Implementing User Mobility in a Tactical Network

M. Malowidzki, M. Sliwka, T. Dalecki, P. Sobonski, R. Urban
Military Communication Institute
05-130 Zegrze
Poland

{m.malowidzki,m.sliwka,t.dalecki,p.sobonski,r.urban}@wil.waw.pl

ABSTRACT

In this paper, we describe our efforts leading to the implementation of transparent user mobility in a next-generation tactical network for the Polish Armed Forces. We discuss the management architecture, the implementation, and how various problems related to the communication technologies employed by the network have been overcome to achieve the goal. We also comment on how our approach complies with TACOMS recommendations on user mobility and assess interoperability capabilities with similar solutions implemented by other NATO member nations.

1.0 INTRODUCTION

A modern military tactical system should support a number of advanced communication services, delivered in a secure and fault tolerant way, together with an appropriate quality-of-service (QoS) level. The telephone service is one of the basic services; however, the requirement to make it work across various terminal types and for mobile users makes the implementation surprisingly complex in practice.

In this paper, we discuss the design and implementation of user mobility in the next-generation communication system for the Polish Armed Forces, which has been designed and implemented by the Military Communication Institute in cooperation with a number of companies. The network employs a few "state-of-the-art" technologies, such as IP, ATM and ISDN; this technological "mix" creates a real challenge for such a project. We especially focus on the telephone service, as this is the most basic service, supported by all terminal types. We discuss in detail, what was necessary to provide the service for mobile users, and how we have achieved the goal. Also, as mobility seems to be one of the leading standardization directions within NATO, we describe how we apply TACOMS project guidelines to assure future interoperability with other member nations.

The paper is organized as follows: First, we briefly comment on basic mobility types, according to TACOMS STANAG documents. Then, we describe the architecture of the next-generation broadband communication system for the Polish Armed Forces, and discuss involved subsystems and their technologies. Further in the paper, we present the mobility management architecture, and present communication scenarios in detailed steps. Then, we discuss interoperability perspectives according to TACOMS requirements. Finally, concluding remarks are made.

Malowidzki, M.; Sliwka, M.; Dalecki, T.; Sobonski, P.; Urban, R. (2006) Implementing User Mobility in a Tactical Network. In *Dynamic Communications Management* (pp. 13-1 – 13-8). Meeting Proceedings RTO-MP-IST-062, Paper 13. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

2.0 TACOMS MOBILITY

According to [7], three kinds of mobility exist:

- *Terminal Mobility*, which allows a terminal to attach to a TACOMS network at any user terminal access point (UTAP) that supports this terminal type;
- *User Mobility*, which enables a user (a person or a role) to use any terminal suitable for his needs within a TACOMS network;
- *Logical (Role) Mobility*, that allows to assign a role to any person capable to perform the role.

All these kinds of mobility are inter-related; in this paper, however, we focus on the implementation of user mobility in the context of the telephone service in the Polish national next-generation network.

2.1 TERMINAL MOBILITY

Two main types of terminal mobility may be defined:

- *Discrete Mobility*, when terminals are offline during motion. This kind of mobility is typical for most terminal types (IP, ISDN) except radio. For example, network nodes cannot work before they get connected to the core and configured;
- *Continuous Mobility*, when terminals are online even during motion. This kind of mobility is typical for radio terminals.

There is undergoing standardization work on terminal mobility within NATO, which includes both physical interface and higher-level services [1]. Currently, our network supports the physical interface for ISDN and IP terminals (L6 and L9 UTAPs [2]); the work on higher-level services, required to achieve full TACOMS compliance, is undergoing.

2.2 USER MOBILITY

The main goal of this work is to enable *transparent* and *fault-tolerant user mobility* across the whole (national) system. What we mean by "transparent" is that users should be able to freely change their terminal types (e.g., an ISDN subscriber switches to a radio station and is immediately available in the new location after a successful registration). Fault tolerance is a more complex issue, although in this context we mean that it should be always possible to make a connection within the same network node, and it should be possible to make inter-node connection as long as critical directory services are available and a physical connection exists.

3.0 THE COMMUNICATION SYSTEM

The general outline of the network's architecture is presented in Fig. 1. The network core is built using ATM technology, which integrates IP traffic generated by a management system and computer networks (LANs), and telephone traffic coming from ISDN subscribers. Besides, the ATM core provides some military-specific quality-of-service (QoS) features and improves fault tolerance.

Thus, the network is composed of three subsystems (see Fig. 1):

- The ISDN network, built with dynamic ATM SVC connections;
- The IP network, which is composed of LANs and WLANs, interconnected with the help of LANE/MPOA technology;

- The radio subsystem, which groups radio terminals (radio stations). The radio subsystem is connected to the IP network through Radio Access Points (RAPs), serving Radio Users (RUs).

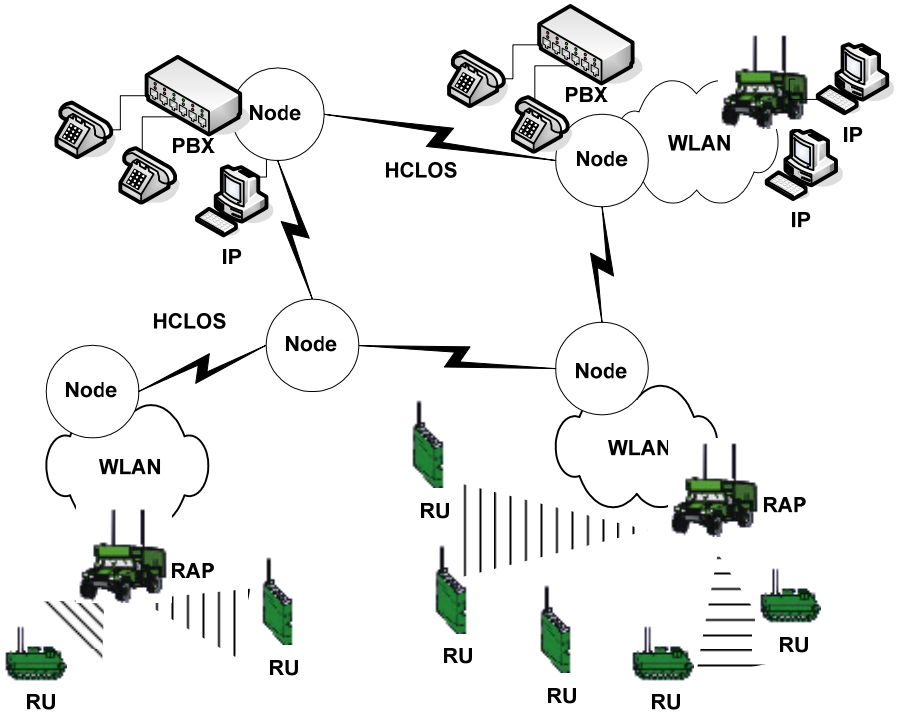

Fig. 1: The tactical network architecture

3.1 THE RADIO SUBSYSTEM

The radio subsystem includes Radio Users (RUs), Radio Access Points (RAPs), and the Radio User Registry (RUR). RUs are equipped with radio stations and dedicated PC terminals with management software. RAPs are attached to the IP network through WLANs. RAPs handle RUs registration and enable external communication (with the IP subsystem or, through IP, with ISDN). The RUR contains a database of all RUs and RAPs in the system, as it is a central management element of the radio subsystem. A RUR could be described as a combination of Gatekeeper and Directory Server, dedicated for the radio subsystem, and supplemented with additional processing logic and administrative functions. The registry is duplicated to provide fault-tolerance, with database replication performed in (soft) real time; also, the communication protocol between a RUR and RAPs has been designed with fault tolerance in mind. Finally, the registry cooperates with LDAP Directory Servers, described further in the paper.

3.2 THE IP SUBSYSTEM

The IP network is composed of a number of node-wide LANs, interconnected by the ATM core with MPOA/LANE technology. IP handles local (intra-node) VoIP connections as well as data communication and control and management traffic (e.g., SNMP). For the tactical network, we have selected the H.323 mobility model; one of the reasons for this choice was the fact that H.323 has been selected for TACOMS Interoperability Points [1].

3.3 THE ISDN SUBSYSTEM

The ISDN network is built atop the ATM core. ATM provides QoS guarantees for ISDN voice connections. All connections between PABX are served using ATM soft virtual connections (SVC), established on demand. Thus, routing for ISDN is handled by ATM, which assures fault tolerance.

ISDN technology provides some basic kind of mobility, called *number relocation*, which allows to redirect connections to a given number to another configured number. Thus, a user who has changed his location (i.e., the PABX where his number is allocated) may still be available in a new place. Unfortunately, this feature is not a real solution to user mobility, as it involves additional configuration complexity and, which is even more important, requires the home PABX to be available during connection establishment. This is a real obstacle to increase fault tolerance of the whole system.

Unfortunately, ISDN does not natively support user mobility, as mobility requires dynamic number resolution. Fortunately, for most typical PABX types, including the one employed in our system, a workaround exist. Using the supplementary *Call Deflection* feature and an additional, cooperating device (the so-called *Mobility Enabler for ISDN* (MEI)), all calls may be intercepted during the connection establishment phase, and redirected to an alternate, dynamically resolved ISDN number. This is further explained in the following sections.

4.0 MOBILITY MANAGEMENT ARCHITECTURE

The mobility management architecture, presented in Fig. 2, involves the following fundamental elements:

- *Battlefield Directory Servers* (BDs), accessed through the LDAPv3 protocol, which maintain a central registry of user profiles. These servers are duplicated, with replicated databases, to provide fault-tolerance. All other mobility elements that either need to acquire (for number resolution) or update (after user registration) information about current user need to refer to BDs.
- *Mobility Enablers for ISDN* (MEIs), which provide user registration capability (in a similar way as specified in [4] Appendix F) and enable dynamic number resolution for ISDN PABX devices (one MEI per PABX is required). An MEI can be regarded as a “mobility upgrade” for a PABX, as it provides, together with the PABX, a non-standard (non-TACOMS) ISDN UTAP.
- *H.323 Gatekeepers* (GKs), which manage H.323 zones. There is a one-to-one relationship between a network node and a H.323 zone. Gatekeepers cooperate with Directory Servers (during registration and address resolution) and gateways.
- *ISDN-IP Gateways* (GII), responsible for bridging between the ISDN and IP subsystems, with one gateway serving a single H.323 zone. Speaking in terms of [7], GII devices perform the ISDN/H.323 translation function.
- *Radio Users Registry* (RUR), which manages the radio subsystem and cooperates with the directory servers. As it was already mentioned, similarly to BD servers, RURs are duplicated.
- *Radio Access Points* (RAPs), which are gateways between the IP network and proprietary protocols, employed by the radio subsystem. *Radio Users* (RUs) are served by the access points and perceived outside of the radio subsystem as regular IP terminals.

Every user in the system is unambiguously identified using a dedicated *public number*, which performs the role of the TACOMS UID [6]. If the user is registered in the system (has successfully logged in), his profile in the BD server contains the information required for connection establishment, irrespectively of the terminal type the user is currently using. For the ISDN network, there is a dedicated directory attribute, which contains his *system* (actual ISDN) *number*. If the user has migrated to the IP or radio subsystem, this attribute will point to an appropriate GII gateway that serves the user’s H.323 zone.

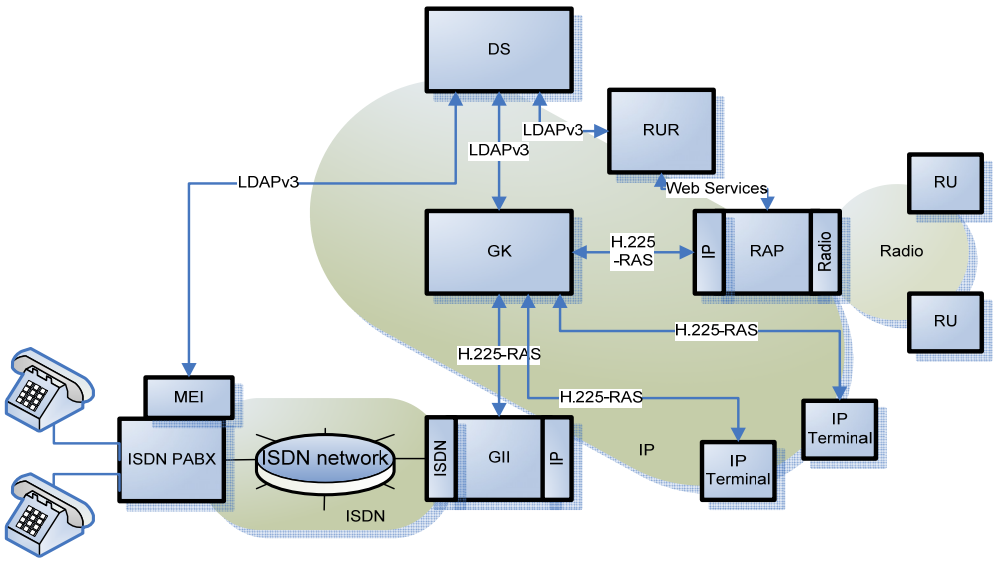

Fig. 2: The mobility management architecture

The user profile in the BD server contains a number of additional data, according to TACOMS requirements (as defined in [7]), including identity, priority, available services and helper location tracking attributes related to the mobility infrastructure.

5.0 COMMUNICATION SCENARIOS

To better explain how the mobility works, let us have a look at the process of connection establishment between two users who, at some point of time, make use of two different terminal types: an ISDN telephone (user A) and a radio station (user B). This is the most complex case, as the connection will cross all the three subsystems.

Before the connection can be made, both users must be registered in the system. User A may register with the help of the MEI device; similarly, user B registers in the RUR and BD through the RAP that is currently serving his radio station. When user A needs to communicate with user B, the connection is established in the following phases (Fig. 3):

1. User A dials user B's *public number*. User A's PABX recognizes a number from a *public numbering zone*; the call is redirected to the cooperating MEI element.
2. MEI contacts the BD server to learn the current ISDN *system number*. The call is immediately redirected to this number. Since user B is available in another subsystem, the number points to an appropriate GII gateway.
3. An ISDN call establishment request is forwarded to the gateway (with the public number attached).
4. The gateway contacts its gatekeeper to learn user B terminal's IP address (RAS ARQ/ACF messages are exchanged [9]). As user B belongs to the radio subsystem, this address points to a RAP, to which user B is attached.
5. A H.323 connection request (Q.931 Call-Setup) is sent to the RAP, as would be done for a plain IP terminal; the public number is still attached.

6. Using radio communications, the end-to-end voice connection is finally established.

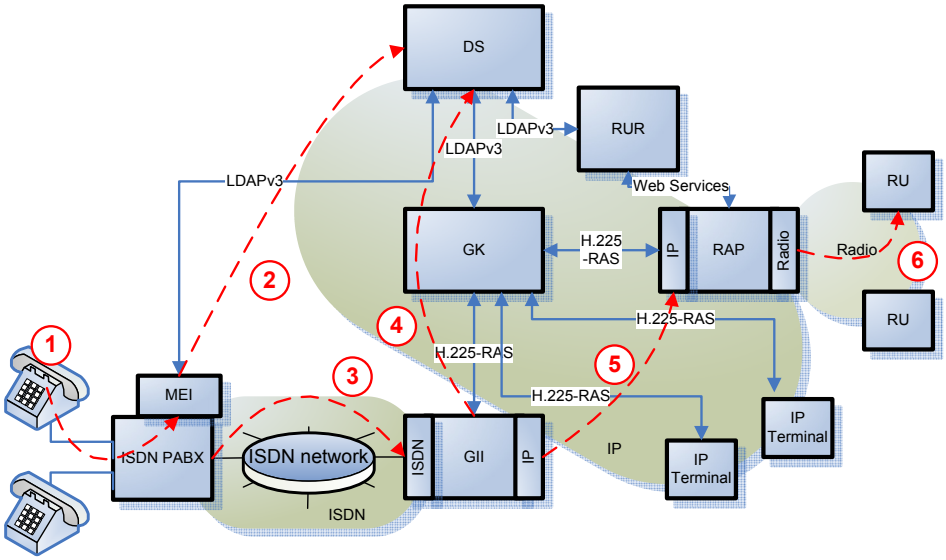

Fig. 3: The communication scenario

The same connection, made in the opposite direction, would be served as follows:

1. User B, using its terminal and a dedicated application, requests a connection to user A's public number; this request is forwarded to a RAP using a proprietary packet-over-radio protocol.
2. The RAP contacts the H.323 gatekeeper to learn the IP number of user A. As user A is not a local (zone) IP terminal, the IP address of the GII gateway is returned.
3. The RAP forwards the call to GII.
4. The GII contacts the gatekeeper to learn (via the BD) the current ISDN *system number*.
5. Finally, a plain ISDN connection is made. For a radio or an IP user from another network node, a system number of the remote GII gateway would be returned.

Note that we decided to route all inter-node connections through ISDN rather than over IP (LANE) to guarantee the required QoS level (QoS is provided by the ATM layer).

As it is easy to see, the whole process is complex, as it may require a number of BD lookups and may involve two or more gateways. However, in this way both location and terminal type transparency may be achieved. For example, from the point of view of the ISDN subsystem, all registered users are ISDN subscribers, and for the IP subsystem, all of them use IP terminals. All activities needed to make things work are handled by directory servers, gateways and gatekeepers.

6.0 TACOMS INTEROPERABILITY

Defining an interoperability framework is one of the most important yet challenging standardization tasks within NATO. Ideally, a future international communication system should support terminal and user mobility across national systems in a completely transparent way. There are three main components of such interoperability:

- physical interfaces
- communication services
- security and identity infrastructure

Physical interfaces and communication services are described in [1] and related documents [2], [3], [6]. This document specifies a protocol stack and services for all interoperability points (IOPs) as well as user terminal access points (UTAPs). For example, the selected stack for the W1 IOP is as follows [1] (from the bottom): fiber optic cable (Gigabit Ethernet), IEEE 802.3, limited MPLS, IP and, for the connection-oriented handling class, H.323 protocol family. Additionally, appropriate SLS QoS classes are defined for both *handling classes* (connection-oriented (CO) and connectionless (CL)). Although the CO class is far more complex in implementation, it can provide the required QoS level. Additionally, for these things to work, BGP must be enabled.

In the Military Communication Institute, we have developed the W1 IOP (for interoperability with other national systems) with the support for the CL handling class, with the QoS traffic classes mapped onto ATM QoS infrastructure. Our implementation has been successfully verified during the TACOMS Winter Exercises 2004 in Ede. Currently, we are working on the CO part of the interface.

We are also working towards providing TACOMS-compliant UTAPs for ISDN and IP. This requires, however, the implementation of full TACOMS Battlefield Directory, including TACOMS-specific extensions to DNS, LDAP and DAP [8], and the integration of the security infrastructure (e.g., authentication with RADIUS [5]).

Finally, national systems need to be compliant with the TACOMS (global) Numbering Plan [6] and the TACOMS (global) Addressing Plan; this should be relatively easy task, as these requirements only approve standard and reasonable rules in these areas, which we are already applying.

As we could observe during NATO exercises, national systems are still far from interoperability in the field of mobility. Given the complex infrastructure needed for TACOMS mobility, and also the required native (for the national system and its technologies) support for mobility, this fact does not surprise. However, works are undergoing and future field exercises are planned. Poland is going to build appropriate infrastructure to support the TACOMS interoperability, including all mobility issues.

7.0 CONCLUSIONS

The implementation of all required elements to enable user mobility for our system has proven to be a challenging task. In fact, the system has not been designed with mobility in mind from the beginning, and adding these features after some fundamental elements have been implemented (e.g., network elements, prototype vehicles, etc.) has proven to present a number of technical obstacles, related to both software and hardware. However, it is out of the question that a modern military network must support transparent mobility of its users and components. Additionally, mobility within the national system will be a cornerstone for full TACOMS mobility.

It is possible that had the network been completely based on IP, some of the mentioned problems would not appear (at least, we would get rid of the “technology mix” and some bridging issues). Well, despite advanced works on IP QoS, there is still lack of proven and commonly deployed solutions. Besides, our task was to solve the problem for a concrete network type that employs concrete communication technologies, still in use within NATO armies. Even after a migration to a “full” IP the work done for the IP and radio subsystems would remain useful.

To summarize, the implementation required the following:

- The implementation of the software infrastructure, namely, the Directory Services and the Radio User Registry.
- The deployment of the H.323 mobility model, together with appropriately modified Gatekeeper software.
- The implementation of gateways which would enable the voice communication to cross subsystem boundaries.
- Overcoming the technical limitations of ISDN technology, which has not been designed with mobility in mind. This required "patching" of PABX devices with additional appliances employing advanced functionality in a somewhat tricky way.

At present, we have a user mobility implementation for both IP and radio subsystems. The approach for ISDN has been technically verified, yet the work on the MEI device is undergoing. Where available, open source software has been used for this project [10], [11], [12]. Of course, we are still far from an implementation of full TACOMS mobility, and much work must still be done to achieve it, especially in the area of TACOMS-compliant terminal mobility. We are actively tracking recent NATO standardization efforts in the field of mobility. We participated in the TACOMS Fall Exercises 2005 and plan to participate in future events to practically check interoperability capabilities of our implementation.

8.0 REFERENCES

[1] STANAG 4637: TACOMS Head Stanag

[2] STANAG 4639: TACOMS *RTO-MP-IST-062*Interfaces

[3] STANAG 4640: TACOMS Lower Level Specifications

[4] STANAG 4641: TACOMS ISDN Access Protocols

[5] STANAG 4642: TACOMS IP Access Protocols

[6] STANAG 4643: TACOMS Connection Oriented Network Protocols

[7] STANAG 4644: TACOMS Connectionless Network Protocols

[8] TACOMS POST 2000, Validation Report (VR) – WP 13406 – Name and directory servers for tactical operations: Dynamic update and authentication; WP 13407 – Name server for tactical operations: Name resolution protocols, April 2004

[9] V. Kumar, M. Korpi, S. Sengodan, *IP telephony with H.323: Architectures for Unified Networks and Integrated Services*, Wiley & Sons, 2001

[10] OpenLDAP: http://www.openldap.org/

[11] OpenGatekeeper: http://opengatekeeper.sourceforge.net/

[12] OpenRadius: http://www.xs4all.nl/~evbergen/openradius/