MIKoBOS - A Mobile Information and Communication System for Emergency Response

Andreas Meissner
Fraunhofer IPSI
andreas.meissner@ipsi.fraunhofer.de

Zhou Wang
Fraunhofer IPSI
zhou.wang@ipsi.fraunhofer.de

Wolfgang Putz
Fraunhofer IPSI
wolfgang.putz@ipsi.fraunhofer.de

Jan Grimmer
Technical University of Darmstadt
jan.grimmer@gmx.de

ABSTRACT

The role of communication and information provision in coping with natural and man-made disasters and emergency situations is becoming increasingly important. In this paper we present an integrated mobile information and communication system, MIKoBOS, for emergency response operations that enables reliable data communication within the emergency site as well as between the site and the headquarters. It provides the responsible personnel involved in the emergency operation at different levels with anytime-anywhere access to relevant information. Compared to traditional voice-dominated approaches, the proposed system can greatly improve the effectiveness and efficiency of communication and coordination during disaster relief operations. Promising experimental performance results are provided for use with a number of terrestrial and satellite networks.

Keywords

Emergency Response Information Systems, Mobile C3I Clients, Mobile Communication, Satellite Communication.

INTRODUCTION

While many industries have now entered the information age, there is one sector where the use of information technology is still very much in its infancy: public safety, or more generally - emergency response. Despite their inherently mobile operations, fire and police departments in many countries still rely on manual information exchange and processing procedures, with modern IT being deployed only in their headquarters, if at all (Meissner et al., 2002; Meissner and Steinebach, 2004; Grasse, 2005). It is still very common for fire departments to carry files of paper in their command post vehicles and to use voice radio for the exchange of information between the emergency site and the headquarters. However, as an emergency situation may develop very dynamically, it is vital to have the right information at the right time, at the right place. The more this is accomplished, the easier it is to overcome what is known as the "chaos phase" at the beginning of a response operation, and to master the situation while it is evolving. In recent years, in particular after the events of September 11, 2001, the need and the role of modern communication and information systems in emergency response have been increasingly recognized by emergency services as well as by the academic world.

Currently there are few solutions to this problem in the market, ranging from the replication of an office-style environment in the command post vehicle (with email-based information exchange) to the installation of a full-blown client in the vehicle that provides the same work environment and functionality a dispatcher at the headquarter (HQ) would be used to (Fraunhofer ITWM, 2001). Knowing that emergency responders face a difficult, sometimes sketchy data communication environment, and knowing that the situation often does not allow for complex user interaction schemes, and knowing that integration with existing HQ information systems is the key for acceptance, we believe that the solutions in the market still leave much room for improvement. Moreover, the solutions we are aware of do not even address the challenge of providing support for senior or frontline personnel roaming at the site away from a vehicle, thus requiring a wirelessly connected personal information device.

This is why we have designed MIKoBOS, an easy-to-use Mobile Information and Communication System for Public Safety Organizations (PSO, known in German as "BOS"). MIKoBOS contains both a command post vehicle client that connects to an existing dispatch information system in the headquarters (currently integration with the commercial CKS-112 system [Tyco CKS-112] has been accomplished) and a component designed for PDA-style devices in the sphere of staff roaming at the site. The basic idea is that selected static and dynamic information at the

headquarters may be accessed in a downstream manner from the emergency site, and that some information - such as situation reports - may be created at the site and transferred upstream directly into the headquarter system. Regarding communication means, MIKoBOS uses a variety of wide area communication technologies, including satellite systems, for data exchange between the site and the headquarters, and it uses WLAN for site coverage.

MIKoBOS is currently a prototype, and in this paper we provide a snapshot of its current state of development. In the following section, we discuss requirements imposed on the system as well as the status quo. We then give a detailed look at the MIKoBOS architecture, including system and network aspects. In the experimental results section, we provide an evaluation from the user's perspective and analyze opportunities for optimizing communication performance. Finally, we conclude and provide an outlook on future work.

REQUIREMENTS VS. STATUS QUO

According to the definition of the US Federal Emergency Management Agency (FEMA), disaster management can be divided into different phases: mitigation, preparation, response and recovery. While mitigation and preparation usually are long term activities requiring information exchange in an office-like manner, response and, to a lesser degree, recovery are time critical activities requiring fast and reliable communication at the emergency site and between the emergency site and the different locations of involved organizations like police, fire departments, and medical emergency services.

Figure 1 shows a typical information flow during the response phase of an operation, which involves frontline responders, operation commanders and headquarters for intra and inter organization coordination. The operation staff at the site need to have access to various distributed information sources, such as hazardous material databases or digital maps of buildings or technical infrastructure. They also need to receive from their headquarters data such as operation plans, resource allocation plans, and dynamic information such as weather updates or simulations of possible hazardous situations, e.g. when smoke is moving towards an inhabited area. Selected information has to be forwarded proactively to the frontline responders, too. For this communication it is crucial to avoid information overload, i.e. that frontline responders receive only the necessary information at the right time. At the same time, operation staff should report current site status to the headquarters, such as measured data of various radioactive, chemical or biological contaminations, or requests for additional resources or personnel, to enable the construction and maintenance of a common operational picture, which is the basis for correct decisions at upper levels.

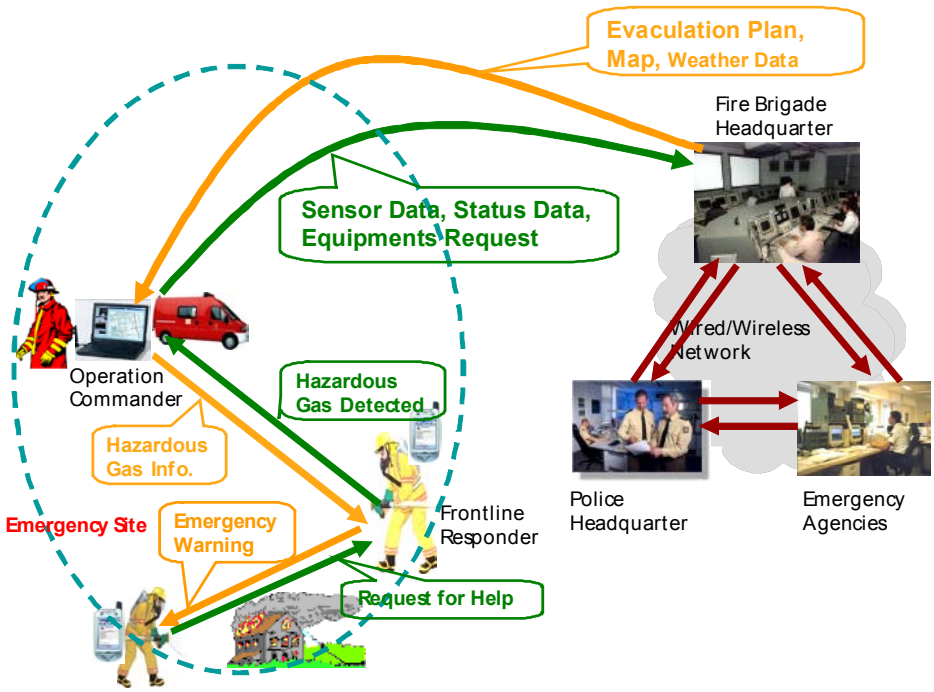


Figure 1. Information Flow during Emergency Operations

Nowadays, the communication among and between frontline responders, operation commanders and headquarters is still accomplished mainly through traditional voice communication, which has several disadvantages in nature. The

channel is usually insecure and error-prone. The frontline responder has to listen to voice messages carefully, at the same time he/she has to be focused on his/her immediate and critical mission. This situation calls for adopting modern information technology to improve communication and coordination during disaster relief.

After interviewing experts in the field and analyzing the state-of-the-art of technology currently used, we briefly summarize below some fundamental requirements for an information system for emergency response.

Rapidly deployable reliable data communication. Digital data communication provides not only improved communication quality and security, but also the possibility for accessing remote databases, communicating with head offices by using video conferencing and other collaborative tools. However, considering the fact that the public fixed communication infrastructure at a disaster site is often unavailable, destroyed, or overloaded, communication for response operations should rely on some kind of infrastructure which can be deployed by responders in a short time after they reach the emergency site. This requires readiness for dynamic and automatic configuration and adaptation of a communication infrastructure. Besides rapid deployment, disaster relief requires reliable and robust communication that is available in virtually any situation at any time. The communication technology has to resist environmental strains like great heat or water, and it has to provide connectivity at all times (MESA, 2005). While resisting the environmental strains is mainly a big challenge for hardware development, continuous connectivity calls for some level of redundancy in the topology of the network to cope with unexpected events.

Provision and distribution of information. The description of the information flow above shows that besides a secure and reliable connectivity it is important to guarantee that the right information be transferred at the right time to the right person. Some intelligent filtering and distribution mechanisms, primarily at the site control, are thus essential to avoid information overload for frontline responders. However, it should be guaranteed that all necessary information arrive in time. To this end, both push-based and pull-based information delivery approaches have to be supported. A typical example could be that the frontline responder pulls down the necessary information on the dangerous substance he/she found, and that the control site pushes down the floor map section where the responder is currently working. Moreover, the information should be distributed and presented in an appropriate format, since responders with different roles may have different types of terminals like laptops, PDAs, or even radio handsets, and user interaction may be difficult. An additional challenge is the seamless integration with existing information systems at the headquarters. On the one hand, such systems usually keep vast amounts of stored data, e.g. on hazardous materials, which might need to be accessed by on-site personnel. On the other hand, staff at the headquarters, due to their physical distance to the disaster site, need up-to-date information from the emergency site for the purpose of coordinating resources and taking decisions. The integration with existing headquarter information systems is essential for acceptance in practice.

Mobile Data Management. Mobile communication in a layered, fast changing network requires specific mechanisms to guarantee a consistent information exchange. It is a challenge to ensure data access and data consistency over low-bandwidth unreliable wireless links in an ever-changing environment. From our point of view, mechanisms like caching or prefetching should be adopted to optimize bandwidth usage and to reduce the impact of disconnection. Moreover, considering that critical data must obtain priority if the communication channel deteriorates, effective bandwidth management is an essential part in mobile data management.

However, current IT support for emergency response usually covers only a subset of these aspects. The conventional HQ information systems are conceived for stationary environments and based on fixed network infrastructures. Some approaches, like a recent project at the fire department of the German city of Leverkusen, extended the system by providing a full-blown client of the headquarter dispatch system in the command post vehicle, such that the same work environment and functionality are available at the emergency site after a VSAT setup time of some 15 minutes. Figure 7 (right) shows their ELW vehicle with the VSAT antenna. In general, such add-on extensions neither address the issue of rapid high availability of wide area communication, nor do they take the special needs at the emergency site, such as information exchange with frontline personnel, into account. There are also several other individual systems focusing on specific topics. For example, the ETSI/TIA project MESA (MESA) and the project WIDER (Nielsen and Mulligan, 2003) address mainly the network aspects in emergency response. The project SAFeR (SAFER) aims at supplying responders at the emergency site with information they need. However, it supports information delivery only in one direction, i.e. from the headquarters to the emergency site, based on static information provision. Exchange of dynamic information created during operations is thus impossible. The ongoing SHARE EU project (SHARE) is promising work towards IT support for cooperative decision making, featuring graphical tools and voice radio archiving with speech indexing, but it does not yet allow for integration with existing HQ systems. The NOAH project (NOAH) helps medical emergency service staff to gather patient information on

their handheld device and to transfer the collected information to the hospital by using mobile communication. While addressing an uncontested need, the NOAH project is designed only for medical emergency services and cannot be applied for general emergency response. Apparently there are no integrated solutions yet which provide reliable ubiquitous access to information from the emergency site and meet the requirements mentioned above.

MIKOBOS ARCHITECTURE

The aim of MIKoBOS is to improve the communication and the coordination within and between public safety organizations during disaster and emergency operations. Therefore, apart from meeting the requirements mentioned above, it is essential that the architecture of MIKoBOS be in line with the workflow of emergency operations. In the next sub-sections we present the architecture of MIKoBOS. We start with the overall system architecture and describe the different functional components. Network aspects are discussed subsequently.

System Architecture

The typical organizational structure of emergency services and the nature of disaster response operations imply that MIKoBOS is a multi-level distributed application. The MIKoBOS system consists of three application components: MIKoBOS-LS for headquarters, MIKoBOS-TEL for on-site operation commanders and MIKoBOS-EP for frontline responders roaming at the site. The software architecture of the overall MIKoBOS system is illustrated in Figure 2.

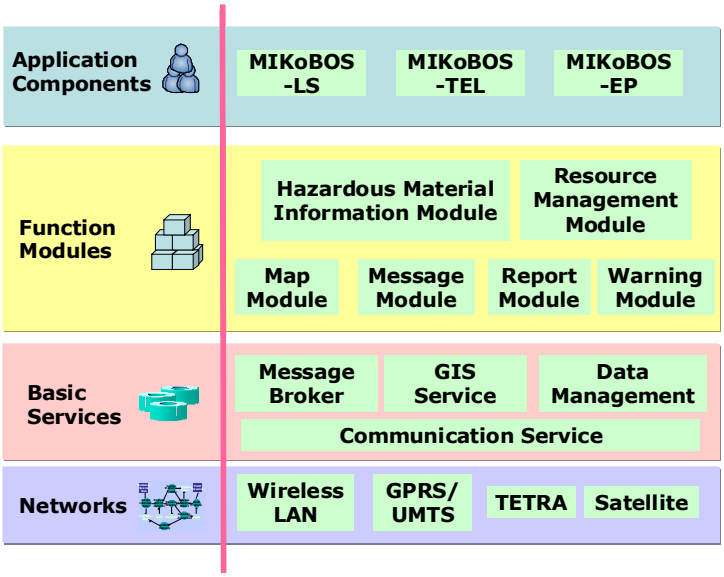


Figure 2. MIKoBOS System Architecture

In the architecture, the networks layer builds the communication infrastructure for MIKoBOS. Its detailed structure will be discussed in the next sub-section. The Basic Services provide commonly used functionalities for function modules. The communication service is a key component that is designed for the dual purpose of supporting multiple network technologies and providing a consistent interface for other modules to utilize communication regardless of the underlying technology used. To deal with the variability effect of underlying heterogeneous networks on communication performance, two application-level lightweight communication protocols are implemented by the communication service, one is based on TCP and the other is based on UDP. Both protocols have been designed with the intention of overcoming disadvantages of unreliable wireless communication – details and observations will be discussed in the next section. The communication service is also responsible for alerts of communication status changes, managing bandwidth allocation, and adapting the data stream to available communication conditions according to associated policies like priority. Upon the basic services, different function modules, such as the hazardous material information module and the resource management module, are built.

The three application components, i.e. MIKoBOS-LS, MIKoBOS-TEL, and MIKoBOS-EP, are configured to run on different hardware platforms with customized functionalities and user interfaces (Figure 3). MIKoBOS-LS is designed for dispatchers in headquarters and acts as a bridge for data exchange between MIKoBOS and the existing dispatch information system. Currently, we have integrated MIKoBOS with a leading headquarters software system, CKS-112 (Tyco CKS-112). With MIKoBOS-LS, headquarters staff can be informed of the current status at the

emergency site in near real time through different means such as collected data, text message, and pictures, which assist them in making a direct situation evaluation in order to come up with more informed decisions.

MIKoBOS-TEL, running on a robust notebook PC which is usually installed inside a command post vehicle equipped with power supply and diverse communication technologies, enables the operation commander at the emergency site to have access to central headquarters databases, to request new resources, and to report the current situation. All the data exchange is scheduled by the communication service based on available communications, message priority and message size. At the same time, MIKoBOS-TEL allows the operation commander to communicate with frontline responders in the field. For example, values taken from sensors may be transferred from responders to the operation commander, where the data can be stored, aggregated, and forwarded to the headquarters if needed. Similarly, the operation commander can reach frontline responders by different ways, either by specifying receivers explicitly (e.g. point-to-point or broadcast) or by sending messages to a selected group based on content or geographic location.

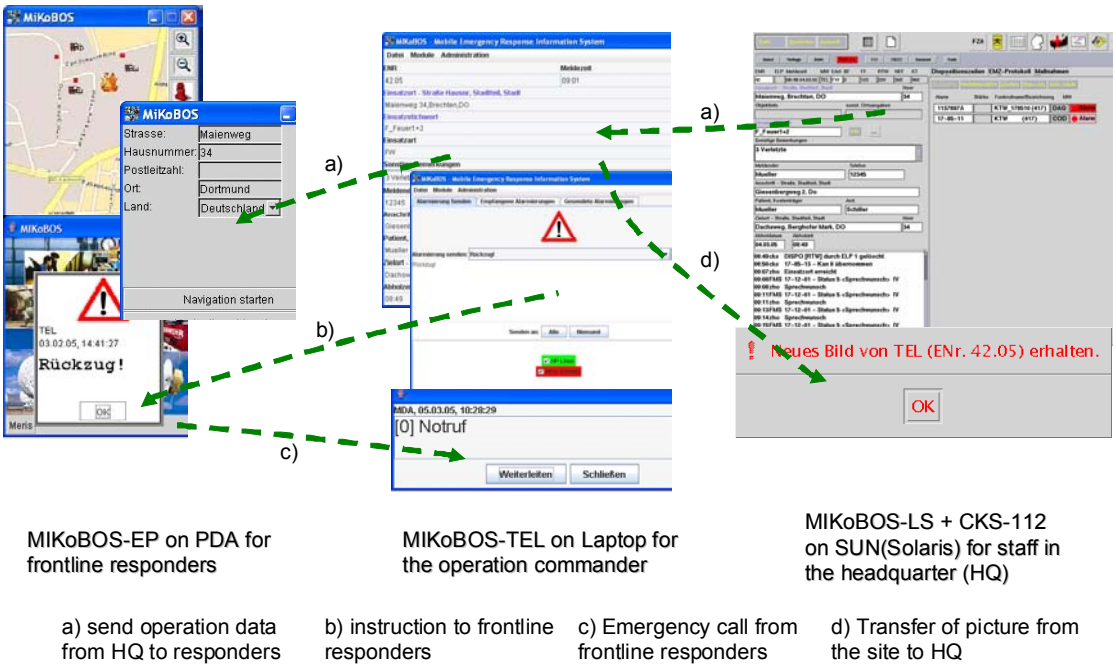


Figure 3. MIKoBOS Applications

While MIKoBOS-LS and MIKoBOS-TEL are mainly designed for operation control, MIKoBOS-EP, running on robust PDAs, is primarily conceived for frontline responders to send and receive information while they work away from vehicles. With MIKOBOS-EP, the frontline responders can access hazardous material information, transfer collected real time data of contaminants, send textual or visual situation reports to the operation commander, and receive instructions and warnings from the operation commander.

Network architecture

The IP-based MIKoBOS network infrastructure includes a local area network at the headquarters, wireless networks at the emergency site, and a variety of wireless wide area network links between the headquarters and the site, as shown in Figure 4. At the disaster site, broadband local wireless networks, such as IEEE 802.11 wireless LAN, are used. Three kinds of communication technologies are supported for the WAN connection: GSM/GPRS/UMTS-based public mobile networks, PSO-proprietary terrestrial trunked radio (TETRA), and satellite communication. For all of them, clients are easy to set up and can be deployed in a short time. However, each of them has its advantages and drawbacks. The GSM-based networks are well known and widely used technology. They provide relatively wide bandwidth at favorable prices with coverage in almost all inhabited areas in many countries. However, their operation is heavily dependent on some kind of fixed infrastructure, such as base stations, which may be totally disrupted in large-scale disasters (Kirchbach et al., 2002) – hurricane Katrina has recently shown the relevance of this concern. Another issue is that, due to its public accessibility, it is difficult to give higher priority for emergency communication over non-emergency communication. Therefore, responders cannot rely solely on such public

communication infrastructure in disaster response. In contrast to GSM/GPRS/UMTS, the terrestrial trunked radio networks (TETRA) (ETSI EN 300 392) may be specially deployed for and thus exclusively used by public safety organizations, which ensures their availability to some extent. However, data communication is not the focus of the current TETRA (phase 1) technology. It supports only 28.8 kbps data transfer rate, in most cases even less. Another issue is that TETRA is still to be widely deployed in some countries like Germany. As another alternative for WAN connection, satellite communication is well known for its high availability. They have very good outdoor coverage and are not affected by local disasters. Recently, new data oriented satellite services, such as Inmarsat's Regional Broadband Global Area Network (RBGAN) or Inmarsat M4 MPDS (Mobile Packet Data Service), are emerging, which makes mobile satellite communication more attractive for public safety organizations. However, satellite communication, compared to the other technologies mentioned above, is more expensive and usually needs an unobstructed line-of-sight to the satellite used. At the headquarters, a normal fixed connection to the Internet is configured for day-to-day usage with satellite communication as backup channel.

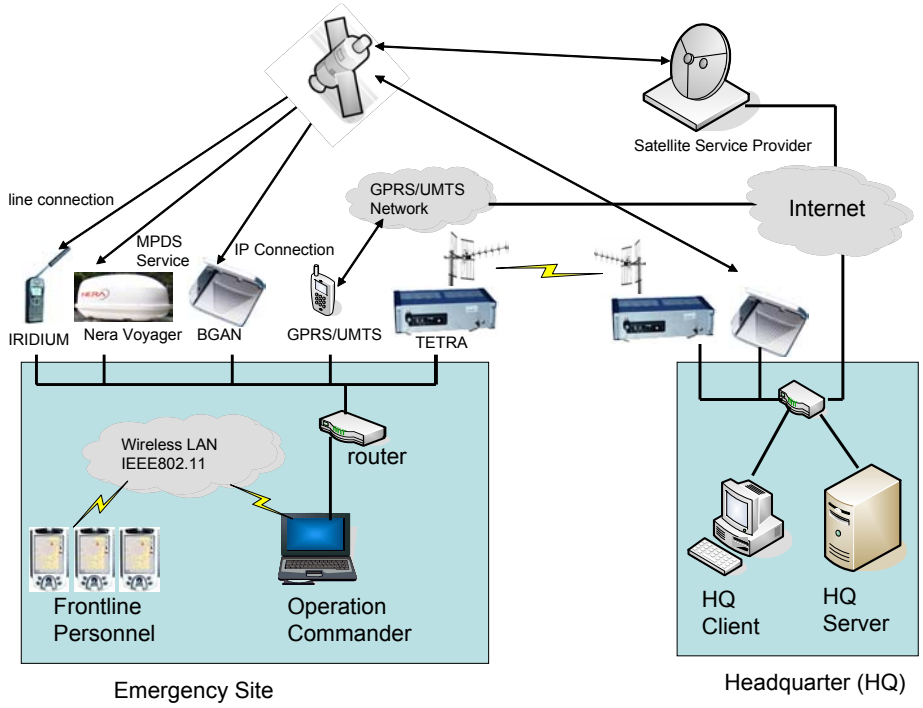


Figure 4. MIKoBOS Network Architecture

Therefore, it can be concluded that there is no single communication technology that fulfills the above-mentioned requirements in emergency response. As a consequence, MIKoBOS uses a network architecture supporting multiple communication technologies simultaneously, which is an essence for emergency operations. By integrating various technologies into one platform and by using them flexibly and interchangeably, the various communication alternatives can complement each other. If one network is unavailable, the system can switch to use another available option. The switch between different technologies can be done automatically according to pre-defined policies, or manually by an operation commander. In this way, an acceptably high availability of communication can be guaranteed without incurring extensive unnecessary costs.

EVALUATION OF COMMUNICATION PERFORMANCE

In order to evaluate the performance of MIKoBOS, we conducted two rounds of experiments. First, from a network engineer's point of view, we compared MIKoBOS' behavior in different communication modes, namely with either UDP or TCP in use for the communication link. Second, from a strict user perspective, we determined the delay between initiating the transmission of certain messages and the reception of those messages at the user terminal at the other end of the wide area link.

TCP/UDP Tradeoff

MIKoBOS works with various communication technologies that are heterogeneous in their network characteristics, such as latency, bandwidth, and link error rate. Prior analytical and experimental studies show that it is difficult and

inefficient to use only one message delivery mechanism for all kinds of links (Lakshman and Madhow, 1997). To optimize operation over heterogeneous links, two application-level lightweight protocols, based on TCP and UDP respectively, have been implemented in MIKoBOS. These protocols have the advantage that no protocol stack modifications or other configurations are necessary at the end devices, even when the underlying link is switched, and thus greatly ease deployment and guarantee interoperability. Additionally, a communication manager is built in the communication service. It decides which types of messages are delivered over which link by using which protocol. In this way, the switchover between protocols and networks is kept transparent for applications.

To investigate the performance of these two protocols and their suitability for different networks and message types, several performance measurements have been taken. In the experiments, both the TCP-based protocol and the UDP-based protocol have similar functionality, i.e. reliable delivery of messages with flow control. While this functionality is inherent in TCP, it is implemented in the UDP-based protocol by our own enhancements. With regard to flow control, three mechanisms, namely simple stop-and-go, sliding window, and sliding window with selective repeat, are provided for measurement.

The most widely used message types in MIKoBOS are text messages (up to some 150 bytes payload) and image messages (variable; ca. 51 kB for these tests). In our experiments, the round-trip time of delivering these two types of messages, i.e. the time used for sending a message from the emergency site to the headquarters and sending the same message back immediately after the message was received by the headquarters, was measured. Figure 5 shows evaluation results over various communication links including WLAN, GPRS, UMTS and satellite RBGAN.

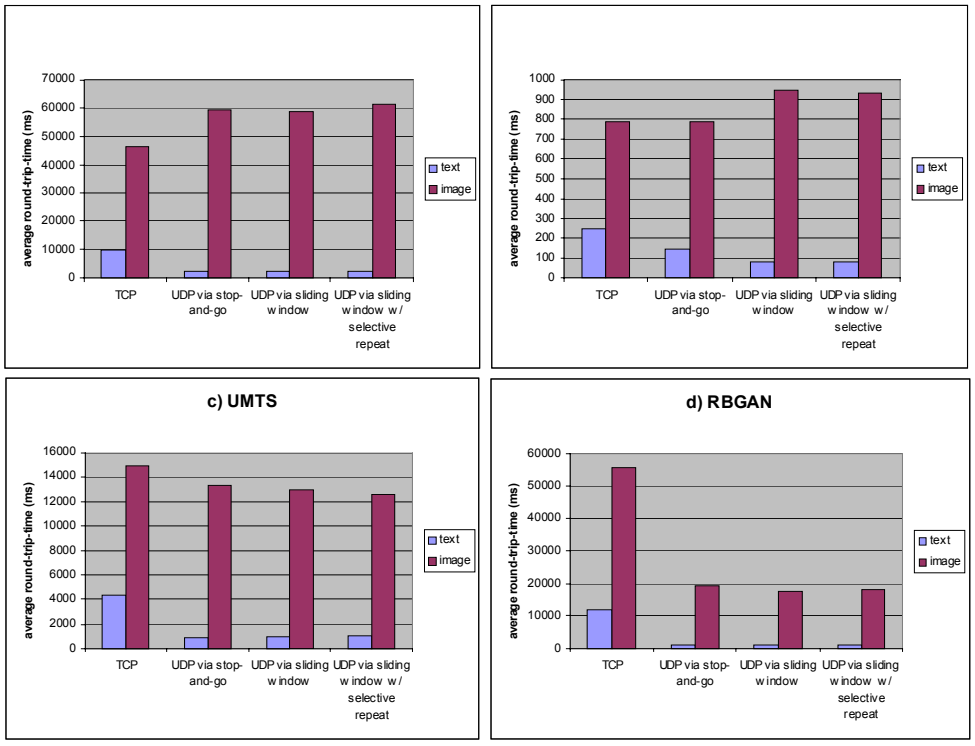


Figure 5. Evaluation of TCP vs. UDP Communication Performance

The results reveal that for small text messages, the UDP-based communication works much better than the TCP-based communication, no matter what kind of network is used. Moreover, the longer the latency of a network is, the greater the difference. The reason behind that is also evident. The TCP-based communication needs a long time for connection setup due to its three-phase handshaking mechanism. While the setup time could be ignored in fixed networks, it is noticeable in wireless networks with long latency. In particular, if the delivered message is very small, the setup time may amount to a great portion of the round-trip time. In contrast, the setup time in UDP is much shorter than in TCP, therefore the UDP-based protocol is advantageous for transferring a message with small size. For image messages, the advantage of the UDP-based communication can be noticed only in those links with a long delay, in particularly in the satellite link. This is due to the well-known performance issues with TCP over satellite links (Allman et al., 2000; Akyildiz et al., 2001). The long propagation delay and relatively high link error rate easily induce a data rate reduction in TCP without actual congestion.

The lessons we learned from these experiments confirmed our prognosis that different protocols should be used for different message types and different network situations, as we currently do in MIKoBOS.

Satellite Networks: Message Transmission Time from the User's Perspective

As previously stated, MIKoBOS is prepared for use on top of a number of wide area networks, including satellite networks that work independently of any terrestrial infrastructure in the emergency region. In order to determine if the message transmission time, as observed by the system users, remains acceptable even for those networks that are mainly designed for voice communication, we conducted a second round of experiments. In line with our intention to reflect a real-use scenario, we also decided to use VPN for a secure end-to-end connection between MIKoBOS-TEL and MIKoBOS-LS. The pre-set VPN tunnel configuration was IPSec-over-UDP; the way our VPN gateway was set up also provided for a known static IP address of the mobile client, so it was straightforward for the server to contact the client despite the dynamic DHCP IP address assigned by the respective satellite network's ISP.

In this experiment setup, we thus established a VPN connection between MIKoBOS-TEL and MIKoBOS-LS using, one after the other, RBGAN, Inmarsat M4 MPDS, Thuraya, Globalstar, and, as a reference, UMTS. With Iridium, VPN connection setup consistently failed, as discussed later. For the tests we made, apart from the Panasonic Toughbook CF-18 Windows XP laptop running MIKoBOS-TEL, use of the following communication hardware taken from our institute's Emergency Services Mobile Communications Lab:

- Inmarsat RBGAN: Hughes Satellite IP modem, connected to PC via Ethernet cable, allowing for up to 144 kbps
- Inmarsat M4 MPDS: Nera World Communicator Voyager with Vehicular Antenna Kit, in MPDS mode with up to 64 kbps; our test car (Figure 7, left) was parked in such a way that a line-of-sight to the satellite was ensured
- Thuraya: Hughes 7101 portable Thuraya phone (in satellite mode), allowing for up to 9.6 kbps
- Globalstar: Telit Sat 550 portable Globalstar phone (in satellite mode), allowing for up to 9.6 kbps
- Iridium: Motorola 9505A portable Iridium phone, allowing for up to 2.4 kbps in standard mode
- UMTS: Samsung Z107 UMTS phone, connected via USB cable

For each network alternative, we sent the following messages (with letters (A)-(E) given here for reference to the diagram in Figure 6):

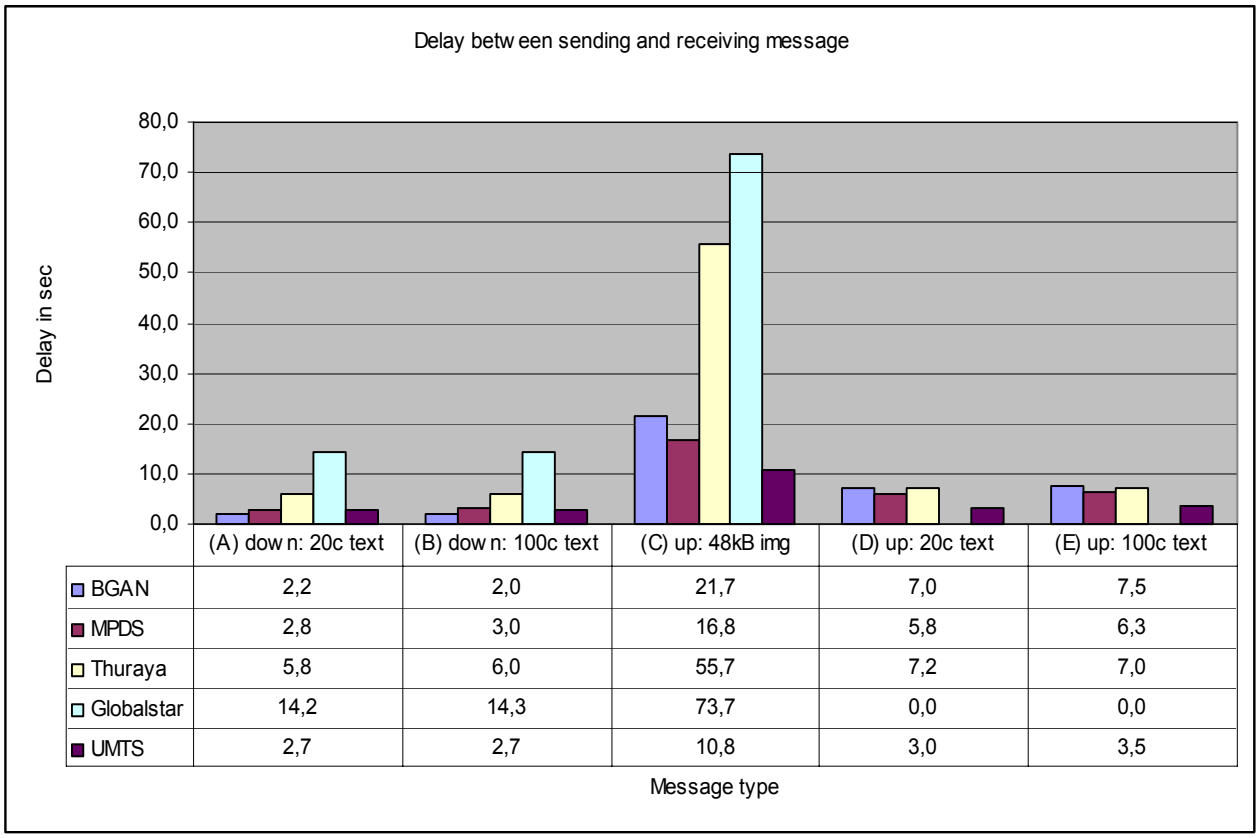
- MIKoBOS-LS → MIKoBOS-TEL (downstream):
  Warning text message with (A) 20 and (B) 100 payload characters, respectively,
- MIKoBOS-TEL → MIKoBOS-LS (upstream):
  (C) 48 kB JPEG image, FMS text message with (D) 20 and (E) 100 payload characters, respectively.

For each instance we measured, with six repetitions yielding an average, the delay between hitting the "send" button at the sender's side and the point of time when the message appeared at the receiver's screen. This is exactly what a user would base his/her performance judgment on.

As an indication of the overhead implied in the communication, we provide the total number of bytes transmitted from the sender to the receiver: (A) 2.8 kB, (B) 2.9 kB, (C) 55.5 kB, (D) 3.2 kB, (E) 3.3 kB.

For Globalstar, no data is available for experiments (D) and (E) because of a persistent problem with VPN connection setup. For Iridium, no data was collected at all since it was impossible to initially set up a VPN connection. This problem was actually expected, as it is well known in the community that Iridium data transmission is highly error-prone and subject to very frequent connection droppings and redial attempts. The reason for this observation is a high number of handovers caused by the fast-moving low-earth-orbit Iridium satellites; a brief deterioration in connection quality during a handover may be tolerable for voice communication, but for data connections, it often proves fatal. Among the three satellite networks designed primarily for voice calls, Thuraya worked best, which is not surprising as it uses a single geostationary satellite, so no handovers are required.

Using VPN with Inmarsat M4 MPDS is somewhat tricky, since a special IP configuration must be requested at the provider's earth station (France Telecom Mobilesat in our case), and even though the sophisticated Nera hardware we used is capable of keeping the antenna aimed at the satellite while the vehicle is moving, the connection is easily dropped when the line-of-sight remains blocked for more than a few seconds. For our on-site command post application, however, unlike the near-realtime sensor data transmission scenario we investigated in (Klappenbach et al., 2004), vehicle movements do not have to be supported.



	(A) down: 20c text	(B) down: 100c text	(C) up: 48kB img	(D) up: 20c text	(E) up: 100c text
BGAN	2,2	2,0	21,7	7,0	7,5
MPDS	2,8	3,0	16,8	5,8	6,3
Thuraya	5,8	6,0	55,7	7,2	7,0
Globalstar	14,2	14,3	73,7	0,0	0,0
UMTS	2,7	2,7	10,8	3,0	3,5

Figure 6. Performance from the User's Perspective

The observations shown in Figure 6 suggest that MIKoBOS can be reasonably used even when only non-terrestrial networks are available for linking the emergency site with the headquarters. Given the fact that with Thuraya and Globalstar, a one-minute call usually costs around one US dollar, transmitting essential messages is not more expensive than with 2G mobile phone networks a few years ago. Inmarsat M4 MPDS and RBGAN are charged on a volume basis (starting at US$ 10 per megabyte), so MIKoBOS traffic, which is typically bursty, is even better supported. In our view, RBGAN is the most appropriate technology for MIKoBOS among all satellite networks considered, with hardware investments of only a few hundred US dollars. With Inmarsat's current migration to BGAN with a much wider coverage area and even higher data rates, this service proves to be a good choice even for those organizations that operate on a worldwide basis for assistance in remote disaster areas.

CONCLUSION AND FUTURE WORK

In this paper, we have presented the mobile information and communication system MIKoBOS for disaster and emergency response operations. Special needs in such critical situations are investigated, and a multi-level system architecture meeting these needs is presented. From a technical point of view, the focus of MIKoBOS is to study the seamless integration of different types of mobile terminals and various heterogeneous mobile communication technologies, ranging from wireless local area networks to wide area communication networks including GPRS/UMTS and advanced satellite communications, having as an objective to support dynamic workflow management in a typical mobile application scenario. From the application's point of view, the contribution of MIKoBOS is to demonstrate the technical feasibility and potential to adopt mobile computing technologies in disaster and emergency operations. Our experimental results show that MIKoBOS can actually be used even in difficult communication environments calling for a satellite link. We believe that by giving responders at several levels anytime-anywhere access to requested information, the effectiveness and efficiency of disaster and emergency operations can be greatly improved.

Currently MIKoBOS is a prototype implementing core functionalities. Future work includes the extension of intelligent management of hybrid networks, as well as flexible support for resource scheduling and workflow management.

Figure 7. Test Platform Vehicle with rooftop Nera WC Voyager Vehicular Inmarsat Antenna; Leverkusen Fire Department's ELW with off-vehicle VSAT Antenna

REFERENCES

1. Akyildiz, I., Morabito, G. and Palazo, S. (2001) TCP-Peach: A new Congestion Control Scheme for Satellite IP Networks. *IEEE/ACM Transactions on Networking*, Vol. 6, 2001.
2. Allman, M. et al. (2000) Ongoing TCP research related to satellites. *IETF RFC 2760,* Feb. 2000.
3. RBGAN, Inmarsat Regional Broadband Global Area Network, http://regionalbgan.inmarsat.com.
4. ETSI, EN 300 392-x, Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D).
5. Fraunhofer ITWM, IGD, CRCG, IITB, UMSICHT (2001) Gemeinsame Studie: Marktanalyse Katastrophen- und Notfallmanagementsysteme, Kaiserslautern. (In German)
6. Grasse, T. (2005) Eine Systemarchitektur zur effizienten Steuerung von mobilen Einsatzkräften – Design und Implementierung. *Diploma Thesis, FernUni Hagen / Fraunhofer IPSI,* September 2005 (in German)
7. von Kirchbach, H. et al. (2002) Bericht der unabhängigen Kommission der Sächsischen Staatsregierung zur Flutkatastrophe 2002. (In German)
8. Klappenbach, D. et al. (2004) From Analog Voice Radio to ICT: Data Communication and Data Modeling for the German NBC Reconnaissance Vehicle, *Proc. ISCRAM 2004: International Workshop on Information Systems for Crisis Response and Management, Brussels, May 3-4 2004,* ISBN 9076971080.
9. Lakshman, T. V. and Madhow, U. (1997) The performance of TCP/IP for networks with high bandwidth-delay products and random loss. *IEEE/ACM Transactions on Networking,* Vol. 5, June 1997.
10. Meissner, A., Luckenbach, T., Risse, T., Kirste, T., and Kirchner, H. (2002) Design Challenges for an Integrated Disaster Management Communication and Information System, *The First IEEE Workshop on Disaster Recovery Networks,* June 2002, New York, USA.
11. Meissner, A. and Steinebach, M. (2004) Neue IT-Infrastrukturen im Notfall- und Rettungswesen - Potential und Risiko. *Kongress Netz- und Computersicherheit,* Universität Düsseldorf, Okt. 2003; Published by W. Bertelsmann Verlag in 2004, ISBN 3-7639-3205-4. (In German)
12. Nielsen, D. and Mulligan, C. (2003) WLAN in Disaster and Emergency Response (WIDER), Ericsson Response. *Workshop on Telecommunications for Disaster Relief,* Geneva, Feb. 2003.
13. Project NOAH: http://www.noah-regensburg.de
14. Project MESA (2005) Service Specification Group - Services and Applications; Statement of Requirements, *MESA TS 70.001 V3.1.2,* Jan. 2005.
15. Project MESA: http://www.projectmesa.org
16. Project SAFeR: http://www-cik.uni-paderborn.de/Forschung/SAFeR
17. Project SHARE: Mobile Support for Rescue Forces, Integrating Multiple Modes of Interaction, http://www.ist-share.org
18. Tyco Fire & Security, CKS-112: http://www.cks-systeme.de/cks_112.html
19. U.S. Federal Emergency Management Agency FEMA: http://www.fema.gov