Management System Requirements for Wireless Systems Beyond 3G

O. Lazaro[1], J. Irvine [1], D. Girma[1], J. Dunlop[1], A. Liotta[2], N. Borselius[3], C. Mitchell[3]

[1]Mobile Communications Group,
EEE Department,
University of Strathclyde,
Glasgow G1 1XW
Scotland (UK)
Tel: +44 141 5482074
e-mail: olazaro@ieee.org

[2]Centre for Communication
Systems Research,
University of Surrey,
Surrey GU2 7XH
UK
Tel: +44 1483 689 808
A.Liotta@eim.surrey.ac.uk

[3]Information Security Group
Royal Holloway
University of London
Surrey TW20 0EX
UK
Tel: +44 1784 443101
c.mitchell@rhul.ac.uk

ABSTRACT

This paper presents a comprehensive description of various management system requirements for systems beyond 3G, which have been identified as a result of the *Software Based Systems* activities within the Mobile VCE Core 2 program. Specific requirements for systems beyond 3G are discussed and potential technologies to address them proposed. The analysis has been carried out from network, service and security viewpoints.

I. INTRODUCTION

As the industry looks to systems beyond Third Generation (3G), a more user-centric approach is being taken. 3G systems have introduced new services on the move that could not be supported by previous generations. However, future systems will see new scenarios with increased opportunities for competition and which will ultimately provide the user with a variety of services with the required quality at the most appropriate cost over the most suitable transport technology [1]. The realisation of this user-centric scenario relies on principles such as openness, personalisation, abstraction and integration [2],[3].

The Software Based Systems work area of the Mobile VCE, a consortium of 7 universities and 28 companies [4], is examining novel software dependent solutions to the issues arising in systems beyond 3G. This work started in full in October 2000 and continues until September 2003. Middleware technology [5],[6], delivering the required level of abstraction for service homogeneity and network integration, shows promise as an enabling technology. Also, the trend towards increasing service provider and network provider separation is leading to the introduction of new business models. In order to support the management of these richer business scenarios – network operators working with several service providers and the user performing ad-hoc selection of his preferred service providers – the software agent paradigm reveals itself also as a key technology. As a result, the focus of this work within Mobile VCE is centred on the use of middleware and/or agent-based solutions as part of the wireless system architecture.

The use of these technologies introduces a number of issues. Future systems must be able to cope with new aspects such as distributed software and service management, as well as greater mobility in its many forms, i.e. terminal mobility, personal mobility, service mobility and code mobility. Mobile VCE is not alone in foreseeing increased software dependency within systems. However, while much effort has been put into the main technologies to drive the design of wireless communication systems beyond 3G, much less effort has been devoted to the analysis of the corresponding management implications. These will not only come from the 4G-like scenarios themselves [1],[7], but also from some of the middleware technologies adopted to realise them. The aim of this paper is therefore to identify various requirements that the realisation of 4G scenarios may pose on future management systems, highlighting where appropriate the limitations that current management strategies may suffer in this context. Particular emphasis has been placed on the security requirements, since a meaningful design of any management system should consider security as one of its fundamental elements.

II. THE MANAGEMENT SCENE

Over the last few years, various factors have initiated a technological convergence between the telecommunication (fixed, mobile and broadcasting) and computer networking domains. The main driving factors have been the great success of the Internet and mobile telephony. Their success in their respective domains has inspired increased efforts for the expansion of both technologies towards new markets, ultimately inducing a requirement for technological convergence between them. This convergence would provide the means for the introduction of new services, which could not be delivered by each domain in isolation.

Future networks will be based on packet technology. New QoS-enabled services will be provided over this underlying transport mechanism, and the control and management aspects of these systems will gradually integrate into an indistinguishable and unified body. New terminals will become more sophisticated and more functionality will be available. Following the successful path set by the Internet, next generation networks will have to consider a clear separation between service and transport provision. Convergence between

The work reported in this paper has formed part of the Software Based Systems work area of the Core 2 Research Program of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.com.

the computing and communication domains enables the design of robust, real-time middleware that can hide complexities of distribution from individual applications. As a software layer lying between applications and networks, middleware, in combination with other software technologies, has great potential for enabling seamless interworking among evolving and emerging wireless systems and services.

The technological context of 4G systems should be set around the effort to achieve full convergence of personal systems, information systems and entertainment while enabling ubiquitous mobile access. Hence, the MVCE vision for mobile communication systems beyond 3G embraces five key elements [7]:

- *Fully converged services*. The user will have secure and personalised access to a seamless pool of content.
- *Ubiquitous mobile access.* Untethered will be the dominant mode of access to the available services.
- *Diverse user devices*. The user will be served by a wide variety of devices to seamlessly access content.
- *Autonomous networks.* Underlying these systems will be highly adaptive and autonomous networks.
- *Software dependencies*. Agents representing mobile users will exist and act continuously to simplify tasks and provide transparency to the user.

Future systems are therefore likely to see increased service customisation, greater service availability and convergence in a mobile environment. The deployment of systems with the above features poses significant challenges in terms of management, since such systems are likely to be characterised by increased distribution, heterogeneity, concurrency and will have to cope with the varying conditions of the wireless link. Increasing dependency on software technology will be needed to realise this vision. In this context, the software agent paradigm could play a significant role, providing new means for more easily and more efficiently structuring large scale distributed systems and applications. In this distributed environment, the ability of agent technology to act on behalf of a user should enable new degrees of service personalisation and increased machine-machine interaction. Therefore, some of the more general management system requirements presented in the following sections are complemented with more specific requirements that arise from the management of a system populated by software agents.

III. NETWORK AND SERVICE DRIVEN MANAGEMENT SYSTEM REQUIREMENTS

Traditional network management systems have assumed a transport technology and a reduced set of services to manage. As highlighted by the key features presented in Section II, the management system under consideration would have a wider scope of operation. The management system would need to manage multimedia services for multifunction, heterogeneous terminals within a converged network environment, significantly increasing management complexity. Therefore, the requirements on the management system from a service and network perspective can be divided as follows:

- **Scalability.** Due to the inherent complexity of the scenarios considered for future systems, traditional approaches to network and system management, e.g. centralised and hierarchical management, may not be able to meet the system requirements as increased encapsulation and distribution in the management functions would be desirable. As a result of the increased encapsulation, the overall management could be decomposed into smaller and simpler tasks that can be efficiently carried out. Innovative distributed management architectures based on software agents capable of roaming the network, locating themselves optimally, and maintaining optimality through migration could play a crucial role in achieving management system scalability. The same management system architecture should then support a small or a large number of users, services and networks. In the context of the open and distributed systems envisioned for 4G systems, scalability will also refer to information, which could similarly scale in availability to particular users and services depending on the access rights granted. The system should be able to operate effectively with various degrees of information availability. Since managerial tasks will potentially have to be performed in a number of domains and information will be required in each, then the system will have to manage secure access to the relevant data.
- **Flexibility and Modularity.** Flexibility is essential to design, deploy, and maintain services efficiently in a competitive environment. Moreover, the middleware management system should allow middleware mechanisms to be tuned as a function of traffic statistics and usage patterns. This implies that a certain degree of *network and service awareness* would be required within a system characterised by a high degree of distribution and heterogeneity, with entities involved in the provision of a service not necessarily co-located and with availability of a variety of transport technologies and services. It should then be possible for middleware management functions to be tuned as a function of network and service conditions to best respond to their variation. Finally, flexibility and modularity in the management system design would allow management policies to be decoupled from the data collection and monitoring processes, thereby enabling the independent incorporation of new elements and algorithms as new techniques emerge or new types of data are required.
- **Adaptation and Controllability.** An important role of the management system will be to co-ordinate the system operation with the objective of providing various forms of adaptation, which are depicted in Figure 1 and discussed below. In this context, traditional network management should additionally incorporate new management aspects such as distributed software entity management and specific service management functionality. Service management functionality does not refer to the management of the service at a micro level for a particular Quality of Service (QoS) provision. It refers to the management requirements that derive from the availability to the user of a pool of services that could be accessed through a number of transport technologies and which therefore needs specific mechanisms to enable service mobility across networks at this macro-level.

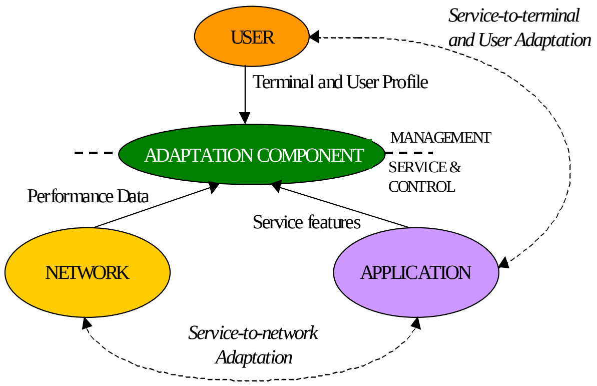

Figure 1 - Adaptable Management System.

- ***Service-to-terminal adaptation.*** The requirement for service-to-terminal adaptation derives from the user ability to access services from different types of terminal, e.g. PDAs, mobile phones, laptops and WebTV, with different visualisation, voice and/or network connectivity capabilities. Therefore, the management system should provide the mechanisms to ensure that the most appropriate QoS for a given service is established through negotiations among the network operator, the service provider and the user terminal. This poses the following requirements on the management system:
  - ♦ Mechanisms to extract terminal and user profile information.
  - ♦ Lightweight, secure (agent) execution environment at the terminal, so that new services could be installed/upgraded on the fly.
  - ♦ Legacy terminal support, no (agent) execution environment, with the same architecture.
- ***Service-to-user context adaptation.*** The "user context" concept, according to the Universal Mobile Telecommunications Systems (UMTS) and in the context of the Virtual Home Environment (VHE), is a combination of the user profile preferences, the current state of the user environment and the user terminal capabilities [8]. Hence, the service is expected to execute according to the user context. It is the responsibility of the management system to gather this information and make it available to the system so that it can be matched with the alternative ways of delivering the service. This poses similar requirements to the ones specified for the service-to-terminal adaptation.
- ***Service-to-network adaptation.*** This type of adaptation is also required since QoS may need to be adjusted as the network conditions change or when the service is offered in different terminals. This type of adaptation allows the user to access services regardless of the underlying network technology. This poses the following requirements:
  - ♦ Networks that are open, to some extent, to the management system that in general may be a different entity from the one that manages the network.
  - ♦ Secure (agent) execution environment close to the network operator site.
  - ♦ User ability to select the conditions to be informed of a change due to QoS variations.
  - ♦ User ability to accept or reject those changes.

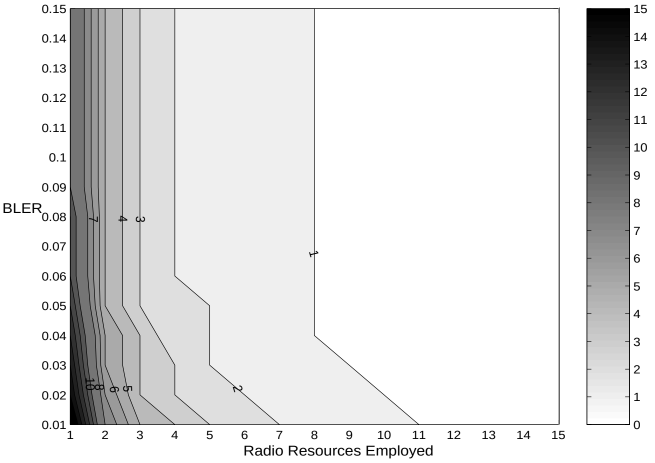

Figure 2 – Service set-up delay for number of negotiating entities involved, BLER and radio resources employed.

The final aspects to be considered in this analysis are the requirements from the management of distributed mobile entities. Management of code mobility in a mobile environment translates into a system that carefully manages the available resources and their allocation to software agents. Software agents are constrained to run as close as possible to the application/service/user but in accordance with specific resource allocation policies. This calls for the following requirements on the management system:

- **Efficient resource management.** Software agents are likely to contain information on resource management policies to prevent them from overloading the managed system.
- **Security.** Section IV is devoted to this issue.
- **Control structures.** Today's mobile agent systems allow the creation, cloning and migration of agents. Code migration should be controlled so that it does not become a source of instability or the origin of significant performance degradation.
- **Service development platform.** The management system assumes the existence of a service platform based on a core, standardised set of APIs over which services are built as components, agents or a combination of both.

Some additional analysis has been undertaken on different management scenarios to refine the requirements, focussing particularly on the new aspects such as code mobility. As an example, the effect of service location on the service set-up delay has been studied, comparing terminal execution and network assisted execution. The initial analysis has considered an EDGE-like network, under different Carrier to Interference Ratios (CIR) conditions. Figure 2 shows the areas where a terminal execution approach leads to reduced service set-up delays compared to a network assisted approach depending on the number of negotiating parties involved. For instance, a network assisted approach would reduce the service set-up delay if negotiation is performed with 2 entities, the BLER is 0.08 and each message exchanged in the negotiation requires at least 4 resource units. The results indicate that a trade off exists between the CIR conditions, the number of entities involved in the negotiation and the most appropriate location to run the service. Thus, the importance of the network and service driven requirements in terms of location of service execution environment is highlighted, and the necessity for flexible and adaptable architectures to address this issue emerges. Current activities are being directed to enhance the initial test-bed to widen the scope of the analysis, which could ultimately assist in the design of innovative management architectures that take the above requirements into consideration.

IV. SECURITY DRIVEN MANAGEMENT SYSTEM REQUIREMENTS

Security is an important component of any management system, as an indispensable element to ensure the non-malicious and reliable function of any kind of system. Therefore, this section is devoted to highlighting the security aspects that can be derived from the availability of management system features similar to the ones described in the previous section.

In the days when PSTN switches were completely mechanical, and all system changes and maintenance had to be carried out by service personnel on site, proper physical security measures were enough to secure the network and its service. As telecommunication equipment became more automatic, mechanisms were introduced to let the operator carry out maintenance and system changes remotely. The network and any offered services would still be provided by a single network operator, who could deploy security mechanisms as deemed necessary. The shift towards more complex communication systems, where an increased number of entities are involved (e.g. network owner, network operator, and various service providers) is already taking place. This has led to new requirements on management services, and security has become an important issue and enabler of these versatile communication systems. This trend towards a greater number of involved entities, providing various services, is likely to continue, also giving opportunities for a variety of different types and sizes of service provider.

The requirements for security originate from different sources [9]:

- **Customers** need confidence in the network and the services offered, including correct billing.
- **Authorities** demand security by directives and legislation, in order to ensure availability of services, fair competition and privacy protection.
- **Network operators/service providers** themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the authorities.

The security objectives for future mobile systems (confidentiality, data integrity, accountability, and availability) are not likely to change drastically from those in 3G. However, the solutions provided in existing systems are unlikely to be sufficient for systems beyond 3G. Challenges are likely to arise from the scale on which trust needs to be managed as well as from the scale and granularity required for authorisation and authentication. The assumption that mobile software entities will be utilised further adds to the complexity.

Security features at the middleware level are of two forms; those which the middleware provides for applications and those which are used to secure the middleware itself. Clearly from a management perspective we are interested in both. This section attempts to present a general description of the security features likely to be required to protect the middleware platform and their motivation. Security features of this type can be divided into the following main categories:

- **Mobile software security.** Mobile software security relates to protecting both the host, which executes the software, and its resources from unauthorised use or manipulation by malicious or misbehaving software. In general terms, this is achieved through controlling the software executed on a (mobile) host and by regulating the actions that can be carried out by a particular piece of software.
- **Availability.** Denial of Service (DoS) attacks are often the most difficult to protect against. They usually exploit weaknesses in protocols or implementation. Therefore, availability issues must be considered during protocol design as well as during implementation.
- **Agent security.** Mobile agents are expected to play an important role in the realisation of the envisioned middleware. Non-trivial security issues arise as soon as executable code is allowed to move freely in the network and to execute at places where the code initiator, or owner, has no control. Therefore, not only may agents need protection from other agents and from the platforms where they execute, but the platform may also require protection from agents running on it. The following are desirable security features in an agent environment.
    - ♦ *Confidentiality.* Any private data stored on a platform or carried by an agent should remain confidential.
    - ♦ *Integrity.* The agent platform should protect agents from unauthorised modification of their code, state, and data, and ensure that only authorised agents or processes carry out any modification of shared data.
    - ♦ *Authentication.* Proper authentication is required for other security features to work. Therefore, entity and origin authentication are likely to be required.
    - ♦ *Accountability.* An agent, or the entity responsible for the agent, should be held accountable for its actions.
    - ♦ *Anonymity.* An agent platform will need to balance an agent's need for privacy with the platform's need to hold the agent accountable for its actions.
    - ♦ *Availability.* The agent platform should be able to ensure the availability of both data and services to local and remote agents.
- **Charging security.** The charging model used in 2G and most likely to be used in 3G wireless telecommunications networks requires the subscriber's home network to have some agreement with the charging party. The home network operator then bills the subscriber or gets paid through a prepaid scheme. New payment schemes and methods are likely to be required in the future.
- **Auditing and monitoring.** In contrast to most other security features, which are in place to prevent security breaches, auditing and monitoring enables follow-up when something goes wrong. Although audit trails,

as well as monitoring, have several purposes and relevant information can be generated throughout the network, a generalised approach for auditing and monitoring is likely to be more efficient.

- **Privacy and integrity of stored data.** In a distributed environment information is likely to be stored at various places throughout the network. In fact, within a system containing agents, confidentiality and integrity issues can become very complex.

The security features provided by the middleware to applications relying on its presence can be roughly classified into three broad categories:

- **Communication Security Services.** Providing a secure communication environment is of paramount importance. A communications environment should encompass not only the well understood air-to-base station interface but also the user's Personal Area Network (or PAN) of devices. A typical PAN may consist of a mobile station, a Personal Digital Assistant (PDA) and a variety of devices, which all need to exchange information with each other and the user. Therefore, the area of secure data transfer can be divide into the following categories:
  - ♦ *Confidentiality of data;*
  - ♦ *Authentication of data origin;*
  - ♦ *Integrity of data;*
  - ♦ *Non-repudiation of data.*
- **Trust Services.** Trust services are likely to be fundamental to many kinds of services. They provide the means for entities to establish secure relationships with the assurance that all parties are who they claim to be. Most of the required functionality can be provided using public key or secret key cryptography. Either solution has its advantages and disadvantages. However, in a highly distributed system where certain resources, e.g. a key distribution centre, might become unavailable, using public key based mechanisms is likely to be the preferred solution for many applications. However, we do not rule out secret key mechanisms, as they are more appropriate for other applications and can be used in parallel.
- **Anonymity Services.** Anonymity services allow a user to perform actions without being tracked or associated to a transaction. This can range from the use of Temporary Mobile Subscriber Identities (TMSIs), in place of the International Mobile Subscriber Identity (IMSI), to prevent geographic tracking, to esoteric protocols that allow truly anonymous purchasing between untrusted parties. However, there is an associated problem, since if a user is completely untraceable to the system then fraudulent actions can be unattributable or attributed to an innocent party. Often some of these protocols are not practicable, so there are systems that will allow a broker to act on behalf of a user and in this way hide their identity.

The design of a suitable security architecture for systems beyond 3G relies on properly addressing the requirements described above. Based on this analysis, during the Core 2 of the Mobile VCE program, a security architecture has been proposed [10]. Current activities are mainly directed towards the assessment of the architecture and associated security protocols.

V. CONCLUSIONS

This paper has identified various requirements which have been identified during the initial stages of software based systems work in Mobile VCE. Those requirements are driven by security, network and service points of view. Thus, the management system should be characterised by:

- Adaptation & flexibility
- Network awareness
- Modularity and distribution
- Controllability
- System and information scalability
- Management of trust at various scales (Security)
- Efficiency
- Information management and representation
- Specific service management functionality

Many of these requirements apply to current systems but will take on increased significance in future systems. These requirements are being carried forward to the next stage of Mobile VCE work currently underway which involves the investigation of new management paradigms that can tackle the challenges of these systems, e.g. very-large scale and highly dynamic networked systems. This is a subject of significant interest as a degree of integration, which cannot be identified in current telecommunication networks, can be foreseen in such context. The introduction of software agents as part of the telecommunication network is an example of those new paradigms. Therefore, there is the requirement to address not only the issues of systems beyond 3G, but also the additional problems introduced by this paradigm shift.

ACKNOWLEDGEMENTS

The work reported in this paper has formed part of the WA1 area of the Core 2 Research Programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.com, whose funding support, including that of EPSRC, is gratefully acknowledged. More detailed technical reports on this research are available to Industrial Members of Mobile VCE.

REFERENCES

[1] Irvine J. *et. al.* "Mobile VCE Scenarios", MVCE Deliverable D1.1 Vol. 1, October 2000.

[2] Pereira J.M. "Fourth Generation: Now, it is Personal!" *Proc PIMRC 2000*, Sept 2000, London.

[3] Mohr W., Becher R. "Mobile Communications beyond Third Generation". *Proc VTC2000-Fall*, October 2000, Boston.

[4] Tuttlebee W., "Mobile VCE: the convergence of industry and academia", IEE ECEJ, 12 (6), 245-8, December 2000.

[5] *Journal on Selected Areas in Communications* "Special issue on Service Enabling Platforms for Networked Multimedia Systems", 17 (9), September 1999.

[6] Lazaro O. *et. al.* "State of the Art Middleware", MVCE Deliverable D1.1 Vol. 2, October 2000.

[7] Evans B.: "Visions of 4G Mobile Radio Systems". IEE ECEJ, 12 (6), 293-303, December 2000.

[8] ETSI, Universal Mobile Telecommunications Systems; Service Aspects; Virtual Home Environment, ETSI TR 122 970 V.3.0.1, (2000).

[9] ITU-T recommendation M.3016, TMN Security Overview, International Telecommunication Union, 1998.

[10] Borselius N., Hur N., Kaprynski M. and Mitchell C. J., A Security Architecture for Agent-Based Mobile Systems, To be presented at 3G2002, London, May 2002