New Directions in Advanced RFID Systems

DISSERTATION SUBMITTED TO

THE SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING

OF THE UNIVERSITY OF ADELAIDE

BY

Damith Chinthana Ranasinghe

IN FULFILMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

January 2007

Abstract

A combination of Radio Frequency Identification technology and ubiquitous computing are revolutionising the manner in which we look at simple objects. Radio Frequency Identification (RFID) allows RFID labeled objects to be identified at a distance without physical contact, and ubiquitous computing provides a virtually connected environment for the objects. RFID labels are frequently referred to as the next generation barcodes.

RFID Systems provide increased productivity, efficiency, convenience and many advantages over bar codes for numerous applications, especially global supply chain management.

RFID labeling has a number of advantages over conventional bar code systems. The optics based bar code systems could be rendered useless by common everyday environments containing dirt, dust, smoke, grease, condensation and by misorientation and misalignment. Furthermore bar codes are subject to fraudulent duplication and counterfeiting with minimal effort.

However, there are limitations and constraints inherent to RFID technology: semiconductor thresholds, limits on transmitted power, costs, antenna and coupling inefficiencies. Thus it is important for RFID designers to understand these limitations and constraints in order to optimise system designs and overcome inefficiencies where possible. Therefore the work presented in this dissertation seeks to improve the performance of advanced RFID systems by overcoming a number of these limitations.

Prior to a discussion of improving performance, the author's interpretation of a modern RFID system along its evolutionary path as a ubiquitous RFID network and its application to supply chain management is described. Performance improvements are achieved by: the development of electromagnetic theory for RFID system analysis and optimisation; design and development of interrogator antennas; analysis of electrically small and tiny antennas for RFID labels; and development and utilisation of a design methodology for creating high performance label antennas and antennas for tagging metallic objects.

Implementations of RFID systems have raised concerns regarding information security and possible violations of end-user privacy. The most profound concerns are raised against low cost RFID technology because of its potential for mass scale deployment, its pervasive nature, and the resource limitations preventing the provision of strong cryptographic solutions. There is a growing need in the RFID community to discover and develop techniques and methods to overcome various hurdles posed by the above-mentioned concerns.

Thus, the thesis also considers the vulnerabilities of low cost RFID systems and associated insecurities and privacy concerns resulting from the latter. Prior to addressing such concerns impeding the deployment of low cost RFID technology, a framework within

which to provide security services is also detailed. It has become important to both define and identify a framework based around low cost RFID systems since RFID has become a "catch all" phrase for various other forms of technology.

Addressing security and privacy of low cost RFID systems requires novel thinking. The later parts of the thesis outline design considerations for security mechanisms and a number of practicable solutions for providing the features of: mutual authentication; confidentiality; message content security; product authentication; anonymity and untraceability, that are necessary for low cost RFID systems to overcome the weaknesses identified in this dissertation. Implementing these security mechanisms requires the generation of true random tag parameters and true random numbers. Achieving these objectives using a hardware based true random number generator is also described and analysed.

A final part of the thesis focuses on active RFID labels and improving their performance. The primary concern with active labels is the life of the onboard battery. Turn-on circuits provide a method of turning "on" and "off" an active label remotely to conserve valuable battery power. Analysis, development and testing of a turn-on circuit concept, based on interrogator field sensing, have provided a means of remotely activating and deactivating active RFID labels and conserving battery power. The final chapter of this thesis provides a detailed analysis, based on coupling relations between electromechanical systems, for evaluating the feasibility of a theft detection sensor, based on a turn-on circuit for an active RFID label, for preventing the theft of high value items.

While low cost RFID needs to overcome certain security and privacy related barriers, RFID technology does provide novel and valid approaches to such security related applications as product authentication, anti-counterfeiting and theft detection. It is believed that the contributions from this thesis will extend and elaborate on the existing knowledge base, paving the way forward to allow further significant deployment of advanced RFID technology.

CONTENTS