Information-Sharing in Out-of-Hospital Disaster Response: The Future Role of Information Technology

Jeffrey L. Arnold, MD;[1] Brian Neil Levine, PhD;[2] R. Manmatha, PhD;[2] Francis Lee, MD, MPH;[3] Prashant Shenoy, PhD;[2] Ming-Che Tsai, MD, MPH;[4] Taha K. Ibrahim, MD, FRCSI, CABS;[5] Daniel J. O'Brien, MD;[6] Donald A. Walsh, PhD, LP[7]

1. Yale-New Haven Center for Emergency Preparedness and Disaster Response and the Section of Emergency Medicine, Department of Surgery, Yale University School of Medicine, New Haven, Connecticut USA
2. Department of Computer Science, University of Massachusetts, Amherst, Massachusetts USA
3. Department of Surgery, Baystate Medical Center, Tufts University School of Medicine, Springfield, Massachusetts USA
4. Department of Trauma Service and Emergency Medicine, National Cheng Kung University Hospital, Tainan, Taiwan, Republic of China
5. Accident and Emergency Medicine Department, Al Ain Hospital, Al Ain, United Arab Emirates
6. Department of Emergency Medicine, University of Louisville, Louisville, Kentucky USA
7. Chicago Fire Department, Bureau of Operations, Emergency Medical Services Division, Chicago, Illinois USA

Correspondence:
Jeffrey Arnold, MD
Yale-New Haven Center for Emergency Preparedness and Disaster Response
1 Church Street
New Haven, CT 06519 USA
E-mail: jeffrey.arnold@ynhh.org

Keywords: disaster; emergency management; geographic information system; global positioning system; information; information technology; Internet; personal digital assistant; wireless peer network

Abbreviations:
COTS = current off-the-shelf
COWS = cell sites on wheels
SatCOLTs = satellite cell sites on light trucks
GIS = geographical information systems
GPS = global positioning systems
HIPAA = Health Insurance Portability and Accountability Act of 1996
ICS = Incident Command System
IR = information retrieval
IT = information technology
OOH = out-of-hospital
P2P= peer-to-peer
PDA = personal digital assistant
RF = radio frequency
RFID = radio frequency identification
SMS = Simple Message Service
SUMA = Supply Management System
WAP = Wireless Application Protocol
WHO = World Heath Organization

Received: 18 June 2003
Accepted: 20 August 2003
Revised: 27 June 2004

Web publication: 29 September 2004

Abstract

Numerous examples exist of the benefits of the timely access to information in emergencies and disasters. Information technology (IT) is playing an increasingly important role in information-sharing during emergencies and disasters.

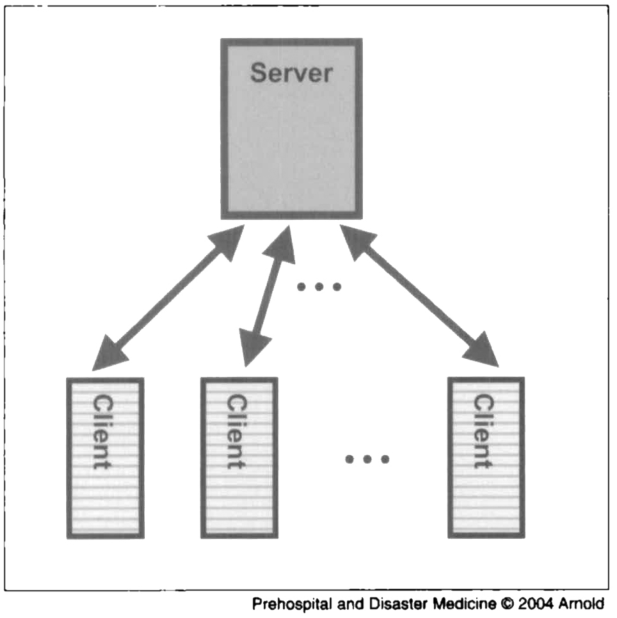
The effective use of IT in out-of-hospital (OOH) disaster response is accompanied by numerous challenges at the human, applications, communication, and security levels. Most reports of IT applications to emergencies or disasters to date, concern applications that are hospital-based or occur during non-response phases of events (i.e., mitigation, planning and preparedness, or recovery phases). Few reports address the application of IT to OOH disaster response.

Wireless peer networks that involve ad hoc wireless routing networks and peer-to-peer application architectures offer a promising solution to the many challenges of information-sharing in OOH disaster response. These networks offer several services that are likely to improve information-sharing in OOH emergency response, including needs and capacity assessment databases, victim tracking, event logging, information retrieval, and overall incident management system support.

Arnold JL, Levine BN, Manmatha R, Lee F, Shenoy P, Tsai MC, Ibrahim TK, O'Brien DJ, Walsh DA: Information-sharing in out-of-hospital disaster response: The future role of information technology. *Prehosp Disast Med* 2004;19(2): 201–207.

Introduction

Many examples exist, both anecdotal and published, of the potential role of information technology (IT) for information-sharing in emergencies and disasters.[1,2] In this article, the challenges and applications of IT are examined and a potential role for wireless peer networks for information-sharing in out-of-hospital (OOH) disaster response is suggested.



Prehospital and Disaster Medicine © 2004 Arnold

Figure 1—Centralized architecture for information sharing

Challenges for Information Technology
Numerous challenges accompany the effective use of IT in OOH disaster response. These challenges exist at the human, applications, communications, and security levels:

Human challenges
The human level of IT poses a number of critical challenges for information-sharing in OOH disaster response. From a practical standpoint, IT implementations should be: (1) user friendly, ensuring that all emergency responders have immediate access to the information they need, when they need it; (2) incorporated by personnel into everyday tasks to ensure functional familiarity during disasters; (3) compatible with existing communication links to contacts outside the immediate disaster scene; (4) easily taught, requiring a minimal amount of training to facilitate usage (e.g., one session); (5) be cost-effective; and (6) deployable via inexpensive current off-the-shelf (COTS) hardware. They should be deployable in forms flexible enough to meet the needs of incidents of various scopes and complexities; and provide useful and reliable information. For example, IT implementations that assist in monitoring events (e.g., biosurveillance) are likely to be ignored or completely shutdown if they generate too many false alarms (false positives). Moreover, technologies, shared data, and terminology should be standardized sufficiently in order to rapidly integrate personnel from a variety of agencies via a common structure for information-sharing.

Applications challenges
A number of technical challenges stem from the applications level of IT, which provides the various services related to information-sharing. Common IT services include: (1) database access; (2) text/audio/photo/video message routing; (3) information retrieval (IR) systems; (4) automated needs assessment systems; (5) localization and directional systems; and (6) automated logging systems. While specific challenges at the application level vary with the goal of each application, a fundamental goal of all systems is increased access to, and sharing of, information for users. Integration issues also should be addressed at the applications level so that desired types of processed information will be available to users. Common information-sharing services are:

- *Database systems*—maintain access and query to structured data. When information is newly gathered or changed, database systems provide reliable updates in a globally-consistent manner.
- *Needs assessment applications*—enable the automated collection, correlation, and annotation of data gathered from remote users or sensors. Needs assessment applications convey information efficiently (otherwise, the network may become overloaded), with alarms that are accurate (least they be ignored).
- *Messaging systems*—provide reliable delivery of messages and information from user-to-user (or from one user to many) in the presence of network or device failures, or asynchronous use.
- *IR systems*—allow the retrieval of relevant information from a collection of documents based on user queries. They are distinguished from database access in their ability to handle unstructured information.
- *Localization and directional systems*—provide users with information about their location on a map. Global positioning systems (GPS) comprise a common and increasingly inexpensive method of aquiring location. However, GPS signals cannot penetrate most structures. Localization methods can triangulate user positions based on signals in the environment (e.g., triangulation of known cellular tower signals or statically placed wireless access points running wi-fi (IEEE 802.11)). Localization methods even may provide a user's location relative to other mobile users broadcasting wi-fi signals.
- *Geographical information systems (GIS)*—enable the mapping of specific data sets to geographic coordinates.
- *Event logging services*—collect information gathered during an event and reliably store it in the presence of adversaries and secondary events that may destroy storage. After an incident, event logs may be analyzed by forensics systems for evaluating response or investigating scene events.

These applications typically are deployed as centralized or distributed architectures (Figures 1, 2). In a centralized architecture, a single server is responsible for processing all user requests. Centralized architectures simplify administration and coordination of a service, and they often require fewer resources. However, centralized architectures also have several disadvantages. A centralized server represents a bottleneck in processing that can delay response time. It may represent a single point-of-failure, and for adversaries, a single point-of-attack, without which the entire service

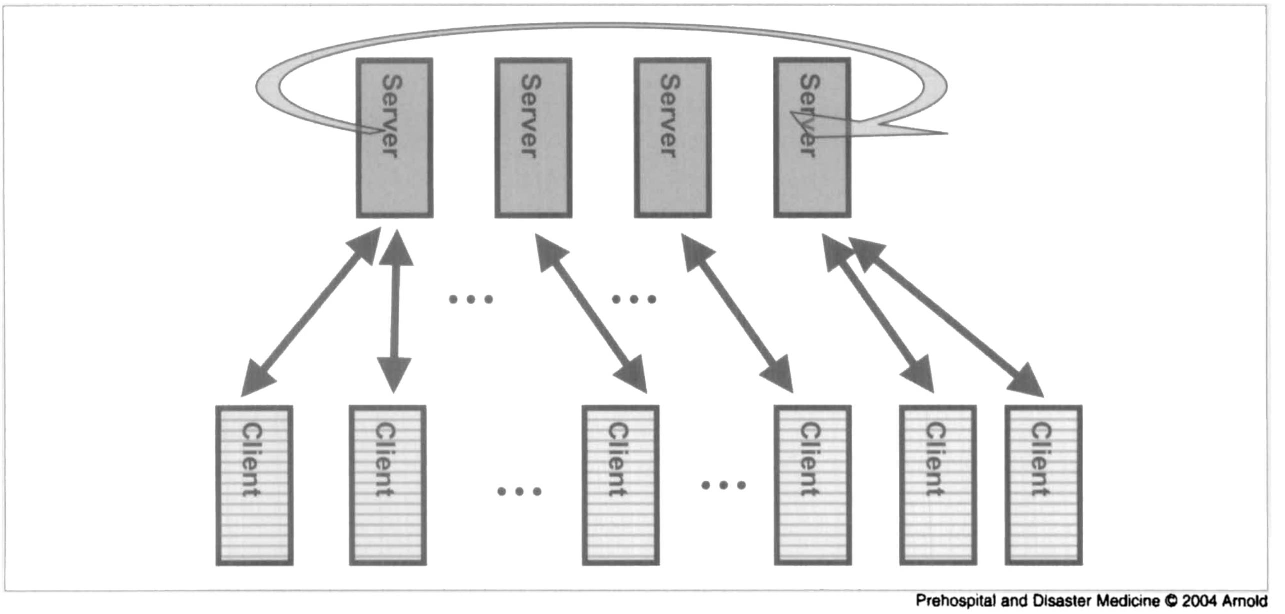


Figure 2—Distributed architecture for infomartion sharing. Clients are mapped to replicate servers that must coordinate wtih each other.

fails. Finally, even if the server is resourceful and available, the routing function provided by the communications layer may fail to provide a path from some clients to the server (or fail between clients).

Distributed architectures replicate a service at many points in a network. Accordingly, some or all of the associated data also may be replicated. Because of replication, distributed applications offer opposite tradeoffs. They are more likely to be available and with lower latency, have no bottlenecks, have no single points of failure or attack, and allow multiple routes to service. However, distributed architectures entail designs that are more complicated (as the servers usually require some form of coordination), may be temporarily inconsistent, and may be difficult to administrate. A special type of distributed architecture, peer-to-peer networks, is described below.

Communications challenges

The communications level of information-sharing routes packets of information between applications running on devices. IT communications infrastructures are wireless or tethered. Wireless communications infrastructures include satellites, cell towers, wi-fi (IEEE 802.11), or Bluetooth. Tethered communications infrastructures include ethernet over coax cables or optical fibers. Most disasters require wireless communication, although tethered communication may be necessary as well (e.g., communication within a hospital).

Network protocols that provide routing over these technologies are a mature and active area of computer science research and commercial product development. Unfortunately, emergencies and disasters typically generate challenges that transcend routine commercial applications. For example, in many events, a pre-existing wired or wireless network-layer infrastructure is unavailable. In physically destructive events, this infrastructure may be destroyed or incapacitated. Because responders cannot rely on coverage by pre-existing infrastructure, information-sharing in OOH emergency response is likely to require that this communication infrastructure be brought to the scene by the responders. Furthermore, communications deployed ad hoc by responders may be too sparse to cover the entire geographic area of the event and still must provide routing despite ensuing network partitions. In addition, continuous or intermittent network partitions may exist due to physically blocked propagation of radio waves. Information-sharing devices, such as PDAs, may be physically damaged in a variety of disaster environments. For example, exposure to water, extreme heat, or radiation may disrupt the operation of devices. In terrorism-related emergencies or war, on-scene adversaries may disrupt communication through physical attack or capture of devices. Perhaps even more worrisome are attacks based on flaws in the design or implementation of network protocols.

Security challenges

The operation of IT in an OOH disaster environment also presents a number of security concerns. Emergency response is likely to utilize wireless networks that are prone to eavesdropping and take place in uncontrolled environments in which adversaries may roam freely. In general, securing IT in OOH disaster response follows the same processes and requirements common to all IT applications. Before IT is deployed in a disaster response, an agency must define its policy for information-sharing, in a similar manner to information-sharing that occurs inside healthcare organizations, such as hospitals.[3]

With such a policy in place, the agency must perform a risk assessment according to the threats posed by the disaster response environment. Critical security requirements

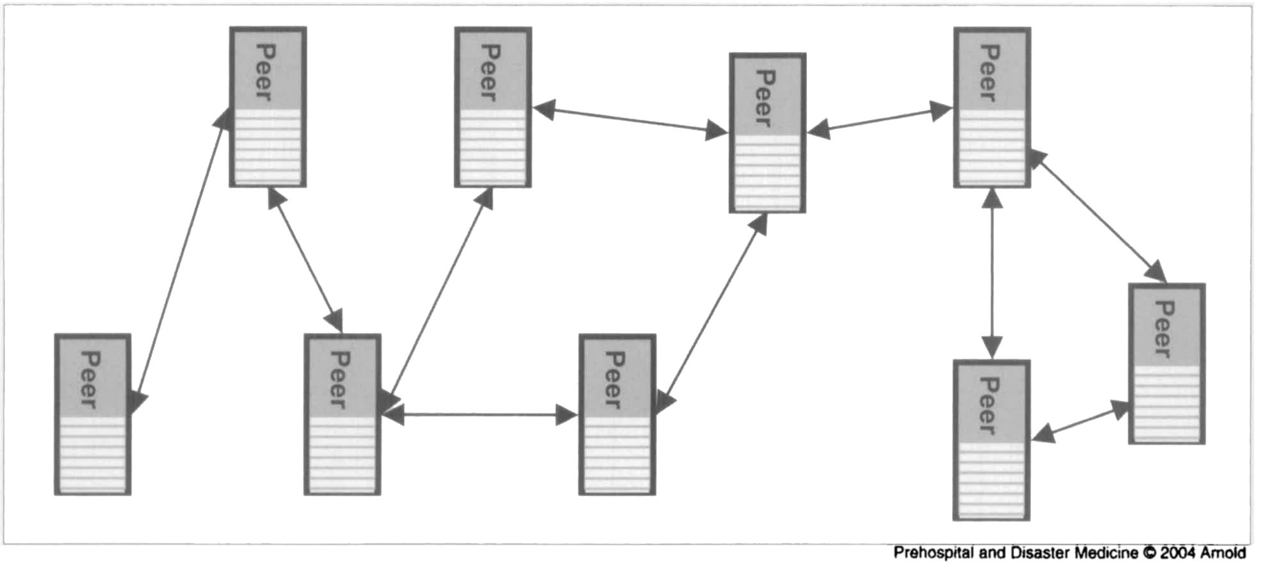


Figure 3—Peer-to-peer architecture for information sharing. Each host functions as a client and server.

include ensuring the following: (1) all communications between emergency response personnel are *authenticated*; (2) only *authorized* users are able to access information; (3) information always is *available* to all authorized users who require it; (4) the *integrity* of all information being shared or collected; and (5) the *confidentiality* of all records being shared or collected. Additionally, event logging and subsequent forensic investigations may require that records created by workers are nonrepudiable.

Authentication is a necessary precursor to authorization. In general, worker identities are authenticated to an account by the entry of a password. Authentication also may occur via a wireless message (e.g., via Bluetooth) from a physical token attached to the person of a worker. The account, in turn, provides the authorization to enact some privilege. Since IT will be used to pass messages between workers, it is vital that the stated author of the message be authenticated by the system. If the message contains directives to other workers without authentication, improper or false directives could be broadcast and carried out. The chaos of an emergency event may result in lost devices or devices changing hands, making authentication based on physical tokens an important consideration.[4]

The availability of information in the system may be disrupted by various denial-of-service attacks depending on the IT system. Various network attacks may target the routing between devices or they may overwhelm a particular device. Enough false messages may be sent to a device rendering it unable to accept new connections.[5,6] Because devices carried by workers are likely to be low in resources, attacks that exhaust the resources of a device are proportionally easier to carry out. Another important consideration is maintaining the integrity of stored records or transmitted messages. Finally, the protection of patient confidentiality is not only ethically desirable, but also is legally mandated. Recently, key provisions of the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) have been instituted that require healthcare organizations that conduct certain administrative or financial transactions electronically to implement reasonable safeguards that protect the security and privacy of patient healthcare information.[7]

Applications of Information Technology

General considerations

Numerous reports exist of the applications of IT to the interdisaster (mitigation, planning, and preparedness), predisaster (warning), and recovery phases of disasters.[1,2,8] Few reports exist of the IT applications during the emergency phase (relief or response phase) of disasters.[2,8]

One of the best-known applications of IT during the emergency phase of disasters is the Supply Management System (SUMA), a computerized information management tool created by the Pan-American Health Organization, that helps national authorities track donated supplies in disasters until they are effectively distributed to the affected population.[9] Another example is the use of commercial software packages (e.g., EIS or SoftRisk) by emergency operations centers in support of emergency management functions, such as incident or resource tracking or mapping, or real-time communication.[1,2]

The Internet has been cited frequently as a potential backbone for information-sharing during the emergency phase of disasters.[10–16] Suggested roles for the Internet include e-mail (e.g., messaging, conferencing, flash news, sensor-linked warnings), voice or video streaming (messaging, conferencing, multimedia information transmission), and Website access (e.g., web pages, databases, libraries, and journals). During the 1997 Cambodian Flood, the government of Cambodia reportedly used the Internet to identify sources from which to obtain snake anitvenom to treat nearly 100 snakebite casualties confronting the country within a relatively short period.[13] Recently, Lawry described the use of the Internet during the terror attacks of 11 September 2001 to disseminate public information about blood donation or the location of patients in Greater New York Area hospitals.[11]

Information technology applications in support of information-sharing in hospitals during the emergency phase of disasters also have been reported. For example, Noordergraaf *et al* reported the use of IT for in-hospital management decision support during simulated and actual mass casualty incidents in the Netherlands.[17] Although a number of commercial and academic groups have been investigating applications of IT to OOH disaster response in recent years, relatively little has been published on this subject.[2] Despite a paucity of literature, two recent trends have emerged, which are likely to affect the future direction of IT applications in this area.

Personal digital assistants

First, personal digital assistants (PDAs) are likely to have an increasing impact on information-sharing in OOH disaster response. Factors enabling the application of PDAs to OOH disaster response include: (1) increased processing power; (2) increased miniaturization of components; (3) increased durability; (4) improvements in batteries (decreased dependence on electric power); and (5) decreased costs.[2]

Personal digital assistants already support data collection in a variety of OOH settings, including routine EMS activities and public health assessments.[18,19] Recently, Cabrera *et al* reported the use of PDAs in support of information-sharing in OOH emergency response.[20] Moreover, Wu reported the construction of hazardous chemical databases for deployment in PDAs during chemical disasters in Taiwan. These databases contained the identities of chemicals present in 65 local factories (based on queries by factory name or chemical characteristic), the characteristics of 234 chemicals, and their recommended medical management.[21]

Wireless technology

Second, wireless technology is poised to play a major role in information-sharing in OOH disaster response. Factors enabling the application of wireless technology to OOH disaster response include: (1) increased bandwidth for radio transmission; (2) increased mobility; (3) miniaturization and durability of devices; (4) improvements in batteries; and (5) decreased cost.[2]

Unidirectional wireless systems already support the transmission of data from OOH emergency responders to hospitals in a number of communities. Teich *et al* reported the transmission of OOH data using a fax "notepad" linked to cell phones, which then transmitted information by fax to hospitals. This group also described a wireless system for OOH data transmission that consists of data-acquisition devices linked to cell phones, which, in turn, are connected to the hospital intranet, enabling hospital personnel to access data via a Web browser.[22]

Little has been reported about wireless systems in support of information-sharing among OOH emergency responders. Recently, Li described the application of cell phones with Internet access to support information exchange using Wireless Application Protocol (WAP) and Internet Protocol-based tools. Li found that while an Internet interface facilitated the querying and collection of data, only certain information can be interactively displayed on cell phones via a WAP interface (the same is likely to be true for newer Simple Message Service (SMS) standards).[23] More recently, Hamilton reported the use of a distributed wireless PDA system in OOH emergency response, in which a dedicated Internet site serves as the hub for information exchange.[10] Although these designs for information-sharing have promise, they are limited by their dependence on centralized architectures and underlying assumptions that: (1) wireless communication infrastructures will pre-exist or always be available in disaster-stricken areas; and (2) power and wireless communication infrastructures will remain unaltered by the event.

Recently, Nextel, a US wireless communications company, introduced self-contained mobile cell sites on wheels (COWS) and satellite cell sites on light trucks (SatCOLTs) in order to bring wireless communication infrastructures to the disaster scene (e.g., hurricane-affected areas).[24] This system also depends on either the survival of pre-deployed infrastructures during the event or the rapid movement of infrastructures mounted on vehicles into the affected area after an event. Limitations to this approach include: (1) road conditions after or during an event; (2) distance to the affected area; (3) deployment time; and (4) the need to ensure the personal safety of wireless communications workers.

The Role of Wireless Peer Networks

Wireless peer networks constitute another potential application of IT to information-sharing in OOH disaster response. Wireless peer networks are created by mobile devices brought to the scene by emergency responders, where each device produces, receives, and relays information. Wireless peer networks offer a promising solution to the major technical challenges posed by the networking and applications layers of IT through two key innovations —ad hoc wireless routing networks and peer-to-peer (P2P) architectures.

Ad hoc wireless routing networks make use of the ad hoc location of mobile peers and discover the shortest route between arbitrary peers when other peers are used as intermediaries. This approach enables two peers out of radio range with each other to communicate via an intermediary peer that is within communication range of both. This allows network routing independent of pre-existing network infrastructure, fixed peer locations, or network partitions.[5,25]

Peer-to-peer architectures are a type of distributed architecture in which all clients also are servers (Figure 3). Although each peer offers only a portion of the full service or data available in the system, a threshold number of peers summate to provide full service or all of the available data.

Peer-to-peer architectures offer several important advantages over centralized architectures. First, P2P architectures are orthogonal to the process of human decision-making, enabling information-sharing to occur both vertically and

https://doi.org/10.1017/S1049023X00001783 Published online by Cambridge University Press

horizontally. No single device or peer is crucial, allowing all information to be widely available. Second, because the architecture is distributed, service in P2P architectures resists disruption. If an arbitrary node is lost temporarily (e.g., due to network conditions) or permanently (e.g., due to secondary events), then other nodes will take its place. Peer-to-peer architecture also provides a natural redundancy that obviates the need for expensive back-up systems. Third, P2P architectures become more robust as more peers enter the network. In P2P architectures, mobile nodes are homogenous in resources (e.g., processing, energy stores, memory, storage, and bandwidth of network connection). Each mobile node is not only a client, but also is a provider of service. As more peers enter, additional resources storage and processing are added, compensating for any additional load that the newcomers generate.

Wireless peer networks composed of ad hoc wireless routing and P2P applications have several potential applications for information-sharing in OOH emergency response.

Assessment databases

Wireless peer networks may enable scene assessment databases to be updated continuously as events unfold, updated scene assessment reports to be distributed over a wide physical area to responders already on-scene, and updated scene assessment reports to serve as a real-time briefing mechanism for new responders arriving on-scene. Wireless peer networks also may support the continuous input and tabulation of data from individual victim assessments to provide real-time estimates of population needs, such as the number of victims with the same triage score or the number of victims requiring a specific on-scene intervention, such as decontamination. Hands-free, voice-response systems may facilitate information capture during emergencies and disasters. Individual victim assessments may be coupled with GIS to map locations of the victim population. Capacity assessments also may be updated instantaneously and collated over a wide area to provide real-time estimates of critical resource availability, including personnel, vehicles, and/or specialized equipment for search and rescue or decontamination. Turning PDAs on or off may trigger automated logging of personnel or vehicles arriving or leaving the scene.

Victim and resource tracking

Wireless peer networks may support the widespread and instantaneous tracking of victims or resources through barcode or radio frequency identification (RFID) systems.[26, 27] In an RFID application, PDAs may be equipped with radio-frequency (RF) cards and interrogator attachments, while RF tags (small computer circuits with identifying information) may be attached to victims during triage. Radio frequency tags also may be attached to responding personnel, vehicles, equipment, or supplies.

An RFID system represents a major advantage over handwritten or bar-code-based identification systems, because it supports the simultaneous collection of information from thousands of RF tagged persons or objects and does not depend on line-of-sight contact between receiver and tag. Moreover, some RF systems enable data stored on RF tags to be updated or expanded (e.g., permitting the revision of triage scores on RF tags attached to individual victims). In addition, RF-tagged victims or resources may be located via GIS to produce a real-time map of the entire population.

Information retrieval

Providing reliable Internet access to multiple mobile users in large-scale disasters (e.g., PICE II–III events) is not feasible at this time. This is especially true in developing countries and in the early phase of emergency response in developed countries. A viable alternative is to locally store the needed information as a digital library and access it using an information retrieval system. Information retreival systems retrieve relevant text from collections of unstructured (or structured) documents. Relevant information includes: (1) field medical manuals detailing the provision of medical care in austere conditions; (2) selected medical references, such as the World Health Organization (WHO) Disaster Medicine Library or an atlas of clinical images; and/or (3) immunization algorithms in the event of a contagious disease outbreak.

In contrast to individual mobile devices, which are resource-poor and lack sufficient robustness for indexing voluminous content or responding to numerous queries, a group of mobile peers may share the work of indexing documents, storing indices, and responding to queries while providing coverage in a wireless environment.

Event logging

Automated logging of key on-scene events—including decisions, communications, interventions, and consequences—may assist ongoing response efforts and future post-emergency planning and preparedness. Still photographs, video images, and sound may be used to generate multi-media event logs from a variety of vantage points during an emergency. Images taken by different responders at the same geographic location over time may be collated to provide a visual record of events at a location of interest. Recorded images and sound may be tagged with the current time and the geographic location of the user.

Audio communication

Wireless peer networks may also support traditional audio communication during disasters. Individual devices may be equipped with voice cards, microphones, and speakers to support audio messaging, while wireless ear plugs may be used for message reception. Audio message overload may be prevented via routing protocols that channel messages to appropriate recipients.

Incident command system support

Perhaps the most important application of wireless peer networks in emergencies and disasters is in support of Incident Command System (ICS) functions. Effective coordination and control of emergency response depends on the effective coordination and control of information-sharing. Applications of wireless peer networks, which may facilitate incident management functions, include: (1) baseline and updated scene assessments, including hazard assessments and the locations of hazards; (2) baseline and updated needs assessments, including numbers, types, and triage status of victims; (3) baseline and updated capacity assessments, through tracking of on-scene and off-site personnel, vehicles, and other emergency response resources; (4) emergency response resource locations (i.e., personnel, vehicles) through GPS-linked devices; (5) pre-selected and pre-loaded ("canned") operational information, including clinical algorithms, maps, and contact information; (6) automated personnel assignments to pre-selected ICS positions through ICS-linked responder registries based on pre-determined criteria; (7) customized event logs relevant to each ICS position to update newly assigned ICS unit leaders; (8) system alerts as scene hazards are discovered or change; and (9) customized alerts relevant to each ICS position, including changes in personnel within each chain of command.

Conclusions

Effective OOH disaster response requires systems for information-sharing that enable responders to rapidly collect, process, and distribute information. Information technology is likely to have an increasingly important role in information-sharing in OOH disaster response. Wireless peer networks offer a promising solution to many of the technical challenges of using IT for information-sharing in OOH disaster response.

References

1. National Research Council: *Reducing Disaster Losses through Better Information.* Washington DC: National Academy Press, 1999, pp 1–61.
2. Stephenson R, Anderson PS: Disasters and the information technology revolution. *Disasters* 1997;21:305–334.
3. Allen JH: *The CERT Guide to System and Network Security Practices.* Addison-Wesley. 2001.
4. Corner M, Noble BD: Protecting applications with transient authentication. In: *The First International Conference on Mobile Systems, Applications and Services.* San Francisco, CA; Mobi Sys, 03 May 2003.
5. Sanzgiri K, Dahill B, Levine BN, *et al*: A secure routing protocol for ad hoc networks. *Proceedings IEEE International Conference on Network Protocols.* November 2002.
6. Anonymous: *TCP SYN Flooding and IP Spoofing Attacks.* CERT Advisory CA-1996-21. 19 September 1996.
7. United States (US) Department of Health and Human Services: Protecting the privacy of patients' health information. DHHS Website. Available at www.hhs.gov/ocr/hipaa. Accessed 17 June 2003.
8. Noji EK: The nature of disaster: General characteristics and public health effects. In: Noji EK (ed), *The Public Health Consequences of Disasters.* New York: Oxford University Press, 1997, pp 3–20.
9. Pan American Health Organization: Humanitarian supply management system. DisasterInfo Website. Available at www.disaster.info.desastres.net/SUMA. Accessed 15 June 2003.
10. Hamilton J: An Internet-based bar code tracking system: Coordination of confusion at mass casualty incidents. *Disast Management Response* 2003; 1(1):25–28.
11. Lawry TC: The Internet as a disaster response tool. *Health Progress* 2002;63:9–10.
12. Libman IM, LaPorte RE, Akazawa S, *et al*: The need for a global health disaster network. *Prehosp Disast Med* 1997;12:11–12.
13. Ochi G, Shirakawa Y, Asahi S, Toriba M: Information transmission through the Internet for the preparedness against venomous snake as the aftermath of Cambodian Flood in 1997. In: *The 4th Asia-Pacific Conference on Disaster Medicine Book of Abstracts.*1998;81.
14. Pan-American Health Organization: Health crisis and the Internet: Harnessing the power of the Internet for emergencies and epidemics. *Prehosp Disast Med* 1998;13:15–20.
15. Piper PS, Burkle FM, Murray RJ: Constructing a World Wide Website for disaster management and humanitarian assistance. *Prehosp Disast Med* 1997;12:92–96.
16. Toro J: The Internet and emergency management. Institute for Crisis, Disaster, and Risk Management Website. Available at www.seas.gwu.edu/%7Eemse232/emse232jan2003com4full.html. Accessed 15 June 2003.
17. Noordergraaf GJ, Bouman JH, Van Den Brink EJ, *et al*: Development of computer-assisted patient control for use in the hospital setting during mass casualty incidents. *Am J Emerg Med* 1996;14:257–261.
18. Chandrasekhar CP, Ghosh J: Information and communications technologies and health in low income countries: The potential and the constraints. *Bulletin of the World Health Organization* 2001;79:850–855.
19. GTRC projects: East Carolina State University Website. Available at http://www.telemed.med.ecu.edu/2001/international/projects.htm. Accessed 01 May 2003.
20. Cabrera MF, Arredondo MT, Rodriguez A, Quiroga J: Mobile technologies in the management of emergencies: The results of a telemedicine solution. *Proceedings/AMAI Annual Symposium* 2001;86–89.
21. Wu TC: The use of a personal digital assistant and network geographic information systems for a first aid drill for a greatly number of injured people at a regional toxic disaster. In: Chiu WT (ed), *International Symposium on Recent Advances in Disaster Prevention.* 2002; Taipei, Taiwan, ROC: *National Institute of Injury Prevention*; 2002:D5–D9.
22. Teich JM, Wagner MM, Mackenzie CF, Shafer KO: The informatics response in disaster, terrorism, and war. *Journal of the American Medical Informatics Association* 2002;9:97–104.
23. Li YC: Constructing a Disaster Medical Resource Information Center and Database. International Symposium on Recent Advances in Disaster Prevention. In: Chiu WT (ed), *International Symposium on Recent Advances in Disaster Prevention.* 2002; Taipei, Taiwan, ROC: National Institute of Injury Prevention 2002;D49–D54.
24. Business Wire: Nextel prepares for Hurricane Isabel. 17 September 2003. ClariNews Website. Available at http://quickstart.clari.net/qs_se/webnews/wed/cm/Bva-nextel.R1gD_DSH.html. Accessed 13 July 2004.
25. Perkins CE, Royer EM: Ad Hoc On-Demand Distance Vector Routing. In: Perkins CE (ed), *Ad hoc Networking.* Addison-Wesley Publishers. 2000.
26. Anonymous: Radio frequency tags. Pacific Northwest National Laboratory Website. Available at http://availabletechnologies.pnl.gov/securityelectronics/rftags.stm. Accessed 02 May 2003.
27. Anonymous: RFID. The Association for Automatic Identification and Data Capture Technologies. Available at www.aimglobal.org. Accessed 02 May 2003.