MANAGEMENT ASPECTS OF WIRELESS AND MOBILE NETWORKS

A. Kalejska[1], O. B. Popov[2]

[1]Faculty of Mining and Geology, Sts Cyril and Methodius University
Goce Delcev 89, PO Box 96, MK-3200 Stip, Republic of Macedonia
[2]Faculty of Natural Sciences and Mathematics, Sts Cyril and Methodius University
Arhimedova b.b., PO Box 162, MK-1000 Skopje, Republic of Macedonia
saskak@rgf.ukim.edu.mk; oliver.popov@miun.se

Abstract: Network management is a daunting task by itself, since it tries to maintain full functionality and induce both efficiency and, transparency in very complex and heterogeneous systems such as networks are. With the presence of wireless and mobile technology, the goals of network management become even harder to attain due to the emergence of problems specific to the technology. such as the variety of mobile devices and services offered, the flexibility provided by ease of migration yet based on the handover mechanisms, the limitations with respect to processing power, storage and energy supplies, and the vulnerability of the air as a transmission media create a specific set of problems, which must be taken into account in order to preserve the basic functionalities of the network management. Most of the aforementioned problems and issues are central to the study presented in this paper.

Key words and phrases: wireless, mobile, network management, configuration management, fault management, performance management, account management, security management

1 Introduction

In principle network management, as all other services associated with the highest layers of the network communication models, should be independent and transparent of the underlying transmission infrastructure. This is even more so for TCP/IP technology due to one of its primary goals, which is to attain semantic integrity starting from layer 3. In practice, however, in addition to many similarities there are also some significant differences when wired networks are contrasted with the wireless ones. Many of these disparities are due to the very nature of the network elements. Hence, the paper tries to outline and underline the problems related to management and the ways to deal with them in the context of wireless and mobile networks.

Ideally, network management systems (NMSs) are integrated tools that provide seamless end-to-end functionality in heterogeneous networks (aggregations of wireless and wireline elements based on variations in technology and vendor involvement). The variety of devices (mobile and fixed) and services offered, the flexibility provided by

ease of migration yet based on the handover mechanisms, the limitations with respect to processing power, storage and energy supplies, and the vulnerability of the air as a transmission media create a specific set of problems, which must be taken into account in order to preserve the basic functionalities of the network management.

Therefore, the presence of different generations of wireless and mobile technology is initially examined, and then followed by the infusion of mobility and its relevance to management. The study of the "core" of network management is done via performance management, fault management, account management, and security management. Finally, the article deals with radio resource and power management issues.

2 Generations of Mobile and Wireless Technology

The development of wireless and mobile technology is traceable through several generations according to Pahlavan [Pa2001].

The first-generation (1G) systems are analog cellular and cordless telephone systems as indicated on Table 1. The services were limited to voice only. Two separate frequency bands for forward and reverse links (Frequency Division Duplex - FDD scheme) were used, along with the analog frequency modulation (in this case the transmission power requirement depends on the transmission bandwidth). Countries were using a variety of frequency bands and standards since frequency administration agencies in each country were bound by law to restrict the range of the possible allocations.

Standard	Forward/Reverse Band (MHz)	Region
AMPS	824-849/869-894	USA, Australia, Africa, se. Asia
TACS	890-915/935-960	Europe
E-TACS	872-905/917-950	UK
NMT 450	453-457.5/463-467.5	Europe
NMT 900	890-915/935-960	Europe
C-450	450-455.74/460-465.74	Germany, Portugal
RMTS	450-455/460-465	Italy
Radiocom 2000	192.5-199.5, 215.5-233.5, 165.2-168.4, 414.8-418 / 200.5-207.5, 207.5-215.5, 169.8-173, 424.8-428	France
NTT	925-940, 915-918.5, 922-925/ 870-885, 860-863.5, 867-870	Japan
JTACS/NTACS	915-925, 898-901, 918.5-922 / 860-870, 843-846, 863.5-867	Japan

AMPS – Advanced Mobile Phone System, RMTS – Radio Molbile Telephone System, TACS – Total Access Communication System, NTT – Nippon Telephone and Telegraph, NMT – Nordic Mobile Telephony

Table 1: 1G

The second-generation (2G) systems include digital cellular systems, personal communication services (PCS), some mobile data services and WLAN standards as shown on Table 2. The 2G digital cellular systems use FDD scheme and Time Division Multiple Access - TDMA technology, except IS-95, which is based on Code Division Multiple Access (CDMA). They operate in the 800-900MHz bands and have higher voice rates. The PCS standards have evolved out of the 1G analog cordless telephones and merged into the 3G cellular systems. Except for CT-2(+) (800-900MHz) all these standards were designed for 1.8 and 1.9 GHz frequency bands (PCS bands), and all use TDMA/TDD except PACS, which adopted FDD. Mobile data services emerged after the success of the paging industry to provide a two-way connection for larger messages. ARDIS and Mobitex use their own frequency bands in 800-900MHz, TETRA uses its own band at 300MHz, CDPD shares the AMPS bands and Metricom uses the unlicensed ISM bands. They offer limited data communication (Fax, SMS, etc.). WLAN standards provide higher data rates (a minimum of 1Mbps) in an area (<100m), as a way to wired LAN and Internet connectivity. All WLANs operate in unlicensed bands that are free of charge and rigorous regulations. The 2G systems have different mechanisms of encryption also.

	Standard	**Channel bit rate (kbps)/ Data rate (Mbps)***	Region
digital cellular standards	GSM	270.833	Europe, Asia
	IS-54/13x	48.6	USA
	PDC	42	Japan
	IS-95 (CDMAone)	1,228.8	USA, Asia
PCS standards	CT-2 AND CT-2(+)	72	Europe, CANADA
	DECT	1,152	Europe
	PHS (PHP)	384	Japan
	PACS	384	USA
mobile data services	ARDIS(DATATAC)	19.2	
	Mobitex	8	
	TETRA	19.2	
	CDPD	36	
WLAN standards	IEEE 802.11	1.2*	
	HIPERLAN-1	23.5*	

GSM – Global System for Mobile Communication, PACS – Personal Access Communication Systems, PDC – Personal Digital Cellular, TETRA – Terrestrial European Trunked Radio, DECT – Digital Europian Cordless Telephone, CDPD – Cellular Digital Packet Data, PHS – Personal Handy System

Table 2: 2G

Somewhere between 2G and 3G systems is 2.5G that offers higher data rates, packet-switching, color displays, and advanced data services (WAP, ring tones and logos,

etc). Next-generation of WLAN standards were introduced, with data rates up to 54Mbps. IEEE 802.11b and IEEE 802.11g operate in 2.4MHz bands, and all other in 5GHz bands. A part of this family is also the WPAN concept (Bluetooth).

	Standard	Channel bit rate (kbps)/ Data rate (Mbps)*
mobile data services	GPRS	115
	HSCSD	57.6
	EDGE	384
WLAN standards	Bluetooth	723.1
	IEEE 802.11a	6,9,12,18,24,36,54*
	IEEE 802.11b	1.2, 5.5, 11*
	IEEE 802.11g	22*
	HIPERLAN-2	6,9,12,18,24,36,54*

GPRS – Global Packet Radio system, HSCSD – High Speed Circuit Switched Data, EDGE – Enhanced Data rate for GSM Evolution

Table 3: 2.5G

The third-generation (3G) systems define standards that combine 2G digital cellular, PCS and mobile data services, in single network with higher data rates, and quality of voiceand some video. Their requirements are defined in ITU IMT-2000 standard. 3G systems support data rates from 144Kbps up to 2Mbps, mobile computing with high speed Internet access, new services like streaming video, video conferencing, location based services, mobile commerce etc. Dominant technology is Wideband-CDMA (W-CDMA). In October 2001, NTT DoCoMo in Japan launched FOMA (Freedom Of Multimedia Access), the world's first fully commercialized 3G mobile service, which enable new range of services like videophone and videomail. In Europe, these 3G systems are known like Universal Mobile Telecommunication System - UMTS (UMTS Forum, 2003) and this is a natural evolutionary choice for operators of GSM network. Today there is UMTS network and services in Austria, Italy, Sweden, UK and Australia. Other 3G "family" of technology is CDMA2000 (CDMA MC- multi carrier), evolved from CDMA (IS-95) includes 1xRTT, 1xEV-DO and 1xEV-DV and UWC 136 evolved from IS-136 networks primary deployed in USA.

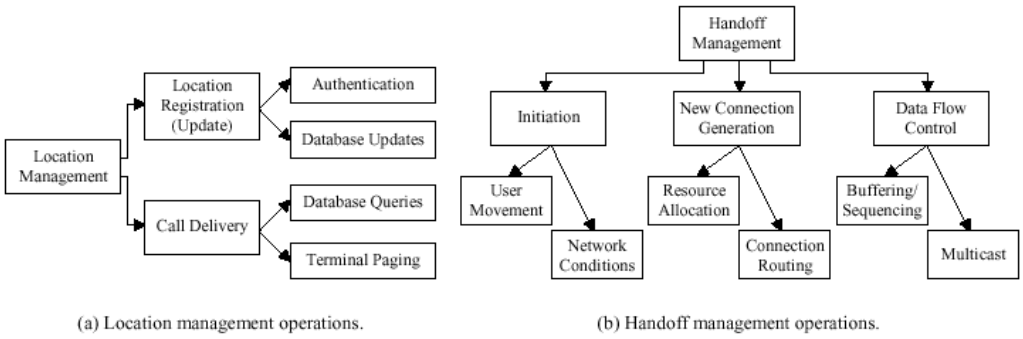
At present, 3G systems are on the start of their deployment curve, while fundamental concepts of the fourth-generation (4G) of mobile and wireless technology are beginning to emerge. Evidently, all the new technologies and the opportunities will make the issue of network management more difficult, and thus more challenging.

3 Mobility management

One of the basic requirements of today mobile systems is personal and terminal (device) mobility. While the former allows users to access their personal services, inde-

pendent of device type or point of attachment, the later refers to the ability of the network to locate a mobile terminal, route messages independent of the attachment point, and maintain full connectivity under roaming.

Mobility management is sually handled by a central system (such as base station, or access point). The management deals with the problems such as location and handoffs. Location management tracks and locates a terminal for delivering of incoming calls and thereat handles information concerning the mobile terminal, like its original cell, current cell, paths and routes toward the current location, etc. The information is updated either periodically or on demand when a specific event occurs and is stored and retrieved in location or paging database, independent of the specific network or location management protocol. Handoff management handles roaming in the same cell (intracell handover) or between cells (intercell handover) and is focuses mostly on the control of the change of a mobile node's access point during data transmission. Conceptually, the location and handoff management are shown in Figure 1 [Su, 2001].



(a) Location management operations. (b) Handoff management operations.

Figure 6: Location and handoff management operations

Mobility management in WLANs is supported by IETF Mobile IP and its extensions [Za2002]. In 2G cellular networks, the framework for the mobility is provided by two international standards: EIA/TIA IS-41 mostly used for the IS-54/IS-136, and 1G AMPS networks and the GSM Mobile Application Part (MAP) for GSM, DCS-1800 and PCS-1900. In both cases, the call processing and location management functions are based on Signal System 7 (SS7) [Za2002].

Mobility management for 3G networks is commonly represented via hierarchical models (Figure 2), where the mobility management is divided into two complementary tasks: macro mobility and micro mobility [Su2001].

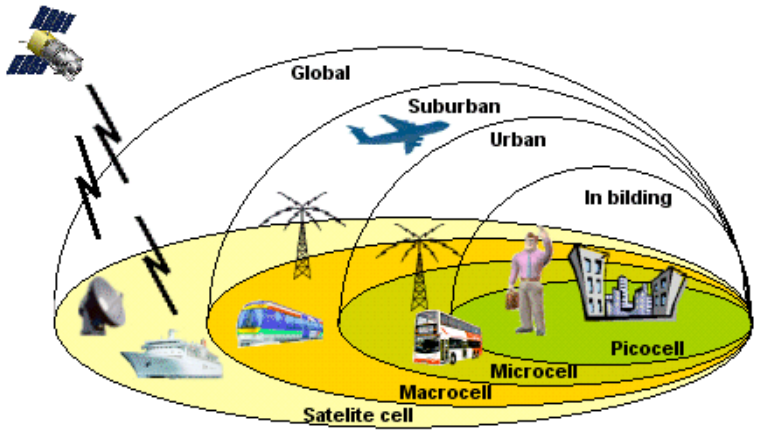


Figure 7: Hierarchical mobility

Many questions with respect to the 3G mobility are still very much open. Due to the difference physical and protocol features along the components that have to be integrated, base stations and control nodes, different way of connecting to other networks (access points - AP, central stations - CS, fixed earth stations - FES, mobile satellite terminals - MST, etc.) and cells with different features.

A very large problem is the vertical handover. Here, the connection is transferred between stations different in type and mechanisms. For example, some of the issues in satellite handover are individual or group transfers, selection of a satellite, and interrupt connection avoidance.

In addition of impairing the overall performance, the handover must be transparent for the end user. In these types of networks there is a need for mapping between the Universal Personal Telecommunications Numbers and IP addresses. Additional requirements with respect to t performance and scalability are:

- fast and seamless handoff
- low overhead signaling
- routing efficiency and effectivness
- QoS
- security support on various levels.

4 Configuration management

The goal of configuration management is to generate an integrated topological map of the whole system that displays all nodes (including access points in the wireless case), links, alarms, and consistent operating stages. Again, the problem eminates from the heterogeneous nature of wireless networks and network elements. Naturally, the description of the system and user status must be part of the whole configuration.

If a network operator wants to change a single parameter in a cell, then this change should be a subject to one action only across the board. Moreover, architectural changes in a particular network element should only affect that element and its manager (architecture-independent allocation strategy).

5 Performance management

The system for performance management according to [IE6] has two components:

- a set of functions that evaluates and reports on the behavior and effectiveness of network equipment, and
- a set of various subfunctions that includes gathering statistical information, maintaining and examining historical logs, determining system performance under natural and artificial conditions, and altering system modes of operation.

Data and information are collected from different networks segments, applications, and transport protocols. They are needed for e planning of future requirements and exploring trends, for better reliability, and response time. Performance management solution must include intelligent object modeling and graphical analysis tools.

Performance management within a technology domain should be consistent regardless of where and how the management action is being performed (from NOCs or remotely) or of the application of the network element within domain (BTC or RNC). An ideal performance management solution must be platform-independent and extensible as well as able to provide integrated and complete network coverage. It should allow service providers to monitor ongoing physical network performance, analyze its data to correlate end-to-end service performance, and to take action based on a complete understanding of network behavior, which enables the delivery of high-performance services to customers that of course are in demand and paid for.

6 Fault management

Very often faults in the system are due to the heterogeneous structure of wireless and mobile networks, hence there is an acute need for fault management. The problem with the 2G network management was that different vendors supplied their network elements with unique network element managers (Figure 2).The interfaces were different and the information models for generic information, such as alarms, were rarely standardized. The consequences for network operators were that network management systems became very complex. Many of them still are. Few of the difficulties the operators had to deal with are redundant or similar information at many levels, repeated knowledge of alarms, and inconsistent representation of similar information. Fault management covers ticketing administration behind the troubles, and simulation packages for prediction and problem status testing.

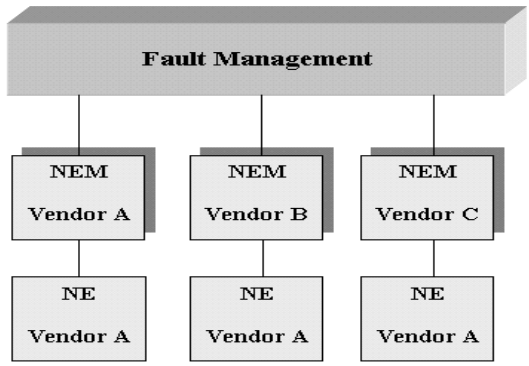


Figure 8: Fault management in 2G networks

7 Account management

The primary objective of the account management is to provide full interoperability between wireless network operators and service providers for the exchange of management and charging information. Account management includes also service level agreements - SLA and set of constraints and warnings in case there is chance for their violation. With occurrence of wide spectrum of new services, there are hardly any service providers that can cover them all, hence they have to cooperate. In such an environment it is very important t o resolve the billing and the exchange of the necessary data for evaluation.

In the early 1990s, billing of wireless services was based on voice minutes using call detail records - CDR. By the late 1990s when new services emerged, like two-way messaging, electronic voice-mail and e-mail, there was a need for new billing model. The so called flat-rate billing, with one bill for charging data and voice services. Later, this model has been replaced with billing by content, which has two objectives: to help service providers to determine

- type of data being transmitted over their networks
- how to capture revenue from the data being transmitted.

Today, 2.5G and new 3G networks support many new types of services, like streaming video, video conferencing, interactive on-line shopping, on-line banking, stock trading, sports reporting, etc. Next-generation billing mechanisms [IE7] must be capable of pricing data and content events in addition of voice calls. They have to be highly flexible, event-based and truly convergent. A number of new parameters for calculating charges can be used, like: number of packets, uploading or downloading of data, QoS, location, content etc.

An ideal billing system [IE7] must

- work in a real time
- adhere to open industry standards

- be highly modular to minimize total cost of ownership
- accommodate all current and future types of services
- support service bundling into cross-product packages to meet I-cenric needs and i markets (including a "customer-centric view" vs. a "service-centric view" of the account
- minimize design and development cycles
- enable each individual to manage his/her own customer portofolio

8 Security management

In general, security relates to the protection of network resources from both physical and remote access of unauthorized persons. Commonly, it is based on authentication of either persons (user name and password, certificates, biometric information) and/or devices (MAC). Confidentiality means need to protection data that are being transmitted over network.

Some clear security risks in the domain of wireless networks are due to the fact that these systems are frequently installed without paying sufficient attention to secure configuration and management. Many organizations do not use any tools that can assist them in monitoring, configuration, and maintaining the elements of the wireless network.

WLAN are liable to unclosing of confidential information, lose of data confidentiality and integrity, and system intrusion. They should be protected both from passive and active attacks.

A fairly frequent passive attack is eavesdropping. The attacker, equipped only with laptop and wireless network card can drive and move through an area and eavesdrop on the network. The information is easily harvested and even a connection to an access point is not a problem. Some protection from this kind of attack is the use of the IEEE 802.11 Wired Equivalent Privacy (WEP) protocol that ensures limited confidentiality (it has a lot of vulnerabilities). Additionally, access control lists related to the MAC addresses can be used. This is not an ideal protection because MAC address can be easily sniffed or changes via software.

The most common active attacks are DoS and "replay" attacks. Protection of network from these active attacks can be improved by:

- implementation of statistic monitoring and configurable alerts
- placing microwave ovens or cordless phones out of the range of WLANs, because their interference is similar to DoS attacks;
- encryption of the traffic;
- lower data rates in presence of significant excess capacity.

Other security risk is insertion of an unauthorized access point into a wireless network. Attackers usually camouflage installed access points or install radio antennas

on places with huge data traffic. Some wireless relays for retransmission have rang to 32km. Mobile phones connected with laptop can also be used like access point.

Leaking of RF signal is mitigated with [Ha2002]:

- selection of antenna and access point placement
- thermal insulated glass windows
- network situation away from high risk areas
- limiting signal power with attenuating transmitter power
- metallic-doped paints on the interior and exterior wall surface
- thin aluminum shielding of sensitive areas.

Intrusion detection may be based on different systems. RF Perimeter Detection System offers protection from attackers located outside a certain perimeter or via network separation to public and private domains. Signal Leakage System can detect abnormal signals emanating from the buildings. Then the administrator who actively monitors the RF perimeter and instantly notify management of a breach. Passive Monitoring Systems are quite similar to ones mentioned, however they work on the inside and can detect unknown Ethernet signals, unregistrated and cloned MAC, and unknown access points.

9 Radio resource and power management

Radio resource management includes management of downlink and uplink stream, multiple reuses of the same frequencies, traffic policing and shaping, and the provision of QoS.

The communication channel has the potential of being shared, hence traffic policing is very important. For network operator two aspects are crucial while providing channel access to customers:

- fair allocation of channel bandwidth among users
- prevention of misbehaving and greedy users

In addition, operators should provide services to the customers based on the nature of traffic, customer needs, and available resources. The peak rate of traffic from each subscriber must to be measured on a continuous basis and must be policed at every request from the subscriber. If this request exceeds its allocated rate, the grant must be delayed, thereby effectively controlling the rate of data transfer from the customer.

QoS is becoming increasingly important especially for real time and multimedia applications, as well as mission critical data transfers. For instance, the Resource reSerVation Protocol (RSVP) allows reservation of resources and guarantees minimal bandwidth, limited delay, and jitter. Problem arise when mobile nodes are located in occupied cell and demand additional bandwidth. Regrettably, IETF standards for RSVP are designed to guarantee QoS only for networks free from errors, which is still very far from the real life networks.

Another problem with wireless and mobile networks is energy consumption due to the very limited energy resources (short battery life). Hardware designers already have designed energy effective systems, but software designers are behind with designing software for mobile nodes which will incorporate power management. Current wireless network power management often substantially degrades the performance of the system. It may even increase overall energy consumption when used with latency-sensitive applications.

The Power-Saving Mode (PSM) of the IEEE 802.11, periodically disables the network interface. In many ways, the energy conservation without substantial performance degradation demands a power management strategy that is tuned to with the nature of the application, the usage patter, the mode of access, and features of the devices, and the characteristics of the network [An2003].

10 Conclusion

In the short history of data networks and the Internet, the issue of system management on all levels has become one of the most important ones due to the complexity of the networks, which reflects their heterogeneous nature with respect to the underlying technologies, the variety of protocols and the range of applications. In order to preserve the full functionality and induce efficiency and independence, as well as the modularity there is a need for a comprehensive set of protocols and tools to address problems with respect to mobility, performance, faults, accounting, security and resource management. This is even more acute whenever a network is defined as a collection of wired and wireless segments due to the specific problems in the wireless part such as the variety of mobile devices and services offered, the handover mechanisms, the bounds imposed on the processing power, storage and energy supplies, and the air as a transmission media.

On the other hand, network management, as any other service provided by the protocols in the upper layers should be technology independent, especially if the networks adhere to the IP paradigm.Hence, we examine and enumrate all the problems against the ideal network management system and along the specifics of each generation wireless and mobile systems. While it is clear that many problems are still open, and even aggregated with the 3G implementation, and the conception of 4G, there is a constant need for research and development of network managements systems since they deal with the most important aspects of the computer networks, including their reliability, security and proper and efficient performance.

11 References

1. [An2003] Anand M., Nightingale E. B., Flinn J.: "Self-tuning Wireless Network Power Management", *MOBICOM*, 2003
2. [Ha2002] Hassick, B.: "Simple Wireless Exposures in traditional networks", *Secure business quarterly*, Vol. 2, 2002

3. [Pa2001] Pahlavan K., Krishnamurthy P.: *Principles of Wireless Network: A Unified Approach*, Prentice Hall, December 2001
4. [Su2001] Sun J.-Z., Howie D., Sauvola J.: "Mobility management techniques for the next generation wireless networks", *International conference on Info-tech & Info-net,* Beijing, China, C:316-321, 2001
5. [Za2002] Zahariadis T. B., Vaxevanakis K.G., Tsantilas C. P., Zervos N. A.: "Global Roaming in Next-Generation Networks", *IEEE Communications Magazine*, February, 2002
6. [3G1999] 3GPP2: "3G Wireless Network Management System High Requirements", Revision 0, *3GPP2 S.R0017*, December 13, 1999
7. [Ie2001] IEC: "Performance Management for Next-Generation Networks", *The International Engineering Consortium, Web ProForum Tutorials*, http://www.iec.org
8. [Ie 2002] IEC: "Billing in a #G Environment", *The International Engineering Consortium, Web ProForum Tutorials*, http://www.iec.org
9. [Um2003]UMTS Forum: "Mobile evolution: Shaping the future", *UMTS Forum white paper*, August 2003
10. [Wa2002] Wavelink: "Securing 802.11 Wireless LANs", *Wavelink white paper*, http://www. wavelink.com