Technische Universität Braunschweig
Institut für Betriebssysteme und Rechnerverbund

Studienarbeit

Entwurf eines auf Ad-hoc-Netzen basierenden Informations- und Kommunikationssystems zur Nutzung bei Großschadenslagen und Katastrophen

von
cand. Wirt.-Inf. Oliver Tacke

Aufgabenstellung und Betreuung
Prof. Dr. Lars Wolf, Dr. Marc Bechler und Dr. Andreas Meißner

Braunschweig, Juni 2005

Kurzfassung

Ziel dieser Arbeit ist es, ein auf einem Ad-hoc-Netz basierendes Informations- und Kommunikationssystem für den Einsatz im Notfall- und Rettungswesen bei Großschadenslagen und Katastrophen zu entwickeln, das als Proof-Of-Concept beispielhafte Funktionen vor Ort demonstrieren kann. Darunter fallen z.B. das Sammeln, Auswerten und Verteilen von Patientendaten. Berücksichtigung finden müssen u.a. der Datenschutz, Dynamik und unterschiedliche Leistungsdaten der Knoten des Netzwerkes sowie dementsprechendes Routing und Anforderungen an die Dienstgüte.

Resultat sind vier in Java geschriebene Demonstrationsprogramme, die für unterschiedliche Geräte innerhalb des Systems zuständig sind, und die über Bluetooth und WLAN miteinander kommunizieren. Führungskräfte erhalten die Möglichkeit, einen Überblick über eingesetzte Helfer zu erhalten und mit diesen Nachrichten auszutauschen. Gleichzeitig können Sie Sensordaten von entsprechenden, sich im Einsatz befindlichen Geräten abrufen. Eingesetzte Helfer erhalten über ein mobiles Gerät, welches im einfachsten Fall ein handelsübliches Mobiltelefon sein kann, ihre Einsatzaufträge und geben stets ihren aktuellen Status an. Verknüpft werden die Geräte über WLAN/Bluetooth-Gateways, die gleichzeitig als Zwischenspeicher für Sensordaten agieren.

Inhaltsverzeichnis

Seite

Abbildungsverzeichnis

Abkürzungsverzeichnis

AODV	Ad-hoc On-Demand Distance Vector Routing
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
DRK	Deutsches Rotes Kreuz
ISM	Industrial, Scientific, Medical
J2ME	Java 2 Micro Edition
JSR	Java Specification Request
LAN	Local Area Network
LNA	Leitender Notarzt
MAN	Metropolitan Area Network
MANV	Massenanfall von Verletzten/Erkrankten
MIDP	Mobile Information Device Profile
NIDA	Notfall Informations- und Dokumentations-Assistent
OrgL	Organisatorischer Leiter
PAN	Personal Area Network
SanEL	Sanitätsdienstliche Einsatzleitung
SEG	Schnelleinsatzgruppe
TEL	Technische Einsatzleitung
TSF	Tree Scatternet Formation
UML	Unified Modeling Language
WAN	Wide Area Network
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

1. Einleitung

Besonders bei Großschadenslagen und Katastrophen herrscht bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) ein hoher Bedarf an Kommunikation und Koordination. Während digitale Informations- und Kommunikationssysteme in zentralen Leitstellen bereits Einzug gefunden haben, muss von den Einsatzkräften vor Ort meist auf analoge Geräte zurückgegriffen werden. Es besteht in diesem Bereich allerdings ein erhebliches Potenzial zur Verbesserung der Einsatzbewältigung durch die Nutzung von moderner Informationstechnologie. Es ist offensichtlich, dass sich am Einsatzort wegen der in der Regel nicht vorhandenen oder zerstörten Kommunikationsinfrastruktur Ad-hoc-Netze anbieten.

Zu den wichtigsten Informationen vor Ort gehört für Führungskräfte die Kenntnis von Art und Anzahl der Einsatzkräfte und des vorhandenen Materials sowie von deren gegenwärtiger Verwendung. Weiterhin können vielfältige Daten der Umgebung oder von hilfsbedürftigen Personen von Interesse sein. Ein auf Ad-hoc-Netzen basierendes Informations- und Kommunikationssystem soll der effizienten Beschaffung, Verarbeitung und Distribution der Informationen dienen. Dabei können entsprechend ausgestattete Personen und Ausrüstungsgegenstände Knoten repräsentieren, die sowohl als Datenquelle als auch als Datensenke agieren. In den meisten Fällen wird ein solches Netzwerk heterogen aufgebaut sein. Für Fern- und Lokalnetze kommen möglicherweise unterschiedliche Technologien zum Einsatz und die Spezifikationen der einzelnen Knoten hinsichtlich Speicherausstattung, Sende- oder Prozessorleistung sind typischerweise verschieden.

Ziel dieser Arbeit soll es sein, ein auf einem Ad-hoc-Netz basierendes System zu entwickeln, das als Proof-Of-Concept beispielhafte Funktionen für den Einsatz vor Ort demonstrieren kann, z.B. das Sammeln, Auswerten und Verteilen von Patientendaten. Hierbei ist dem Datenschutz durch geeignete Kryptographieverfahren Rechnung zu tragen. Es soll untersucht werden, wie die Knoten sinnvoll verteilt werden können, um z.B. auch innerhalb von Gebäuden die Kommunikation sicherzustellen. Dabei ist die mögliche Dynamik der Knoten sowohl durch Bewegung als auch durch Ausfall zu berücksichtigen. Je nach Art und Einsatz der Knoten können die Anforderungen an Sendeleistung, Zuverlässigkeit oder Geschwindigkeit der Übertragung variieren. Diese unterschiedlichen Charakteristika sollen berücksichtigt

werden, indem z.B. angemessene Routingverfahren genutzt werden. Einsatzkräfte müssen sich auf ihre eigentlichen Aufgaben konzentrieren können und sollten in Gefahrensituationen nicht unnötig abgelenkt werden. Es ist deshalb bei der Anwendung auf eine einfache und möglichst intuitive Handhabbarkeit zu achten. Da Leben von der Zuverlässigkeit und Robustheit eines solchen Systems abhängen können, müssen Überlegungen zur Dienstgüte Berücksichtigung finden.

Nach einem kurzen Abriss der Problemstellung und der Zielsetzung dieser Arbeit erfolgt im zweiten Kapitel eine definitorische Einordnung des Begriffs der Ad-hoc-Netze sowie der Begriffe, die nicht der Informatik zuzuschreiben sind. Im folgenden Teil wird ein knapper Überblick darüber gegeben, wie derzeit größere Einsätze von BOS ablaufen. Es sollen ein Überblick über bestehende Prozesse und Stellen für mögliche Verbesserungen aufgezeigt werden. Der vierte Abschnitt widmet sich der Anforderungsanalyse an ein Informations- und Kommunikationssystem, wie es durch BOS verwendet werden könnte und die zuvor aufgezeigten Probleme umgehen kann. Dabei sollen die eingangs erwähnten Punkte Berücksichtigung finden. Kapitel 5 befasst sich dann mit dem Implementierungsdesign. Der sechste Abschnitt fasst die wesentlichen Punkte der Arbeit abschließend zusammen und gibt einen Ausblick auf eine mögliche weitere Entwicklung bei Informations- und Kommunikationssystemen im Bereich der BOS.

2. Definitionen

In den folgenden Abschnitten werden Begriffe definiert, die für die Arbeit von wesentlicher Bedeutung sind. Neben Ad-hoc-Netzen, die die Grundlage für das zu entwickelnde System bilden, sind dies „Behörden und Organisationen mit Sicherheitsaufgaben“ und „Großschadenslagen und Katastrophen“. Diese stammen nicht aus dem Bereich Informatik und bedürfen daher näherer Erläuterung.

2.1. Ad-hoc-Netze

Knoten eines Computernetzwerkes sind im Regelfall stationär und kommunizieren über Kabel. Dies trifft sowohl auf die Hosts als auch auf die Router zu. In Ad-hoc-Netzen hingegen sind beide über eine Funkverbindung gekoppelt und mobil. Host und Router sind normalerweise in demselben Computer untergebracht (vgl. Tanenbaum (2003), S. 414). Die Topologie des Netzes kann ständigen Veränderungen unterworfen sein bedingt durch Bewegung oder Ausfall einzelner Knoten. Dadurch ergeben sich Besonderheiten für das Routing infolge der sich laufend ändernden Pfade.
Als weiteres Merkmal von Ad-hoc-Netzen kann das Fehlen einer zentralen Instanz betrachtet werden (vgl. Tanenbaum (2003), S. 87); die einzelnen Rechner kommunizieren direkt untereinander. Ist dies nicht möglich, z.B. weil die direkt Funkverbindung gestört ist, werden nach Möglichkeit andere Rechner als Überbrückung genutzt (vgl. Perkins (2001), S. 4). Dies ist möglich, weil jeder Knoten sowohl als Host als auch als Router dient. Solche Netze werden auch als Multi-Hop-Netze[1] bezeichnet. In Abbildung 1 ist ein solches dargestellt. Die Geräte (Knoten) A und C können nicht direkt kommunizieren, da sie zu weit voneinander entfernt sind. Da beide jedoch innerhalb der Sende- und Empfangsreichweite[2] von Gerät B liegen, kann dieses als Zwischenstation Nachrichten zwischen A und C vermitteln.

1 Im Gegensatz dazu stehen Single-Hop-Netze, bei denen nur direkt mit Knoten in Reichweite kommuniziert werden kann.

2 Sende- und Empfangsreichweite können unterschiedlich sein.

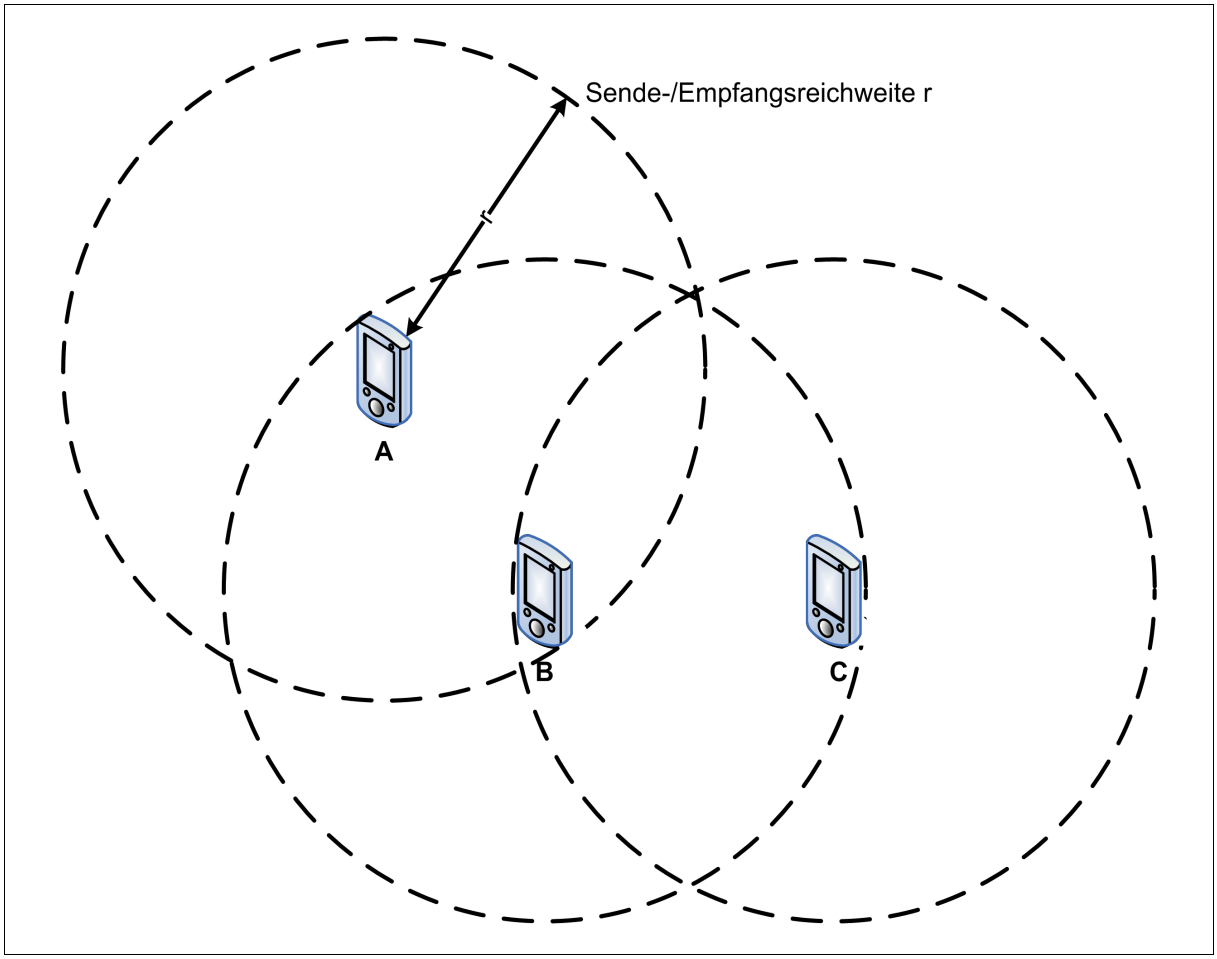

Abbildung 1: Ad-hoc Netzwerk

2.2. Behörden und Organisationen mit Sicherheitsaufgaben

Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sind solche, deren Maßnahmen und Leistungen der Rettung von Leben und Sachwerten sowie der Abwehr von Gefahren für die Bevölkerung und ihre Lebensgrundlagen dienen (vgl. Meißner/Steinebach (2004), S. 321). Darunter fallen neben Polizei, Feuerwehr und Rettungsdiensten auch ehrenamtliche Einheiten des Katastrophenschutzes wie z.B. aus dem Bereitschaftswesen im Deutschen Roten Kreuz (DRK).

2.3. Großschadenslagen und Katastrophen

Eine Situation, die dazu führen kann, dass das Notfall- und Rettungswesen mit täglichen Mitteln das Geschehen nicht allein bewältigen kann, wird in Deutschland als Massenanfall von

Verletzten/Erkrankten bezeichnet (MANV). Typischerweise wird dieser ausgerufen, wenn fünf oder mehr Personen auf einmal zu versorgen sind. Die Großschadenslage soll synonym zum Begriff des MANV verwendet werden. Im Gegensatz zum Einsatz bei individuellen Notfällen entsteht neben der notfallmedizinischen Versorgung ein Bedarf zur Koordinierung und Führung der Einsatzkräfte, die oftmals unterschiedlichen Organisationen entstammen (vgl. Peter/Mitschke/Uhr (2001), S. 7). Diese übernehmen in Kooperation Aufgaben entsprechend ihrer jeweiligen Bestimmung. Ein weiteres Abgrenzungskriterium gegenüber alltäglichen Notfallsituationen ist der größere Zeitraum, über den sich die Bewältigung des Geschehens erstreckt.

Unter einer Katastrophe ist eine Großschadenslage zu verstehen, bei der neben hilfsbedürftigen Personen zusätzlich in großem Umfang Infrastruktur zerstört wurde, wie es z.B. durch ein Erdbeben geschieht. Katastrophen werden durch die Katastrophenschutzbehörde, d.h. in der durch die kreisfreie Stadt oder den Landkreis, ausgerufen.

3. Klassische Bewältigung von Großschadenslagen und Katastrophen

Bei einem alltäglichen Einsatz von Rettungsdiensten stehen die notfallmedizinischen Tätigkeiten im Vordergrund. Bei Großschadenslagen und Katastrophen muss jedoch zuerst geführt und organisiert werden, bevor sich den Betroffenen zugewendet wird. „Wird diese Reihenfolge nicht eingehalten, beispielsweise wird ein Verletzter behandelt und keine Führungsorganisation aufgebaut, werden an der Notfallstelle Zustände erwachsen, die eine geordnete Schadensabwehr im notfallmedizinischen Bereich erschweren oder sogar unmöglich machen.“ (vgl. Peter/Mitschke/Uhr (2001), S. 9).
Im Regelfall werden notfallmedizinisches Personal und Feuerwehr parallel bei Großschadenslagen oder Katastrophen zum Einsatz kommen. Die Technische Einsatzleitung (TEL) wird dabei meist von letzterer übernommen. Ihr unterstellt wird die sanitätsdienstliche Einsatzleitung (SanEL), die sich zusammensetzt aus dem Organisatorischen Leiter (OrgL) und dem Leitenden Notarzt (LNA). Die jeweiligen Aufgaben lassen sich klar trennen und werden folgend auch einzeln betrachtet.

3.1. Aufgaben der Feuerwehr

Die Aufgaben der Feuerwehr lassen sich an deren Leitspruch „Retten, Löschen, Bergen, Schützen“ festmachen. In Kooperation mit anderen Hilfsorganisationen ist insbesondere das Retten und Bergen von Personen von Interesse, da entsprechend ausgerüstete Einsatzkräfte der Feuerwehr die einzigen sind, die sich in Gefahrenbereiche begeben dürfen. Als Beispiel sei das Vorgehen in ein brennendes Gebäude unter Nutzung von Atemschutzgeräten genannt. Weiterhin unterstützt die Feuerwehr Rettungsdienste durch technische Gerätschaften, wodurch z.B. in Fahrzeugen eingeklemmte Personen befreit werden können.
Gerettete Betroffene werden von den Einsatzkräften der Feuerwehr an einer Verletztenablage dem notfallmedizinischen Personal zur weiteren Versorgung übergeben.

3.2. Aufgaben des notfallmedizinischen Personals

Das notfallmedizinische Personal lässt sich untergliedern in hauptamtliche Kräfte der Rettungsdienste sowie ehrenamtliche Kräfte, wie sie z.B. im Katastrophenschutz zum Einsatz

kommen. Letztere übernehmen bei Großschadensfällen und Katastrophen eine unterstützende Funktion, die jedoch nicht von geringerer Bedeutung ist. Auf beide Bereiche wird im Folgenden getrennt eingegangen.

3.2.1. Rettungsdienstliche Aufgaben

Die folgende Beschreibung basiert auf den zehn Geboten für einen Rettungsdiensteinsatz mit Massenanfall von Behandlungs- und Betreuungsbedürftigen (vgl. Peter/Mitschke/Uhr 2001, S. 40-49). Das ersteintreffende Rettungsdienstteam muss dabei von der rettungsdienstlichen Tagesroutine abweichen und sich bewusst werden, dass zuerst organisatorische Aufgaben zu bewältigen sind.

Nach kurzer Erstrückmeldung, die die Leitstelle befähigen soll, die bisher selbst eingeleiteten Maßnahmen zu überprüfen, wird das Ausmaß des Schadens erkundet. Dazu gehört zum einen das Feststellen der medizinischen Lage, d.h. welche Verletzungen in welchem Ausmaß zu erwarten sind. Zum anderen muss die eigene Lage bestimmt werden. Darunter fällt der Bedarf an zusätzlichem medizinischen Personal und Material sowie technischer Unterstützung. Des Weiteren müssen mögliche Gefahren für Einsatzkräfte und Patienten erkundet werden.

Gewonnene konkrete Erkenntnisse über die Lage werden in einer Zweitrückmeldung der Leitstelle mitgeteilt. Der dortige Disponent übernimmt die Nachforderung von Personal und Material sowie die Abfrage von Klinikkapazitäten.

Das Einsatzteam vor Ort übernimmt kommissarisch die Aufgaben von OrgL und LNA bis diese eintreffen. Ersterer hat für eine erste Ordnung des Raumes zu sorgen. Dazu gehört die Bestimmung des Platzes für Verletztenablagen und ggf. eines Behandlungsplatzes, des Bereitstellungsraumes für Rettungsfahrzeuge und -material sowie eines Landeplatzes für einen Rettungshubschrauber. Dies erfolgt in Absprache mit der TEL, die um bestehende Gefahren wie z.B. Brandausbreitung weiß. Dem LNA obliegen die medizinische Einsatzleitung und die Herstellung des Kontakts zu anderen Kräften der Gefahrenabwehr.

Zu versorgende Patienten werden zunächst gesichtet und nach Prioritäten in Kategorien einsortiert. Zu unterscheiden sind beispielsweise Personen, die lediglich der Betreuung bedürfen oder solche, die schnellstmöglich in ein Krankenhaus befördert werden müssen. Für letztere ist in Rücksprache mit der Leitstelle ein Abtransport zu organisieren werden.

Treffen OrgL und LNA an der Schadenstelle ein, übernehmen sie die SanEL. Sie benötigen einen genauen Überblick über die Lage, eingeleitete Maßnahmen und den Versorgungszu-

stand der Patienten, um aufbauend auf dem bisher geleisteten sinnvoll arbeiten zu können. Die abgelösten Kräfte bekommen neue Aufgaben zugeteilt. Typischerweise wird es sich dabei um die Versorgung von Verletzten oder deren Transport handeln.

3.2.2. Unterstützung der Rettungsdienste durch ehrenamtliche Kräfte

Um die hauptamtlichen Kräfte des Rettungsdienstes bei Großschadensfällen und Katastrophen zu unterstützen, sind ehrenamtliche Helfer des Katastrophenschutzes in Einsatzeinheiten organisiert. Diese seien hier am Beispiel der Einsatzeinheiten des DRK näher erläutert. Ähnliche Konzepte finden sich jedoch auch bei anderen Hilfsorganisationen.
Ein Einsatzzug setzt sich aus mehreren Gruppen[3] zusammen, die im Einsatz unterschiedliche Aufgaben übernehmen. Neben der direkten nofallmedizinischen Unterstützung durch Personal und Material sowie der Dokumentation (Sanitätsgruppe) übernehmen die ehrenamtlichen Helfer das Errichten von Notunterkünften in Zelten sowie den Betrieb und die Überwachung von technischen Anlagen, z.B. Notstromgeräte oder Beleuchtung (Gruppe Technik und Sicherheit). Weiterhin wird sich um soziale Belange von Betroffenen gekümmert und für Verpflegung und Versorgungsgüter gesorgt (Betreuungsgruppe).
Koordiniert werden diese durch den Führungstrupp, der zudem den Kontakt zur SanEL herstellt. Er selbst wird ggf. durch eine Gruppe Information und Kommunikation unterstützt, die durch geeignete Mittel langfristig die Kommunikation sichert und Stabstellencharakter genießt.
Neben einem Einsatzzug, der 30 Personen umfasst und für den Einsatz bei Katastrophen gedacht ist, gibt es zudem das Konzept der Schnelleinsatzgruppe (SEG). Eine solche setzt sich aus mit Funkmeldeempfängern ausgestatteten Helfern zusammen, die zügig zu Großschadensfällen gerufen werden können (vgl. Deutsches Rotes Kreuz, Generalsekretariat (1995), S. 6-12).

3.3. Potenzial zur Verbesserung durch Informationstechnologie

Durch die Nutzung von Informationstechnologie könnten Einsatzprozesse bei Großschadenslagen oder Katastrophen effektiver gestaltet werden. Die gesamte Kommunikation findet bisher meist über wenige, auf analoger Technik basierende Funkkanäle statt, die vorwiegend für

3 Diese werden ggf. noch in verschiedene Trupps unterteilt.

Sprachübertragung genutzt werden . Mit der Größe der Schadenslage steigt das Funkaufkommen und eine Überlastung und damit eine zeitliche Verzögerung drohen, sofern nicht auf zusätzliche Kommunikationsmittel wie Mobiltelefone, Feldkabelsysteme oder menschliche Melder zurückgegriffen wird. Das Aufrechterhalten der Kommunikation während Großschadensfällen und Katastrophen gehört zu den primären Herausforderungen (vgl. Meißner et al. (2002), S. 2).
Weiterhin ist es ohne Weiteres nicht möglich, einzelne Fahrzeuge oder Helfer direkt anzusprechen, d.h. es findet immer eine Broadcast-Kommunikation statt, die ggf. vom Einsatzgeschehen ablenken kann. Die Übertragungen sind zudem unverschlüsselt und somit nicht abhörsicher. Erst mit der Einführung eines Digitalfunksystems können diese Probleme sinnvoll überwunden werden.

Allgemein besteht Interesse an einer umfangreicheren und flexibleren Informationsgewinnung. Verbessert werden könnte die Lage, wenn mit Sensoren ausgestattete Geräte von den Helfern mitgeführt würden. So ließen sich unterschiedlichste Daten sammeln, ggf. aufbereiten und an entsprechende Führungskräfte weiterleiten. Es würde sich z.B. anbieten, in brennenden Gebäuden Temperaturen zu erfassen oder permanent die Vitalfunktionen von Verletzten aufzuzeichnen, um diese bei Bedarf abzurufen.
Weiterhin scheint der Einsatz eines Lokalisierungssystems in Kombination mit einem geographischen Informationssystem sinnvoll. Der Standort von Helfern, ggf. in Verbindung mit Angaben über die augenblickliche Tätigkeit, könnte so ermittelt werden. Dadurch ließen sich einzelne Einsatzkräfte gezielter einsetzen und bei drohender Gefahr warnen (vgl. Meißner/Steinebach (2004), S. 330). Denkbar ist auch die Kennzeichnung von besonderen Orten wie Verletztenablagen oder gar die Erfassung der Position jedes einzelnen Patienten.
Alle gesammelten Daten könnten automatisch ohne Sprachkommunikation der Einsatzkräfte gesammelt und so zur Führung und zur Einsatzdokumentation automatisch verarbeitet werden. Ebenso lassen sich in Gegenrichtung gezielt einzelne Helfer oder Helfergruppen mit Informationen oder Anweisungen versorgen. Dadurch entfiele das ständige „Abhören des Funkkanals“ nach für einen selbst bestimmten Mitteilungen und das Personal könnte sich auf seine eigentlichen Aufgaben konzentrieren.
Nachrückende Einsatzkräfte, wie z.B. eine SEG oder der LNA, könnten sich bereits auf der Anfahrt ein Bild von der Schadenstelle und den eingeleiteten Maßnahmen machen, sofern eine entsprechende Verbindung zu diesen außerhalb des angedachten Ad-hoc-Netzes

ermöglicht wird. Selbiges gilt für die Disponenten der Leitstelle, die bereits frühzeitig Krankenhäuser über die Anzahl von Patienten und deren Krankheitsbilder informieren könnten.
Bei der Feuerwehr besteht ein konkreter Bedarf an robusterer Kommunikation mit unter Atemschutz eingesetzten Helfern in Gebäuden. In der entsprechenden Dienstvorschrift heißt es: „Die Erreichbarkeit der vorgehenden Trupps ist wegen der begrenzten Reichweite von Sprechfunkgeräten zu überprüfen und sicherzustellen. Bricht die Funkverbindung ab, muss der Sicherheitstrupp soweit vorgehen, bis wieder eine Sprechfunkverbindung besteht oder er den Atemschutztrupp erreicht hat. Es ist sofort ein neuer Sicherheitstrupp bereitzustellen.“ (Ausschuss für Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung (2004), S. 9). Bei schlechter Funkverbindung, wie es z.B. in Kellern der Fall sein kann, besteht also möglicherweise die Notwendigkeit, ständig neue Sicherheitstrupps einzusetzen und somit Personal von anderer Stelle abzuziehen.

4. Anforderungsanalyse an ein System für den Einsatz von Behörden und Organisationen mit Sicherheitsaufgaben

In diesem Kapitel sollen die Anforderungen analysiert werden, die BOS an ein Informations- und Kommunikationssystem stellen. Betrachtet werden dabei neben allgemeinen Anforderungen Sicherheitsaspekte, Dienstgüte und Nutzbarkeit. Einleitend dazu erfolgt eine Abgrenzung zu bereits bestehenden Systemen.

4.1. Abgrenzung zu bereits bestehenden Systemen

Bestehende Systeme wurden lediglich für den alltäglichen Einsatz entworfen, nicht aber für größere Schadenslagen. Dabei bieten sie jedoch schon diverse Funktionen, die in die vorhandene Kommunikationsinfrastruktur eingebunden sind. So unterstützt z.B. das System NIDA (Notfall Informations- und Dokumentations-Assistent) Rettungsassistenten durch die Möglichkeit, Einsatzaufträge und -koordinaten für das Navigationssystem über analoge Funktechnik zu empfangen, durchgeführte Maßnahmen und Materialverbrauch zu protokollieren[4] und entsprechende Dokumentationen zu generieren (vgl. Gongolsky (2004), S. 30-32).
Mit den Funksystemen Tetra 25 und Tetrapol[5], von denen eines in den nächsten Jahren in Deutschland bundesweit eingeführt werden soll, wird ein Wechsel zur Digitaltechnik innerhalb der BOS vollzogen. Dadurch wird die Möglichkeit bestehen, effektive Verschlüsselung und Datenübertragung, Gruppenbildung und weitere Vorzüge zu nutzen (vgl. Dau (2003), S. 13). Dieses System bedarf jedoch einer umfangreichen Infrastruktur, die errichtet werden muss und von der nicht überall ausgegangen werden kann. Es ist vorstellbar, dass diese zerstört worden ist oder gar nicht vorhanden war.
Das in dieser Arbeit propagierte System soll möglichst unabhängig von einer Infrastruktur betrieben werden können. Eine ergänzende Nutzung von Tetra 25 oder einer anderen Technologie für Kommunikation außerhalb des verwendeten Ad-hoc-Netzes ist jedoch denkbar.

4 Bei NIDA gibt es z.B. die Möglichkeit, Daten eines EKGs über eine Bluetooth-Verbindung in das Protokoll einfließen zu lassen.

5 Auf Funkzellen basierende Systeme ähnlich GSM

Neben der Informationsgewinnung, -verarbeitung und -verteilung, wie sie bestehende Systeme wie NIDA in begrenztem Rahmen bereits bieten, steht vor allem die Sicherung der Kommunikation der Beteiligten Hilfskräfte vor Ort im Vordergrund.

4.2. Allgemeine Anforderungen

Die Anforderungen an ein Informations- und Kommunikationssystem für den Einsatz von BOS ähneln denen, die auch das Militär stellt. Handlungen von Einsatzkräften oder -gruppen müssen koordiniert und eine dauerhafte Verbindung unter Vermeidung von „Single Points Of Failure“ zu diesen sichergestellt werden. Dabei darf nicht von einer vorhandenen Infrastruktur ausgegangen werden. Zudem bleibt zu bedenken, dass bei Frequenzen weit über 100 MHz Schwierigkeiten bestehen, eine Funkverbindung über die „Line Of Sight“ hinaus aufzubauen. Probleme sind häufig im 2m-Funk zu beobachten, der derzeit in Deutschland lokal an Einsatzstellen zum Einsatz kommt. Diese Anforderungen legen den Gebrauch von Ad-hoc-Netzen als Grundlage der Kommunikation nahe (vgl. Freebersyser/Leiner (2001), S. 31).
Weiterhin sind Anschaffungskosten für die Organisationen zu berücksichtigen. Sofern es möglich ist, ohne größere Kompromisse eingehen zu müssen, sollte das System auf bestehenden Geräten aufbauen oder diese zumindest einbeziehen. Hinzu kommt die Verwendung von möglichst etablierter, adäquater Technologie, die im Regelfall ein niedriges preisliches Niveau aufweist. Zudem besteht hier eine hohe Wahrscheinlichkeit, dass künftige Weiterentwicklungen genutzt werden können.
Bei mobilen drahtlosen Geräten muss beachtet werden, dass diese möglichst stromsparend arbeiten, um eine lange Laufzeit zu garantieren. Je nach Anwendungsgebiet und bestehenden Geräteressourcen können deshalb verschiedene Technologien sinnvoll sein. So müssen Sensoren, die z.B. von Einsatzkräften zwecks Datensammlung mitgeführte werden, stärker mit ihrem Energievorrat haushalten als ein in einem Einsatzfahrzeug untergebrachtes Gerät.
In Betracht gezogen werden muss das Vehrkehrsaufkommen innerhalb des Netzes. Während für einzelne Helfer lediglich lokale Informationen von Bedeutung sind, fließen zahlreiche Daten bei den Führungskräften zusammen. Vom System ist eine sinnvolle (halb-)automatische Aggregation und Präsentation der Daten wünschenswert, so dass die Führungskraft entlastet wird und keine Informationsproliferation droht. Weiterhin sind die durch das höhere Ver-

kehrsaufkommen gestiegenen Anforderungen an das zu verwendende Funksystem hinsichtlich der Bandbreite zu berücksichtigen.
Zudem sind Geräte dem Einsatzgebiet anzupassen. So erfordern z.B. Geräte im Bereich von Löscharbeiten einen Spritzwasserschutz. Bei der Arbeit im medizinischen Bereich sind Regularien des Medizinproduktgesetzes zu beachten.

4.3. Sicherheitsaspekte

Grundsätzlich ist anzunehmen, dass abgesehen von möglichen terroristischen Aktivitäten nicht mit ernsten Angriffen auf die Sicherheit eines Funksystems von BOS zu rechnen ist. Allenfalls der bekannte „Notfall-Voyeurismus“ in Form von ungesetzlichem Belauschen der Meldungen, was heute sehr einfach ist, spielt eine wesentliche Rolle. Dennoch sollten die Anforderungen an die einzelnen Sicherheitsdienste betrachtet werden: Vertraulichkeit, Authentifizierung, Integrität, Nicht-Anfechtbarkeit, Zugriffssteuerung und Verfügbarkeit (vgl. Stallings (2001), S. 25).

Die bisherigen anlogen Funksysteme der BOS weisen keinerlei Schutzmaßnahmen auf. So ist es zwar gesetzlich verboten, die entsprechenden Frequenzen zu nutzen, doch mit speziellen, frei verkäuflichen Geräten ist ein Abhören problemlos möglich, die Funksprüche abzuhören (Vertraulichkeit) oder selbst an der Kommunikation teilzunehmen (Zugriffssteuerung). Ob ein Funkspruch tatsächlich von einer bestimmten Person abgegeben wurde, ist dabei nicht nachvollziehbar (Authentizität). Weiterhin ist der Empfang von Nachrichten von Gegenstellen nicht sichergestellt (Verfügbarkeit). Die Integrität ergibt sich allenfalls aus der direkten Sprachkommunikation, die in Echtzeit vermutlich nur schwerlich auf ihrem Weg vom Sender zum Empfänger verändert werden kann.

Folgende Anforderungen an die Sicherheitsdienste ergeben sich:

- **Vertraulichkeit:** Sobald es sich bei den übertragenen Daten um persönliche oder personenbezogene handelt, müssen diese adäquat geschützt werden. Ist mit Aktivitäten von Terroristen zu rechnen, die anhand der abgefangenen Informationen möglicherweise Ziele

für einen Angriff ausmachen möchten, so bedarf es der Verschlüsselung der gesamten Kommunikation.

- **Authentifizierung:** Der Empfänger einer Nachricht muss sicher sein können, dass sie auch von der Quelle stammt, von der sie zu stammen vorgibt. Ansonsten wäre es z.B. möglich, falsche Aufträge zu erteilen.

- **Integrität:** Die Integrität der Daten ist sicherzustellen. Zum einen ist einer Modifikation durch mögliche Eindringlinge vorzubeugen. Zum anderen ist es aber auch wichtig, dass Messwerte von Sensoren korrekt übertragen werden. Ein falsch übermittelter Wert von Vitalfunktionen beispielsweise könnte einen Notarzt zur Gabe von inadäquaten Medikamenten verleiten, was tödliche Folgen haben könnte.

- **Nicht-Anfechtbarkeit:** Die Nicht-Anfechtbarkeit ist zu vernachlässigen, da kaum Interesse bestehen dürfte den Erhalt oder das Abschicken einer Meldung zu beweisen.

- **Zugriffssteuerung:** Der Zugriff auf das System muss autorisiert werden, so dass z.B. bestimmte Anwendungen oder Informationen nur einem bestimmten Personenkreis zugänglich sind.

- **Verfügbarkeit:** Insbesondere die Verfügbarkeit der Kommunikation ist sicherzustellen. Ihr Ausfall könnte zum Chaos führen und in kritischen Situationen Leben gefährden. Es ist ggf. ein nicht auf Informationstechnologie basierendes Sicherungssystem bereitzustellen.

4.4. Dienstgüte

Bei den Anforderungen an die Dienstgüte ist ein Kompromiss zu finden zwischen möglichst großer Bandbreite und möglichst geringer Verzögerung der Übertragung. Sollten größere Datenbestände übertragen werden, z.B. Kartenmaterial, so wäre ein hoher Datendurchsatz von Vorteil, um die Übertragung schnell abzuschließen. Meist ist es jedoch von größerer Bedeutung, dass kleinere Datenmengen schnell übertragen werden. Ein Alarmsignal an einen Helfer, der sich in einer Gefahrenzone befindet, muss unverzüglich weitergeleitet werden. Einer

geringen Verzögerung ist somit Vorzug zu geben, wenn beides zeitgleich nicht garantiert werden kann.

4.5. Benutzeranforderungen

Das Informations- und Kommunikationssystem muss einfach zu nutzen sein. Eine komplizierte Bedienung erfordert zu viel Zeit und lenkt unnötig vom eigentlichen Einsatzgeschehen ab. Die Handhabung sollte intuitiv sein oder auf bekannten Vorgehensweisen aufbauen, so dass auch technisch weniger Versierte mit den Geräten umgehen können. Informationen sollten nach Möglichkeit automatisch ohne Zutun der Einsatzkraft zugänglich gemacht werden. Eine teilweise Sprachsteuerung ist wünschenswert (vgl. Meissner et al. (2002), S. 3).
Eine Fehlbedienung der Geräte darf nicht möglich sein bzw. muss abgefangen werden. Zudem sollte der Helfer durch eine Plausibilitätsprüfung der Eingaben unterstützt werden.
Die Geräte müssen dem Einsatzzweck angemessen gestaltet werden. So müssen sie z.B. in bestimmten Situationen auch mit Einsatzhandschuhen bedienbar sein.

5. Implementierungsdesign

Dieser Abschnitt befasst sich mit dem Implementierungsdesign des Systems. Als Programmiersprache kommt Java zum Einsatz, um ohne Änderungen auf möglichst vielen verschiedenen Rechnersystemen zum Einsatz kommen zu können. Der Entwurf folgt allgemein den Richtlinien der Unified Modeling Language (UML) nach Rumbaugh (Rumbaugh/Jacobson/Booch (2005)) sowie speziell für Geräte mit geringen Hardware-Ressourcen den Richtlinien für das Mobile Information Device Profile (MIDP) in Version 2.0 nach Bloch (Bloch/Wagner (2003)). Bei Abweichungen wird gesondert darauf hingewiesen. Folgend werden die dem Design zugrunde liegenden Entscheidungen dargelegt.

5.1. Begründung des Designs

In diesem Abschnitt werden die Designentscheidungen beleuchtet. Nach einer Betrachtung der allgemeinen Architektur des Systems wird auf die verwendete Technologie sowie dementsprechende Geräte eingegangen. Es folgen Ausführungen zur Sicherheit, zur Dienstgüte und zu den Benutzeranforderungen.

5.1.1. Architektur des Systems

Bei der angedachten Architektur kommen verschiedene, sich überschneidende Funknetze zum Einsatz (vgl. Tanenbaum (2003), S. 31-34; Meissner et al. (2002), S. 2):

- Stadtnetz (MAN) bzw. Fernnetz (WAN) für die Abdeckung von Bereichen innerhalb einer Stadt bzw. einer Region
- Lokales Netz (LAN) mit einer Reichweite zwischen zehn Metern und einem Kilometer und
- Persönliches Netz (PAN) für die unmittelbare Umgebung einer Person bis hin zu zehn Metern Entfernung.

Dadurch wird gewährleistet, dass auf unterschiedliche Anforderungen und Gegebenheiten Rücksicht genommen wird. So fallen durch den hierarchischen Aufbau der BOS in höheren Führungsebenen wesentlich mehr Informationen an als in den unteren, was eine höhere Band-

breite zur Übertragung erfordert. Hier können jedoch auch Gerätschaften mit höherer Leistungsaufnahme zum Einsatz kommen, da durch die typischerweise stationäre Lage eine kontinuierliche Energieversorgung eher gesichert werden kann.

Die Leitstellen der einzelnen BOS sind über ein geeignetes MAN bzw. WAN mit den Kräften an der Einsatzstelle, dem Hotspot, verbunden. In Deutschland bietet sich zu diesem Zweck das Digitalfunknetz an, dessen Einführung beschlossen wurde. Dieses soll auf Tetra oder TetraPOL basieren. Andere Technologien sind vorstellbar. MAN und WAN sind jedoch nicht Thema dieser Arbeit und werden nicht näher behandelt.
Im eigentlichen Zentrum des Geschehens steht die Schadensstelle. Hier wird als Rückgrat des Systems ein drahtloses Local Area Network (LAN) aufgebaut, über das die Kommunikation stattfindet. Dessen Zugangspunkte werden entweder fest an wichtigen Punkten der Einsatzstelle installiert, z.B. Einsatzleitfahrzeug oder Verletztenablage, oder können von geeignetem Personal mitgeführt werden. Es bietet sich hier an, z.B. Gruppenführer eines DRK-Einsatzzuges damit auszustatten. Sie führen eher organisatorische statt praktische Tätigkeiten aus, weshalb zusätzliche Ausrüstung weniger hinderlich wirkt als bei Helfern, die mit der Rettung von Personen beschäftigt sind. Zudem stehen sie in engem räumlichen Kontakt zu den Geführten, so dass auf dieser Strecke Technologie zum Einsatz kommen kann, die über eine geringere Reichweite verfügt, dafür aber über auch über geringere Leistungsaufnahme.
Einzelne Einsatzkräfte wiederum sind in ein PAN eingebunden. Dieses verbindet sie zum einen mit Helfern der unmittelbaren Umgebung, zum anderen aber auch mit Sensoren oder anderen Geräten, die sie mit sich führen. Man spricht hier auch von Body Area Networks.

Da die Geräte im LAN das Rückgrat des Netzes bilden, sollen hier möglichst viele Verbindungen zwischen allen Knoten bestehen. Die Geräte im PAN werden in einer Baumstruktur organisiert, um einen klar definierten Zugangspunkt zu diesem Netzabschnitt an der Wurzel des Baumes zu erhalten. Den Übergangspunkten vom LAN zum PAN kommt eine besondere Bedeutung zu. Sie fungieren nicht nur als Gateway zwischen den unterschiedlichen Technologien, sondern zusätzlich als DataMarts. Ein solcher stellt spezifische Ausschnitte der gesamten Datenbasis zur Verfügung und kann als themenbezogenes Data Warehouse betrachtet werden. (vgl. Voss/Gutenschwager (2001), S. 264). Ein solches wiederum speichert alle operativ anfallenden Daten inklusive einer Zeitmarkierung zur späteren Auswertung. Im hier vorliegenden Fall ist ein DataMart jeweils für die ihm in angegliederten PAN-Geräte zustän-

dig. Deren Daten werden in den DataMarts zwischengespeichert und ggf. aggregiert. Erst bei Bedarf werden diese abgerufen. Ausnahmen bilden z.B. Auftragsnachrichten, die unverzüglich dargestellt werden. Ziel dieses Verfahren ist eine Verringerung der Systemlast. Es werden z.B. nicht laufend alle Sensornachrichten an die Führungskräfte gesendet. Vielmehr können diese gezielt selektieren, welche Daten sie wann benötigen. So ist es denkbar, dass von den in den DataMarts gesammelten Sensorwerten jeweils nur die aktuellsten von Interesse sind und nicht alle bisherigen. Die aktuellsten werden abgerufen und damit übertragen, die übrigen jedoch ignoriert. Den Aufbau des Systems verdeutlicht Abbildung 2.

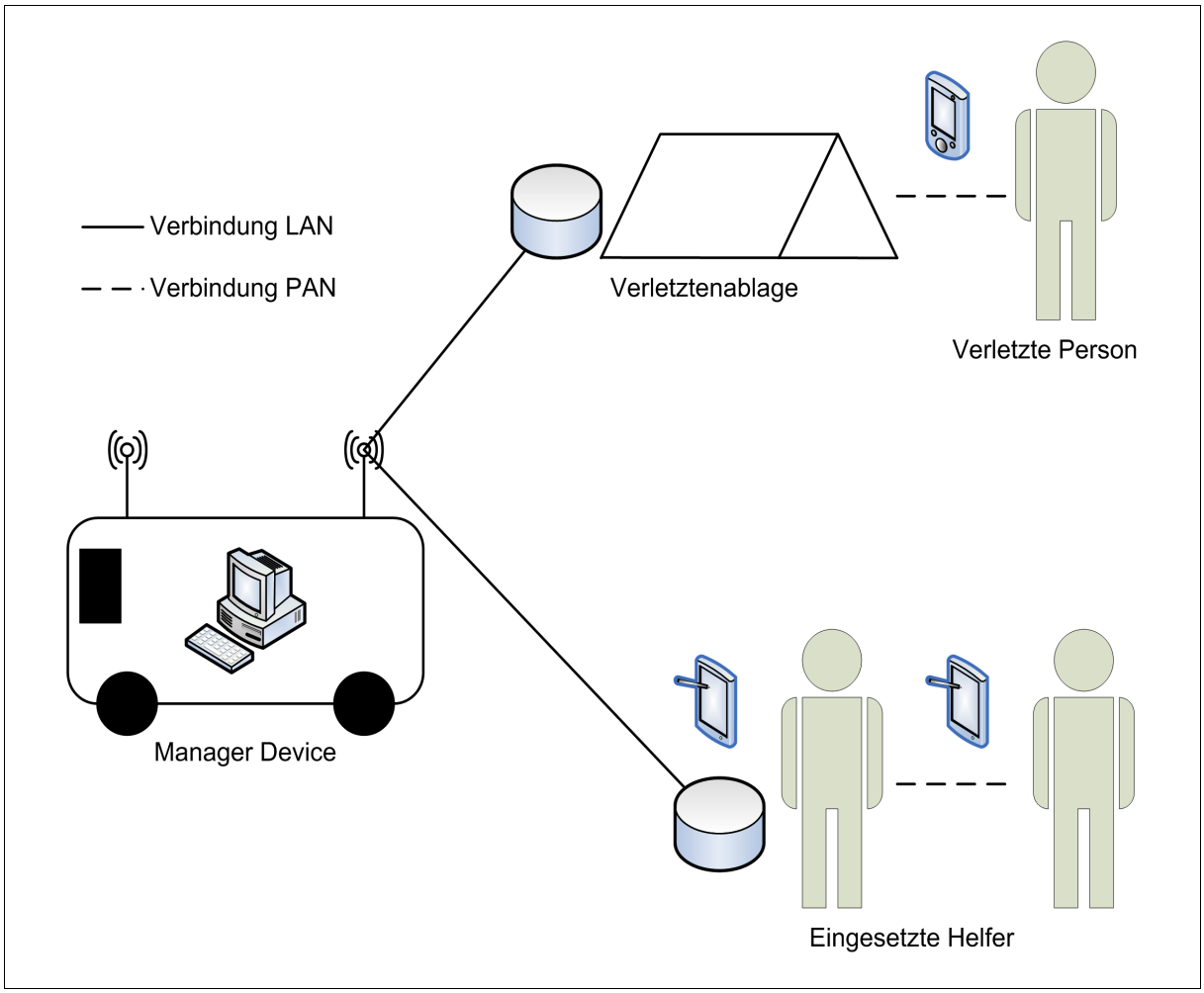

Abbildung 2: Darstellung der Kommunikationsarchitektur, in Anlehnung an Meissner et al. (2002), S. 2

5.1.2. Verwendete Technologien und Geräte

Als Funktechnologien zum Einsatz kommen die Standards IEEE 802.11 für das LAN und Bluetooth für das PAN. Ersterer wird häufig auch einfach als WLAN (Wireless Local Area Network) bezeichnet. Streng genommen kann diese Bezeichnung jedoch für beliebige andere Technologien zur Etablierung von drahtlosen lokalen Netzen verwendet werden. Der Einfachheit halber sei folgend mit WLAN der Standard IEEE 802.11 gemeint. Die weit verbreitete Variante IEEE 802.11g bietet eine Datentransferrate von brutto 54 Mbit/s (vgl. IEEE (2003)).

Die Ursprüngliche Idee von Bluetooth war es, kleine lokale Single-Hop-Netze aus bis zu acht Geräten zu bilden (ein Piconet), um z.B. Peripherie wie Drucker oder Scanner drahtlos an einen Rechner anschließen zu können. Die Spezifikation sieht jedoch auch komplexere Topologien vor, bei denen mehrere Piconets zu einem Scatternet verbunden werden können. Dadurch sind auch Multi-Hop-Netze möglich (vgl. McDermott-Wells (2004a), S. 33). Derzeitige Bluetooth-Implementierungen für Java nach JSR-82 (vgl. Java Community Process Organisation (2002)) sehen dies jedoch noch nicht vor, weshalb für das Demonstrationsprogramm lediglich Punkt-zu-Punkt-Verbindungen genutzt werden. Einen entsprechenden Design-Vorschlag für eine Multi-Hop-Umgebung in Java liefern Pabuwal/Jain/Jain (vgl. Pabuwal/Jain/Jain (2003)), der zukünftig Abhilfe schaffen könnte.

Sowohl WLAN als auch Bluetooth nutzen einen Frequenzbereich, der keine Lizenzierung erfordert (das 2,4 GHz-ISM-Band). Weiterhin sind beide etabliert, so dass auf eine Vielzahl von Geräten und Bauteilen zurückgegriffen werden kann. So ist es möglich, einen handelsüblichen Personalcomputer mit einer WLAN-kompatiblen Netzwerkkarte auszurüsten und in das System zu integrieren. Eine Vielzahl von Helfern verfügt zudem über ein Mobiltelefon. Viele aktuelle Modelle sind mit einer Bluetooth-Schnittstelle ausgestattet und können Java(-Micro-Edition)-Programme ausführen. Auch diese Telefone können sinnvoll im Zusammenhang mit dem Kommunikationssystem verwendet werden.

Durch das Zurückgreifen auf etablierte Technologie, lizenzfreie Frequenzen und bereits vorhandene Geräte können die entstehenden Kosten zur Einführung des Systems niedrig gehalten werden. Gerade dieser Aspekt entscheidet im Bereich der BOS oft für oder wider eine Einführung von Neuerungen bzw. verzögert diese, wie das Beispiel Tetra/TetraPOL in Deutschland verdeutlicht. Mögliche Nachteile, die die Verwendung von WLAN und Bluetooth mit sich bringen, werden insbesondere im folgenden Kapitel diskutiert.

Für den Datenaustausch wird die Sprache XML (vgl. W3 Konsortium (1997)) genutzt. Diese ist vielseitig anwendbar, und erlaubt es, ggf. einfach in andere Datenformate konvertiert zu werden. Von Bedeutung ist dies, da bisher in diesem Bereich kein Standard existiert. Hersteller von Systemen, die für den Einsatz im Alltag der BOS genutzt werden, verwenden eigene proprietäre Protokolle (vgl. Gongolsky (2004), S. 34). Fremdgeräte sollen jedoch später einfach integrierbar sein, weshalb XML der Vorzug zu geben ist.
Ein Nachteil, der sich durch die Verwendung von XML ergibt, ist die Größe der zu übermittelnden Daten durch lange Tag-Namen (vgl. Meissner et al. (2002), S. 4). Diesem kann jedoch durch Komprimierung und geschickte Wahl der Tag-Namen entgegengewirkt werden.

5.1.3. Sicherheitsaspekte

Ein allgemeiner Nachteil für die Sicherheit des Systems ergibt sich zum einen durch die Verwendung eines Funknetzes, da dieses ein Broadcastmedium darstellt. Das Abhören ist somit prinzipiell einfacher als bei drahtgebundenen Netzen (vgl. Eckert (2004), S. 813). Zum anderen birgt die verwendete Technologie zusätzliche Risiken. Zugriff auf die Frequenzen des ISM-Bandes zu erlangen ist nicht schwierig, und für jedermann mit handelsüblichen Geräten zu bewerkstelligen. Neben den Sicherheitsmechanismen, die WLAN und Bluetooth selbst bieten, sind zusätzliche, von der Technologie unabhängige, notwendig, um die Anforderungen an die Sicherheitsdienste zu erfüllen. Diese sollen im Wesentlichen dazu dienen, um das Mithören des BOS-Funks zu unterbinden. Gelegenheitsmithörer werden vermutlich den nötigen Aufwand scheuen, um ihre Neugier zu befriedigen. Es darf jedoch gemutmaßt werden, dass gegen ambitionierte terroristische Angriffe im Bereich IT oder Social Engineering noch Schwachstellen bestehen.

Vertraulichkeit

Um die Vertraulichkeit der Daten zu sichern, selbst wenn die Sicherheitsmechanismen von WLAN und Bluetooth überwunden wurden, werden diese zusätzlich verschlüsselt übertragen. Zur Anwendung kommt dabei unter Berücksichtigung der möglicherweise geringen Rechenleistung einzelner Geräte ein symmetrisches Verschlüsselungsverfahren mit einem 128-Bit-Schlüssel. Ein solcher gilt als hinreichend sicher (vgl. Stallings (2001), S. 52). Die entsprechenden Methoden sind im Quelltext zwar angelegt und werden genutzt, jedoch findet noch keine Verschlüsselung statt.

Da die Schlüsselverteilung in Ad-Hoc Netzen schwierig ist, weil nicht davon ausgegangen werden kann, dass ein sicherer Kanal zur Verfügung steht, wird ein anderer Weg gewählt. In jeder BOS muss im Vorfeld ein geeignetes Prozedere entwickelt werden, um regelmäßig neue Schlüssel zu generieren und den Einsatzkräften mitzuteilen. Dies kann z.B. in Form von in den Fahrzeugen bzw. bei den Geräten deponierten, versiegelten Briefumschlägen geschehen, die jeweils das für den aktuellen Monat gültige Passwort (128 Bit) enthalten. Zu berücksichtigen sind dabei sinnvolle Strategien zur Generierung von Passwörtern (vgl. Stallings (2001), S. 373-378).

Authentizität

Die Authentizität wird über die Zugriffssteuerung realisiert. Es wird davon ausgegangen, dass Nachrichten nur von korrekt im System angemeldeten Teilnehmern versendet werden, und diese ihre Senderadresse nicht fälschen.

Geräte, die sich im System anmelden, müssen sich über ihre Geräteadresse identifizieren. Diese muss eindeutig sein. Hier kommt die 48 Bit lange Bluetooth-Adresse zum Einsatz, die diese Anforderung erfüllt (vgl. Eckert (2004), S. 854). Sie ist zwar fälschbar, jedoch müsste zuvor Kenntnis über verwendete Adressen innerhalb des Systems erlangt werden.

Die Adresse wird an die Autorisierungsstelle übersendet, die bei der obersten Führungskraft der BOS vor Ort, z.B. der SanEL, untergebracht ist. Erstes Autorisierungsmerkmal ist die Kenntnis des gültigen Passworts, da sonst eine Entschlüsselung zu unsinnigen Daten führt. Bei der SanEL wird eine Liste der zugelassenen Bluetooth-Adressen geführt. Ist das Zugang erbittende Gerät hier aufgelistet, wird die Anmeldung akzeptiert. Sollte ein Gerät gestohlen werden, so kann dessen Kennung aus der Liste der zulässigen Geräte gelöscht werden und somit der Zugang zum System unterbunden.

Integrität

Die Integrität der Daten wird wie die Authentizität über die Zugangskontrolle bzw. die Verschlüsselung realisiert. Sofern Nachrichten von einem authentifizierten Nutzer kommen und mit dem geheimen Schlüssel chiffriert wurden, wird davon ausgegangen, dass sie nicht verändert worden sind.

Verfügbarkeit

Ein noch zu evaluierendes Problem besteht hinsichtlich der Verfügbarkeit in der Nutzung des freien ISM-Bandes. Je mehr Geräte vor Ort mit den zugehörigen Frequenzen arbeiten, desto schlechter steht es um die Verfügbarkeit, denn die Wahrscheinlichkeit von Fehlern auf dem Kanal steigt. Sollte die Dichte von drahtlosen LANs einen kritischen Wert übersteigen, könnte sich die Technik als untauglich erweisen, da ggf. keine gesicherte Kommunikation möglich wäre. Auch ließe sich relativ einfach ein Denial-of-Service-Angriff ausführen, indem der Frequenzbereich gezielt gestört wird. Dieser Nachteil besteht aber bei allen funkbasierten Systemen und ist in der Praxis höchstens bei terroristischen Aktionen von Relevanz.

5.1.4. Dienstgüte

Die nicht auf Sicherheitsaspekte bezogene Verfügbarkeit des Systems spielt auch im Bereich der Dienstgüte eine Rolle. Um bei einem Ausfall von einzelnen Knoten die Verfügbarkeit des Systems sicherzustellen, muss vor Ort eine gewisse Dichte an Knoten installiert werden. Für Großschadenslagen sind wegen der vergleichsweise geringen Ausdehnung der Schadenstelle bei genügend großer Anzahl von entsprechend ausgestatteten Geräten keine Probleme zu erwarten. Von Bedeutung ist hier allenfalls das Vorgehen in Gebäude, wo durch Mauern eine starke Abschirmung der Signale vorliegen kann. Hier bietet es sich an, immer wieder Knoten auszubringen, um eine Kette zu erzeugen, die die Kommunikation sicherstellt. Von Interesse ist hierbei die Frage, wann eines Knoten ausgebracht wird. Es wird vorgeschlagen, dass sich in Reichweite eines Knotens mindestens zwei weitere befinden. Einer davon soll so positioniert werden, dass er gerade noch im Empfangs- und Sendebereich liegt. Der andere soll dort ausgebracht werden, wo die Sende- und Empfangsleistung gerade die Hälfte des Maximalwertes beträgt. Auf diese Art und Weise besteht auch bei Ausfall eines Knotens noch die Möglichkeit, die Kommunikation aufrecht zu erhalten. Sollte die Umgebung es erfordern, z.B. weil Hindernisse die Signale stark blockieren, so lassen sich auch mehr als zwei Knoten in regelmäßigen Abständen in Bezug auf die Leistung ausbringen. Von dieser Regel abweichend sollten von den Helfern auch Knoten an Abzweigungen positioniert werden. Dies ist beispielsweise dann sinnvoll, wenn man an einer Tür angelangt und dann einen Raum betritt, dessen Wände die Funksignale blockieren könnten. Da eine größere Anzahl solcher „Relay“-Knoten benötigt werden kann, ist es empfehlenswert, diese ausschließlich für diesen Zweck fertigen zu lassen. Durch den Verzicht auf weitere Funktionen und eine große potenzielle Stückzahl

können Kostendegressionseffekte genutzt und der Preis gesenkt werden. Im vorliegenden Demonstrationsprogramm kann das beschriebene Vorgehen zur Ausbringung der Knoten bedingt durch die Beschränkungen der Spezifikation von JSR-82 auf Punkt-zu-Punkt-Verbindungen noch nicht getestet werden.[6]

Zur Etablierung der Baumartigen Struktur wird die „Tree Scatternet Formation“ (TSF) nach Tan et. al. vorgeschlagen (Tan et al. (2001)). Diese besteht aus einem oder mehreren spannenden Wurzelbäumen bei denen laufend versucht wird, diese zusammenzufügen und die Anzahl der Bäume zu reduzieren. Obwohl die Gefahr eines Bandbreitenengpasses an der Wurzel besteht, ist das Verfahren besonders für Umgebungen mit hoher Dynamik, hoher Knotendichte und Energierestriktionen geeignet (vgl. McDermott (2004b), S. 38). Da ein Selbstheilungsmechanismus vorliegt, der bei Ausfall von Knoten zügig versucht, die möglicherweise ausgefallenen Verbindungen wieder zu etablieren, ist die TSF besonders geeignet für das System.

Wie bereits erwähnt, ist eine geringe Verzögerung der Kommunikation eines Systems für BOS von größerer Bedeutung als hohe Bandbreite. Evaluationen von Boukerche (Boukerche (2004)) haben gezeigt, dass proaktive Routing-Verfahren die geringste Verzögerung aufweisen. Diese haben jedoch den Nachteil, dass durch die periodisch aufgefrischten und an alle Knoten verteilten Routendaten ein hoher Overhead erzeugt und dementsprechend ständig Energie der Geräte verbraucht wird. Unter den Ad-Hoc-Routing-Verfahren, die nur bei Bedarf eine Route ermitteln, bietet das Ad-hoc On-demand Distance Vector Routing (AODV) die geringsten Verzögerungen für ein Szenario von Großschadensfällen und Katastrophen (vgl. Johansson et al. (1999), S. 205). Zudem gibt es Varianten des AODV, die auch eine maximale Verzögerungen und bei Bedarf eine minimale Bandbreite garantieren können (vgl. Perkins/Royer (2001), S. 204)

6 Dasselbe Ausbringungsprinzip kann bei Katastrophen bzw. bei Großschadensfällen mit großflächiger Ausdehnung auch auf die WLAN-Knoten angewandt werden.

5.1.5. Benutzeranforderungen

Im Rahmen dieser Arbeit werden nicht alle Benutzeranforderungen erfüllt, da es sich lediglich um ein Proof-Of-Concept handelt. So bleibt derzeit die Bedienbarkeit der Geräte mit Schutzhandschuhen außen vor. Auch verzichtet werden muss derzeit auf Nutzung von Bluetooth-Scatternets.

Im Bereich der BOS gibt es ein auf den Analogfunk aufgesetztes Funkmeldesystem, dass es ermöglicht, über eine Zifferntastatur am Funkhörer Statusmeldungen abzugeben. In Abbildung 3 sind diese für den Bereich Rettungsdienst aufgeführt ergänzt um mögliche Bedeutungen für den Einsatz an der Schadenstelle. Aufbauend auf diesen Kenntnissen ist es in dem im Rahmen dieser Arbeit vorgeschlagenen System möglich, ein mit Bluetooth ausgestattetes Mobiltelefon für Statusmeldungen zu nutzen. Der Sprechfunk wird dadurch deutlich reduziert, und Einsatzkräfte werden deutlich kürzer von ihrer Arbeit abgehalten, als es bei Sprachkommunikation der Fall wäre.

Statusmeldung	Bedeutung
0	Notruf (Unterstützung erforderlich, z.B. bei Unfall)
1	frei auf Funk (Einsatzkräfte unterwegs, aber bereit, Aufträge anzunehmen)
2	frei auf Wache (Einsatzkräfte an bestimmtem Punkt, bereit Aufträge anzunehmen)
3	Einsatz übernommen
4	am Einsatzort
5	Sprechwunsch (Kommunikation erwünscht)
6	außer Dienst (Pause, o.ä.)
7	Patient aufgenommen (unterwegs zur Verletztenablage, zum Behandlungsplatz, usw.)
8	am Zielort
9	Handquittung

Abbildung 3: Statusmeldungen im Funkmeldesystem von BOS (Rettungsdienste)

5.2. Implementierte Bausteine

Das System (AMBOSS: **A**d-hoc-**M**obile-**BOS**-**S**ystem) setzt sich aus verschiedenen Geräten zusammen, die in den beschriebenen Bereichen PAN (User-Geräten oder Sensor-Geräten) und WAN (Manager-Gerät) zum Einsatz kommen, bzw. die Schnittstelle zwischen diesen bilden

(Repository-Gerät). Bevor diese in den nächsten Abschnitten einzeln betrachtet werden, soll an dieser Stelle ein allgemeiner Überblick über deren Funktionsweise gegeben werden.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE Amboss:Trm SYSTEM "amboss_transmission.dtd">
<Amboss:Trm>
      <Amboss:Snd>134.169.75.20</Amboss:Snd>
      <Amboss:Rcp>134.169.75.16</Amboss:Rcp>
      <Amboss:Typ>3</Amboss:Typ>
      <Amboss:Msg>Ich mache mal Pause...</Amboss:Msg>
</Amboss:Trm>
```

Abbildung 4: Beispiel für eine XML-Übertragung

Die Geräte kommunizieren über ein Request-Reply-Protokoll, das auf XML aufsetzt (vgl. Kapitel 5.1.2). In Abbildung 4 ist ein Beispiel für Übertragungen mittels XML dargestellt. Die Struktur ist einfach gehalten, da bisher für die J2ME kein XML-Parser zur Verfügung steht. Beim Msg-Tag z.B. wären komplexere Strukturen in Form weiterer Untergliederungen jedoch von Vorteil.

Die Tags `<Amboss:Snd>` und `<Amboss:Rcp>` sind für die IP-Adresse des Senders bzw. des Empfängers bestimmt. `<Amboss:Typ>` bezeichnet den Typ der Übertragung. Dabei bedeuten 0 = Request, 1 = Reply, 2 = Statusmeldung und 3 = Nachricht. `<Amboss:Msg>` enthält schließlich die zu übertragenden Nutzdaten, die verschlüsselt werden. Weitere Verwendung findet XML bei der Speicherung der Voreinstellungen der Geräte.

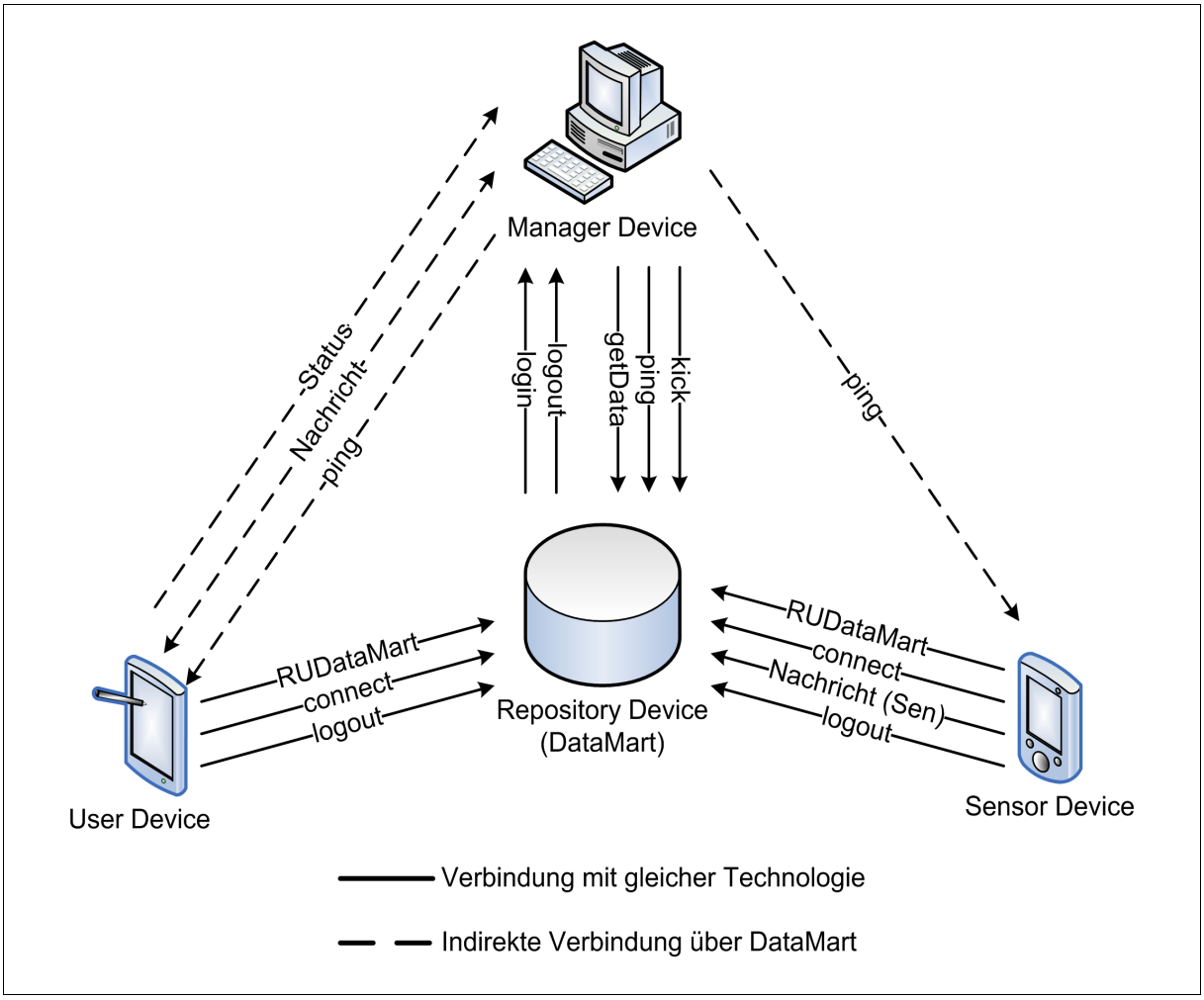

Abbildung 5: Übersicht über Anfragen zwischen den Geräten

Eine Übersicht über mögliche Anfragen zwischen den Geräten liefert Abbildung 5. Das Repository-Gerät übernimmt hierbei die Funktion des Gateways zwischen WAN und PAN.
Eine Erklärung samt Syntax der Nutzdaten für Requests sowie der zu erwartenden Replies ist Abbildung 6 zu entnehmen.

Request	Syntax	Zweck	Reply
RUDataMart	RUDataMart	Ein User- oder Sensor-Gerät fragt ein gefundenes Bluetooth-Gerät, ob es sich um ein Repository-Gerät handelt, bei dem es sich einloggen kann.	RUDataMart:true bzw. RUDataMart:false
connect	connect:Geräteart##Gerätebeschreibung	Ein User- oder Sensor-Gerät bittet das Repository-Device, eine Login-Anfrage beim Manager-Gerät zu stellen. Die IP-Adresse dafür erhält das Repository-Gerät aus der XML-Transmission, die Bluetooth-Kennung wird direkt über die Verbindung ermittelt, so dass Fälschung dieser schwieriger wird.	connect:true bzw. connect:false
login	login:IP-Adr.##Bluetooth-Kennung##Geräteart##Gerätebeschreibung[##Sensortyp]	Ein Gerät versucht sich beim Manager-Gerät anzumelden. Dazu übersendet es seine IP-Adresse, seine Bluetooth-Kennung, seine Art (User-, Repository- oder Sensor-Gerät) sowie dessen Beschreibung. Sensoren fügen zusätzlich ihren Typ an, z.B. Temperatur. Als Reply erfolgt eine Bestätigung bzw. Ablehung unter Angabe der IP-Adresse des anfragenden Gerätes	login:OK##IP-Adr. bzw. login:DENIED##IP-Adr.
logout	logout:IP-Adr.	Ein Gerät meldet sich „vorschriftsmäßig“ aus dem System unter Angabe der eigenen IP-Adresse ab.	logout:OK##IP-Adr. bzw. logout:DENIED##IP-Adr.
getData	getData:IP-Adr.[##timestamp1##timestamp2]	Der Manager fordert beim Repository-Gerät den letzten Sensorwert des zur angegebenen IP-Adresse gehörenden Sensor-Geräten an. Alternativ kann unter Angabe der Start- und Endzeit ein Zeitintervall festgelegt werden, aus dem alle gemessenen Werte übertragen werden sollen.	GetData:[timestamp##Wert]*
ping	ping	Das Manager-Gerät stellt eine ping-Anfrage zwecks Messung der Laufzeit	pong
kick	kick	Das Manager-Gerät gibt bekannt, dass das Gerät aus dem System entfernt wurde. Das entfernte Gerät sendet eine Bestätigung, die jedoch als Ausnahme nicht zwingend erforderlich ist.	kick:OK

Abbildung 6: Übersicht über mögliche Requests und Replies

Zusätzlich zu den Requests gibt es die Möglichkeit, Daten zu übermitteln. Dies können Nachrichten (oder darin verpackte Sensordaten bzw. Aufträge für den Nutzer) sein oder Statusmeldungen. Ein Reply erfolgt durch das bloße Zurücksenden der eingegangenen Daten mit dem Präfix „MsgRep:“ bzw. „StsRep:“. Eine Übersicht darüber liefert Abbildung 7.

Nutzdaten	Übermittlungstyp	Beschreibung
0-9	2	aktueller Status des Nutzers
beliebiger Text	3	Nachricht, die zwischen Manager- und User-Gerät ausgetauscht wird
A:beliebiger Text	3	Auftrag, der vom Manager dem Nutzer zugeteilt wird
Sen:timestamp##Wert	3	Sensordaten inkl. Zeitpunkt der Messung, die dem Repository-Gerät zwecks Speicherung übermittelt werden.

Abbildung 7: Übersicht über Nachrichtentypen

Folgend werden die einzelnen Gerätetypen sowie deren Handhabung näher erläutert.

Das User-Gerät

Als User-Gerät soll ein Gerät bezeichnet werden, das an der Schadenstelle vom Helfer genutzt werden kann, um mit dem Verantwortlichen Nachrichten auszutauschen, sowie Aufträge zu empfangen und Statusmeldungen dazu abzugeben. Im einfachsten Fall kann dies, wie beschrieben, ein Mobiltelefon sein.

(a) (b) (c)

Abbildung 8: Screenshots eines User-Geräts

Nach dem Starten des Programms wird geprüft, ob die Voreinstellungen für das Gerät bereits getätigt wurden. Dazu gehören eine IP-Adresse, die dem Gerät zuvor zugeteilt worden sein muss, das gültige Passwort sowie eine Beschreibung, z.B. den Namen des Nutzers. Sollten diese noch nicht gesetzt worden sein, so fordert das Programm den Nutzer erst dazu auf, dies nachzuholen, bevor weitergearbeitet werden kann (vgl. Abbildung 8a).

Im anschließenden Menü hat man die Möglichkeit, sich Informationen über das Programm anzusehen, die Voreinstellungen nochmals zu ändern oder zu versuchen, sich in das System einzuloggen. Letzteres löst die in Abbildung 9 dargestellten Vorgänge aus.

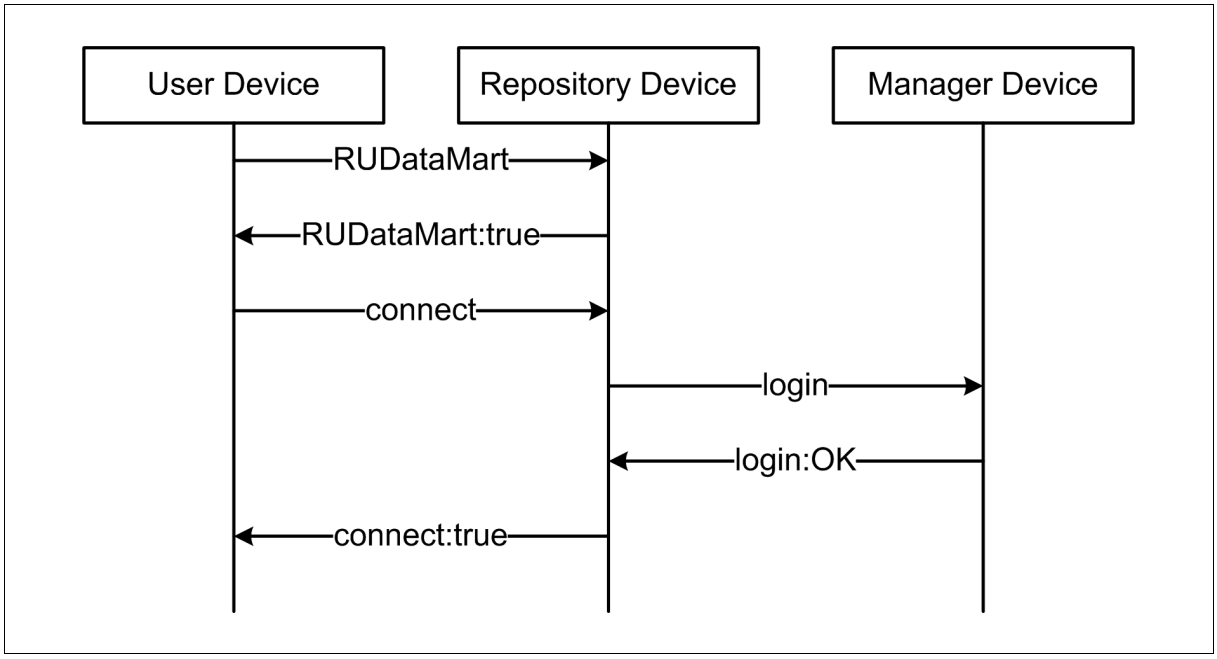

Abbildung 9: Normaler Login-Vorgang eines User-Geräts

Nach erfolgreichem Login gelangt der Nutzer zum Übersichtsbildschirm, auf dem ihm sein eigener Status, sein derzeitiger Auftrag sowie die zuletzt eingegangene Nachricht angezeigt werden (vgl. Abbildung 8b). Es besteht nun die Möglichkeit, den aktuellen Status an das Manager-Gerät zu senden. Zu diesem Zweck wird zuerst die entsprechende Ziffer eingegeben und anschließend die Senden-Taste gedrückt. Erfolgt dieses nicht im Abstand von höchstens drei Sekunden, wird die Eingabe der Ziffer wieder zurückgenommen. Es wird damit ähnlich der Tastensperre von Mobiltelefonen der Zweck verfolgt, ein versehentliches Senden eines Statuscodes durch ungewollt gedrückte Tasten auf dem Gerät zu verhindern.
Über Status 5 (vgl. Kapitel 5.1.5) ist es zudem möglich, dem Manager-Gerät Nachrichten zu schicken. Um dies zu ermöglichen, wird eine neue Eingabemaske geöffnet (vgl. Abbildung 8c). Nach Absenden der Nachricht bzw. Abbruch des Vorgangs wird wieder zum Übersichtsbildschirm zurückgekehrt.

Entgegen der Empfehlungen für J2ME-Programme (vgl. Bloch/Wagner (2003), S. 11) blockiert das User-Gerät beim Senden, d.h. Es ist kein Weiterarbeiten möglich, bis ein Reply

empfangen oder die Übertragung per Timeout als gescheitert angesehen wird. Dies zwingt den Nutzer dazu abzuwarten, bis er sicher sein kann, ob seine Meldung beim Verantwortlichen angekommen ist. Hinderlich ist dies nicht, da die Geräte keine weitere Funktionen erfüllen, die nebenläufig ausgeführt werden müssen.

Das Sensor-Gerät

Dem Sensor-Gerät fällt die Aufgabe zu, Messwerte zu ermitteln und automatisch an das Repository-Gerät zu versenden. Dort werden diese gesammelt und für den späteren Abruf durch einen Verantwortlichen bereitgehalten.
Das Anmelden im System erfolgt analog zum User-Gerät. Nach erfolgtem Login wird der periodisch gemessene Wert angezeigt und versendet. Für das Demonstrationsprogramm wird statt eines real gemessenen Wertes ein Zufallswert ermittelt.

Das Repository-Gerät

Dem Repository-Gerät fallen zwei Aufgaben zu. Zum einen stellt es als Gateway die Verbindung zwischen Bluetooth (PAN) und WLAN (LAN) her. Eingehende Botschaften werden entsprechend weitergeleitet, sofern anhand der IP-Adresse ein angeschlossenes Gerät erkannt wird. Zum anderen speichert das Repository-Gerät die von angeschlossenen Sensor-Knoten übermittelten Werte samt Zeitmarkierung zwecks späterem Abruf durch das Manager-Gerät.
Der Zugang zum System erfolgt per WLAN beim Manager-Gerät, dessen IP-Adresse zuvor bekannt und eingestellt sein muss. Anschließend kann das Gerät seinen Dienst ohne menschliches Zutun verrichten.

Das Manager-Gerät

Das Manager-Gerät soll es der verantwortlichen Führungskraft ermöglichen, einen Überblick über eingesetzte Helfer zu erhalten und mit ihnen zu kommunizieren. Zusätzlich ist das Beobachten von Sensordaten möglich.

Nach dem Start des Programms öffnet sich das in Abbildung 10 dargestellte Fenster. Von hier aus werden die einzelnen Aktionen gesteuert. Zuerst bedarf es der Einstellungen, die analog zu den übrigen Geräten erfolgen und über den Menüpunkt „Prefs/Netzwerk“ aufgerufen werden können. Über den Menüpunkt „System“ gelangt man zudem zum Punkt „Informa-

tionen“, der selbige über das Programm liefert, und man erhält die Möglichkeit, das Programm zu beenden.

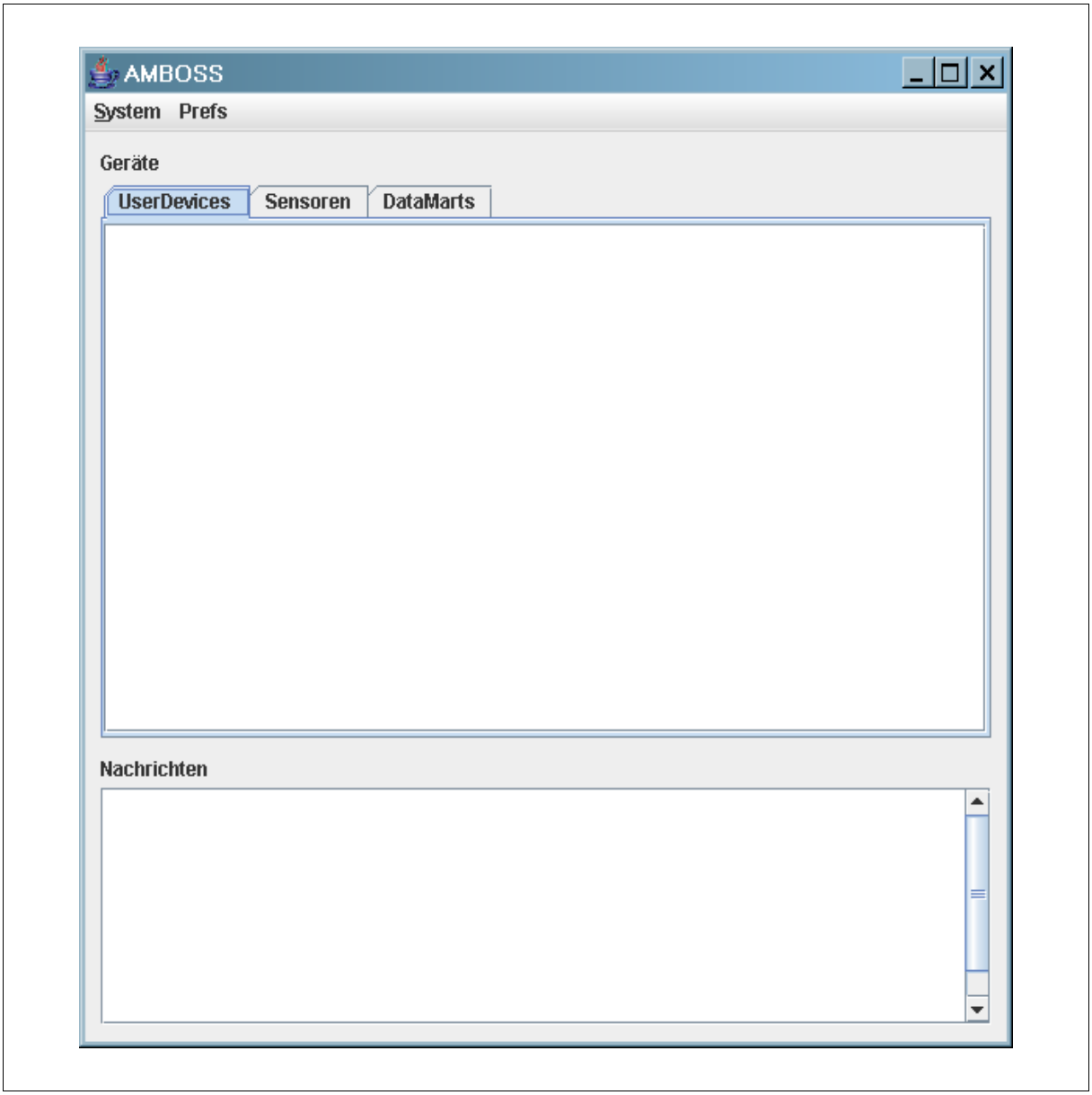

Abbildung 10: Hauptfenster des Manager-Geräts

Über die Karteireiter lassen sich in einer Liste alle im System angemeldeten User-, Sensor- und Repository-Geräte (DataMarts) anzeigen. Zu den Geräten werden jeweils die IP-Adresse und die Beschreibung angegeben. Bei User-Geräten werden zusätzlich der derzeitige Auftrag sowie der Status eingeblendet, im Falle eines Sensor-Knotens der zuletzt erfragte gemessene Wert.

Wählt man aus der Liste eines der Geräte an, so öffnet sich für dieses ein eigenes Fenster. Über dessen Menü ist es dann möglich, die Laufzeit von Nachrichten zu diesem Gerät per „ping“ zu bestimmen bzw. es aus dem System zu entfernen. Im Falle eines User-Geräts hat man weiterhin die Möglichkeit, Aufträge und Nachrichten zu versenden. Bei Sensoren kann vom Repository-Gerät der zuletzt eingegangene gemessene Wert abgerufen werden. Sollte eine Übertragung nicht binnen des voreingestellten Timeouts durch ein Reply bestätigt werden, wird der Nutzer darauf hingewiesen. Es erfolgt automatisch ein „ping“ an das verantwortliche Repository-Gerät, um zu prüfen, ob dieses möglicherweise ausgefallen ist. Der Nutzer wird über das Resultat der Ermittlungen informiert und erhält entsprechende Vorschläge zum weiteren Vorgehen.

Im unteren Bereich des Hauptfenster werden eingehende und ausgehende Nachrichten unter Angabe der Versenders und einer Zeitmarkierung angezeigt.

5.3. Fehlende Funktionalität

Einige der geplanten Funktionen wurden bisher nicht komplett implementiert. So wird z.B. beim Anmelden beim Manager-Gerät geprüft, ob die angegebener IP-Adresse auch Zugang zum System erhalten darf, das Verwalten der entsprechenden Liste von Adressen ist jedoch noch nicht möglich.
Auch kann das Repository-Gerät gemessene Werte eines Sensors über einen bestimmten Zeitraum unter Angabe zweier begrenzender Zeitmarkierungen liefern, doch fehlt im Manager-Gerät bisher die Möglichkeit, eine solche Anfrage zu stellen.
Weiterhin werden die Methodenrümpfe für Ver- und Entschlüsselung bereits genutzt, doch tatsächlich finden diese nicht statt und das System prüft noch nicht, ob die „verschlüsselten“ Nutzdaten tatsächlich gültige Anfragen darstellen, oder bedingt durch Verschlüsselung mit einem falschen Passwort lediglich Unsinn darstellen. Stattdessen werden solche Anfragen einfach ignoriert.
Eine Behandlung des Ausfalls des Manager-Gerät bzw. eines Repository-Gerät findet bisher weder im User- oder im Sensor-Gerät statt. Selbiges gilt für das Repository-Gerät im Bezug auf die übrigen Geräte.

Bedingt durch die Tatsache, dass JSR-82 noch keine Multi-Hop-Umgebungen unterstützt, ist derzeit ein „Verfolgen“ von Personen, wie es in Kapitel 5.1.4 beschrieben wurde, nicht möglich.

6. Zusammenfassung und Ausblick

In der vorliegenden Arbeit wurde die Arbeit von Kräften der BOS im Katastrophenfall knapp erläutert. Eine verantwortliche Führungskraft koordiniert ggf. unter Mithilfe eines Stabes die Einsatzkräfte. Informationen müssen ausgetauscht und Handlungsanweisungen gegeben werden können.
Aufbauend darauf wurden die Anforderungen analysiert, die sich für ein auf Ad-hoc-Netzen basiertes Informations- und Kommunikationssystem ergeben. Von besonderer Bedeutung ist hier die Verfügbarkeit, die bei derzeitig genutzter analoger Funktechnik die Schwachstelle darstellt. Weiterhin ist hervorzuheben, dass der Verwendungszweck der Geräte unterschiedliche Anforderungen an verschiedenste Ressourcen stellt und beachtet werden muss.
Es wird eine Architektur vorgeschlagen, die die untersuchten Gesichtspunkte berücksichtigt. Abschließend wurden die Funktionsweise und die Handhabung der implementierten Bausteine erläutert. Mit dem System ist er derzeit bereits möglich, eingehende Sensordaten bei der entsprechenden Führungskraft anzeigen zu lassen sowie Kommunikation zwischen Beteiligten in einer Form ähnlich des Chattens per Internet herzustellen. Sinnvoll ergänzt wird letzteres durch die Möglichkeit, typische Meldungen durch Drücken einer einzelnen Taste abzusetzen.
Als Schwierigkeit stellte sich während der Entwicklung das Fehlen vollständiger Unterstützung von JSR-82 durch derzeit verfügbare und eigentlich entsprechend ausgestattete Mobiltelefone heraus. Neben daraus resultierendem Fehlen von Funktionalität im Bereich der Netztopologie wurde ein Feldtest deshalb bisher nicht durchgeführt, sondern zur Simulation der J2ME-Geräte das Wireless Toolkit von Sun Microsystems verwendet.

Um das System alltagstauglich zu machen und über den Status eines Demonstrationsprogrammes zu erheben, müssten noch diverse Funktionen implementiert werden. Es liegen z.B. das Speichern des Nachrichtenprotokolls zwecks Dokumentation oder das Austauschen von Dateien verschiedenster Art nahe. Sinnvoll erscheint auch das Verwalten der im Repository-Gerät eingehenden Messwerte in einer Datenbank, da Anfragen dadurch flexibler gestaltet werden könnten. Wünschenswert wäre sicherlich auch eine Übersichtskarte, auf der die verantwortliche Führungskraft den Standort jedes Gerätes sehen kann. Hierzu wäre jedoch eine geeignete Lokalisierung notwendig.

Literaturverzeichnis

Ausschuss für Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung (2004): *Feuerwehr-Dienstvorschrift 7 - Atemschutz*, Berlin 2004

Bloch, C./Wagner, A. (2003): *MIDP 2.0 Style Guide for the Java 2 Platform, Micro Edition*, Boston et al. 2003

Boukerche, A. (2004): *Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks*, in: Mobile Networks and Applications, Heft 9, 2004, S. 333-342

Dau, V. (2003): *Wie funktionieren TETRA und TETRAPOL?*, in: Im Einsatz: Kommunikation, Heft 6, 2003, S. 11-15

Deutsches Rotes Kreuz, Generalsekretariat (1995): *Die Einsatzeinheit*, Bonn 1995

Gongolsky, M. (2004): *Retten, klicken, funken*, in: Rettungs-Magazin, Heft 5, 2004, S. 30-34

Java Community Process Organisation (2002): *Spezifikation von JSR-82 V1* [online], verfügbar: *http://www.jcp.org/en/jsr/detail?id=82*

Meißner, A. et al. (2002): *Design Challenges for an integrated Disaster Management Communication and Information System*, New York 2002

Meißner, A./Steinebach, M. (2004): *Neue IT-Infrastrukturen im Notfall- und Rettungswesen - Potential und Risiko*, in: Knop, J. von / Frank, H. (Hrsg.): Netz- und Computersicherheit, Bielefeld 2004, S. 321-336

Eckert, C. (2004): *IT-Sicherheit*, 3. Aufl., München 2004

Freebersyser, J. A. / Leiner, B. (2001): *A DoD Perspective on Mobile Ad Hoc Networks*, in: Perkins, C. E. (Hrsg.): Ad Hoc Networking, Boston et. al. 2001, S. 29-51

IEEE (2003): *Spezifikation von IEEE 802.11* [online], verfügbar: http://ieee802.org/11

McDermott-Wells, P. (2004a): *What is Bluetooth*, in: IEEE potentials, Bd. 23, Heft 5, 2004, S. 33-35

McDermott-Wells, P. (2004b): *Bluetooth scatternet models*, in: IEEE potentials, Bd. 23, Heft 5, 2004, S. 36-39

Pabuwal, N./Jain, N./Jain, B. N. (2003): *An Architectural Framework to deploy Scatternet-Based Applications over Bluetooth,* in: Proceedings Of IEEE International Conference on Communications (ICC 2003), Anchorage, Alaska 2003

Perkins, C. E. (Hrsg.) (2001): *Ad Hoc Networking*, Boston et. al. 2001

Perkins, C. E. / Royer, E. M. (2001): *The Ad Hoc On-Demand Distance-Vector Protocol*, in: Perkins, C. E. (Hrsg.): Ad Hoc Networking, Boston et. al. 2001, S. 173-219

Peter, H./Mitschke, T./Uhr, T. (2001): *Notarzt und Rettungsassistent beim MANV*, Edewecht, Wien 2001

Rumbaugh, J./Jacobson, I./Boochs, G. (2005): *The Unified Modeling Language Reference Manual*, 2. Aufl., Boston et al. 2005

Johansson et al. (1999): *Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks*, in: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, New York 1999, S. 195-206

Stallings, W. (2001): *Sicherheit im Internet*, München 2001

Tan, G. et al. (2001): *Forming Scatternets from Bluetooth Personal Area Networks*, in MIT Technical Report, MIT-LCS-TR-826, 2001

Tanenbaum, A. (2003): *Computernetzwerke*, 4. Aufl., München et al. 2003

Voss, S./Gutenschwager, K. (2001): Informationsmanagement, Heidelberg 2001

W3 Konsortium (1997): *Spezifikation von XML* [online], verfügbar: http://www.w3.org/XML