2.3 Crisis Management

A crisis management system has been developed that enables crisis response teams to respond with critical resources where needed in real time. It uses deployable and in-situ sensors that configure themselves to provide real-time monitoring of the environment. Networking supports reliable, dynamically configurable, and highly secure communications to enable real-time delivery of information to distributed decision-makers and real-time information development using remote, on-line resources.

2.3.1 Scenario Description

In 2015, “perfect” conditions exist for multiple fires in the U.S. DoD has deployed a "staring" missile launch detection satellite system approved for military and civilian use. NASA has orbited Firesat, capable of providing twice-a-day high-resolution data over multiple spectral bands (for higher informational content), and multi-instrument views of forest fire activity around the world.

A large collection of wireless devices with embedded chips has been deployed in cellular phones. They support “spotcasting,” ad hoc communications, a sensor mode, and general purpose programming and processing capabilities. Optical fiber is extensively deployed at the core of the network. A rich assortment of sensors is deployed in homes, commercial buildings, public infrastructure, and the natural environment. Computation, communications, and sensor resources are widely available over the Internet.

On the day of crisis, DoD reports dozens of new fires from a single highly charged lightning storm. By mid-day, the early morning Firesat images and data have been processed and disseminated to hundreds of state and Federal agencies. Hot-spot data are combined with vegetation cover and dryness models to produce detailed next-24-hour maps for the worst-hit regions. These maps and digital models are disseminated instantly to government command and control centers and are spotcast to the individual homes and businesses most in danger.

Department of Interior and other Federal agency supercomputing systems are organized on-line to model the existing situation and begin “nowcasting” the predicted tracks of the worst fires. The models and nowcasts are transmitted by satellite communications to the forest fire field units, which return validation and update information. This field information, along with real-time atmospheric, chemical, and other environmental data from sensors deployed throughout the area – both in-situ microsensor platforms deployed in advance as well as self-contained, self-powered sensors dropped from aircraft that same morning – are continuously integrated into the nowcast models. Customized warning and evacuation messages are automatically provided to all the homes and businesses in the area.

Emergency mobilization forces are directed by computer into the affected area. They establish a high performance field network instantly capable of local area and remote

communications, using truck-based wireless technologies tied into regional networks via high performance satellite communications.

Telemedical facilities are established to attend to fire victims in the worst-hit areas. Mobile whole-body scanners, sophisticated medical instruments, and mini chemical analysis labs are plugged into the network. This allows deep resources of medical specialists, data and information resources, and analysis facilities to support on-site paramedics in real time. Command and control units have real-time high performance network access to all needed statewide and Federal resources.

2.3.2 Disaster Scenario Networking and Networking Research Needs

The disaster scenario discussion identified networking challenges including:

- Sensornet: An ad hoc network of sensors configured for and attached to the existing infrastructure. High bandwidth connections, e.g. gigabyte satellite to reach rural areas.
- Heterogeneous environment of sensors, networking capabilities, and administrative structures
- Dynamic environments and changing user requirements providing a need for new network management and visualization tools and automatic reconfiguration, management, and control
- Technology reuse: Using surviving resources for purposes other than the primary purpose they were designed for
- Data resources: Satellite sensors and deployed video sensors that produce data at the rate of hundreds of megabytes per second. These data are used in modeling and by command centers. Rapidly changing loads place emphasis on QoS based on media type (sensor data, voice, video) and user.
- Real-time modeling: Significant distributed computational and communications resources to support nowcasting

The disaster scenario discussion identified research needed to meet these challenges, including**:**

Interoperability

Organized sensors and networks will have to operate seamlessly with the existing infrastructure and with each other to overcome existing incompatibilities, routing mismatches, and security mismatches between different providers.

Robustness and dynamic reconfiguration

The infrastructure must be designed to cope with a wide variety of faults and dynamically changing resources by providing redundant resources and paths and the ability to actively reconfigure. Redundant technologies should be used so that their failure modes are as distinct as possible to decrease the probability of system failure.

Reuse of technologies

Reuse of wireless devices (including routing, spotcasting, ad hoc communication, sensing, and application software download) could help ensure that local resources are available during a disaster response. Reuse could also support functions needed to transform from short-term crisis management to longer-term emergency response.

Self-organizing, self-healing networks

Self-organizing, self-healing networks will expedite the organization of remaining and newly deployed sensors and technologies to establish routes and to connect to the existing infrastructure with minimal human intervention. The involvement and coordination of government agencies, companies, and individuals may require establishing a temporary administrative domain including components from the different organizations.

Dynamic, adaptive, time-varying QoS

In a crisis response, bandwidth resources may not match the workload and workloads may vary significantly over time and space. For example, time criticality and video quality requirements may vary depending on whether it supports telemedicine or media reporting. Thus, mechanisms are needed to deliver QoS within an ad hoc network that are appropriate to the application and network technology.

Discovering resources and their location

Establishing an ad hoc infrastructure for disaster response requires resource discovery such as identifying and locating available links and their capacities; information, computational, and other resources; and QoS capabilities to support priority information distribution and delivery of telemedical resources.

Trust: security, privacy, and reliability

Issues of trust, encompassing security, privacy, and reliability, pervade the disaster scenario. The disaster response resources must provide differing levels of security, assurance, and reliability based on the needs of the end users and their applications such as medical data transmission and patient privacy over heterogeneous, ad hoc networks and devices. Research needs to address:

- Heterogeneity of parties involved: A major disaster will involve many government agencies (local, state, and Federal), companies, and individuals. Disaster response networks must be responsive to their diverse security and trust policies that may

contain incompatibilities and hinder sharing data and other resources. This issue can be further complicated if other sovereign nations are involved.

- Flexibility: Disaster responses may require temporary flexible modification or violation of security and trust policies. For example, an emergency medical team may need to access patient records for which it ordinarily would not have authorization.
- Reuse of technologies: Technologies may be designed so they can perform actions in crises that are not their primary functions. They also need to be designed so they are not then susceptible to third party invasion during normal times of operation using their crisis response capabilities.
- False alarms: Research should be conducted on detecting a false alarm by an intruder and being able to identify that intruder.

Network visualization and network management

Current network visualization and management tools are not able to handle the ad hoc heterogeneous networks needed for disaster response. New network monitoring and measurement tools are needed to support visualization and management.

Spectrum conflicts

Spectrum conflicts that arise whenever different technologies (for example, Medium Access Control (MAC) protocols and cellular standards) share the same portion of the spectrum will need to be overcome.

Metrics and performance

Metrics are needed to measure the time to set up a network and the amounts of traffic supported at different levels of QoS. Simulation and analysis tools are needed to deal with time dependent response problems and networks with many orders of magnitude difference in speeds from one part of the network to another. Solutions to the time dependent response problems should be evaluated in multiple ways including simulation using benchmarks. In addition, training exercises are needed to stress and test different solutions.