AND WINDOWS 8

Microsoft's upcoming Windows 8 operating system (OS) will include built-in NFC functionality. Although Microsoft has yet to set a date for the product's release, the company reports that the new system will include an NFC function known as "tap to share," enabling Windows 8 PCs, laptops or tablets to support NFC RFID readers. In that way, the firm indicates the computing world will join a limited number of mobile phones that are NFC-compatible, acting as 13.56 MHz passive NFC readers and writers that can interrogate tags and capture as well as send data wirelessly when within range of those tags. Microsoft have recently released a Developer Preview build of Windows 8, known as Build 8102, for software and hardware developers to download and begin working with.

The tap-to-share application includes software and driver files to enable the use of a plugged- or built-in NFC reader in order to receive or transmit information to or from another device, such as an NFC tag, an NFC-enabled phone or another NFC-enabled computer running Windows 8. With Windows 7, on the other hand, a user can connect an NFC reader to a computer, but additional software and a driver, supplied by the reader manufacturer or a third party, are necessary to capture and interpret data transmitted to that reader. During its Build conference, Microsoft demonstrated the tap-to-share application by means of an NFC-enabled tablet computer loaded with an early version of Windows 8. In response to Microsoft's new OS plans, chip manufacturer NXP Semiconductors has announced that its PN544 NFC radio controller is compatible with the new operating system. In fact, NXP provided the NFC technology used on Windows 8-based tablets distributed at the conference, enabling the computers to not only read and encode NFC RFID tags, but also support peer-to-peer and card-emulation functions specified by NFC standards developed by the NFC Forum.

The use of Near Field Communication will grow as NFC support in Windows 8 should spur the new community of developers and end-product manufacturers to create new applications. NFC's use in personal devices which may now include tablets and laptops, as well as mobile phones should enable brick-and-mortar stores to link their products with the Internet.

GOOGLE WALLET

Google Wallet (http://www.google.com/wallet) is an Android app that makes your phone your wallet. It is primarily aimed at the payments market as it stores virtual versions of your existing plastic cards on your phone. It works however by people tapping their phone to pay and redeem offers using near field communication (NFC). It is just being rolled out around the world. Google Wallet has been designed for an open commerce ecosystem. It aims to eventually hold many cards people keep in their leather wallet today. Because Google Wallet is a mobile app, it will be able to do more than a regular wallet ever could, like storing thousands of payment cards and

Google Offers but without the bulk. Google hope that eventually our loyalty cards, gift cards, receipts, boarding passes, tickets, even our keys will be seamlessly synced to our Google Wallet. Every offer and loyalty point will be redeemed automatically with a single tap via NFC. The vast majority of phones however do not support NFC but Google believe that NFC will be surging in popularity over the next couple of years, and for the time being this is really a first step. Google also has a plan to enable older devices to use a more limited version of the app - stickers that you can put on the back of your phone.

Google is a little vague to date on this but it seems the plan is that users will be able to obtain special NFC stickers with a single credit card associated with them (such stickers already exist, but these stickers will apparently be able to communicate with the Google Wallet app). Transactions made using the sticker will be relayed to the Wallet application on an Android device via the cloud. It is possible this functionality will be extended to other platforms as well, as Google says it is willing to partner with everyone to help broaden support for Google Wallet. Google Wallet is now released on the Nexus S 4G by Google. It is possible that there may be real opportunities in the ambient intelligence arena to use the NFC on the Google phones to provide added value and services. The obvious feature is knowing the location of people.

NFC SECURITY ISSUES

It is estimated that the market in NFC devices will grow rapidly over the next few years, and with this comes the always-present issue of security. The requirement for the two devices to be close to each other is something that helps with the security of the transaction by limiting eavesdropping. The range of NFC is only a few centimetres. This makes it inherently safer than longer range technologies but there are still security flaws that, if not addressed, can be exploited. NFC is not encrypted and this is to make it backward compatible with RFID technologies. Encryption may be implemented with future NFC applications but only as a best practice, not as a requirement. The wireless signal generated by data transfers can be picked up by antennas, modified, and dispatched. This makes NFC inherently vulnerable to this kind of attack. In active mode where the two devices are communicating, eavesdropping is significantly easier compared to passive mode as the antenna signal gain is lower; therefore the listening range is greatly decreased. It has been found that when in it is easy to successfully eavesdrop from around 30cm. The AES encryption method is developed into a series of NFC security standards to protect against eavesdropping and data manipulation. An NFC skimmer device, similar to the magnetic strip skimmer used in ATM machines could be possible to implement. With a disguised device placed close to the two NFC devices, it would be able to record all NFC activity in a given time and be collected at a later date. NFC is starting to become popular as a form of advertising, where the interested user taps their device onto the advert to view the message, URL or phone number. Fraudsters can take advantage of NFC tags in public places by removing the legitimate tag and replacing it with a tag directing the user to a bogus website of a premium number set up to the fraudsters' account. Using a wireless communication protocol it is inevitable that the data will be prone to attack such as eaves dropping where an attacker could use an antenna to intercept the transmitted signals. It is possible to eavesdrop on the active device from a distance of up to 10m when it is in transmission mode, but this reduces to only 1m when the device becomes passive.

In fact, rather than eavesdropping on the communication, an attacker might instead try to modify the data being transmitted by disrupting the communication by preventing the receiving device from being able to understand the data that is being transmitted from the active device. Another attack is data modification which changes the data that is received rather than preventing the transmission as with the data corruption attack, because the attacker wants to make changes to the data that is being transmitted. Related to this is the possibility of inserting messages into the data exchanged between the two devices, but if the messages overlap, then the data becomes corrupt and the communication fails. Finally a man-in-the-middle type of attack could occur where the two devices are tricked into believing they are communicating directly with each other, when in fact they are communicating through a third party. The two devices are not aware of the third party and so any data exchanged will be accessible to the device in the middle, and hence the name "Man-in-the-middle". However, because of the way that NFC devices use a message and reply protocol, it is deemed virtually impossible to set up a man-in-the-middle attack. This is because it is impossible to align perfectly two RF fields and the attack would be discovered.

Devices using NFC are expected to operate in environments with varying security, some with a high level of security and others that do not need any security. As the NFC Forum has repeatedly stated the technology is 'inherently secure' because of the small transmission distance. The best solution to these security issues is to have a layered security model with a minimum requirement of authentication before the start of communication. Developers can then add higher levels of security according to their application needs. This is not required by the ISO standard but will be essential for making money from the technology. So there is much room for research into these areas in secure ambient intelligent Near Field Communications.

So, onto the contents of Vol 4., No. 1 of IJACI. Cinque, Coronato, and Testa in "Dependable Services for Mobile Health Monitoring Systems" posit that the design and realization of health monitoring systems has attracted the interest of large communities both from industry and academia. Remote and continuous monitoring of patient's vital signs is the target of an emerging business market that aims both to improve the quality of life of patients and to reduce costs of national healthcare services. Such applications, however, are particularly critical from the point of view of dependability and in this paper and in this paper the authors present the design of a set of services for the assurance of high degrees of dependability to generic mobile health monitoring systems. The design is based on the results of a detailed failure modes and effects (FMEA) analysis, conducted to identify the typical dependability threats of health monitoring systems and ultimately allowing them to comprehend a set of configurable monitoring services, enriching the system with the ability to detect failures at runtime, and enabling the realization of dependable services for future mobile health monitoring systems.

In a "Rule-Based Approach to Automatic Service Composition" Santofimia, del Toro, Villanueva, Barba, Moya, and Lopez begin by stating that the incapability to foresee or react to all the events that take place in a specific environment supposes an important handicap for Ambient Intelligence systems, expected to be self-managed, proactive, and goal-driven. Endowing such systems with capabilities to understand and reason about context, seems like a promising solution to overcome this hitch. Supported on the service-oriented paradigm, composing rather than combining services provides a reasonable mean to implement versatile. This paper describes how systems for Ambient Intelligence can be improved by combining automatic service composition and reasoning capabilities upon a distributed middleware framework.

"Man in the Browser Attacks" by Dougan and Curran introduces Man-in-the-Browser attacks which are a sophisticated new hacking technique associated with Internet crime, especially that which targets customers of Internet banking. The security community has been aware of them as such for time but they have grown in ability and success during that time. These attacks are a specialised version of Man-in-the-Middle attack, and operate by stealing authentication data and altering legitimate user transactions to benefit the attackers. This paper examines what Man-in-the-Browser attacks are capable of and how specific versions of the attack are executed, with reference to their control structure, data interaction techniques, and methods for circumventing security. Finally they discuss the effectiveness of counter-Man-in-the-Middle strategies, and speculate upon what these attacks tell us about the Internet environment.

The paper "Sounds Relaxing–Looks Cool: Audio and Visual Selections for Computer Systems that Support Wellness" by Cunningham and Picking considers the design of audio and visual user interface elements for pervasive computer systems that aim to support wellness, specifically for promoting calm, relaxation and for the relief of emotional stress. Their methodology included conducting a survey of people's favourite everyday sounds, as well as those they found the most annoying. They then took the most popular of these and correlated them with colours that people associated with those sounds. An adapted repertory grid approach was used for this exercise. The results suggest there is potential for a classification of sound and emotion on a shared scale based on the colour spectrum.

Finally, in "The Pursuit of Flow in the Design of Rehabilitation Systems for Ambient Assisted Living: A Review of Current Knowledge" by Middleton and Ward, key sources on the science of engagement and immersion, in particular the concept of flow are gathered together. Flow is a psychological description for full immersion in an activity. It provides a useful framework within which to understand the coupling between pervasive computing and end users. The article discusses the concept of flow in a general psychological sense and extracts those features relevant to gaming, and in particular the human-computer interaction (HCI) aspect of such systems. The requirements for achieving flow such as reward, situational control, feedback and clarity of purpose as applicable to a pervasive computing environment are discussed in detail. The primary application focus of flow in this paper lies in the area of ambient-assisted living solutions for rehabilitation purposes. In the context of using virtual environments to aid in skill training or medical rehabilitation, dynamic difficulty adjustment (DDA) and enjoyment are two key elements used to create a fully immersive experience. This paper both reviews the techniques for creating these elements and describes possibilities for harnessing related methods as evaluation techniques for immersion in HCI-based rehabilitation environments, which may offer an alternative to current survey-based mechanisms.

Kevin Curran
Editor-in-Chief
IJACI

Kevin Curran BSc (Hons), PhD, SMIEEE, FBCS CITP, SMACM, FHEA is a Reader in Computer Science at the University of Ulster and group leader for the Ambient Intelligence Research Group. His achievements include winning and managing UK & European Framework projects and Technology Transfer Schemes. Dr. Curran has made significant contributions to advancing the knowledge and understanding of computer networking and systems, evidenced by over 650 published works. He is perhaps most well-known for his work on location positioning within indoor environments, pervasive computing and internet security. His expertise has been acknowledged by invitations to present his work at international conferences, overseas universities and research laboratories. He is a regular contributor to BBC radio & TV news in the UK and is currently the recipient of an Engineering and Technology Board Visiting Lectureship for Exceptional Engineers and is an IEEE Technical Expert for Internet/Security matters. He is listed in the Dictionary of International Biography, Marquis Who's Who in Science and Engineering *and by* Who's Who in the World*. Dr. Curran was awarded the Certificate of Excellence for Research in 2004 by Science Publications and was named Irish Digital Media Newcomer of the Year Award in 2006. Dr. Curran has performed external panel duties for various Irish Higher Education Institutions. He is a fellow of the British Computer Society (FBCS), a senior member of the Association for Computing Machinery (SMACM), a senior member of the Institute of Electrical and Electronics Engineers (SMIEEE) and a fellow of the higher education academy (FHEA). Dr. Curran's stature and authority in the international community is demonstrated by his influence, particularly in relation to the direction of research in computer science. He has chaired sessions and participated in the organising committees for many highly-respected international conferences and workshops. He is the Editor-in-Chief of the* International Journal of Ambient Computing and Intelligence *and is also a member of 15 Journal Editorial Committees and numerous international conference organising committees. He has served as an advisor to the British Computer Society in regard to the computer industry standards and is a member of BCS and IEEE Technology Specialist Groups and various other professional bodies.*