# User-Centred and Context-Aware Identity Management in Mobile Ad-Hoc Networks

# User-Centred and Context-Aware Identity Management in Mobile Ad-Hoc Networks

By

Abdullahi Arabo

CAMBRIDGE SCHOLARS

PUBLISHING

User-Centred and Context-Aware Identity Management in Mobile Ad-Hoc Networks,
by Abdullahi Arabo

This book first published 2013

Cambridge Scholars Publishing

12 Back Chapman Street, Newcastle upon Tyne, NE6 2XX, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library



ISBN (10): 1-4438-4796-8, ISBN (13): 978-1-4438-4796-4

Amin Arabo
&
Family

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF ACRONYMS

| | |
|---|---|
| AI | Artificial Intelligence |
| AWDS | Ad-hoc Wireless Distribution Service |
| CBAC | Context Based Access Control |
| CI | Context Information |
| CIA | Confidentiality, Integrity and Availability |
| CID | Corporate Identity |
| CoI | Community of Interest |
| CP | Context Provider |
| CPU | Central Processing Unit |
| CR | Context Requestor |
| CS | Context Server |
| CSMA/CA | Carrie Sense Multiple Access/Collision Avoidance |
| DSTL | Defence Science and Technology Laboratory |
| EMD | Emergency Medical Dispatch |
| ESA | Enhance Situation Awareness |
| ESN | Electronic Serial Numbers |
| FTP | File Transfer Protocol |
| GloMo | Global Mobile |
| GPS | Global Positioning System |
| GUI | Graphical User Interface |
| HCI | Human Computer Interaction |
| ICT | Information Communication Technology |
| IdPs | Identity Providers |
| ID | Identity |
| IETF | Internet Engineering Task Force |
| IM | Identity Management |
| IMEI | International Mobile Equipment Identity |
| IMMANets | Identity Management in Mobile Ad-hoc Networks |
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| ISO | International Standards Organization |
| MATTS | Mobile Agent Topology Test System |
| MANets | Mobile Ad-hoc Networks |
| MEID | Mobile Equipment Identifiers |
| MoD | Ministry of Defence |
| NHS | National Health Service |

| | |
|---|---|
| NTDR | Near-Term Digital Radio |
| NTP | Network Time Protocol |
| OS | Operating System |
| OSI | Open Systems Interconnection |
| P2P | Peer-to-Peer |
| PARC | Palo Alto Research Centre |
| PCBone | Pervasive Computing Bone |
| PC | Personal Computer |
| PDA | Personal Digital Assistant |
| PEG | Parsing Expression Grammar |
| PID | Personal Identity |
| PRNET | Packet Radio Networks |
| PKI | Public Key Infrastructure |
| RBAC | Role Based Access Control |
| RFID | Radio Frequency Identification |
| SID | Social Identity |
| SIM | Subscriber Identity Module |
| SMTP | Simple Mail Transfer Protocol |
| SoS | System of Systems |
| STVN | Segment-Tree Virtual Network |
| SSA | Secure Situation Awareness |
| SURAN | Survivable Adaptive Radio Networks |
| TCP | Transfer Control Protocol |
| TDMA | Time Division Multiplex Access |
| UCIM | User-centred and Context-aware Identity Management |
| UDID | Unique Device Identifier |
| UDP | User Datagram Protocol |
| UI | User Interface |
| XML | Extensible Mark-up Language |

# EPIGRAPH

A book presented on the security issues of Identity Management in Mobile Ad-hoc Networks, considering the issues and utilisation of contextual information, user-centricity and user control in a new User-centred and Context-aware Identity Management (UCIM) Framework.

# ABSTRACT

The emergent notion of ubiquitous computing makes it possible for mobile devices to communicate and provide services via networks connected in an ad-hoc manner. The network is becoming more versatile as a result of the availability of various computing resources and communication technologies as well as the increasing use of mobile handheld devices within business and individual contexts. These devices are now essential tools that offer competitive business advantages in today's growing world of ubiquitous computing environments. These have resulted in the proliferation of wireless technologies such as Mobile Ad-hoc Networks (MANets), which offer attractive solutions for services that need flexible setup as well as dynamic and low cost wireless connectivity. However, the growing trend outlined above also raises serious concerns over Identity Management (IM) due to a dramatic increase in identity theft. The problem is even greater in service-oriented architectures, where partial identities are sprinkled across many services and users have no control over such identities. To tackle these problems, it is essential to allow users to have control over their own identities in MANet environments. So far, the development of such identity control remains a significant challenge for the research community.

In this book, we review some issues of contextual computing, its implications and usage within pervasive environments. The main focus of this book is on the area of identity management in MANets and emergency situations by using context-awareness and user-centricity together with its security issues and implications. Context-awareness allows us to make use of partial identities as a way of user identity protection and node identification. User-centricity is aimed at putting users in control of their partial identities, policies and rules for privacy protection. These principles help us to propose an innovative, easy-to-use identity management framework for MANets. The framework makes the flow of partial identities explicit; gives users control over such identities based on their respective situations and contexts, and creates a balance between convenience and privacy. The book presents our proposed framework, its development and lab results/evaluations, and outlines possible future work to improve the framework.

# ACKNOWLEDGEMENTS

I would like to take the opportunity to express my thanks and gratefulness to the people who have helped and supported me throughout the period of writing this book and doing the research work needed to accomplish the goals of the book. Without their support and contribution, successful completion of my research would not have been possible.

First and foremost, I will like to thank my parents Dr Arabo Sr, Yapendo, Nana Asma'u, Umar Atiku and Hadiza; my wife Halima, my grandparents more especially Alhaji and Hajja; my brothers Amin (the coolest Bro), Abba, Auwal, Hassanu, Ahmed, Usman Abdul-kadir; Mammado, Abdul-Aziz; my sisters Rashida, Nafisa, Aisha, Jamila, Hanifa, and Bahijja.

I would like to express my gratitude to Professor Qi Shi, Professor Madjid Merabti and Dr. David Llewellyn-Jones for their invaluable contributions, continuous support, encouragement, guidance and invaluable suggestions during this research.

# CHAPTER ONE

# INTRODUCTION

*"The most profound technologies are those that disappear. They wave themselves into the fabric of everyday life until they are indistinguishable from it"*
—Mike Weiser, 1991

We once assumed that Personal Computers (PC) would be the main medium of using the Internet and consumption as a device within all sectors of the economy. But currently in most markets the mobile Internet is overtaking the fixed Internet phenomenon. With the continuous growth and development of computer networks, the notion of ubiquitous computing coined by Mark Weiser has received increasing attention. This notion also leads to the proliferation in the usage of Mobile Ad hoc Networks (MANets). However, this evolution faces a barrier in many ways. On the one hand, people want to construct a ubiquitous network to make the best use of computers. On the other hand, they must secure their network, protect their identity information and be in full control of their information, in order to deal with a number of security threats from malicious entities. One solution for this is to provide a framework that will offer the users with such abilities in an efficient, dynamic and lightweight format, allowing users to be in full control of the system so as to minimise or eliminate relevant security threats.

The main focus of this book is a combined study of identity management, context-awareness and user-centricity together with their security issues and implications in MANets and emergency situations where different systems need to interact in an ad hoc manner. The emergent notion of ubiquitous computing makes it possible for mobile devices to communicate and provide services via networks connected in an ad hoc manner. The use of contextual information in ad hoc environments can extensively expand the adaptation and usage of such applications. Context is information that can be used to characterize situations or an entity that is considered relevant in the interaction process of a user or an application. Context-awareness allows us to make use of partial identities

as a way of user identity protection and node identification. This is coupled with user-centricity that aims to put users in control of their partial identities, policies and rules for privacy protection. These principles help us to propose an innovative, easy-to-use identity management framework for MANets. The framework makes the flow of partial identities explicit, gives users full control over such identities based on their respective situations and contexts, and creates a balance between convenience and privacy. The book presents the development of the proposed framework and its methodologies, and outlines some possible future work to improve the framework.

This chapter is organized as follows. The topic of the book and background information is presented. Next, the aims and objectives of the book are stated. Then, the novel contributions of the approach hypothesized in the book are summarised. Next, a brief summary of our methodology is presented. Next, an overview of the chapters of the book is provided. Then, the chapter is summarized.

## 1.1 Background

With the emergence and development of wireless networks, the notion of "Ubiquitous Computing" coined by Mark Weiser (Weiser 1999) has received increasing attention. One of the fundamental building blocks for such ubiquitous computing applications is MANets, which is increasingly used to support mobile and dynamic operations such as emergency services, disaster relief and military networks. MANets can be defined as a platform or a set of nodes that can move freely and establish a transient self-configuring wireless network. A MANet offers a temporary network without relying on any predetermined network infrastructure, and communicates in a self-organising manner. Moreover, MANets play curial roles in many application areas such as surveillance, marketing and the military.

While bringing huge benefits to these applications, they also raise serious privacy/security concerns, more specifically on the protection of users' private information and identity.

Users currently rely on numerous forms of identities to access services via MANets. The inconvenience of processing and using these identities creates significant security vulnerabilities as well as significant user discomfort, including the disclosure of personal information. These growing trends have raised serious concerns over identity management (IM) due to a dramatic increase in identity theft (Mercuri 2006; Bertino, Paci et al. 2009). IM in this context is about managing relevant digital

identities of users and ensuring that they have fast, reliable and secure access to distributed resources and services via MANets within ubiquitous computing environments.

Ubiquitous computing has the capability of providing computational environments that facilitate the provision of information through the use of "invisible interfaces" and allowing limitless sharing of information. If developed properly, ubiquitous computing could offer invaluable support for many aspects of our society and its institutions. However, neglecting the above mentioned security or privacy issues and aspects such as proper integration of contextual data, use of efficient user control and centricity, and the adaptation of relevant access control policies can present a great likelihood that the end products will resemble an Orwellian nightmare (Andersson, Martucci et al. 2008).

## 1.2 The Book's Aims and Objectives

The main goal of this book is to develop interoperability among different IM techniques and to propose a User-centred and Context-aware Identity Management framework (UCIM) for fulfilling such interoperability in MANets. The key objectives of the research are to make the proposed UCIM efficient, user-centred, context-aware and lightweight so as to meet the specific needs of MANets. Context-awareness allows us to make use of partial identities as a way of user identity protection and node identification. User-centricity is aimed at putting users in control of their partial identities, policies and rules for privacy protection. On the other hand, a UCIM that is efficiency and lightweight allows the application to be deployed on devices with less memory and fewer processing requirements in order to increase the adaptability and usability of UCIM.

UCIM should possess a number of capabilities. Particularly, it should be able to manage multiple identities for different MANet situations and perform negotiations with other peers about necessary identity information to be used for identification in relation to given security policy settings and situation awareness. UCIM should also be able to provide users with a friendly control over their own identity information and security in terms of mobility across different MANets. Moreover, it should be able to separate users from the complexity of the technical implementation and operation issues of IM in MANets while allowing users to focus on policy aspects of IM. This ability is essential, as users typically do not want to learn detailed security techniques.

## 1.3 The Book's Scope

In this section we briefly highlight the scope of our work by pointing out what it is all about and what we are not covering.

The book covers the following contents:

- Knowledge and information within our field of research.
- Our design of mechanisms for the privacy protection of user information.
- Our definition of user profile types needed for different application scenarios.
- Our design and implementation of a new dynamic policy specification language.
- Our adaptation of XML to make the proposed framework lightweight.
- Our design and implementation of a new algorithm for context filtering based on user policies and contextual information.
- Our development and evaluation of a new identity management framework, which is context-aware, lightweight and user-friendly.

The book does not cover:

- Acquiring contextual information using sensors or other means.
- Developing communication protocols for the dissemination of contextual information among devices.

The above two points imply that our work is based on the assumption that necessary contextual information is available to individual devices when needed.

## 1.4 Novel Contributions of this Book

Our main novel contributions include a new methodology (i.e. a new framework with a user policy definition ContextRank), the utilisation of an existing technology in a new way (i.e. Identity and Social Identity Theory), and the improvement of other methodologies (e.g. hybrid metrics based on energy metrics, and Context Based Access Control (CBAC) based on Role Based Access Control (RBAC)). The details of these contributions are summarised below:

- **New Framework UCIM:** Our framework represents contextual information and user profiles using XML semantic representation. It facilitates the realisation of a more balanced solution to IM in MANets to cater for the desirable features of privacy, user-centricity, context-awareness and user-friendliness in a systematic and consistent manner. At present, based on our knowledge there is no such framework available for MANets.
- **User-Centred:** Our framework gives total control of the system to users in terms of profile disclosure as well as the usage and definition of rules and policies. We introduce an improved version of the Role Based Access Control concept, i.e. Context Based Access Control (CBAC), where the context constraint of a profile type is used to restrict which users within the environment will be able to request and view other users' contextual information. The usage of portable user profiles within our framework enables users to be in total control of their information usage with minimal technical knowledge. This mechanism is highly portable and consistent with the mobility feature of ubiquitous networks.
- **Dynamic Policy Specification:** This allows users to dynamically specify policies using predicates and functions. Policies are built from predicates (which are just inequalities containing properties and values) and sub-functions, joined together using logical operators. The use of sub-functions eliminates the problem of tackling complex mixtures of conjunctions and disjunctions. A policy can be easily translated and used in many other applications. The methodological design can be implemented for any scenario and is adaptable. It is our aim for policies to be stored in a tree structure in memory or in XML files in a way that is lightweight and portable. The design is modular, meaning that new modules can be plugged in to improve functionality. The technique could be easily integrated into current existing solutions, *e.g.* Ponder, to act as client applications and pass on created policies to the Ponder engine for processing. Policies can also utilize users' partial identities. Users can modify policies, which will take effect dynamically and with minimal interruption of the system.
- **ContextRank:** This algorithm is designed to function in two main ways: either used as a filtering algorithm considering only the relevant contextual information for a user, or integrated with user defined policies from a Dynamic Policy creation module (to be presented in chapter five) or any other policy in a filtering context. It is designed to take in the criteria under which contextual information

can be filtered, and to produce an output for the users who meet the required criteria. The expected inputs for the algorithm are: an array or a list of all available contextual information within the range of a given user and one or more policy files. The expected outputs are: a list of relevant contextual information for the user, access to users' data or profile information and possibly a request for further information if required.

- **Lightweight:** This is achieved via the use of XML representation of contextual information and new resource-efficient schemes, including protocols and mechanisms that are conceived for the formation and distribution of context information and the negotiation of identity information. A novel hybrid Euclidean Metric-based algorithm has been devised to determine how to access or request contextual profiles from other nodes by using a restrictive hybrid metric that measures the balance of system resources such as energy levels, CPU usage and distances between nodes. Accordingly, the framework is also designed in a way that the user effectively influences the resource usage by introducing the concept of user-centric design to reduce the additional resources consumption on networks. The use of identity and social identity theory in influencing relevant context information to be displayed to the user will also help to limit the overhead of the framework on devices.

## 1.5 Methodology

The process for achieving the book's aims and objectives is divided into the following phases: requirement analysis and specification, design, implementation and evaluation. The first phase, requirement analysis and specification, is based on identifying current works within the domains of MANets and IM, and capturing necessary requirements for the proposed framework. This includes an extensive literature survey to obtain a comprehensive knowledge of existing IM systems, MANets, lightweight privacy-enhanced mechanisms, key management, efficient trust management, context-aware systems, user-centric concepts and mechanisms. An awareness of the issues and limitations of these available techniques is then established. To tackle the issue of identities, personal and device attributes are investigated to derive a set of partial identities suited to MANet-based applications, which helps to specify privacy policies for access to identity information. From these studies, a set of requirements for the proposed framework is defined and documented.

The design phase of the project involves transforming the requirements identified in the first phase into effective solutions for their realisation, including the design of data structures, system architectures, interfaces and components. Before addressing the data structure issue, methods for collecting information required for IM in MANets have been explored. This helps us to build context-awareness from a mixture of different information such as locations, time, proximity selection, automatic contextual reconfiguration and context-triggered actions. For outdoor location information we suggest obtaining such information via the use and exploration of GPS technology, to provide a means that will allow the possibility of using active badges when required. As many small and low-cost devices do not necessarily have GPS, the method proposed by *Bulusu* (Bulusu, Heidemann et al. 2000) using a connectivity-based localisation technique is explored. Since GPS does not support data communication (Guanling 2000) in such situations, our framework provides the means of allowing devices to track locations by listening to beacons from a cell-based station or to query a local database for their current locations. Users can choose to advertise their current locations with respect to their privacy policies. Other low-level context information such as time, nearby objects, network bandwidth and orientation is also examined with reference to necessary quality context indicators (Sheikh 2007).

The design phase also selects other suitable existing techniques for IM, key management, efficient trust establishment and lightweight privacy enhancement in relation to the requirements set out in the first phase. These techniques are then tailored, extended and integrated together with the context-aware solutions to produce necessary schemes, mechanisms and protocols, which collectively form the proposed framework.

In the implementation and evaluation phases, simulation techniques and tools (Stuart 2005) such as NS-2 (Altman and Jienez 2003), GTNet (Dr. George F) and OPNET (Lucio 2003) are examined to find an effective way to implement the framework designed. However, we decided to broaden our in-house developed simulator to test the security of composed system-of-systems for the needs of our framework and to provide a means of integrating the new simulator to work with other simulators when time permits. The main reason for using a simulation tool for the implementation is due to its cost-effectiveness for the framework evaluation and subsequent refinement as well as the limitation of resources needed for a real implementation. The simulated framework is assessed based on case studies to determine its compliance with the requirements specified in the first phase. We also try to test the framework on available portable hardware devices within the laboratory.

## 1.6 Book Organisation

***Chapter two:*** It reviews the issues related to the development of ubiquitous computing from its inception by Weiser, where the three main phases: the Mainframe era, the PC (Personal Computing) era and the Ubiquitous Computing era are presented. A brief history of computer networking is covered while presenting its future direction. The chapter also looks at the layered network in relation to the development of network security. It continues with several related areas in which smaller and cheaper computer chips are embedded into many appliances from a greeting card to a smart home so that people's daily lives can be closely connected to computers and beneficially become ever more convenient. Finally, along with the benefits, the vulnerabilities of ubiquitous computing are discussed. Security is one of the major concerns for any computer network, including ubiquitous computing.

***Chapter three:*** In this chapter, we will narrow down the related work and provide more insight into the areas provided in chapter two. The chapter first introduces network security and identity management. It then further presents the historical issues (e.g. development, attacks and frameworks) of IM and an introduction to MANets in relation to IM. An overview of research issues in these areas is provided. The chapter also classifies users' personal identities into sub-identities to make it easier to protect user identities and define policies, which will be further expanded in chapter five. The chapter explores the importance of user-centricity and context awareness for both MANets and IM by highlighting how these two techniques can help to provide more security to users and networks. Other benefits include the efficiency of resources used, its impact on helping to create a lightweight framework, and its ability to help improve service provisions, etc. Context reasoning and representation have also been introduced in this chapter.

***Chapter four:*** In this chapter, we will summarise the weaknesses of the related work identified in chapters two and three. The weaknesses identified are mainly focused on IM, including the issues of defining user profiles, user control and centricity, the usage of contextual information, and allowing users to define policies dynamically. These provide a justification for proposing a new framework to solve the weaknesses. For example, existing frameworks and solutions for IM are mainly aimed at wired networks, which do not meet the requirements of ubiquitous ad hoc environments, and also they neglect the important role of users and are not lightweight. From these identified weaknesses we will present our motivations for the book.

***Chapter five:*** Building from the identified limitations in chapter four, this chapter presents the aims and objectives of our project for the development of the proposed UCIM framework. This is followed by the requirements of the framework and its overall design showing what modules or components are needed to create the framework. The chapter looks further into the details of each module by mainly focussing on how they meet the specified requirements of the framework and how they overcome the limitations summarised in the previous chapter. Some desirable features such as portability, heterogeneity, lightweight, dynamic policy creation and context filtering are also explained in detail with regard to the proposed framework.

***Chapter six:*** In this chapter we provide the proof of concept of UCIM. The proposed UCIM framework is implemented by extending our in-house built simulator, and developing new mobile and other relevant applications that provide the functionality of UCIM. The implementation is supplemented by scenarios that are aimed at helping readers understand the reason behind such implementations and the methods used. The implementation is deployed on various portable devices and desktop computers with web based interfaces for other modules of UCIM. The chapter further presents the results of the implementation and deployment using screenshots. It also presents some of the code used in the implementation of UCIM to aid readers' further understanding and show how we have managed to turn our proposed algorithms and mechanisms in chapter five into a workable framework and solution so as to fulfil the goal of the book.

***Chapter seven:*** This chapter takes us back to chapter one by re-visiting the aims and objectives of the book as presented in both chapter one and five respectively. The chapter further provides the evaluation of the implemented UCIM with respect to the book's aims and objectives as well as the requirements set out in chapter five, including a security analysis and test results. The chapter also provides justification of how UCIM is able to rectify the limitations of the existing work summarised in chapter four and most importantly fulfil the main aims and objectives of the book.

***Chapter eight:*** This chapter presents our conclusions and future work.

## 1.7 Summary

In this chapter we have presented an overview of the content of the book. We have highlighted the fact that computing applications are becoming ubiquitous, which has created serious threats to users' privacy and security. Trivial embedded systems with the abilities of computing and

communication are becoming widely available and spreading everywhere for the purposes of sensing, control and information display. Hence, the need for the privacy and security protection of users is an inevitable and critical issue. These must be planned effectively to meet the future large-scale implementation and deployment of ubiquitous computing applications. Current IM frameworks are not fit for such an environment due to the resource constraints and heterogeneous infrastructure of ubiquitous computing. Therefore, this book provides a novel solution to the problem: UCIM for users' identity protection in MANets. This framework utilises flexible and adaptive system architecture to provide resource-efficient security protection against malicious activities, and gives users full control of their identity information.

In the next chapter, the history of computer networks and the trend towards ubiquitous computing will be introduced.

# CHAPTER TWO

# THE DEVELOPMENT OF UBIQUITOUS COMPUTING

In this chapter, a brief introduction to the history of computer networks is presented. Then our focus is directed to the continuous growth and development of computer and network technologies, including introducing the early stage of the information era to ubiquitous computing and highlighting its possible future directions.

The development of computers has undergone three major waves, which are: mainframe computers, personal computers and the introduction of the concept of ubiquitous computing. A number of decades have passed since the first version of mainframes was introduced. It was only in the 1960s that the notion of computers–which were supposed to work alone and process programs locally–set a new milestone and initiated a change pattern for this concept. The new concept came about allowing a set of computers to be connected together to allow remote access to computer resources. Since then, the world has witnessed one of the greatest miracles in human history–the Internet. Following this, the notion of ubiquitous computing was explored by Mark Weiser in the CS lab at Xerox PARC (Terry Accessed 12/06/2011).

When analysing such developments within computer technology over the last century, a clear trend of events and shifts can be seen. Over the years as time goes by, when mapping the relation of how many people use how many computing devices, it can be seen that it goes from many-one in the 1960s to many-many in 2010. A summary of this trend has been presented in Figure 2-1 (Vertegaal 2003).

The three main developments or waves of computing have been summarised by Weiser. The first wave of computing from 1940 to about 1980 was dominated by many people using one computer. The second wave, still peaking, has one person and one computer in uneasy symbiosis, staring at each other across the desktop without really inhabiting each other's worlds. The third wave, just beginning, has many computers

serving each person everywhere in the world, which is called "ubiquitous computing" (Weiser 1999).

Weiser further states that: "The defining words [for the third wave in computing] will not be 'intelligent' or 'agent', but rather 'invisible' and 'calm' and 'connection'" (Weiser 1999).

The development of ubiquitous computing itself has undergone various phases. The first phase has been where hundreds of computing devices ranging from the size of a memo pad to wall-size boards have become available for users in different ways, i.e. iPads, mobile, body sensors etc. The means of connection between devices are via wireless networks with abilities such as shared meeting applications and location-based services. Weiser envisioned the scenarios where "embedded computers [...] will bring other worlds to us in new ways–sometimes in ways so unobtrusive we will not even notice our increased ability for informed action". Weiser described the kind of tune in a future alarm clock: "the kind of tune [it] plays to wake me up will tell me something about my first few appointments of the day. A quick urgent tune: 8 am important meeting. Quiet, reflective music: nothing until noon". Hence, devices "can be suggestive without being intermediating". Ubiquitous computing would allow us to focus on those issues that are really important, interesting and challenging.

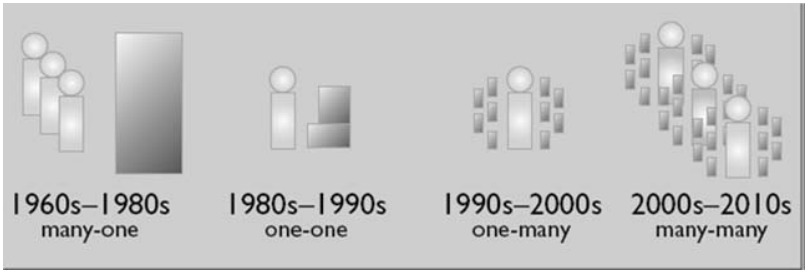


Figure 2-1 Mainframe to Ubiquitous Computers (Vertegaal 2003)

In order to turn Weiser's dream into reality, research organisations and industry need to be more focused on developing the required techniques, hardware and software with careful consideration of security measures that will motivate users to adapt this new wave of interaction and gain its benefits. This research will include several areas related to such issues as: security protocols, policy definition interfaces, user-centricity, context-awareness, low cost devices, low power devices, identity management frameworks and techniques, mobility, applications for small devices,

effective user interface, etc. The above issues are vital in order to encourage users to acclimatize to new developments. As in today's growing world of threats most users will only settle on new technologies when they are satisfied that they are in full control of their personal and identity information.

The concept of ubiquitous computing has other related research areas such as the concept of calm technology, which extends the notion of ubiquitous computing and uses its principles to create technology that utilizes both the centre and periphery of a user's attention. Another area is augmented reality that makes heavy usage of the principles of ubiquitous computing to improve users' perception of computation by enhancing physical objects (such as a desk), using computer generated sensory inputs (such as sounds or graphics) to provide a direct or indirect view of a physical, real-world environment. Such technological advancement allows better interaction and usage of the physical objects. However, these areas are not related to our work.

In the following sections we will turn to the issues of computer networks and security.

## 2.1 A Brief History of Computer Networks

The initial stage of computer development was stand-alone mainframe computers with each occupying an entire room. As time went by with the development of more portable mainframe computers, the industry realised that there would be an advantage if these super-computers could be connected in a way to allow them to talk to each other, i.e. share information. From this, the notion of computer networks was born. Hence, the term "network" in computer science can be seen as a means of interconnecting computer systems by making use of transmission technologies.

The early development of computer networks came about in the late 1960s with the main aim of connecting researchers to remotely accessible expensive computer resources that individual research centres or institutions could not afford. This came about via the ARPA (Advanced Research Projects Agency) project ARPAnet (Peter T. 1998), which produced the first prototype of modern networks. Its connection speed at that time was 50 kbits/s, but ARPAnet brought a fundamental change from centralized to distributed computing and incorporated features of reliability and robustness, e.g. multiple links and distributed routing. The ARPAnet project was initiated in 1969, and is sometimes referred to as the grandfather of the Internet. The network was designed as a computer

version for a nuclear bomb shelter to protect the flow of information between military installations by creating geographically separated computers capable of exchanging information via the use of the Network Control Protocol (NCP). The initial connection consisted of four computers from the UCLA (University of California Los Angeles) Research Lab, Stanford Research Institute, UC (University of California) Santa Barbara and the University of Utah. The first data exchange within the network was between UCLA and Stanford Research Institute. In the first attempt to log into Stanford's computer by typing "login", researchers in UCLA managed to crash the network when they typed the letter "g".

From then on, the ARPA development led to an array of new hardware and protocols, and this eventually emerged as the Internet. The Internet is defined as a set of networks connected by routers that are configured to pass traffic among any computers attached to a network in the set. Initially the Internet had only a few hundred computers and a few dozen sites. Today, hundreds of millions of computers, small portable devices and thousands of networks worldwide are connected together.

Another analogy on the development of the Internet as seen by Frank Casanova, who was a Director of Apple Computer Inc. is (Casanova):

> "The concept of computers as things that you walk up to, sit in front of and turn on will go away. In fact, our goal is to make the computer disappear. We are moving towards a model we think of as a 'personal information cloud'. That cloud has already begun to coalesce in the form of the Internet. The Internet is the big event of the decade. We'll spend the next 10 years making the network as it should, making it ubiquitous."

The development of the Internet brought about a new industry. Companies like Cisco, IBM and Microsoft continuously work out new products on networking hardware, computers and relevant software. Today, the Internet has become a new phenomenon and networks are an important part of everyday activities. Through the Internet, we can do shopping at home, finish a degree without going to a university, make friends with people from anywhere in the world, etc. In many ways, it changes the way we live. Currently, it is even possible to produce specially designed objects (tables, chairs, clothes, shoes, etc.) from a computer and print them using a 3D printer. In the paper (Weinberg November 2010), Michael wrote "the ability to reproduce physical objects in a small workshop and at home is potentially just as revolutionary as the ability to summon information from any source onto a computer screen".

## 2.2 Mobile Ad Hoc Networks (MANets)

A MANet is a collection of mobile nodes forming a network on demand without the assistance of any centralized structures. These networks can be well used and suitable for environments where either the infrastructure is lost or the deployment of an infrastructure is not very cost-effective. With today's growing use of technology, MANets are used in a number of environments for various reasons.

Historically, the whole life cycle of ad hoc networks could be categorized into the first, second, and third generation ad hoc network systems. Existing ad hoc network systems are considered the third generation (Taneja and Patel 2007).

The first generation goes back to 1972. At the time, they were called PRNET (Packet Radio Networks) (Tobagi, Binder et al. 1984). PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The IEEE 802.11 subcommittee had adopted the term "ad hoc networks" and the research community had started to look into the possibility of deploying ad hoc networks in other areas of application.

In the intervening time, the work was going on to advance the previously built ad hoc networks. GloMo (Global Mobile Information Systems) and the NTDR (Near-term Digital Radio) (Leiner, Ruth et al. 1996) are some of the results of these efforts. GloMo was designed to provide an office environment with Ethernet-type multimedia connectivity anywhere and anytime in handheld devices.

The requirements of MANets represent a spectrum of network challenges. During the last few years, almost every aspect of MANets has been explored to some level of detail. Yet, more questions have arisen than have been answered (Royer and Toh 1999).

The major open problems are listed as:

- *Identity Management*–How to protect users' identity information such as text, address books, emails, personal information, etc.
- *Autonomous*–No centralized administration entity is available to manage the operation of the different mobile nodes.
- *Dynamic topology*–Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary in time and are based on the proximity of one node to another node.
- *Device discovery*–Identifying relevant newly moved in nodes and informing about their existence need dynamic updates to facilitate

automatic optimal route selection as well as other contextual information.

- *Bandwidth optimization*–Wireless links have a significantly lower capacity than the wired links.
- *Limited resources*–Mobile nodes rely on battery power, which is a scarce resource. Also, storage capacity and power are severely limited.
- *Scalability*–It can be broadly defined as whether a network is able to provide an acceptable level of service even in the presence of a large number of nodes.
- *Limited physical security*–Mobility implies higher security risks such as peer-to-peer network architecture or a shared wireless medium accessible by both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.
- *Infrastructure-less and self-operated*–A self-healing feature demands that a MANet should be able to realign itself to blanket any node moving out of its range.
- *Poor transmission quality*–This is an inherent problem of wireless communication caused by several error sources that result in a degradation of received signals.
- *Ad hoc addressing*–Standard addressing schemes should be developed.
- *Network configuration*–The whole MANet infrastructure is dynamic and is the reason for the dynamic connection and disconnection of variable links.
- *Topology maintenance*–Updating the information of dynamic links among nodes in MANets is a major challenge.

The issues mentioned above still form the fundamental research issues today. In our work and sections to follow we try to address some of the issues by focusing more on the security aspects. Having introduced the history of computer networks, the next section will look at security issues within computer networks.

## 2.3 An Overview of Network Security

With the rapid developments of computer networks as summarised in the previous section, security issues became of concern to the community, and ways of trying to tackle such issues became of paramount importance. Looking back to 20 years ago, network security was mainly at the level of