Towards a Distributed Crisis Response Communication System

Dirk Bradler
TU Darmstadt
bradler@tk.informatik.tu-darmstadt.de

Benjamin Schiller
TU Darmstadt
schiller@rbg.informatik.tu-darmstadt.de

Erwin Aitenbichler
TU Darmstadt
erwin@tk.informatik.tu-darmstadt.de

Nicolas Liebau
TU Darmstadt
nicolas.liebau@kom.tu-darmstadt.de

ABSTRACT

Reliable communication systems are one of the key success factors for a successful first response mission. Current crisis response communication systems suffer from damaged or destroyed infrastructure or are just overstressed in the case of a large scale disaster. We provide an outline for a distributed communication approach, which fulfills the requirements of first responders. It is based on a layered network topology and current technology used in research projects or already established products. In addition, we propose a testing framework for the evaluation of a crisis response communication system.

Keywords

Crisis Response, communication system, distributed systems.

1. INTRODUCTION

Efficient communication architectures are vital for handling larger scale disaster management, and existing communication mechanisms have several shortcomings due to the heterogeneity of the first response groups. The need for reliable first response communications was one of the findings of the 9/11 attack on the Pentagon: [7] "In the first few hours, foot messengers at times proved to be the most reliable means of communicating." In this paper we present the requirements, current technology and simulation tools leading us to develop a first response communication solution, which is intended to be used after the existing communication infrastructure has been heavily damaged. Besides the massive overload in case of a disaster, interoperability between rescue groups is nearly impossible due to different radio frequencies and communication protocols [14]. In order to get realistic requirements and address the needs of first response helpers, we analyzed findings of disaster reports, research contributions and interviewed first response helpers. Based on the requirements we present a state-of-the-art technology overview of currently used technology and present research contributions, which might influence the next generation of first response communication systems.

2. SCOPE AND SCENARIO

We present an overview of the basic requirements and current technical solutions for a P2P-first-response communication system. We have analyzed different use cases and requirements in our earlier work [9]. The requirements are based on reports of first response cases as well as extensive telephone interviews with first response professionals. The main use of a distributed communications infrastructure in first response is in organizing on-site communications in situations where most of the existing infrastructure has failed. The on-site teams need a reliable group communication which supports the organizational hierarchy of the response teams. Communication takes place over wireless links and between small handheld devices carried by the personnel. The networks are typically augmented with access points or more powerful communication nodes (e.g., communication vans). Our goal is to augment the classical first response communication approach, which is often supported by foot messengers and replace these with a distributed communication system.

This paper is organized as follows. In chapter 3 we present design criteria and requirements for establishing a distributed crisis response communication (DCRC) system. Section 4 presents the proposed network topology of Homeland Security. Section 5 proposes necessary modules for a holistic simulation of the complete crisis response mission. Section 6 presents current technologies, which support the proposed network topology. In section 7 we conclude and give an outlook.

3. REQUIREMENTS

When a crisis occurs, first responders from different professions, organizations and jurisdictions meet. Helpers from fire departments, law enforcement agencies, emergency medical services (EMS) and government agencies must work together in order to manage the situation and save lives. Depending on the scenario, hazardous material (HAZMAT) workers, waste disposal technicians or victim rescue teams are also needed.

In order to work together successfully, first responders from all professions, organizations and jurisdictions need a way to communicate with each other. They must be able to communicate with their colleagues, the command center and other first responders.

The reliance on voice-oriented communication alone is one of the three major problem areas of first responder systems identified by [2].

Communication Types and Devices Types

The information content of voice alone is not rich enough and can easily be misunderstood. In order to support first responders appropriately, they need the possibility to exchange information of miscellaneous types: Floor plans and area maps can provide better orientation; images and videos of the incident scene can help the command center to make more informed decisions instead of just relying upon voice messages.

The lack of interoperability is also a major problem. Most agencies and departments use different systems and equipment for communication. Sometimes not even police and firefighters from the same county are able to communicate inter-disciplinarily using their standard devices.

Information Infrastructure

The third major problem is the limited situational awareness of first responders and command center. Even if a good way of communication is established, the command center cannot rely on reports from first responders alone. They need access to databases, maps, personnel location, etc. to overview the situation and make well informed and fast decisions based on reliable information and a complete picture of the incident.

In order to meet any of these requirements, an incident scene network must be established. It is formed without any existing infrastructure and is dismissed when the mission is accomplished. Connectivity between all participants must be provided as well as seamless communication across incompatible devices and agencies.

The system is mobile and temporary in nature and needs to be scalable to the dimension of the incident. It must allow mobile users and cannot rely on specific users or specific relay stations. Users must be able to connect or disconnect at any time without affecting the system negatively.

Network Structure

Mobile communication devices carried by first responders could simply form a wireless ad hoc network to communicate. Since the mobility pattern of first responders is not predictable, this kind of network is not reliable [3]. Therefore, nomadic relay devices should be used, that can be carried and deployed by first responders. They form a stationary ad hoc backbone network to link first responders to each other. Considering the nature and properties of incident scene networks, a flexible architecture is needed to establish a reliable communication infrastructure. A peer-to-peer (P2P) network is the perfect fitting solution. P2P networks are decentralized, distributed and server-less. They self-organize in a so called overlay network and don't rely on a single entity's performance or availability. All peers in the system can connect to each other direct or via any path. The architecture is flexible enough to add features subsequently to address future needs [2], [1]. Hence, using a P2P overlay network on top of an established connection of all participants will perfectly meet first responders' needs. In order to support first responders, different types of information need to be exchanged [12]. Voice-oriented messages will always be important and require strict timeliness and high quality. Live video feeds from the incident scene improve situational awareness and make remote meetings and assistance possible. Databases need to be accessible and the needed information must be presented to first responders in a helpful way. Therefore the underlying network infrastructure needs to meet certain delay requirements as discussed in [3].

Communication Schemes

When looking at the information exchange of first responders, two different types of information flow can be identified: vertical (upward and downward) and horizontal (parallel) communication [12], [8]. Vertical communication represents the information exchange between entities at different levels of the command hierarchy. It flows upward from first responders to commanders or downward from the command center to first responders. Horizontal communication includes all information flows between first responders. Figure 1 shows the vertical and horizontal communication needs of first responders. Therefore a communication infrastructure needs to implement different communication interfaces. These interfaces must be implemented such that they overcome interoperability issues between heterogeneous devices and agency policies. One-to-one as well as one-to-many communication schemes must be available to address messages to certain first responders or groups according to their location and profession.

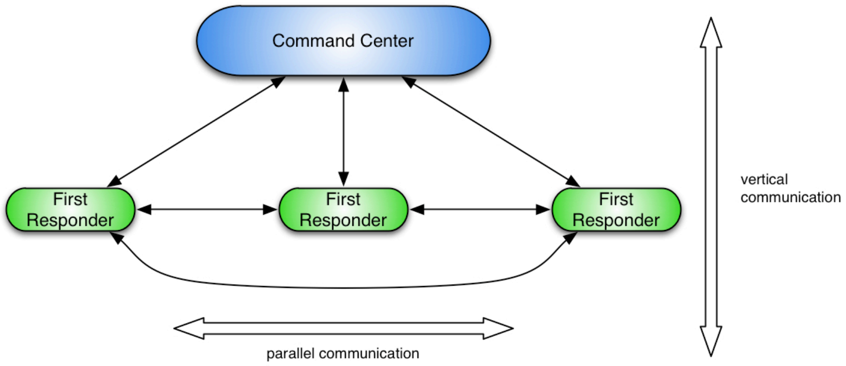

Figure 1 Information flow during crisis response

Design Criteria

Design criteria for incident scene communication networks can be derived from the presented requirements. The system must be interoperable to exchange information across organizational domains and consider different security policies and service level agreements. The network needs to be scalable, self-organizing and self-recovering to ensure the upkeep of communication flow in case of failures and malfunctions. Users and information flows need to be prioritized according to role and direction. Also, security mechanisms need to be implemented to ensure confidential and secure information exchange. Furthermore, the network must be protected against vulnerabilities and threats from attackers [12].

4. SYSTEM OF SYSTEMS

In the SAFECOM report [15], the Department of Homeland Security introduces the so called "System of Systems". It describes a network topology used to meet the requirements of first responder communication during an incident. It is designed to provide connection between first responders and to the command center.

In [12], a similar network is described. The authors also survey implications on the architecture of first responder networks and discuss design criteria.

These communication networks are **mobile** and **temporary in nature** since they must be deployed without the presence of an infrastructure. They are dismissed when the mission is accomplished. They must allow the integration of other networks to connect incident scenes and provide access to remote information sources. To support incidents of any size and allow first responders to connect or disconnect at any time, the architecture needs to be **scalable** and **dynamic**.

In present systems, communication often takes place between first responder and command center. First responders cannot communicate among each other. Neither they nor the commanders are able to send messages to a certain subset of all helpers or address all personnel in a certain area. **Multicast**, **publish subscribe** systems and similar communication models are required to close this gap. These group communications are only possible if a network is established, that allows connections between every involved person.

While the primary objective is to transport information between first responders, the infrastructure must also allow the exchange of video feeds and miscellaneous data. This is necessary to raise the level of situational awareness.

The **System of System's** network is hierarchically structured. It consists of *PANs*, *IANs*, *JANs* and an *EAN* which are logical concepts. The hierarchy with the proposed connection method is shown in Figure 2.

Personal Area Networks (*PANs*) represent the set of devices which are carried by first responders or embedded in their clothing. These small-scale networks are used for communication among a first responder's devices and sensors. They may be wired via USB and FireWire or wireless using technologies such as Bluetooth. First responders can wear heart rate monitors and location sensors to record information about their health and track their position. They can carry video cameras to record live video feeds from the incident scene. These feeds can be transmitted to the command center to increase situational awareness.

Each first responder carries a Public Safety Communications Device (*PSCD*) which is his primary tool for communication with other helpers and the command center. It links the first responder's *PAN* to *IANs* and thereby connects him to the network. It also connects the first responder's devices in the *PAN*, records data from sensors and sends them to the command center. In [12] these devices are called First Responder's Communication Devices (*FRCDs*).

An Incident Area Networks (*IAN*) is centered on wireless access points such as droppable relay devices or vehicle-mounted nodes. They are deployed on demand and create multi-hop ad hoc wireless networks to connect *PANs* and *JANs*. It thereby acts as a gateway for mobile first responders that connects them to the network. These access points are deployed at the incident scene and can scale to the magnitude of the emergency.

Jurisdiction Area Networks (*JANs*) form the main communication network by handling the access of *IANs* to the network and the *EAN*. They also provide connection to a *PSCD* if the responsible *IAN* fails. This private network of agencies handles access to sources and information via the command center. It is of a more permanent nature and includes communication towers. If no *JAN* node is available, *IANs* will form an ad hoc network among themselves to maintain connectivity.
The Extended Area Network (*EAN*) is the backbone network for connecting *IANs* and *JANs*. It provides access to the internet as well as county, regional, state and national systems. This includes databases and communication services to off-site personnel.

When planning a new first responder communication system, the presented network topology should be used to maintain connection between first responders and command center at all times.

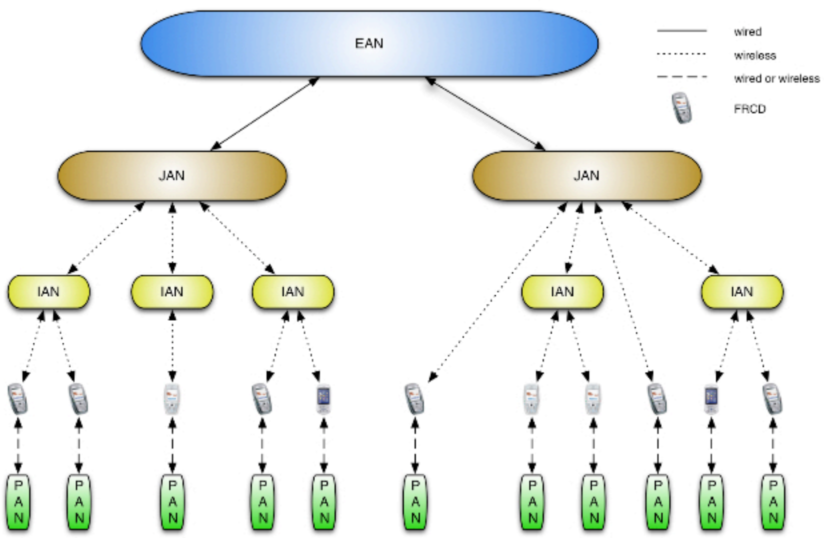

Figure 2 Communication Hierarchy proposed by Homeland Security

5. ANALYSIS BY SIMULATION

Testing a Distributed Crisis Response Communication System in a large scale scenario would require a prohibitive high effort. Therefore, simulations are the preferred evaluation method during development. Simulating a first response scenario involves from a simulation point of view three separate simulation domains: the communication **network simulation**, the peer **movement simulation** and the **environment/disaster simulation**.

Network simulation is a widely used approach in order to identify the runtime behavior of a proposed communication system. Network simulators can either be used in order to simulate a distinct part of a protocol very precisely or they are used to evaluate the large scale connections and effects between several hundred up to thousands of devices. In order to simulate a first response communication approach, specific details of protocols need to be neglected in order to be able to simulate a large scale rescue scenario with distributed communication architecture. There are many P2P simulators, which are built especially for a large number of distributed devices and are therefore a good choice for simulation of first responder communication. The following criteria are used for evaluation of suitable network simulators: System architecture, usability, scalability, result presentation, extendibility. Table 1 shows a selection of well known P2P simulators, with individual strengths and weaknesses, they are all developed in the JAVA programming language, except *OMNeT++*, which is developed in C++.

Both inactive network simulators (GnutellaSim and Query-Cycle-Sim) were not considered as candidates for network simulation. OMNeT++ is actively developed, but the C++ programming language makes it dependent on a specific platform.

The simulators *PlanetSim* and *Peerfact.KOM* are both well structured and come with a good documentation. They have clear interfaces for all needed functionality and provide the possibility to generate reports. *PeerSim* was more scalable than any other simulator under test, but this comes with a high abstraction, network delay is not modeled at all in this simulator.

In addition to network simulation, movement models need to be established in order to simulate a first response mission. Heinemann [11] summarizes the **movement models** Manhatten Grid, Gauss-Markov, and Random Waypoint as follows:

Table 1 P2P Network Simulators

Simulator	**URL**	**Focus**	**Status**
PeerSim	http://peersim.sourceforge.net	High scalability	Active
Peerfact.KOM	http://sourceforge.net/projects/peerfactsim	Complete system, precise network models, and peer locations	Active
PlanetSim	http://planet.urv.es/planetsim	Flexible architecture	Active
GnutellaSim	http://www.cc.gatech.edu/computing/compass/gnutella	Special purpose simulator	Inactive
OMNeT++	http://www.omnetpp.org/index.php	Strong GUI support	Active
Query-Cycle Sim	http://p2p.stanford.edu/www/qcsim.htm	File Sharing	Inactive

The **random waypoint** is simple and often used [6, 13, 10]. Within this model, a mobile node begins by staying at one location for a certain period of time, the so-called pause time. Once the pause time expires, the mobile node chooses a random destination in the simulation area and a speed. This speed is uniformly distributed between a predefined minimum and maximum speed. The mobile node moves towards the newly chosen destination at the chosen speed. Upon arrival, the mobile node pauses for a new randomly chosen pause time before starting the process again.

In the **Manhattan Grid model**, mobile nodes move only on predefined horizontally and vertically arranged paths. This model mimics a typical street network in an urban area. A mobile node starts at a randomly selected position on a path, chooses its speed between a defined range and direction and moves along a path. Periodically the chosen speed is adjusted. In addition, a node may pause for a certain time or turn its direction at a crossing.

The **Gauss-Markov Model** eliminates sudden stops and sharp turns encountered in the Random Waypoint Mobility Model by allowing past velocities and directions to influence future velocities and directions. A mobile node is assigned a certain speed and direction. Periodically new values for speed and direction are chosen from a normal distribution with a mean of the respective old value. Speed values are constrained to a certain interval. If a newly chosen speed value is outside this interval, it is reset to the closest value inside the interval.

These movement models are not especially adapted for crisis response situations. In [4], we propose to add roles and behaviors to each moving entity. Different classes define mood and tasks, which influence the movement decision for each entity.

Disaster simulations like a fire are already required for each public building, the National Institute of Standards and Technology (*NIST*) provides analysis software for the aspects Outdoor Fire (ALOFT-FT), Sprinkler Response (*LAVENT*, *DETACT-QS*, *DETACT-T2*) and a fire dynamics simulation toolkit (*FDS*), which calculates the fire and smoke propagation with a computational fluid dynamics (*CFD*) model

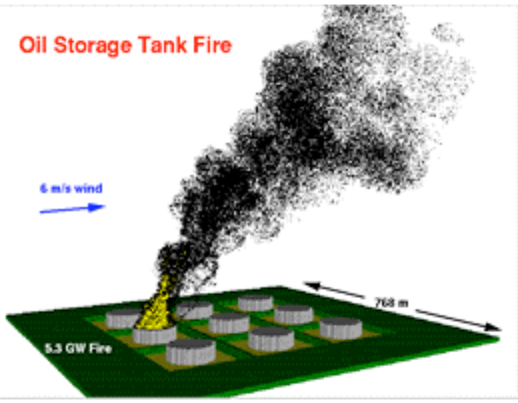

Figure 3 FDS and Smokeview Simulation

Figure 3 shows a graphical representation of *FDS* and *Smokeview* simulating an oil storage fire; the simulator can be used for indoor scenarios as well. These simulations are needed in order to quantify the effects of a *DCRC* system in terms of the needed time span and the chosen procedural method.

Integrating network, movement and disaster simulation in one simulation framework is goal of current research activities. An early prototype which integrates network simulation and movement simulation is already available [4]. Figure 4 shows a typical disaster scenario, the First Response Communication Sandbox (*FRCS*) is able to simulate both concurrently, movement of all involved persons and vehicles and the corresponding wireless network [5]. Nevertheless disaster simulations of buildings or any outdoor equipment is not yet integrated and part of future work.

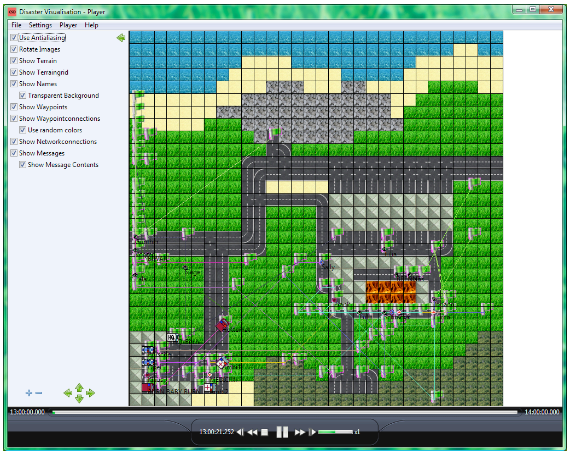

Figure 4 First Response Communication Sandbox

6. TECHNOLOGY

PSCD: Public Safety Communication Device

PSCDs are the personal devices of first responders. They record data from the Personal Area Network (*PAN*) and also provide the link to the higher-order Incident Area Network (*IAN*). Communication over the *IAN* allows first responders to convey information to the command center and to receive orders or notifications.

Computing devices come in many different form factors and use different input and output methods. However, regarding their user interfaces there are only two large distinct classes, namely *ears & mouth* and *hands & eyes* devices. The former draw their efficiency mainly from the semantic richness developed over millennia (speech, music, etc.) and from the orthogonal usability in many working contexts ("hands-free operation"), the latter draw their efficiency mainly from the output bandwidth (a picture is worth more than a thousand words) and input intuitivity. Controls may resemble well-trained activities such as steering, drag-and-drop, or pointing.

The application domain requires the *PSCD* to be designed as a wearable computer. Because the user interface should only put a minimum of additional cognitive load on the user, neither computers with head-up displays, nor traditional palmtops qualify as good solutions. Using wearables with head-up displays and single-handed keyboards (e.g., Twiddler) puts a very high cognitive load on the user, because computer interfaces using unnatural modalities are used while the wearer is performing some other, more primary, task in the physical world. An audio-based device with a speech user interface is more natural to use and does not require the level of attention that reading a display or operating a keypad would require. The most important functionality of the

PSCD is speech communication with the command center or within peer groups. Consequently, the interaction with the computer should also take place in the same modality. The advances in speech recognition over the past few years also allow using it in noisy environments, e.g., pilots of the interceptor plane *Eurofighter* can use voice commands to control the communication systems of their plane.

Properties of Networking Technologies

Similar to the performance of microprocessors, the capacity of wireless networks is also increasing drastically. Notebook computers primarily access the local area network using the IEEE 802.11a/b/g/n WLAN standards. The development leads towards higher data rates, while the relatively high power consumption of WLAN is considered to be tolerable for notebook computers. However, WLAN is not suitable for many other applications. Beside higher data rates, one of the following aspects may be more important when designing a specific device:

Power consumption: In many cases, sensors sleep most of the time. If they are equipped with wireless network interfaces, it is important that listening for incoming data packets does not consume much energy. The ZigBee and IEEE 802.15.4 standards were specifically developed for sensor networks and address this issue. Similarly, the low power requirements of GSM when solely listening for incoming calls enable to build cellphones with long standby times.

Size: Bluetooth modules together with the necessary antennas are considerably smaller than WLAN or GPRS solutions. ZigBee products are not yet very mature. However, the industry is working on complete system-on-chip (SoC) solutions containing microcontroller, baseband, and radio.

SCO/ACL: In addition to Asynchronous Connection Less (ACL) connections, some technologies support Synchronous Connection Oriented (SCO) connections. The latter are required to enforce data rate and latency guarantees on the Media Access Control layer for the transmission of audio, media, or sensor data streams.

Number of nodes: For example, a Bluetooth piconet is limited to one master and 7 slaves. Furthermore, only a master can initiate the communication, inquiry is slow and consumes a lot of power. With these properties, Bluetooth is suitable for PANs, but a bad choice for ad-hoc networking and event-driven applications.

Level of Mobility: The maximum UMTS data rate of 2 Mbps is only available at short range for terminals moving slower than 10 km/h. 384 kbps are usable up to about 120 km/h, and 144 kbps up to 500 km/h. GSM is designed for a top speed of 250 km/h. The extension GSM-R allows for using GSM handsets on high-speed trains with 300 km/h and more. According to tests, WLAN can be used up to 80 km/h.

These considerations indicate that no single wireless networking standard existing today meets the requirements of all possible applications in the emergency response domain. We will have to cope with a heterogeneous landscape of different standards suited for certain applications only. In addition, multiple wireless networks using different standards will be available in the same region of space.

PAN: Personal Area Network

The Personal Area Network is a small-scale wireless network for communication among devices and sensors, carried or embedded in clothing. The *PSCD* is the central communications hub of a person and has three different networking interfaces: a wired field bus, a low-power wireless radio, and a WLAN radio. The first two allow communication with other devices in the PAN, while the latter one forms the uplink to the *IAN*.

A wired field bus allows connecting small devices, such as sensors embedded in clothing to the *PSCD*. It could be implemented using the Controller Area Network (*CAN*) standard. Since radio communication always costs additional power, a wired bus is very efficient in terms of energy. In addition, peripherals can be directly powered through the bus.

To integrate wireless devices in the *PAN*, the ZigBee standard can be used, which has been specifically designed for low-power sensor applications. Technologies like WLAN or Bluetooth do not meet these requirements. Consequently, body worn sensors are mostly based on proprietary radio technologies today, e.g., the Nike+iPod shoe pedometer or Polar heart rate monitors.

The WLAN interface of the *PSCD* provides the uplink into the *IAN*. Compared to the *PAN*, it requires a higher range and a higher bandwidth. Therefore, it will also require more power. To implement this radio interface, the well-established 802.11 standards can be used.

IAN: Incident Area Network

The Incident Area Network (*IAN*) is deployed on demand in the incident area. The *IAN* can be fully built based on 802.11 and Internet standards. The basic 802.11 infrastructure can be provided by access points integrated into police cars, *EMS* vehicles, and vehicles of other emergency services. If the range of a network is insufficient, then it can be extended using WLAN repeaters. Such repeaters can be deployed ad-hoc on ground or in the air using small balloons.

Internet technologies such as Dynamic Host Configuration Protocol (DHCP) allow *PSCDs* to join the *IAN* in an ad-hoc manner. When *PSCDs* contact command centers or access databases in the Internet, the corresponding addresses can be obtained using the standard Domain Name Service (DNS). To find mobile resources provided by other peers in the *IAN*, discovery can be implemented based on the Web Service standards, i.e., WS-Discovery.

JAN: Jurisdiction Area Network

A Jurisdiction Area Network (*JAN*) is a private network of an agency, e.g., police or an *EMS*. Through the *JAN*, the specific command centers can be reached for secure database access, certificate management, task dispatch, and resource mobilization. The vehicles by such agencies provide the base infrastructure for the *IAN* and provide radio uplinks into the specific *JANs*. On the lower layer, these uplinks will utilize various radio technologies, while the higher layers can be fully based on Internet standards.

Such uplinks can be implemented using Terrestrial Trunked Radio (TETRA). If it is necessary to support also remote incident sites, satellite radios, e.g., based on the Iridium technology can be used as a fallback. In addition, it is advisable to utilize the civil cellphone networks, such as GSM, UMTS, or CDMA2000, because they add additional redundancy to the communication system, provide high mobile data rates, and the associated technology is cheap and small. However, because civil networks tend to be overloaded in case of large accidents, a separate network such as TETRA will always be the first choice.

On the higher layers, such uplinks will be realized using Internet tunnel protocols, such as the Point-to-Point Protocol (PPP), or the Point-to-Point Tunneling Protocol (PPTP).

EAN: Extended Area Network

The *EAN* is based on the infrastructure of the Internet. Different agencies can interconnect their individual *JANs* by using secure Internet tunnels. *IANs* may also connect directly connect to the Internet and then use secure Internet tunnels into specific *JANs*, thereby participating in the *EAN*.

7. CONCLUSION AND OUTLOOK

We presented the requirements, the technology and the simulation approach needed in order to build a *DCRC* system. While the underlying technology is either already available or in the phase of research prototypes, it will be just a matter of time until a complete *DCRC* solution is available. The management of crisis response situations did not adapt to the new communication possibilities, yet. Already established management schemes are based on a strict command and control approach. This is applied almost worldwide, but with a new communication system, nearly every team is able to get an overview of the whole crisis at any time. Future management approaches should allow communication between peers.

Decisions may be faster, because they are not slowed down by a bottleneck somewhere in the organizational hierarchy. The flexibility provided by modern and future crisis response communication systems must be considered already today when designing crisis response processes. We expect to see a more distributed organization of crisis response teams in the future.

REFERENCES

[1] AS Bahora, T. Collins, S. Davis, S. Goknur, J. Kearns, T. Lieu, T. Nguyen, J. Zeng, BM Horowitz, and SD Patek. Integrated peer-to-peer applications for advanced emergency response systems. Part II. Technical feasibility. In *Systems and Information Engineering Design Symposium, 2003 IEEE*, pages 261–268, 2003.

[2] AS Bahora, TC Collins, SC Davis, SC Goknur, JC Kearns, TN Lieu, TP Nguyen, JS Zeng, BM Horowitz, and SD Patek. Integrated peer-to-peer applications for advanced emergency response systems. Part I. Concept of operations. In *Systems and Information Engineering Design Symposium, 2003 IEEE*, pages 255–260, 2003.

[3] J.Q. Bao and W.C. Lee. Rapid Deployment of Wireless Ad Hoc Backbone Networks for Public Safety Incident Management. In *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, pages 1217–1221, 2007.

[4] D. Bradler, K Panitzek, I. Schweizer, and M. Muehlhaeuser. First response communication sandbox. *11th Communications and Networking Simulation Symposium*, pages 115–122, 2008.

[5] Dirk Bradler, Jussi Kangasharju, and Max MÃ¼hlhÃ¤user. Demonstration of first response communication sandbox. In *CCNC'2009 Demonstration Proposals*, Las Vegas, USA.

[6] J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 85–97. ACM Press New York, NY, USA, 1998.

[7] Prepared by Titan Systems Corporation. Arlington county after-action report on the response to the september 11 terrorist attack on the pentagon. 2002.

[8] R. Chen, R. Sharman, H.R. Rao, and S. Upadhyaya. Design Principles of Coordinated Multi-incident Emergency Response Systems. *Lecture Notes in Computer Science*, 3495:81–98, 2005.

[9] Dirk Bradler and Jussi Kangasharju and Max Mühlhäuser. Systematic First Response Use Case Evaluation. *Workshop on Mobile and Distributed Approaches in Emergency Scenarios*, 2008.

[10] J.J. Garcia-Luna-Aceves, M. Spohn, and CALIFORNIA UNIV SANTA CRUZ DEPT OF COMPUTER ENGINEERING. Source-Tree Routing in Wireless Networks, 1999.

[11] A. Heinemann. Collaboration in Opportunistic Networks. *Doctoral Thesis*, 2007.

[12] Y. Huang, W. He, K. Nahrstedt, and W.C. Lee. Requirements and System Architecture Design Consideration for First Responder Systems. In *Technologies for Homeland Security, 2007 IEEE Conference on*, pages 39–44, 2007.

[13] S.J. Lee, W. Su, and M. Gerla. On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks. *Mobile Networks and Applications*, 7(6):441–453, 2002.

[14] B.S. Manoj and Alexandra Hubenko Baker. Communication challenges in emergency response. *Communications of the ACM*, 50(3):51–53, 2007.

[15] Department of Homeland Security. Public Safety Statement of Requirements for Communications & Interoperability - Qualitative. In *The SAFECOM Program - Volume I, Version 1.2*, pages 49–56, 2006.