Report Number: WUCSE-2011-100

2011

A Survey on Communication Networks in Emergency Warning Systems

Yan Li

2011-100

A Survey on Communication Networks in Emergency Warning Systems

Authors: Yan Li

Abstract: N/A

Type of Report: MS Project Report

A Survey on Communication Networks in Emergency Warning Systems

Student: Yan Li Advisor: Raj Jain

Contents

List of Tables

List of Figures

1 Introduction

1.1 Motivation

The emergency warnings to the public are issued once a day at least in the United States [53]. Some of them will warn a dozen of people while many of them still need to warn a population of substantial size in quick response (less than 1 minute response time) to the emergencies such as earthquake, tsunami and so on. When such emergency occurs, the network infrastructure is vulnerable to such emergencies and tend to be destroyed or partially destroyed, which renders the emergency districts disconnected to the outside world. It creates several critical problems. First, it reduces the opportunities of reporting the emergency to the world outside. In an earthquake, we need to propagate the emergency message outside of the earthquake focus so as to allow early warning of the earthquake and then evacuate people surrounding the earthquake focus. Second, we may lose the best time to rescue people in the emergency areas. As stated in [46], the 72-hour after an emergence occurs is called the golden hours. Lives can be saved in great chance in the golden hours. With the help of a emergency communication network, we can expedite the rescue of people in the areas of emergency. Also the recent spate of highly frequent natural disasters also have brought the emergency warning networks under scrutiny [9].

1.2 History

There are varieties of research centers promoting the use of wireless technologies and a universal design in future generations of wireless devices and applications all around the world. In this section, we mainly focus on history of the technologies of the emergency warning systems in the US and Japan.

1.2.1 US

In 1951, the first national emergency alerting and warning system was based on radio communication in the US [22]. Later in 1963, Emergency Broadcast System (EBS) was adopted to replace the older one. With EBS, state and local authorities were permitted to send warnings and alerts through broadcast stations. In 1994, a new system called Emergency Alert System (EAS), which incorporated cable systems, was established to replace EBS. Further, EAS was extended to wireless cable systems in 1997. With the steady rise of cell phone coverage in the U.S, 91% of people [23] have a mobile wireless phone. Therefore

since 2004, the Federal Communications Commission (FCC) has been conducting research activities on using the mobile wireless phones. This led to the creation of the Commercial Mobile Alerting System (CMAS) [32]. In 2006, the Wireless RERC launched a Wireless Emergency Communications [54] project (WEC) with emphasis on "the critical role of ensuring that emergency alerts and information was accessible to people with disabilities, by the most practical and preferable methods utilized". Table 1 summarizes the current state of development and application of monitoring and detection technology in the United States.

Table 1: Status of monitoring and detection technology and application coverage for warning systems. Source: [53]

Hazards	Monitoring technology	Detection technology	Application coverage
Hurricane	Well developed	Well developed	Good
Flash flood	Well developed	Well developed	Partial
Riverine flood	Well developed	Well developed	Good
Tornado	Developed	Difficult	Good
Avalanche	Developed	Difficult	Poor
Earthquake	Developing	Difficult	Poor
Tsunami	Developed	Problems	Good
Landslide	Developed	Problems	Poor
Volcano	Developed	Problems	Poor
Dam failure	Developing	Problems	Poor
Transported hazardous materials	Poor	Difficult	Good
Fixed-site hazardous materials	Developing	Poor/Good	Poor/Good
Nuclear power	Developed	Developed	Complete
Terrorism	Developed	Problems	Good/Poor
Nuclear attacks	Developed	Developed	Good

1.2.2 Japan

In Japan, there have been several studies carrying out on earthquake early warning systems. One example is the UrEDAS (Urgent Earthquake Detection and Alarm System) [57] for trains, which was used by Railway Technical Research Institute in Japan in 1992.

Meanwhile, since Oct. 2007, the Japan Meteorological Agency (JMA) provides the Earthquake Early Warning [56] by several means such as TV and radio to houses and offices.

For land mobile vehicles, Honda used the Internavi weather system [38] to send warnings to their customers' vehicle, with the help of JMA's Earthquake Early Waning.

It was reported recently [7, 68] that residents of Tokyo have about 80 seconds of warning ahead of the real occurrence of an earthquake, thanks to a new early warning system. Also they have minutes of warning before the tsunami generate waves first strike the coast. The Japan earthquake early warning system has more than 1,000 seismographs scattered over the country, which "detect tremors and allow for brief advance warnings not only to vulnerable sectors like railroads and utilities". The warning message can be propagated to the public via television, Internet and text-messages.

1.3 How Disaster Early Warning Works?

We take the earthquake early warning system for example. When an earthquake occurrs, two main types of seismic waves: P-waves, or initial tremors, and S-wave, or main tremors, are generated. P-waves travels 7 km/s and are the first to travel outwards. Following P-waves, S-waves travels 3 km/s and would cause stronger tremors. It is these S-waves that cause most earthquake-induced damage. Whenever the P-waves are detected, the earthquake early warning systems would quickly send message to the public that an earthquake is occurring. Then residents have some time to evacuate before the arrival of S-waves caused by the quake. But in those areas extremely close to the focus of the earthquake, however, the earthquake early warning may not be transmitted before the S-waves hit [56]. The mechanism is illustrated in Figure 1.

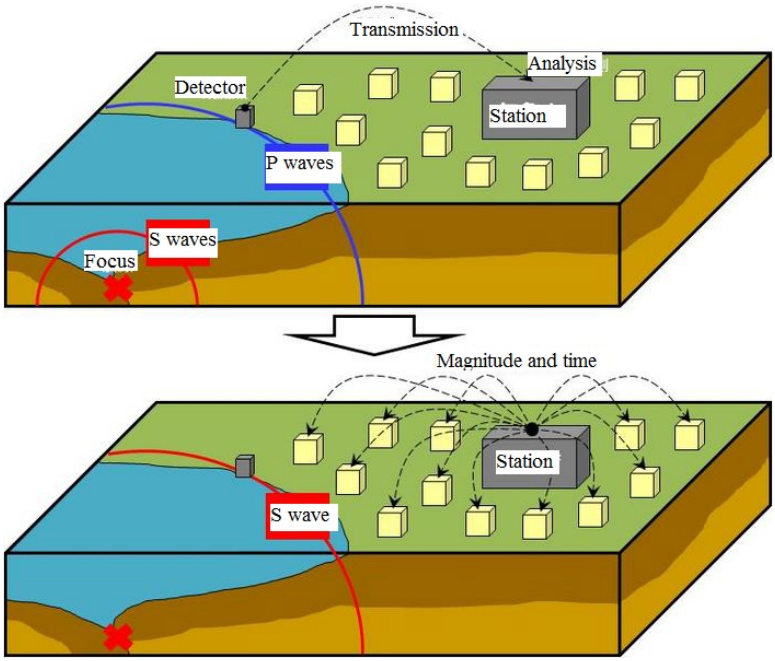

Figure 1: How earthquake early warning works. Source: en.wikipedia.org/wiki/Earthquake_Early_Warning_(Japan)

1.4 Scope

In this survey, we cover several aspects of communication networks in emergencies. Some more independent research areas are classified as follows:

Challenges: there are three major types of challenges in establishing networks for emergency communication.

System architecture design: we will introduce several groups of emergency communication networks.

Protocols: due to the heteronomous nature of the emergency communication networks, specific network protocols have to be proposed.

Security: Fake warning messages can render the whole system useless. To avoid that, security issues are extremely critical in emergency communication networks.

Modeling, Evaluation and Simulation: we need to perform some evaluation and simulation of the network before establishing the real network.

2 Challenges

There are three categories of communication challenges: technological, sociological, and organizational. These three major challenges are all critical for us to develop and maintain an effective emergency communication network.

2.1 Technological Challenges

When a disaster is occurring, the primary technological challenge is to rapidly deploy a warning system for quick response and disaster management. Regardless of whether communication networks are destroyed or partly destroyed (such as power, telephone, mobile base station, and/or other network connectivity infrastructure), the warning system should be able to connect to the network outside the disaster areas. Another technological challenge is the multi-organizational radio inter-operability issue. That is different organizations or technology may use different radio.

If the communication network is destroyed, it needs to be restored quickly. Residents may have a higher chance of survival after a disaster if rescue actions can be taken in "Golden 72 Hours" [47].

Several potential solutions to technological challenges are proposed in [49]. The first one is to employ a dual-use technology. Devices with dual-use technology could work in two operational modes, normal and emergency operational modes. During normal circumstances, the device works on normal mode while during disasters, the device would enter the emergency operational mode, in which the user may have limited access to the network and get specific information from the network.

The second one is to utilize built-in architectural and protocol redundancy. Devices have multiple network capabilities. Failure of one type of network does not disconnect the device from the network. For example, cellular phones have IEEE 802.11 (WLAN) or Bluetooth interfaces that can form a local network even when the mobile base station are destroyed.

Another alternative is to use a hybrid wireless mesh network, such as the CalMesh platform [49]. More such hybrid networks will be introduced in Section 3.

Several specific technological challenges are proposed in [14]. It presents Extreme Networking System (ENS), a hybrid distributed wireless networking architecture and provides large set of performance observations collected from a real distributed hybrid wireless mesh network used for supporting a medical emergency response application. There are at least seven technological challenges described below.

1. Deployment Issues: The network deployment takes time. To deploy a network in an optimized topology is even more difficult and time-consuming. For example, during the experiments in [14], the network deployment took about 30 minutes, which is longer than the requirement of the communication networks in emergencies.

Further, the time to optimize protocol parameters based on the network topology after deploying a wireless mesh network for emergency networks cannot be neglected. Therefore, the paper proposes to use adaptive topology management and topology-oriented protocols to help enhance the achievable capacity and scalability.

2. Application Survivability: The whole network may get split into two partitions if the network infrastructure is greatly damaged. Therefore, applications should consider the possibility of network partitioning.

3. Time Sensitive Traffic Support: The detection of an occurring disaster must be transmitted to the data center for quick response action. This poses very strict requirements on the network protocols (specifically on the network layer and MAC layer).

4. Robust Backhaul Connectivity: All the critical information from the emergency communication networks should be transmitted to the Internet. However, disasters may destroy the vital network infrastructure required to connect to the Internet. So relying on only one type of communication backhaul may be too risky. To increase the robustness, we may adopt multiple types of backhaul in an emergency communication network.

5. Bandwidth Aggregation and Load Balancing: When multiple types of backhauls exist, we need to aggregate the bandwidth from each of them. There are two problems to overcome. One is to minimize the mis-ordering of packets when TCP is used as the transport layer protocol (TCP is

sensitive to packet mis-ordering). The other problem is how to balance the load between different types of backhaul links. Load balancing is firmly related to the performance of the network.

6. Network Survivability: With the use of a popular networking standard such as 802.11, the security issues are more critical than other protocols. Also the wireless mesh network integrating existing devices, protocols, and algorithms may be used. Thus the network compatibility become an important aspect. Furthermore, different networks may interference with each other.

7. Control Overhead: The wireless mesh network may consume a large fraction of bandwidth for control packets. Too high control overhead poses restrictions on the network scalability. So the network protocol should be designed to minimize the control overhead.

Andreas Meissner et al. also brought forward two aspects of technological challenges in [50], data management and resource scheduling. They suggested to use XML as the standard data interchange format on different devices (or different types of devices) at the top layer and to use the predictive allocation and resource re-allocation to improve the efficiency of resource utilization.

2.2 Social Challenges

Since the emergency communication networks serve to save lives and property, it may intervene residents' daily life or affect public behavior. Actually, there are debates on the ethical issues on adopting such systems. In early 1970s, an effective alert device, DIDS (Disaster Information Dissemination System) was not widely adopted since it could cause a breach of privacy [53]. Another issue is whether emergency warning should guide the public. Sometimes residents might refused to evacuate. To the opposite, the local government may order public evacuation although the legal authority may be lacking.

Also the "to warn or not to warn" dilemma is always surrounding us. The warnings are sometimes withheld to avoid negative social and economic effects. The reason is that it is a widespread belief, though unfounded, that the public becomes unnecessarily informed if the disaster would occur with low probability but severe-consequence. This results in the reluctance to announce the warning to the public until it is definitely necessary. This kind of dilemma will persist for short-term emergency warnings because most disasters cannot be predicted with 100% accuracy or even high accuracy.

To be aware of this, it is mentioned in [53], that emergency communication networks design should

"incorporate an understanding of human activity and communication behavior model". Also it points out that, to communication between organizations and citizens demands a common language. In other words, the emergency communication networks should be affordable, available, and applicable to ensure that they will be used during disasters. More detailed issues are introduced in [25], such as, the resistance to adopt new technology, interoperability, and so on.

2.3 Organizational Challenges

Organizational challenges arise from several reasons. One problem is the conflicts among organizations in terms of responsibilities. For example, the probability of recognizing a future disaster is determined by to what degree the indicator of the potential threat can be detected. So different organizations may detect different phenomenon. It is quite possible that the observation of a cloud may just suggest rain at one city, but a tornado threat to another city. Then the organization succeeding to detect the cloud formation may be able to predict the tornado while another organization failing to detect the cloud formation may be unable to predict a tornado.

Another problem is in disaster response, we need to make decision based on a flatter, dynamic, ad-hoc organization. As we use collaborative technologies such as mobile applications, Web-based email, and communications networks such as wireless mesh networks, there may be too many resources and too much information that restricts our ability to manage emergency and affects the capacity of emergency communication systems.

Groove is a peer-to-peer collaboration technology that enables groups across organizations to monitor communication and data flow across locations in a time-pressured situation. An observational study of Groove was conducted in [31] using various civil and military groups at the heart of the disaster zone over the course of ten days. The study summarized observations of social and communication challenges in crisis situations that impact technology adoption and concluded that we need to innovate technologies to support new types of organizations.

In this survey, we mainly focus on the technological challenges and many alternative solutions will be introduced in the next section.

3 System Architectures

Characteristic Many technologies are introduced in communication networks. Based on the mainly adopted technology, we classify the communication networks for emergency warning systems into four groups labeled as WiFi, P2P, Cellular Network, and Satellite. Most of emergency communication networks make use of wireless devices. Also emergency communication networks are often heterogeneous, consisting of different types of devices such as laptops, cell phones, PDAs and so on, which use different protocols such as WiFi, Bluetooth, GSM and so on.

Also the emergency warning systems have some uniform communication pattern listed below.

1. Real-time requirement: The warning message should be transmitted to residents in real-time (i.e. in tens of seconds or seconds).

2. Redundance: To guarantee assured communication, multiple lines such as text-message, radio, and Internet, may be used simultaneously to transmit the same warning message.

3. Large coverage of population: A warning message may be transmitted to millions of residents (i.e. an earthquake warning).

Though we classify the emergency communication networks into several groups in the following, the classification of groups is not orthogonal to each other. There may be no obvious border between different groups. The only focus is that each group of emergency communication networks puts emphasis on different technologies. Sometimes we tend to integrate them to establish a more reliable emergency communication network. More detailed examples are described as we examine each type of network architectures.

3.1 WiFi

This group of emergency communication neworks uses wireless transmission techniques such as Wi-Fi and WiMAX. Tarchi et al. [66] presented such an efficient emergency management system that integrates the mobile grid paradigm in the communication infrastructure. As shown in Figure 2, a combination of different communication infrastructure is used to transport and share information among operators. Specifically, they suggested using wireless sensor network systems for monitoring in local areas. Also they proposed to use broadband wireless networks such as WiMAX based networks as the secure and

reliable communications network, which allows reliable communications with suitable QoS for different traffic types in varying propagation conditions and independently of the disaster environments.

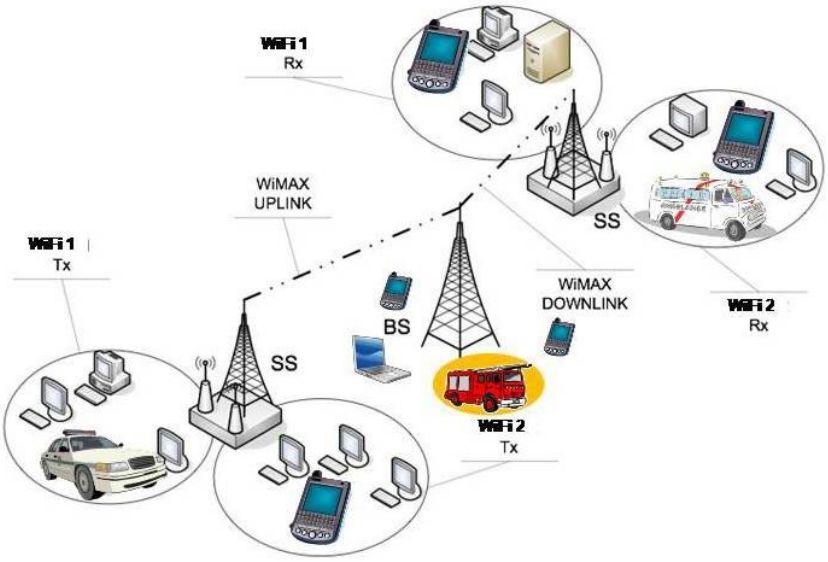

Figure 2: A heterogeneous WiFi-WiMAX network. Source: [66]

Bai et al. [11] proposed an integrated communication system composed of heterogeneous wireless networks, as illustrated in Figure 3. Wireless sensor network (WSN) and mobile ad-hoc network (MANET) are deployed on the disaster site for local communication and information collection. Then, to communicate with the remote disaster-safe areas, satellite gateway is used for the local networks to interconnect with the satellite mobile network. Furthermore, cellular gateways are used as alternative remote communication means when local networks reaches a working cellular base station.

To employ the existing wireless network infrastructure, it was proposed, in [66], to combine multiple LANs with different transmission characteristics and selectively switch to the best suitable link to maintain connectivity with a high transmission rate. with user policy as those networks as the networks are changing. The LANs are powered with a combination of solar panel, wind turbine and battery. In the actual disaster cases, when the electric power line is damaged, these wireless LANs can still work.

Fujiwara and Sharma et al. [33, 62] proposed a hybrid wireless network scheme enhanced with ad hoc networking for disaster damage assessment and emergency communications. The network aims to maintain the connection between a base station (BS) and nodes by way of multi-hopping. A routing protocol proposed in this paper is capable of building a route using unicast-based route discovery process without route request flooding. A proposed MAC protocol satisfies the requirement of maintaining accessibility and a short delay even in emergency circumstances.

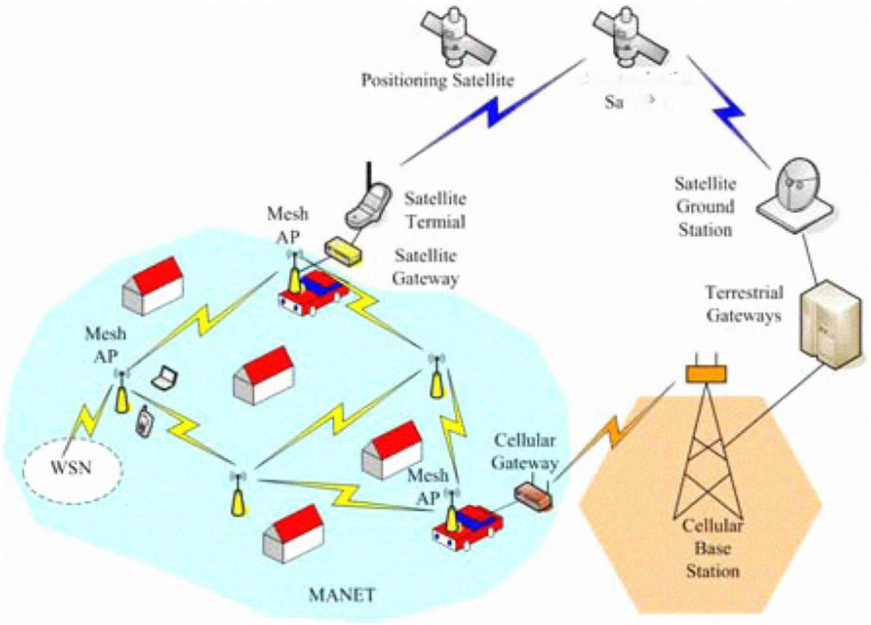

Figure 3: Illustrative diagram of integrated emergency communication system. Source: [11]

There are several deployed WiFi-based systems such as DUMBO [43], DUMBO II [42], and MIKoBOS [51]. DUMBO allows streaming video, VoIP and short messages to be simultaneously transmitted from a number of mobile laptops or PDA's to/from the central command center, or to the other recovery workers within the same or different disaster sites. DUMBO II deployed an emergency wireless network for post-disaster rescue operation with an emphasis on connecting the emergency wireless networks the fixed infrastructure. It used an Internet connected MANET. MIKoBOS is another mobile information and communication system for emergency response.

To strengthen the reliability of emergency communication networks, different technology can be integrated into WiFi-based network. Dilmaghani and Rao [25] proposed to use a Hybrid Wireless Mesh Network (HWMN) for highly reliable communication infrastructure. The network is capable of working in a heterogeneous environment with different available backhaul technologies for Internet connectivity. They also suggested that cellular networks can be integrated if the service is available in an emergency situation.

3.2 P2P

P2P-based emergency communication networks use P2P technology to quickly deploy a serverless network even there is no preexisting networking infrastructure. The nodes in P2P networks can be laptops,

cell phones, PDAs and so on. There are several papers proposing P2P-based emergency networks [47]. Dilmaghani et al. [47] analyzed the causes that paralyzed the entire communication systems in Jiji Earthquake and proposed a P2Pnet that uses notebook PCs to construct a MANET based emergency communication and information system. The architecture of the P2Pnet is illustrated in Figure 4. It is a peer-to-peer communication network based on MANET to support temporary information communication network in the group.

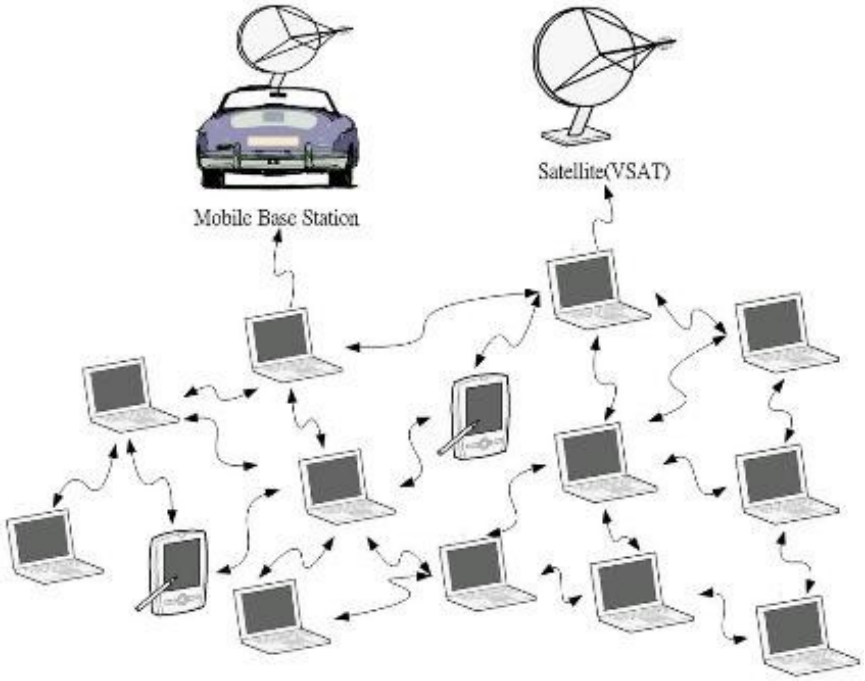

Figure 4: Architecture of P2Pnet. Source: [47]

Some nodes capable of accessing the satellite communication network can act as gateways so that all other nodes can be connected to Internet through the gateway, which is illustrated in Figure 4.

On top of MANET, there is a layer of peer-to-peer communication service to support higher level services. Three basic communication modes are supported as followings:

U1net: U1net stands for "Uncontrolled Single-Hop Group Communication Network". Each node can broadcast data to neighboring nodes in one-hop distance. No authorization is enforced.

UKnet: In Uncontrolled K-Hop Group Communication Network (UKnet), each node can broadcast data to neighboring nodes in a K-hop distance. No authorization is enforced. U1net and UKnet can be used at the early hours of the emergency, when the network is not in place yet.

CKnet: Controlled K-Hop Group Communication Network (CKnet) is more advanced in that the nodes are more organized and even unique IP address can be assigned to each node.

3.3 Cellular Network

Cellular emergency communication networks leverage the existing cellular infrastructure. The basic idea of cellular emergency communication networks is that cell phones are able to work in dual mode: normal mode and emergency mode. In normal circumstance, cell phones can connect to the base station so that traffic is transmitted by the base station while in emergencies, once cell phones lose the connection to the base station, it enters emergency mode and work as a mobile ad-hoc network. Several architectures are proposed in [69, 70]

They proposed a novel communication system for evacuation operation and three scenarios to efficiently reach out to evacuees in the case of emergencies by utilizing existing cellular communication infrastructure augmented with ad-hoc networking among mobile stations as a tool to reach out to evacuees.

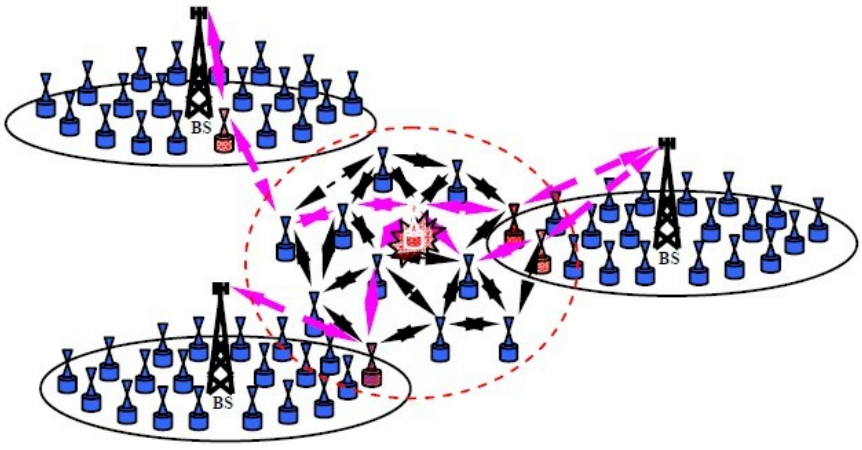

Figure 5: Hybrid communication system. Source: [70]

As depicted in Figure 5 and 6, when network infrastructure has been destroyed, these mobile stations work in the ad-hoc mode. Some mobile stations work as the cluster head to reach the external network. If cluster heads cannot reach the external network directly, they may employ satellite communication to attain connectivity with external network. Sensor devices scattered in the geographic area under consideration. A similar mechanism is described in [40].

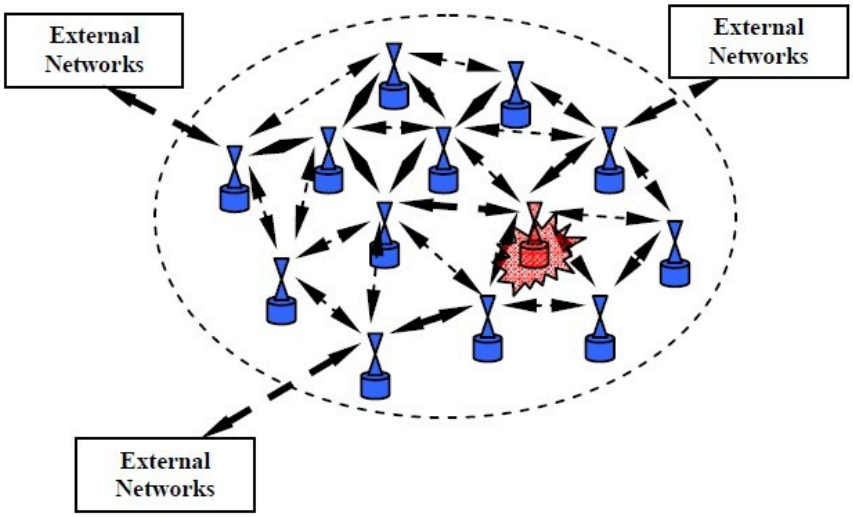

Figure 6: Infrastructure-less communication system. Source: [70]

3.4 Satellite

The satellite communication networks are better suited in the wide area, broadcasting, anti-disaster applications for the nationwide disaster emergency communication networks build-up than the other communication networks [21].

In Japan, the satellites used for the disaster communications include the ETS-VIII (Engineering Test Satellite VIII), WINDS satellite, the Superbird-D satellite, etc. In Europe, the European Space Agency (ESA) is the cental organization that performs various disaster emergency satellite communications network projects. One such project is the REMFILESAT project [21].

In the literature, Dervin et al. [24] presented a satellite-based communication system dedicated to disaster recovery. The proposed solution relies on the underlay transmission of low power emergency signals in the frequency band of a primary transparent satellite telecommunication system. Then, an end-to-end system study was carried out that concluded that the use of several satellite transponders could allow a rapid and simple deployment of a wide range of emergency services - from data broadcasting to voice communications - over a widespread stricken area.

In other types of emergency communication networks, satellites can also perform as the gateway to gain access to Internet. If the communication infrastructure is greatly damaged, it is necessary to consider satellites as a part of the network. One such example is depicted in [37]. It proposed an interesting mobile ad-hoc satellite wireless mesh networking approach designed for an emergency scenario, in which,

one of the most important requirement, namely, the full mobility of rescue teams at the disaster site is assured by combining ad-hoc mobility together with IPv6 mobility mechanisms.

To summarize, we compare each group of emergency communication networks in Table 2, in terms of application coverage, survivability in emergencies, self-organizing abilities when the network infrastructure is partially damaged, the deployment cost, the ability to monitor emergencies, and whether there is preexisting infrastructure in reality.

Table 2: A comparison between different group of emergency communication network technologies

	Coverage	**Self-organizing**	**Survivability**	**Cost**	**Monitor emergency**	**Existed**
WiFi	Wide	Good	Low	Low	Good	Yes
P2P	Not wide	Good	Low	Low	Good	Yes
Cellular Network	Wide	Good	High	Low	Good	Yes
Satellite	Wide	Good	Extremely High	Extremely expensive	Not Good	No

3.5 Actual Deployed Systems

In this section, we will explore two existing warning systems, the Japanese Earthquake Early Warning System and St. Louis Tornado Warning System.

3.5.1 Japanese Earthquake Early Warning System

Since October 2007, the Japan Meteorological Agency (JMA) starts the new Earthquake Early Warning [3], a new service that advises of strong earthquake tremors before they arrive. The new system works as follows:

1. Monitoring: Seismometers detect the first shockwave.

2. Analysis: Computers analyze the wave and estimate how powerful the tremors will be.

3. Warning: If that wave is estimated to be more powerful than a certain threshold ("lower 5" on the local scale), an alert is issued.

Monitoring To monitor and collect seismic waveform data in real-time, Japan has the world's most advanced earthquake early-warning system, with more than 1,000 seismographs scattered over the country

[7].

Figure 7 shows a seismic station operated by JMA. The box on the right is the communication facilities located in shelter. Inside the box includes a seismometer and seismic intensity meter.

Figure 7: JMA Seismic Station. Source: [3]

To have a overview of the monitoring network, Figure 8 illustrates the distribution of the seismometers network in Japan. Besides the network operated by JMA, JMA also collects and analyzes seismic data from universities and disaster management research institutes such as the National Research Institute for Earth Science and Disaster Prevention (NIED), as shown in the figure, in order to conduct a comprehensive assessment on seismic activities for promotion of research activities in cooperation with the Ministry of Education, Culture, Sports, Science and Technology (MEXT). The products of this analysis are shared with relevant organizations.

Analysis JMA has developed a computer system for data collection and processing. This comprehensive system is composed of one central system and five local systems. The central one, which is called EPOS (Earthquake Phenomena Observation System) and installed at the JMA headquarters, is responsible for issuing tsunami warning for the central part of Japan, nationwide earthquake information and information about Tokai Earthquake. The other local systems, which are called ETOS (Earthquake and Tsunami Observation System) and installed at the District Observatories in Sapporo, Sendai, Osaka, Fukuoka and Okinawa, are responsible for issuing tsunami warning and earthquake information for each district.

The system automatically calculates the focus and magnitude of the earthquake and estimates the

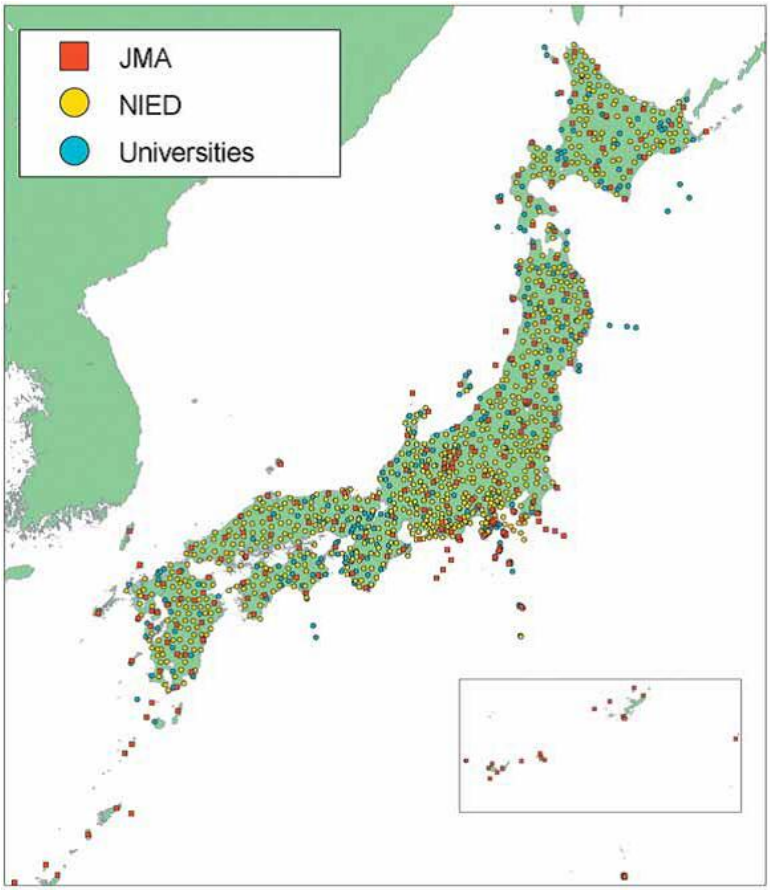

Figure 8: Seismometers Network in Japan. Source: [3]

seismic intensity for each location by detecting the quake near its focus. If the magnitude is above some threshold, an alerting will be issued.

To transmit the information, a scheme is designed by JMA to guarantee assured communication, as shown in Figure 9. JMA transmits various warning and information to disaster management authorities, local governments and mass media online over the computer network across the country. Also JMA applies a scheme to avoid congestion of the communication lines and uses the MT-SAT communication function as a back-up line, so that JMA can collect data and disseminate warning and information even in the middle of major disaster.

Warning As shown in Figure 9, JMA will send warning to the disaster management authorities, local governments, telephone companies, mass media and so on, with the satellite MT-SAT to strengthen the reliability of communication. Then residents can obtain emergency information via text messages, TV, Internet (i.e. the JMA website) or even radio.

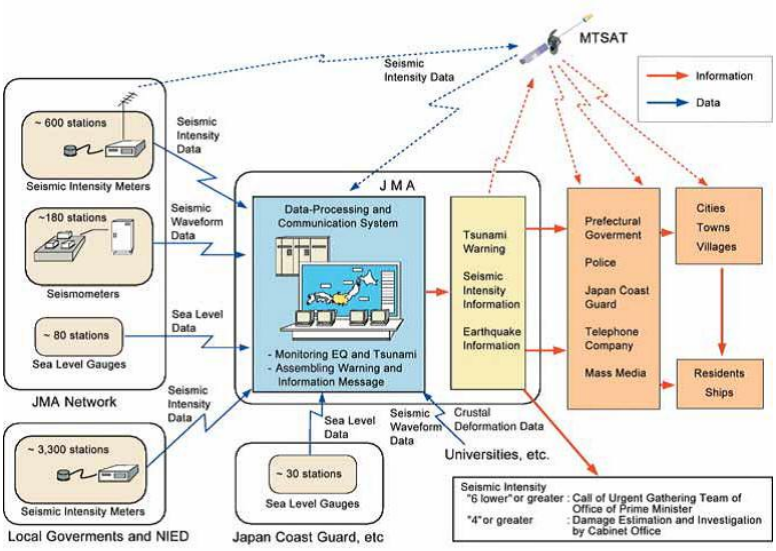

Figure 9: Data Collection and Dissemination of Information. Source: [3]

Specifically, we examine how the cellular networks in Japan provide emergency warning messages.

Any cell phone serviced by NTT Docomo, Japan's dominant cell phone carrier, can opt to have alerts about earthquakes pushed directly to their phones. The technology that makes this possible, the Area Mail Disaster Information Service (AMDIS), is designed to deliver detailed alerts as quickly as possible. AMDIS is designed by JMA and subscription of the AMDIS incurs no monthly charge or communications charges.

The service utilizes the technology known as Cell Broadcast, or SMS-CB. It is totally unlike traditional, point-to-point SMS, in that it can be broadcast directly from cell towers to every phone in range and does not use more bandwidth when sent to more users. This is extremely important in the event of a disaster because cell broadcast has the potential to reach millions of users in seconds in a targeted area. Full details can be accessed at [1].

To minimize damage, emergency information is also sent to companies, such as utilities, petrochemical plants, rail and bus operators, and others so that they can shut down facilities.

3.5.2 Saint Louis Tornado Warning System

Since fall in 2011, a $7.5 million project to revamp the outdoor tornado warning system in St. Louis County is in operation to replace the old one [6]. The old system in St. Louis was installed prior to the heavy subdivision build-up of South and West County, so thousands of residents in those areas had

no siren umbrella. With the new system, which includes 185 new multi-speaker sirens, as shown in Figure 10, is expected to reach 99.6 percent of county residents as compared to only about 88 percent of people in the county for the old system. The map of all the 185 sirens can be identified online at the official website of St. Louis County Government.

Figure 10: St. Louis County Outdoor Warning Siren. Source: [6]

The distribution of all the 185 sirens are shown in Figure 11.

Besides sirens, the radio is also adopted to broadcast weather information. National Oceanic and Atmospheric Administration (NOAA, a federal agency focused on the condition of the oceans and the atmosphere) Weather Radio in the St. Louis Metro area is broadcasting on a frequency of 162.55 MHz, which broadcasts continuous weather information 24 hours per day.

4 Protocols

Emergency warning networks are mostly made up of ad-hoc networks. The network devices contains cell phone, laptop, PDA, and so on. Each of the devices works with some specific (and usually different) protocol(s). The heterogeneous networks naturally requires a novel protocol that could integrate all the devices and protocols. We need to interconnect the hybrid network, i.e. an environment where wired and multi-hop wireless technologies are used, without raising problems or inconsistencies in the network. The basic idea of such networks is that a sublayer between layer 2 and layer 3 is introduced. One of the representative applications is proposed in [29]. As depicted in Figure 12, Ana4 creates a sublayer, called ad-hoc virtual interface between layer 2 and layer 3. The sublayer can be designed to unify hybrid

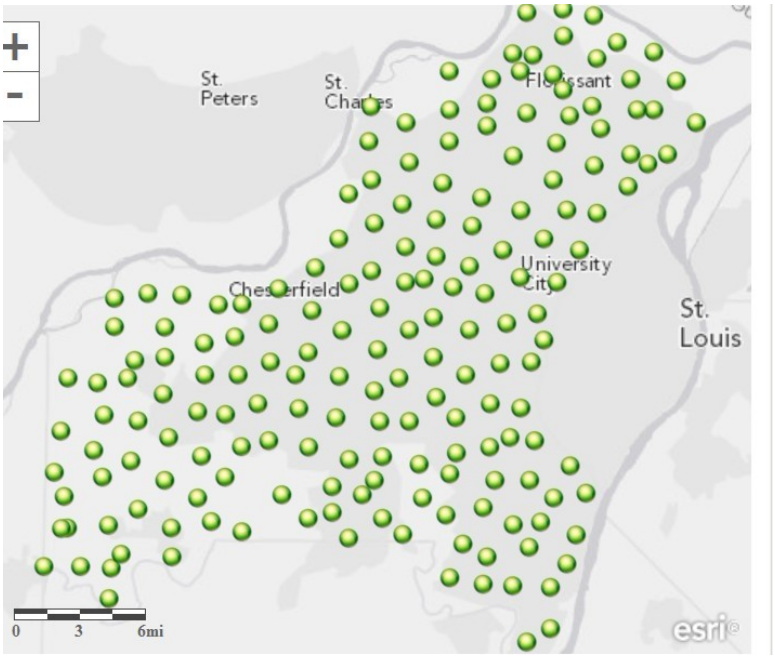

Figure 11: St. Louis County Tornado Sirens Distribution. Source: [6]

networks by defining a uniform address and packet format. In this way, this architecture is particularly useful since it does not require any modifications neither in device (layer 1) nor in the TCP/IP stack (layer 3 and 4). In this section, some examples are described first and especially, we then examine how to improve the current cellular networks to adapt to the emergency situations.

4.1 Heterogeneous Networks

The Distributed Virtual Network Interfaces (DVNI) [28] was proposed in the context of Personal Area Networks (PANs), which could provide heterogeneous devices and nodes the ability of discovering, seamless handover and routing capabilities. By employing a Virtual Network Interface (VNI) to address the issue of changing IPs due to mobility, DVNI is able to provide the "Always Best Connected (ABC)" solution.

Ana4 Framework [29] is another relevant work proposed by N. Boulicault et al. The goal of Ana4 Framework is to allow communication between devices of a hybrid and heterogeneous network environment, such as for Intranet connectivity scenarios. It provides end-to-end communication independent of the number of network interfaces in each node and supportes TCP/IP applications to keep interoperable inter-networking over a heterogeneous networking infrastructure.

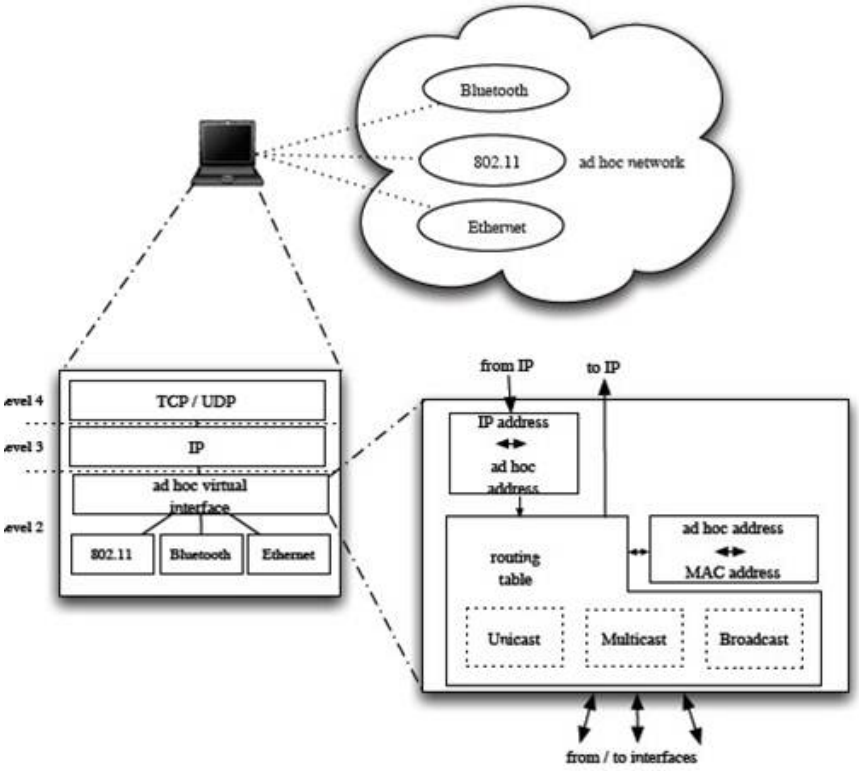

Figure 12: Ad-hoc architecture of Ana4. Source: [29]

Lilith [30] is also a similar architecture. In Lilith, an interconnection architecture for spontaneous edge networks is proposed. The authors referred to the hybrid and heterogeneous networks formed on the edge, such as home networks. Lilith is based on MPLS to provide a connection-oriented solution for spontaneous networking scenarios, which is similar to Ana4's layer 2.5 underlay approach.

The 3D underlay routing protocol [39] aggregates and exchanges device context information. It splits the whole protocol into three major phase, the bootstrapping phase, the route construction phase, and the policy management phase. In the bootstrapping phase, it can handle different technologies. After the heterogeneous network is formed, seamless inter-operability take place independently of bootstrap technological differences with context awareness of each node. Even context awareness may provide each node the geographical information of nearby nodes.

Sharma and Fujiwara et al. [33, 62] proposed a hybrid wireless network scheme augmented with ad-hoc networking for emergency communications. The network aims to maintain the connection between a base station (BS) and nodes by way of multi-hopping. The routing protocol proposed is capable of building a route using unicast-based route discovery process without route request flooding. A MAC protocol is also proposed to satisfy the requirement of maintaining accessibility and a short delay even

in emergency circumstances.

4.2 Cellular networks

Potential: The advantage of cellular networks for emergencies is to leverage the existing cellular infrastructure. From [72], we can sense the tremendous potential of such network. Petros Z. [72] presented a preliminary analysis of short message service based on traces collected from a nationwide cellular carrier. It analyzes the traces and characterize them in different granularity, namely, message-level, "storing-and-forwarding", and thread-level. Specifically, the report examined the message size distribution and message arrivals, and how messages are "stored-and-forwarded" at the conversation thread level.

An interesting result is that approximately 73.2% of the short messages reach their recipients within 10 seconds, as shown in Figure 13.

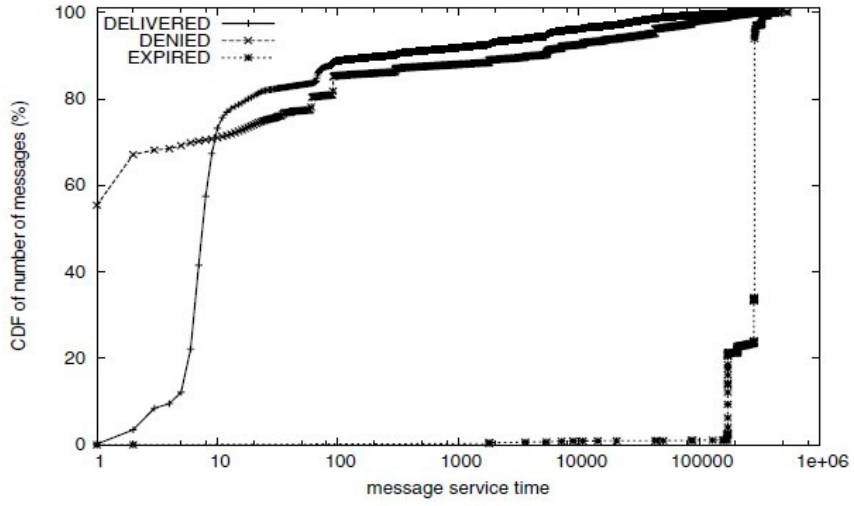

Figure 13: Cumulative distribution function of message service time. Source: [72]

This measurement report can serve as a benchmark for protocol design, performance evaluation, planning and provisioning of short message service or other messaging systems. From the report, we see the tremendous potential to leverage the quick response of cellular networks. Also we could further develop new protocols to improve the performance of cellular networks. First, the emergency traffic can be distinguished from public traffic. Then, separate queue can be set to store emergency calls and public calls, and finally scheduled the calls from the two queues according to different scheduling schemes so as to provide priority to emergency calls. An alternative is that emergency service can preempt public service without queuing calls. A combination of the above two approaches can also be adopted as a

tradeoff.

Protocols: One example of the protocols using separate queue is proposed in [74] where both emergency traffic and public handoff traffic are put into queues, and scheduled according to a weighted earliest deadline scheme. It provided the flexibility of adjusting the priority between National Security/Emergency Preparedness traffic and public handoff traffic. The authors present some low complexity methods to compute the loss probability and the average waiting time of calls. Yet in that work the public originating traffic was not well protected when the emergency traffic was high. It was possible that the public traffic is delayed for a too long time.

While Beard [12] studied different preemptive schemes for supporting emergency traffic. The effects on low priority traffic and the whole system utilization were shown. But it was assumed that all preempted sessions will be dropped, which can cause high termination probability for low priority traffic and thus high dissatisfaction from the customers.

In [76], it improved the preemptive scheme by introducing a threshold-based preemption strategy for supporting emergency traffic in cellular networks. As shown in Figure 14, if the number of active emergency sessions is more than the preemption threshold, the scheme guarantees a certain amount of resources to public customers. But if the number of active emergency sessions is less than the preemption threshold, a random public session will be preempted by the emergency session. In this way, the scheme could provide immediate access for emergency users and flexibility for providers to adapt to different requirements and operating scenarios. In addition, under the combined preemption and queuing framework, interesting analytical relationships among channel occupancy, gross service time and success probability for public traffic are revealed. Based on this, guidelines for further improving satisfaction of public customers can be provided.

Specifically, when an incoming emergency session fails to find free capacity, and if the number of active emergency sessions is less than the preemption threshold, it will preempt resources from a randomly picked ongoing public session. There is no buffer for emergency users and thus it incurs no access delay. A binary search method is used to tune the preemption threshold.

The applications of combined preemption and queueing schemes in wireless networks can be seen in Wang, Zeng and Agrawal [13], and Tang and Li [65]. In these works, real-time (voice) traffic can preempt resources from non-real-time (data) traffic. Each type of traffic consists of both originating and handoff traffic. However, the behavior for expiration (reneging due to impatience, or thrown away by

the system after a certain time [18, 35, 74]) of preempted sessions in the queues was not studied, and to ignore such behavior is unrealistic even for non-real-time data sessions.

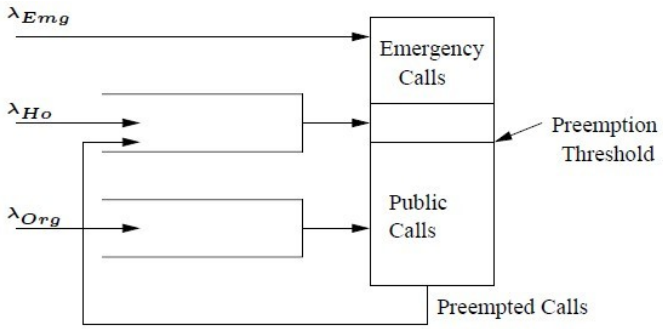

Figure 14: Combined preemption and queuing scheme. Source: [76]

Zhou and Beard [73] further introduced a "single preemption" policy on the basis of the combined preemption and queueing scheme. This strategy helped protect public traffic from preemptions and is a big improvement over the pure preemption policy that employ no queues, but the protection is not strong enough when emergency traffic is unexpectedly high.

In [73] and [75], preemption was considered and a combined preemption and queueing method was provided to lessen the "harshness" of preemption policies so they could be adopted and tuned to practical operation in real environments.

Cho and Un [20] propose a combined preemptive/nonpreemptive priority discipline. When a discretion rule is satisfied, preemptive priority is applied. Otherwise, non-preemptive priority is used. The discretion rule is based on the parameters of low priority traffic, the elapsed service time, the remaining service time, or the ratio of elapsed to total service time. In [26], the discretion rule is based on the number of preemptions experienced by the low priority tasks. After being preempted for a certain number of times, the task can be promoted to a higher priority class, or forbidden to be preempted. Both works mentioned above set the discretion rule based on the behavior of each session or task. Another possible approach is based on the behavior of the whole class. Kim and Un [45] considered the resource utilization taken by the high priority class for deciding preemption to be allowed or not.

Each of the three types of approaches has its advantages and a comparison is shown in Table 3.

Table 3: A comparison of different improvement on cellular network protocols

	Delay	Utilization	Fairness
Queue-based	May be high for public service	High	Medium
Preemption	High for public service	May be low	Low
Combination	Medium	Medium	Good

5 Security

Security is an important issue in the networks. Networks for emergency communication put even more emphasis on security issues in that emergency communication networks should guide people's behaviors in emergencies. Threats of security can cause tremendous negative social and economic effects to the society.

To guarantee security, approaches of reputation (or trust) computation and analysis have been studied to establish and quantify the trust of an entity in different types of networks [8, 27, 44, 59]. Also there are a lot of work on trust dynamics, such as trust prediction [15, 63], propagation [19, 60], and aggregation [10, 19]. Most of the existing techniques are based on reputation (or trust) score and try to detect or predict any malicious or selfish behaviors and then publish or revoke them so as to enhance the overall security of the network. We examine in details several reputation score-based techniques.

5.1 Security issues analysis

Before introducing the reputation score-based techniques, we examine seven generic security properties and issues in emergency warning systems [17].

1. Authentication: Authentication relates to the ability of a host or system to correctly identify another host or system.

2. Data confidentiality and secrecy: Data confidentiality and secrecy aims to hide of the content of a message to unauthorized users. It can be implemented with asymmetric or symmetric cryptography.

3. Data and origin authentication: Data and origin authentication is the capability of a system to identify the sender of a message correctly.

4. Authorization and access control and accountability: Authorization is related to the granting of access rights to the resources of the system (or the network) to only specific users. It is usually performed after the authentication procedure, and is related to the accountability property.

5. Data integrity: Data integrity is the capability of a user to verify if a message sent over a network, or data stored in a memory, has been modified since its creation. Data integrity can be achieved by using secure hash functions [16].

6. Non repudiation: Non repudiation is related to the capability of a system to prevent a user from denying the sending (or the reception) of a given message.

7. Availability: This is the ability of a system to be prompt and usable when the user needs it. This property is particularly important in emergency communication networks.

More specifically, Adam and Casoni et al. [8, 17] present a careful analysis of the security issues and properties for an emergency network, to find those that most affect the design of the whole crisis response network. Authentication, confidentiality and availability affect significantly from topological constraints imposed by some of the authentication method described before, to the difficulties related to the implementation of cryptography together with QoS mechanisms.

5.2 Reputation score

To satisfy all the security properties, the reputation score based mechanism is proposed, in which each node in the network is assigned some score (defined as a perception regarding its behavior norms). After score assignment, the reputation score will evolve depending on its behavior. As reputation score evolves, the uncooperative or malicious nodes will get a score below some threshold. Then the neighbors of the node could cut off the connection to them until the nodes cooperate.

As described in [48], this reputation system has at least three desired advantages listed below.

1. Valid: The system is effectively able to distinguish honest nodes from uncooperative or malicious nodes

2. Distributed: The reputation system is completely distributed. No centered database is demanded to manage the reputation score.

3. Timely: The reputation score is dynamic and could reflect the trustworthiness of each node in a up-to-date way.

There are several representative mechanisms in the literature. For example, Karakostas and Markou [44] proposed a reputation score based protocol in multi-hop wireless networks. They model the protocol as a game. As the game evolves, the author tried to find the necessary and sufficient conditions for the existence of non-trivial Nash equilibria, in which each node defines a threshold of tolerance for any of its neighbors, and then cuts off the connection to any of these neighbors that does not wish to forward an amount of flow above that threshold. When a node relays a packet on behalf of a neighbor, it does so with the same probability with which this neighbor forwards its own packets. Similar mechanisms can be found in [52, 64]. In this way, the reputation mechanism will identify uncooperative behavior first, and then punish uncooperative nodes by cutting off its connection to its neighbors.

Also in [27], Durresi et al. make use of asymmetric key cryptography to securely distribute information of a node using the infrastructure of the cellular network during the ad-hoc mode. When cellular network become dysfunctional, cell phones enter ad-hoc mode and form an ad-hoc network. The mechanism can be decomposed into the following steps:

1. Each node has a private key corresponding to its ID in the ad hoc mode and thus messages with the signature of the public key can be verified using the ID.

2. Each node is given its reputation score in the form of a certificate which has the its ID and score and then broadcasts messages within the network.

3. With the asymmetric key cryptography, whenever the receiver of a broadcast message believes that the sender of the message is malicious, the receiver sends a negative recommendation to all the nodes within the same group.

4. Nodes are revoked if its reputation score is below some threshold.

As describe above, security issues play a critical role in the emergency communication networks. To guarantee security, some general properties should be considered. To satisfy the requirements of security It has been well-established in the literature to use the reputation score mechanism to guarantee security in the networks.

6 Modeling, Evaluation and Simulation

It is often costly to build up emergency communication systems and its quality is directly related to the survival rates or to what degree it can save lives or properties. So before deploying such a system, it is strongly recommended to verify the effectiveness of the system quantitatively, by evaluating how much the system contributes to decrease "preventable deaths" [58] when the emergency occurs. A testbed environment is needed that helps to evaluate such emergency response systems. As most of these emergency communication systems make use of wireless devices, wireless network simulators are preferable in these scenarios. However, in fact, most existing simulators do not focus on emergency situations even though a lot of works have been conducted to discuss the the significance of mobility models in network simulations and some realistic mobility models have been developed [5, 34, 36, 41, 55, 71].

Wu et al. [67] presented an interesting model, in which the emergency network is regarded as a deterministic network in which the capacity of each arc isinvariable. With certain saturated models, they could analyze the system reliability.

Specifically, the saturated model defines a emergency network as a directed network, $G = (s, t, v, e, f, c)$, where $s, t \in V$ is the source and the sink separately, the directed network (V, E) where V is a set of nodes and E is a set of arcs, and f, c is a set of flow and capacity of each arc. Based on the network reliability theory, the system reliability is defined as the sum of probabilities of all flow distributions that satisfy some threshold demand.

Besides modeling, some testbeds for evaluation and simulation of emergency networks have been described in the literature. For example, in [25], Dilmghani and Rao deployed a communication testbed for disaster scenarios. The testbed was a hybrid wireless mesh network made up of Calit2's inter-operable CalMesh [2] nodes at a full-scale crisis response drill organized by the San Diego Metropolitan Medical Strike Team (MMST). During crisis, the hybrid wireless mesh network is capable of restoring a communication infrastructure when the existing communication infrastructure is damaged or unavailable. With

the testbed, network statistical data can be collected from the medical first responders' communication over the network deployed. [25]

Keisuke et al. [58] also propose a testbed environment to support evaluation and simulation on network-aided emergency communication systems, Basically, they make use of original language to describe all the behaviors and incorporates essentially geographical model and node behavior model. This original language describes all disaster response behaviors and actions depending on the locations, surroundings and information received from emergency support systems via wireless networks. The geographical model used is extended from [4]. The notion of regions is introduced, called areas, as shown in Figure 15. Areas are in rectanglular shape and can be defined as a tuple of six terms (identifier, set of initial points, generation time, scale function, area attribute, behavior restrictions). The node behavior model is also a simple extension from [4].

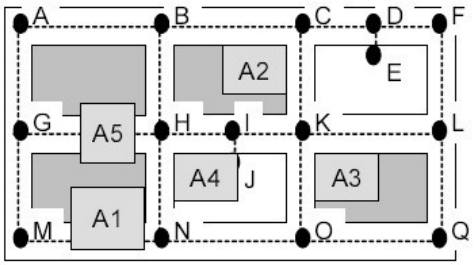

Figure 15: Example of areas. Source: [47]

Also a function is defined to evaluate a real system running on mobile terminals by a real-time network emulation function of MobiREAL simulator [4]. With this model, they can conduct simulation experiments on the testbed to verify the capability of the proposed systems.

A state of the art survey on modeling and simulation tools on emergency response systems is presented in [61]. It indicates a large number of efforts have been focused on plume simulation for radiological device, building fire simulations, and storm simulation. But each of these tools only focuses on a specific aspect of the problem, such as, the modeling of dispersion of an agent in the environment using plume simulation.

Therefore, Sanjay and McLean [61] propose a framework, called Integrated Emergency Response Framework (iERF), to integrate modeling, simulation, and visualization tools for emergency response.

iERF consists of three major concepts: disaster event, entities of interest, and applications. Nine types of disaster events, identified by the report by the National Research Council (2002) are focused

on. Entities of interest are targets impacted by the disaster events. These should include resident and the disaster response workers. For example, the fire fighter may get injured during fire fighting. The capacities of different modeling and simulation tools are based on the applications designed. There are a number of applications such as planning, vulnerability analysis, identification & detection, training, and real-time response support.

To summarize, before deploying a real emergency communication network, we need to conduct performance evaluation and network simulation to ensure its feasibility. Even models can be built up to verify that the proposed networks should work in emergencies. There have been some simulators and testbeds proposed in the literature we can choose from.

7 Summary

In this survey, we extensively explore the communication networks in emergency warning systems in several aspects. First, several challenges are identified to deploy the emergency communication networks, namely, technological, social, and organizational challenges. Then we focus on the technological challenges and examine four groups of networks, which are classified according to the employed technology. With a comparison between different types of networks, the cellular networks have tremendous potentials in terms of the preexisting infrastructure and its quick response to the emergencies. To adapt to the emergency circumstances, protocols modifications on the basis of existing protocols are proposed, to avoid violating the existing protocols too much. Two mainstream approaches are examined in details. For heterogeneous networks, a sublayer between layer 2 and layer 3 is introduced while for cellular networks, mechanisms are proposed to provide priority to emergency traffic. Another crucial problem in emergency communication networks is the security. We concentrate on reputation-based mechanisms that have been fully studied in the literature. Finally, the modeling, evaluation and simulation issues of emergency communication networks are covered.

References

[1] Area mail disaster information service of celluar networks in japan (in japanese). http://www.nttdocomo.co.jp.

[2] Calmesh. http://calmesh.calit2.net/.

[3] Japan meteorological agency. http://www.jma.go.jp.

[4] Mobireal. http://www.mobireal.net/.

[5] ns-2. http://www.isi.edu/nsnam/.

[6] Office of emergency management (oem) at st. louis county. http://www.stlouisco.com/LawandPublicSafety/EmergencyManagement.

[7] David Talbot. Japan earthquake: How tokyo got an 80-second head start. http://www.csmonitor.com/Innovation/Latest-News-Wires/2011/0314/Japan-earthquake-How-Tokyo-got-an-80-second-head-start.

[8] Nabil R. Adam, Vijay Atluri, Soon Ae Chun, John Ellenberger, Basit Shafiq, Jaideep Vaidya, and Hui Xiong. Secure information sharing and analysis for effective emergency management. In *Proceedings of the international conference on Digital government research*, 2008.

[9] Alexander Campbell. Lessons from Japan: Communication key to business continuity. http://www.risk.net/operational-risk-and-regulation/feature/2111999/lessons-japan-communication-key-business-continuity.

[10] Y. Bachrach, A. Parnes, A. Procaccia, and J. Rosenschein. Gossip-based aggregation of trust in decentralized reputation systems. *Autonomous Agents and Multi-Agent Systems*, (2):153C172, 2009.

[11] Yong Bai, Wencai Duh, Zhengxin Ma, Chong Shen, Youling Zhou, and Baodan Chen. Emergency communication system by heterogeneous wireless networking. In *Proceedings of the IEEE International Conference on Wireless Communications Networking and Information Security WCNIS*, Jul. 2010.

[12] C. Beard. Preemptive and delay-based mechanisms to provide preference to emergency traffic. *Computer Networks Journal*, pages 801–824, April 2005.

[13] C. Beard. Preemptive and delay-based mechanisms to provide preference to emergency traffic. *Computer Networks Journal*, pages 801–824, April 2005.

[14] B. Braunstein, T. Trimble, R. Mishra, B. S. Manoj, L. Lenert, and R. R. Rao. Challenges in using distributed wireless mesh networks in emergency response. In *Proceedings of the 3rd International ISCRAM Conference.*, May 2006.

[15] L. Capra and M. Musolesi. Autonomic trust prediction for pervasive systems. In *Proceedings of the 20th International Conference on Advanced Information Networking and Applications*, 2006.

[16] Maurizio Casoni and Alessandro Paganelli. Security engineering: A guide to build dependable distributed systems. In *ISBN 0-471-38922-6*, August 2001.

[17] Maurizio Casoni and Alessandro Paganelli. Security issues in emergency networks. In *Proceedings of the Wireless Communications and Mobile Computing Conference (IWCMC)*, August 2011.

[18] C. J. Chang, T. T. Su, and Y. Y. Chiang. Analysis of a cutoff priority cellular radio system with finite queueing and reneging/dropping. *IEEE/ACM Transactions on Networking*, (2):166–175, 1994.

[19] H. Chen, H. Wu, X. Cao, and C. Gao. Trust propagation and aggregation in wireless sensor networks. In *FCST' 07: Japan-China Joint Workshop on Frontier of Computer Science and Technology*, 2007.

[20] Y. Z. Cho and C. K. Un. Analysis of the m/g/1 queue under a combined preemptive/nonpreemptive priorty discipline. *IEEE Transaction on Communications*, pages 132–141, 1993.

[21] Kyung Soo Choi and Seong Pal Lee. A proposal of the national disaster emergency satellite communications networking. In *Proceedings of the ICACT*, Feb. 17-20, 2008.

[22] CONELRAD (1951). Providing for Emergency Control over Certain Government and Non-Government Stations Engaged in Radio Communication or Radio Transmission of Energy. Executive Order No. 10,312, 51 Fed. Reg. 14,769.

[23] CTIA - The Wireless Association. (2009). Wireless Quick Facts Year End Figures. Retrieved from http://www.ctia.org/advocacy/research/index.cfm/AID/10323.

[24] Mathieu DERVIN, Isabelle BURET, and Celine LOISEL. Easy-to-deploy emergency communication system based on a transparent telecommunication. In *Proceedings of the First International Conference on Advances in Satellite and Space Communications*, 2009.

[25] R. Dilmaghani and R. Rao. On designing communication networks for emergency situations. In *Proceedings of ISTAS.*, 2006.

[26] S. Drekic and D. A. Stanford. Reducing delay in preemptive repeat priority queues. *Operations Research*, pages 145–156, 2001.

[27] Arjan Durresi, Mimoza Durresi, Vamsi Paruchuri, and Leonard Barolli. Trust management in emergency networks. In *Proceedings of International Conference on Advanced Information Networking and Applications*, 2009.

[28] K. Sethom et al. Distributed virtual network interfaces to support intra-pan and pan-to-infrastructure connectivity. In *Proceedings of the GLOBECOM*, Dec. 2005.

[29] N. Boulicault et al. Ana4: a 2.5 framework for deploying real multi-hop ad hoc and mesh networks. In *the Ad Hoc and Sensor Wireless Networks: an International Journal (AHSWN)*, Dec. 2006.

[30] V. Untz et al. Lilith: an interconnection architecture based on label switching for spontaneous edge networks. In *Proceedings of the MOBIQUITOUS*, Dec. 2004.

[31] Shelly Farnham and Elin R. Pedersen. Observation of katrina/rita groove deployment: Addressing social and communication challenges of ephemeral groups. In *Proceedings of the 3rd International ISCRAM Conference.*, May 2006.

[32] Federal Communications Commission (2008). First Report and Order In the Matter of the Commercial Mobile Alert System (PS Docket No. 07-287). Washington, DC.

[33] T. Fujiwara, N. Iida, and T. Watanabe. A hybrid wireless network enhanced with multihopping for emergency communications. In *Proceedings of IEEE International Conference on Communications.*, 2004.

[34] M. Hollick, T. Krop, J. Schmitt, H. P. Huth, and R. Steinmetz. Modeling mobility and workload for wireless metropolitan area networks. *Computer Communications*, (8):751C761, 2004.

[35] D. Hong and S. S. Rappaport. Traffic model and performance analysis for cellular mobile radio telephone systems with prioritized and non-prioritized handoff procediires. *IEEE Transactions on Vehicular Technology*, (3):77–92, 1986.

[36] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang. A group mobility model for ad hoc wireless networks. In *Proceedings of the ACM/IEEE Int. Symp. on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM' 99)*, 1999.

[37] G. Iapichino, C. Bonnet, O. del Rio Herrero, C. Baudoin, and I. Buret. A mobile ad-hoc satel-lite and wireless mesh networking approach for public safety communications. In *Proceedings of the 10th International Workshop on Signal Processing for Space Communications*, 2008.

[38] Internavi Premium Club website., August 2008. [Online]. Available: http://www.premium-club.jp/index.html (in Japanese).

[39] B. Jacinto, L. Vilaca, J. Kelner, D. Sadok, and E. Souto. 3d routing: a protocolfor emergency scenarios. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, IWCMC' 10*, 2010.

[40] A. Janefalkar, K. Josiam, and D.Rajan. Cellular ad hoc relay for emergencies (care). In *Proceedings of IEEE Vehicular Technology Conference*, Sept. 2004.

[41] A. Jardosh, E. M. BeldingRoyer, K. C. Almeroth, and S. Suri. Towards realistic mobility models for mobile ad hoc networks. In *Proceedings of the ACM Mobile Int. Symp. on Computing and Networking (MobiCom' 03)*, 2003.

[42] K. Kanchanasut, T. Wongsaardsakul, M. Chansutthirangkool, A. Laouiti, H. Tazaki, and K. R. Arefin. Dumbo ii: A v-2-i emergency network. In *Proceedings of AINTEC' 08*, November 18-20, 2008.

[43] Kanchana Kanchanasut. Dumbo: Networking in an emergency. In *AsiaFI-APAN Joint Workshop*, 2009.

[44] G. Karakostas and E. Markou. Emergency connectivity in ad-hoc networks with selfish nodes. In *Lecture Notes in Computer Science*, 2008.

[45] Y. H. Kim and C. K. Un. Bandwidth allocation strategy with access restriction and preemptive priority. *Electronics Letters*, pages 655–656, 1989.

[46] Y. N. Lien, T. C. Tsai, and H. C. Jang. A manet based emergency communication and information system for catastrophic natural disasters. In *The Second International Workshop on Specialized Ad Hoc Networks and Systems*, June 26, 2009.

[47] Yao-Nan Lien, Hung-Chin Jang, and Tzu-Chieh Tsai. A manet based emergency communication and information system for catastrophic natural disasters. In *Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops.*, 2009.

[48] J. Liu and V. Issarny. Enhanced reputation mechanism for mobile ad hoc networks. In *Trust Management: Second International Conference*, March 29CApril 1, 2004.

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

[50] Andreas Meissner, Thomas Luckenbach, Thomas Risse, Thomas Kirste, and Holger Kirchner. Design challenges for an integrated disaster management communication and information system. In *The First IEEE Workshop on Disaster Recovery Networks.*, June 2002.

[51] Andreas Meissner, Zhou Wang, Wolfgang Putz, and Jan Grimmer. Dumbo ii: A v-2-i emergency network. In *Proceedings of AINTEC' 08*, November 18-20, 2008.

[52] F. Milan, J. J. Jaramillo, and R. Srikant. Achieving cooperation in multihop wireless networks of selfish nodes. In *Proceedings of the workshop on Game theory for communications and networks (GameNets)*, 2006.

[53] D. S. Mileti and J. H. Sorensen. Communication of emergency public warnings: A social science perspective and the state-of-the-art assessment. ORNL-6609, Dept. of Energy, Oak Ridge National Laboratory, Oak Ridge, Tenn.

[54] H. Mitchell, M. Jones, and J. Peifer. Development Strategies to Advance the Creation of Wireless Technologies. Proceedings of State of Technology Conference on Mobile Wireless Technologies for People with Disabilities. Atlanta, GA, USA.

[55] M. Musolesi, S. Hailes, and C. Mascolo. An ad hoc mobility model founded on social network theory. In *Proceedings of the ACM/IEEE Int. Symp. on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM' 04)*, 2004.

[56] Tomotaka Nagaosa and Seitaro Moriya. An emergency earthquake warning system for land mobile vehicles using the earthquake early warning. In *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety*, September 22-24, 2008.

[57] Y. Nakamura. Uredas, urgent earthquake detection and alarm system, now and future. In *Proceedings of 13th World Conference on Earthquake Engineering*, August 2004.

[58] Keisuke Nakatay, Kumiko Maeday, Takaaki Umeduy, Akihito Hiromori, Hirozumi Yamaguchiy, and Teruo Higashino. Modeling and evaluation of rescue operations using mobile communication devices. In *ACM/IEEE/SCS 23rd Workshop on Principles of Advanced and Distributed Simulation*, 2009.

[59] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos. Trust establishment in emergency ad hoc networks. In *Proceedings of the International Conference On Communications And Mobile Computing*, 2009.

[60] S. Reidt and S. Wolthusen. Efficient distribution of trust authority functions in tactical networks. In *Proceedings of the 2007 Information Assurance and Security Workshop*, 2007.

[61] J. Sanjay and C. McLean. A framework for modeling and simulation for emergency response. In *Simulation Conference*, Dec. 2003.

[62] G. Sharma and R. Mazumdar. Hybrid sensor networks: a small world. In *Proceedings of ACM MobiHoc.*, May 25-28, 2005.

[63] F. Skopik, D. Schall, and S. Dustdar. Start trusting strangers? bootstrapping and prediction of trust. In *Proceedings of the 10th International Conference on Web Information Systems Engineering*, 2009.

[64] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. Rao. Cooperation in wireless ad-hoc networks. In *Proceedings of IEEE INFOCOM' 03*, 2003.

[65] S. Tang and W. Li. An adaptive bandwidth allocation scheme with preemptive priority for integrated voice/data mobile networks. *IEEE Transactions on Wireless Communications*, (9), September 2006.

[66] Daniele Tarchi, Romano Fantacci, and Dania Marabissi. The communication infrastructure for emergency management: the integrated system for emergency vision. In *Proceedings of IWCMC' 09.*, June 21-24, 2009.

[67] Wei wei Wu and Xuan xi Ning. Evaluation of the reliability of emergency networks under time constraints. In *Proceeding of the IEEE International Conference on Automation Science and Engineering*, 2006.

[68] Will Knight. How japan's earthquake and tsunami warning systems work. http://www.technologyreview.com/blog/editors/26505/.

[69] Qing-An Zeng and Heng Wei. Synthesis of emergency evacuation communication system for disaster detection and information dissemination. In *Proceedings of the 11th International IEEE Conference on Intelligent Transportation Systems*, October 12-15, 2008.

[70] Qing-An Zeng, Heng Wei, and Vineet Joshi. An efficient communication system for disaster detection and coordinated emergency evacuation. In *Proceedings of IEEE WTS*, 2008.

[71] X. Zeng, R. Bagrodia, and M. Gerla. Glomosim: A library for the parallel simulation of large-scale wireless networks. In *Proceedings of the ACM Parallel and Distributeal Simulation (PADS' 98)*, 1998.

[72] Petros Zerfos, Xiaoqiao Meng, and Starsky Wong. A study of the short message service of a nationwide cellular network. In *Proceedings of IMC' 06*, October 25C27, 2006.

[73] J. Zhou and C. Beard. Comparison of combined preemption and queuing schemes for admission control in a cellular emergency network. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, April 3-5, 2006.

[74] J. Zhou and C. Beard. Weighted earliest deadline scheduling and its analytical solution for admission control in a wireless emergency network. In *Proceedings of International Teletraffic Conference*, August 29 - September 2, 2005.

[75] J. Zhou and C. Beard. Tunable preemption controls for a cellular emergency network. In *IEEE Wireless Communications and Networking Conference*, March 11-15, 2007.

[76] J. Zhou and C. Beard. A controlled preemption scheme for emergency applications in cellular networks. In *IEEE Transactions on Vehicular Technology*, Sept. 2009.