Initial Project Report - RFID

The subject of the project is the use of RFID (Radio Frequency Identification Technology)....a technoogy that while in some ways is relatively 'old' (appearing in more primitive form in the late 1960's), has in the last few years, and particularly the last year, been 'on the move' as far as technological advancements and practical possibilies for it's use are concerned. The possible impending widespread use of the technology has many implications on both the business and social arenas. The aim of our project is to examine the nature of RFID, and look at the issues and consequences involved in it's use in a general context, and thereafter focus on a particular application field.

PART 1

What is RFID?

RFID is one of many technologies that fall under the description 'auto identification', whereby machines can identify objects, for example through automised data capture techniques. Other 'auto identification' technologies include bar codes, smart cards, some biometric technologies (eg retinal scans), and optical character recogniton, to name a few.

RFID is a generic term, encompassing technologies that make use of radio waves to automatically identify individual items The most common method used in RFID is to store a serial number (often referred to as an EPC ..Electronic Product Code..) and possibly other additional information on a microchip that has an antenna attached (together they are referred to as a 'transponder' or 'tag'). A RFID system comprises these tags, and 'readers', which transmit a radio signal that is picked up by the tag(s), and in response a signal carrying the stored data is sent back to the reader.

Why use RFID?

The technology has a myriad of potential uses, and also perceived 'benefits' in terms of cost reductions, data collection, monitoring etc. ('benefits' is quoted since whether they are perceived as benefits depends on the point of view of those involved in, or affected by, it's use ....as shall be discussed later).

Through the use of RFID to auto identify objects, data concerning the monitoring and management of the movement (and/or interaction) of items (and/or people) has the potential to be available much faster, and in more accurate and precise form. This principle can be used in a vast number of application fields, as mentioned. Some of these are discussed later.

RFID can be seen to have some advantages over other auto identification technologies, in that it is not line-of-sight dependant, is a 'contactless' technology, and there can be increased distance between the items being identified and the device doing the 'reading' (depending on the type of RFID system used). Radio waves can travel through most non-matallic materials, and as such tags can be placed in protective coatings and even inserted within material/organic structures, allowing for greater durability, reliability and flexibility with regard to potentially destructive environments. The amount of data that can be stored using tags can be significantly higher than other technologies, for example bar codes.

Until recently, any perceived benefits for those considering implementing RFID were often countered by the cost of implementation , and also the technical limitations of the physically available technology. Recent advances in design have meant decreased tag sizes, increased ’performance’ (in terms of data throughput and storage capability), and decreasing tag prices (both production costs and retail prices), and have meant that implementation of the technology has become both more commercially viable and practically viable . For example, passive (see below) tag prices have dropped from over US$1 per tag to around 20 to 30 cents per tag, and prices are expected to drop even further as the production and demand cycle for tags and associated technology begins to gain momentum. Many analysts predict prices around 3 - 5 cents within the next five years or so[1] . Active tags (see below) are much more expensive, typically US$50+.

How is RFID implemented?

There are 3 main categories of tags - ’passive’ tags, ’active’ tags, and ’semi-passive’ tags. Passive tags have no battery, and to transmit their data, they use an electrical current that is induced in their antenna by the radio waves sent from the reader. Active tags have a battery as power source, and this allows the tags to transmit their data over much greater distances. Semi-passive tags are a hybrid form, using a battery to power the chips’ circuitry, and the induced power from the radio waves to transmit the data.

Tags typically use a particular radio wave frequency - low frequency (eg.13.56Mhz), high frequency, or ultra high frequency (UHF - typically 868Mhz or 915MHz). The frequency for the tag will also affect it’s ’read range’ (ie the distance form which it can be read) - the higher the frequency the higher the read range. The read ranges for low-frequency tags are typically around 0 - 30 cm, high-frequency around 0 - 90cm, and UHF around 4 meters (active tags can have a higher range because of the battery boosting - perhaps to around 100m) [2] . The size of the chip (and it’s antenna) will also affect range. For example, a "Mu chip" from 2001 (0 .3 mm x 0.3 mm , with antenna 5 -7 cm) has a range <30cm , while a recent antenna -on -chip version (0.3mm x 0.3mm, antenna included) has a range <4mm [3]. Higher frequencies generally mean higher data throughput (for example, reading large volumes of tags close together) than with lower frequencies, but new technology has reportedly [3] started to overcome this problem. Tags have a data storage capacity which can range up to around 8KB, depending on the tag type, but typically they carry about 2KB of data, which is enough to store a serial number and some basic information about the object to which it is attached.

Tags can be read-only, or read-write, but read-write tags are generally too expensive for use on low-value items. Some read-only tags can have been ’pre-programmed’ with some non-erasible information during their manufacture, and can never be overwritten, while a another type of read-only tag actually does allow for overwrite (once only). The latter are called EEPROM tags (electrically erasable programmable read-only memory).

Readers come in many shapes and forms (both stationary and portable), and are often capable of reading at multiple frequencies. Many reader / tag systems are currently proprietary systems and intercompatibility is a big problem. Standards are slowly being proposed (some exist already for very specific applications) but will probably not be widely adopted for some time.

Who uses RFID?

The technology is already in use (to different degrees) by businesses, government agencies, armed forces, and the general public (for example automatic toll-station passing).

Where is RFID used?

The list of potential application fields is endless. Major fields include tracking of items in the transport and logistics industry, and monitoring of supply chains from manufacturing to distribution to salepoint, but there are many more. A (non-exhaustive) list of example applications, to give an idea of the breadth of existing and possible use, is:

- car immobilizer systems (reader in key)
- theft reduction (in retailing/workplace)
- supply planning / preventing out-of-stock situations
- document management (tags placed in business documents to automate logistics systems/processes)
- recovery and identification of stolen items (enabling police to identify items that were stolen from a particular place)
- library operations
- elimination of labor-intensive stocktakes
- tracking animals
- product handshaking eg incompatible items that should not be connected together
- identification/tracking of items/tools (and the item-carriers) under industrial processes (eg painting, assembly of cars etc)
- tags carry information necessary for an items assembly in composite products - read by robots etc
- payment systems eg. Sony and Phillips are developing an RFID system called Near Field Communication (NFC), which will enable RFID communication between PCs, handheld computers, and other electronic devices. Consumers will log on to their personal online portal by using their smart card, embedded with a RFID tag, which will be read by a RFID reader plugged into the USB port on the computer. Consumers can then purchase online, for example a ticket, the information will then be transmitted to an RFID tag in their mobile phone, which they can wave near a reader at the event for automatic admission **.** Visa and Mastercard are also combining smart cards/prepaid cards with RFID chips, allowing contactless transactions , and to help prevent forged cards. [3][4]
- vehicle and terminal management (eg buses and trucks at depots, bus priotory systems to reduce delays for public transport, automatic toll stations etc)
- tags in clothing, for easier tracking in supply chains/sales outlets (eg. washable RFID tags designed to be sewn into clothing. [5]
- counterfeit prevention (eg medications, valuable documents, passports etc. The European central bank has been reported to be considering embedding RFID tags into banknotes, as a means of preventing money-laundering, black-market transactions, and assist automated counting procedures [5])

- automatic transaction recording at waste disposal sites, mines, recycling plants etc
- tracking of people (eg Alexandra Hospital in Singapore recently implemented a tracking system in its accident and emergency department as a result of SARS . All patients, visitors, and staff entering the hospital were issued a card embedded with an RFID chip, which could be read by sensors installed in the ceiling, to record the person's movements (spatially and temporally) in the department. The information is stored for 21 days. The principal aim of the system is that if anyone is later diagnosed with SARS, a record of all other individuals with whom that person has been in contact can be immediately determined. [6] Similarly, tags can be used for additional security for personnel working in high risk areas in case of an emergency evacuation.
- reduction of medication errors and patient safety (eg tags on special syringes, specifying it's specific type, so that computerised infusion pumps can check the administration rate and strength. Such use implies that 100% reliability is required.) [1]
- ticketing, using embedded tags (eg 2006 FIFA World Cup Germany, EXPO Japan, London Transport)
- combining RFID tags with sensors (eg tags used to track items can also alert if the item has experienced undesirable changes/conditions, for example temperature or contamination)
- security control (eg controlling access to buildings etc, using tags in ID cards)
- time/attendance controls (eg replacing 'punch cards')

Issues involved in the use of RFID

Privacy

The issue of personal privacy is perhaps the most prevalent issue related to the use of RFID. The technology allows (perhaps embedded) tags on items to be detected automatically from varying distances,and the prospect of people and their movements, behaviour and activities being monitored (directly or indirectly) through their possession of tagged items leads to a number of concerns over potential impingements on personal privacy (both in the legal and ethical sense).

As the recent advances in the technology have made it's use more prevalent and widespread, it's impact with regard to privacy concerns has also grown. A number of interest groups have been formed as a result, focusing their efforts on the protection personal privacy. Issues raised include scenarios such as the possibility of being tracked or profiled at, and after leaving, the site of purchase. For example, "*Currently, some RFID readers have the capacity to read data transmitted by many different RFID tags. This means that if a person enters a store carrying several RFID tags, for example in articles of clothing or cards carried in a wallet, one RFID reader can read the data emitted by all of the tags, and not simply the signal relayed by in-store products.This capacity enables retailers with RFID readers to compile a more complete profile of shoppers than would be possible by simply scanning the bar codes of products a consumer purchases.*" [6] Such profiles, possibly linked directly to a customers identity, could conceivably also be sold to other organizations, and/or the data used for another purpose than that for which it was originally obtained.

In most countries a court order or similar is required to access/use private data such as phone records, bank/credit card records etc, and the data can only be used in a strictly defined way. Some concerned with privacy have advocated that the legal status of data obtained using RFID should be similar [7][12], although it is conceivable that the misuse of data, both ethically and legally, is still a potential problem.

Other scenarios include criminal use / detection of tags (for example thieves ’scanning’ people or locations to determine potential targets/items for theft), and the possibilty of surveillance by other parties, for example government agencies.

Another concern is the general loss of anonimity with regard to movements and transactions. The psychological aspect of the ever-present possibility of one’s activities and movements possibly being recorded or monitored (in an Orwellian ’Big Brother’ sense) is perhaps significant, although such an aspect would likely vary according to an individual’s background and the society itself. Delegates to a recent Communist Party Congress in China were required to wear an RFID ID-card at all times so that their movements could be tracked and recorded [8] - such monitoring can of course have it’s advantages, but it can also have it’s ’darker’ sides, and may or may not be acceptable in other societies or situations. Recently, Marks and Spencer, Tesco and Benetton reportedly trialled (unknown to the customers) the use of RFID technology in some of their stores, but cancelled the trials after their existence became known and the stores experienced protests and oppositon from interest groups, the public and media. Perhaps in contrast, a survey has reportedly indicated that many US consumers would not be averse to monitored to a certain extent (using RFID in-store) if it meant they could save money and time. [9]

The possibility of bank notes being tagged could be another instance whereby the feeling of anonimity could be eroded - cash transactions would no longer necessarily be anonymous. Similarly, as exemplified in the film ’Minority Report’, your private data could ’follow’ you around and perhaps be used in a public arena, for example advertisements flashing up on screens, based on your spending patterns and ’profile’.

To help deal with the prospect of monitoring via an item’s RFID after leaving the site of purchase, the concept of a ’kill’ mechanism built into tags has been proposed, whereby the tag can be permanently disabled. Such disablement could occur at the point of sale, but whether this is to be done by default, or only if the customer requests it, is an open question, and the policy of each retailer would likely be individual. A potential problem with this approach is the scenario whereby the tagged items will purposely have their tags ’read’ after the purchase. For example, a washing machine might automatically adjust it’s behaviour or give a message depending on the tags on the clothes within it. Similarly, the much-touted ’intelligent refridgerator’ (knowing it’s own contents etc) would be rather ’stupid’ if the tags on it’s contents had already been deactivated. Tags might also useful for categorization for recycling purposes.

Another possible approach is the use of so-called ’blocker’ tags, which are passive RFID tags that ’block’ readers by simulating vast numbers of, or alternatively particular subsets of, possible ID-codes. For example those codes used by a particular manufacturer, or the codes in a dedicated range (ie a so-called ’privacy zone’[10]). ***<blocker tags to be continued..>***

Voluntary self-regulatory frameworks have been proposed by interest groups on both sides of the

RFID fence (both proponents and privacy groups) , and are basically as follows [11]:

1. *The right of the consumer to know what items possess RFID tags*
2. *The right to have tags removed or deactivated upon purchase of these items*
3. *The right of the consumer to access of the data associated with an RFID tag*
4. *The right to access of services without mandatory use of RFID tags and*
5. *The right to know to when, where, and why the data in RFID tags is accessed.*

On a technical note, privacy and monitoring would of course also be affected by the nature of the data stored on tags and whether such data is in any way ’meaningful’ or not (for example, it may be encrypted, or the data may only be meaningful/intelligible to a very limited group eg the item supplier). Thus the possibilties for interpretation and misuse of data would be more limited. Similarly, the read range of the tags would also play a role, with privacy fears perhaps being reduced if the tags can only be read from a very short distance. As far as eavesdopping is concerned, the "*risks can be reduced through the design of appropriate over-the-air protocols and data encryption methods. In addition, the reader changes frequencyrapidly and the eavesdropping reader must follow the main reader exactly. This is very difficult since the hopping sequence is random.*" [12]

Privacy concerns are of course well founded, and need to be addressed. RFID as a technology has a principal objective, and that is to identify and possibly trace entities. As Rhodes [13] says while discussing ubiquitous computing, "*sometimes privacy leaks are inherent in the application itself. For example, an application that shows where a person is on a map has no choice but to reveal that information; that’s its job. Our goal is not to maintain total privacy, but rather to design a system whereby personal data is distributed on a need-to-know basis.*" Technological implementations and societal changes occur, and what people and societies in general are willing to accept (or adapt to), whether consciously or not, is difficult to predict.

Health concerns

<still researching>

Balancing opposing interests

<to be discussed> <janus faces etc>

PART 2

Specific Application Field

<In our project we will be doing a case study looking at the possibilites for a particular application of RFID. Our plan is to examine the situation with regard to Oslo Sporveir / Trafikanten. Currently they have a ticketing system whereby passengers' tickets are only checked on random occasions. Otherwise, passengers are free to enter and use stations and public transport. Different types of tickets (single trip, day cards, week cards, month cards etc) are available. We would like to look at at a number of factors, related to the potential introduction of an RFID enabled ticketing system, for example:

- ***possible benefits eg .***
  - ***cost savings***
  - ***labor savings***
  - ***logistical improvements***
  - ***raffic /passenger flow improvements***
  - ***reduce 'sneaking'***
  - ***possible benefits through easier data collection eg.***
    - ***how many people take a specific route at a certain time***
    - ***which stations are the most used***
    - ***how much time does a train (bus) really takes at certain hours***
    - ***which stops experience most traffic, and when***

- ***possible drawbacks of RFID in the situation eg.***
  - ***increased congestion at entrance barriers***
- ***possible technological hindrances***
- ***is Oslo too small for such a system***
- ***what sort of requirements might need to be met inorder to implement such a system***
- ***why has such a system not already been introduced here***
- ***how the public feels about possible implementation of such a system***

We shall examine and compare some other case examples eg Tokyo, London, Seoul etc. We will try to obtain data about passengers feelings about such a system and it's implications, most likely through active surveys. We shall try and talk to Trafikkanten's administartive director Jarl Eliassen to discuss the theme and obtain his points of view. We aim to examine some possible models of implementation. In addition we aim to include more references to the course articles, where relevant.>

REFERENCES

[1] IDTechEx Web Journal: Smart Labels Analyst , Issue27 , april2003
http://www.idtechex.com/documents/en/

[2] RFID Journal - FAQ
http://www.rfidjournal.com/article/articleview/207

[3] IDTechEx Web Journal: Smart Labels Analyst , Issue32 , september2003
http://www.idtechex.com/documents/en/

[4] 'RFID Chips Are Here' , Scott Granneman 27/06/2003
http://www.theregister.co.uk/content/archive/31461.html

[5] 'RFID tags: Big Brother in small packages' , Declan McCullagh 13/1/ 2003
http://news.com.com/2010-1069-980325.html

[6] Electronic Privacy Information Centre - Radio Frequency Identification (RFID) Systems
http://www.epic.org/privacy/rfid/

[7] Surpriv: RFID Surveillance and Privacy
http://www.stapleton-gray.com/surpriv/archives/000016.html

[8] 'RFID Devices and Privacy', Junkbusters.com
http://www.junkbusters.com/rfid.html

[9] RFID: 'You know you want it', Jo Best 7/1/ 2004
http://www.silicon.com/management/government/0,39024677,39117651,00.htm

[10] 'The Blocker Tag : Selective Blocking of RFID tags for Consumer Privacy'
Ari Juels, Ronald Rivest, Michael Szydlo, MIT and RSA Laboratories
http://theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.pdf.

[11] "Interaction of RFID TechnologyAnd Public Policy", Rakesh Kumar ,
WiproTechnologies, India 2003
http://www.rfidprivacy.org/papers/kumar-interaction.pdf.

[12] AIM RFID Privacy Work Group - FAQ
http://www.aimglobal.org/technologies/rfid/rfid_faqs.asp

[13] 'Wearable Computing Meets Ubiquitous Computing: reaping the best of both worlds'
Rhodes BJ, Minar N and Weaver J, 1999. Symposium on wearable computing.
http://www.media.mit.edu/~rhodes/Papers/wearhive.ps.