Communications Interoperability in Disaster Relief/Crisis Situations

Assigned Track:

C2 Architecture

Names of Authors:

Alfred W. Mitchell (principal point of contact)
Science Applications International Corporation
4015 Hancock St.
San Diego, CA 92110
Ph: 858-826-5632
Fax: 858-826-5672
Email: mitchella@saic.com

Nicholas North
Science Applications International Corporation
4015 Hancock St.
San Diego, CA 92110
Ph: (858) 826-5982
Fax: 858-826-5672
Email: northn@saic.com

Chuck Zumbrun
FourD Development
2000 North Wells Street
Fort Wayne, IN 46808
Ph: (260) 918-2211
Fax: (260) 572-0535
Email: czumbrun@fourthwavellc.net
Abstract

Communications Interoperability in Disaster Relief/Crisis Situations

Recent national disaster relief efforts, such as the Hurricane Katrina and Hurricane Rita natural disasters, have once again demonstrated that solving the multi-agency/command communications interoperability issue remains at the forefront of communications needs. Additionally a myriad of multi-agency Homeland Defense exercises has shown that the “lowest common denominator” of incident response interoperability is centered on the largely paper-based National Interagency Incident Management System (NIIMS) Incident Command System (ICS). The principal issue revolves around differing data formats and different RF communications device interfaces that result in a vertical “stove pipe” communications infrastructure with little data exchange between specific agency systems. Developed and matured in conjunction with DOD Advanced Concept Technology Demonstrations and tailored to the needs of public safety sector agencies, the new “SentryPoints” combination of software/hardware allows disparate RF and data exchange systems to be linked in a common network using existing methods of RF and wired communications. This paper discusses the potential application of SentryPoints technology to the pressing issue of communications interoperability in disaster relief and homeland defense applications.
I. Introduction of problem

The common thread among scores of stories both during and after the unprecedented string of natural disasters striking the US Gulf Coast late this summer and fall was the recurring theme of what happens when infrastructure is destroyed and multiple governmental and non-governmental agencies arrive to assist. The common issue in all these stories is that command, control and communications interoperability, both in voice and data realms, still remains an elusive commodity.

Hurricanes Katrina and Rita laid bare the bones of the underlying communications infrastructures used by such widely varying agencies as the Department of Defense, Homeland Defense, National Guard, and multiple layers of law enforcement and emergency response from FEMA to FBI to state and local authorities. Each of these agencies maintains, and generally operates successfully, their own voice and data systems. The RF spectrum is crowded with multiple types of radios whenever these fundamental elements of disaster response converge on the scene. What remains most problematical is that despite ongoing funding to alleviate potential interoperability issues, the fact remains is that specific agencies use frequency bands allocated through Congress via the cumbersome World Administrative Radio Conference (WARC) process that assigns bands for certain uses.

This guarantees that when DOD, law enforcement and first responders arrive on scene they will be carrying different radios operating on different frequency bands and with different inherent voice and data capabilities. DOD radio systems invariably contain mandated NSA Type 1 crypto devices not available to most law enforcement units or emergency teams. State and local law enforcement and fire departments operate on different frequency bands. They may or may not have their own encryption devices. There are stories of ambulance services that have to maintain as many as nine separate radios in their vehicles due to the need to communicate with agencies on differing bands.

Throw this into a situation where the lowest common communications denominator, namely phone service (either wired or cellular) is removed through widespread devastation to community infrastructure and the result is communications chaos. This is painfully apparent in the early hours of immediate disaster response as the emergency teams arrive on scene and attempt to coordinate actions. The quickest short-cut to allow interoperability is the assignment of agency Liaison Officers (LNO’s) at command centers. These personnel have their own agency communications equipment and data systems to allow information to be manually distributed from the command center to agents in the field. However the translation of the data can often be time consuming, and transcription errors are frequently made in the heat of the moment (e.g. fog of war). Such situations can result in situations like the now well-known picture of the city of New Orleans school buses that might have been available to support evacuation, but the right people not knowing where they are until they were flooded and useless.

There is no doubt that the emergency teams deployed during Katrina and Rita did their best, often in exceptionally hazardous conditions. However, new technologies in
development through the Department of Defense Advanced Concept Technology Demonstration (ACTD) programs may offer low-cost solutions to allow a rapid increase in overall voice and data communications interoperability without having to completely replace the massive infrastructure investment each agency has in their existing RF communications systems.

Several assumptions need to be made whenever talking about communications interoperability in disaster relief situations:

1. You must assume that basic civilian communications infrastructure such as wired telephone and cellular service may be severely disrupted or even eliminated for a significant period of time during the critical initial hours of a disaster response.
2. Voice communications restoration generally has the highest priority.
3. Data networks may be severely degraded to non-existent
4. Reliance on web-based collaborative planning applications may not be feasible if network is not functioning
5. Each agency will bring current inventory communications system to the disaster. These will operate on many separate radio bands and may or may not be easily integrated into a common disaster support communications architecture.

As an example of the specific issues facing emergency response teams during the Hurricane Katrina relief effort, the following observations were critical:

“On September 14, 2005, the 9/11 Public Discourse Project issued a report asserting that the response to Hurricane Katrina was a classic failure in command and control. It found no unity of command—or more specifically, no one in charge and no unified incident reporting system to coordinate efforts of local, state and federal agencies. Fixed communications systems failed with no ready means for their restoration. This was not surprising, given that there exists no incentive for the intensely competitive information systems industry to finance ruggedness, redundancy or rapid restoration.”

- AFCEA Signal magazine, DEC 2005

This report issued five major findings on the specific issues of Emergency Preparedness and Response. They are provided in the following table.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Status</th>
<th>Next Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide adequate radio spectrum for first responders</td>
<td>Minimal Progress</td>
<td>Congressional action to allocate spectrum</td>
</tr>
<tr>
<td>Establish a Unified Incident Command System</td>
<td>Minimal Progress</td>
<td>Local, state and federal agreement on system</td>
</tr>
<tr>
<td>Allocate homeland defense funds based on risk and vulnerability</td>
<td>Minimal Progress</td>
<td>Congressional action to allocate funding</td>
</tr>
<tr>
<td>National critical infrastructure risks and</td>
<td>Unsatisfactory</td>
<td>Executive department action</td>
</tr>
</tbody>
</table>
The rest of this paper investigates the first two major issues from the 9/11 Public Discourse Project, and offers a potential low-cost solution for easily providing voice and data interoperability supporting the third issue while allowing all users the ability to continue to use their existing communications equipment.

II. Discussion of communications interoperability issues in Katrina/Rita relief

Part I, item 1 of the Report on the Status of 9/11 Commission Recommendations is to “Provide adequate radio spectrum for first responders”. Inadequate radio frequency spectrum, both during the September 11, 2001 terrorist attack in New York City, and during and post Hurricane Katrina in New Orleans, Louisiana and Hurricane Rita in Texas, was but one of the issues that demonstrates common threads that exist in emergency response that cause chaos in communications. Other communications issues include lack of regional standard operating procedures (SOPs) and the inability of surviving communications systems or those brought into the arena after the storm to function in an interoperable manner.

SOPs will require governance bodies to convene and to concur on what processes will be followed during a major crisis. After the September 11th, 2001 attack and post Katrina and Rita, communications collapsed even though assets became available as out of area responders arrived at the scene. Some of these responders included the Louisiana National Guard, FEMA, the United States Army 101st Division, the United States Coast Guard and the United States Navy. Though these assets provide enormous capability, no procedures were in place to readily create an environment for interoperable communications.

Since the New York attacks, and before Hurricanes Katrina and Rita, the Department of Homeland Security (DHS) under the Office of Domestic Preparedness (ODP), now known as the Office of Grants and Training (OG&T), has conducted communications based exercises around the country. The after action reports from these exercises have been delivered to the jurisdictions where they were conducted. These exercises all demonstrated that lack of SOPs, inadequate interoperable technologies, inadequate training, and agency cultures are all obstacles to creating functional, cohesive interoperable communications. The exercise findings were born out during and subsequent to the hurricanes.

Communications interoperability during a major incident or natural disaster is a 3-dimensional issue. After the local agencies are overwhelmed in an emerging crisis, state and federal assets will respond. At this point the communications picture becomes more complicated. All of these agencies will respond with their own, familiar communications equipment. Levels of training will vary. Observation has shown that personnel operate best with that equipment that is within their comfort zones. The 3-dimensional model breaks down quickly in today’s emergency response environments. In one
communications based exercise observed in 2005, the exercise radio was bypassed in favor of the one the responder was comfortable with even though the new radio was inherently interoperable in the area. The problem appeared to be three-fold:

1) Unfamiliar equipment,

2) Inadequate training, and

3) Inability to link existing legacy systems.

The issues mentioned here have been shown to be common throughout the United States, from the east coast to the west and from the gulf coast to the northern states. The common denominator is that there are few common communications methods, resulting in the probability that wired or cellular phone service becomes that basic standard by default. Changing cultures and establishing SOPs will take time. Training and technology however can be applied more quickly. Still, if the responder is able to use communications equipment that is familiar, and use it in an interoperable manner with other jurisdictions and agencies, the network will be more functional.

III Discussion of communications interoperability issues in Homeland Defense crises response scenarios

Communications interoperability problems during man made crises, such as a terrorist incident, are essentially the same as during a natural disaster. Some additional agencies may be added to the puzzle, but the end result remains. Local responders can be overwhelmed by the magnitude of the event, the state responds with additional assets followed by a federal response. Each of these levels of the 3-dimensional response arrives with their own equipment, to include communications, and the equipment is generally not interoperable. There is a need to be able to link these disparate communications systems, but it is not in place.

Whether the incident is a of a natural origin such as hurricanes Katrina and Rita, or of a man made disaster like the World Trade Center or the Oklahoma Federal Building, the communications issues are the same. Responders need to be able to use their inherent systems to communicate with each other, and can’t. Due to the large infrastructure costs associated with each agency fielding their own equipment, there is general institutional reluctance to “buy interoperability through completely new radio systems”.

IV. Data Communications Protocols and Methods of Interoperability

Critical to any discussion of interoperability is agreement on the basic formats for data exchange between often widely disparate systems. This has been the principal stumbling block for a large majority of “big iron” systems over the course of multiple years of development. Web-based application interfaces have eased this problem to some degree with the advent of HTTP and XML data exchange formats. However, many command
and control systems still depend on often highly unique data formats to exchange data with their component parts.

This reliance on specialized formats, often selected with good reason for the specific tasks associated with any given system, can result in “data gridlock” when these system attempt to “talk” to other systems with similar format restrictions. The shift to more web-based application interfaces does not totally eliminate this issue, which often becomes even more problematical as bandwidths decrease often exponentially as the user gets close to the “tip of the spear”.

For the past several years alternate methods of data connectivity have been explored through a series of Department of Defense sponsored Advanced Technology Demonstrations and Advanced Concept Technology Demonstrations. Central to the thesis of providing more “far forward” bandwidth and data utility, a dedicated team of operational command and control specialists and engineers have been experimenting with new paradigms for connecting a wide range of communications equipment to not only the local LAN but also the WAN at large. The remainder of this paper will discuss one of those systems as it may be applied to disaster relief interoperability scenarios.

V. Development history of SentryPoints software/hardware suite

SentryPoints is a software/hardware suite designed to support rapid deployment of interoperable systems for crisis management and disaster relief. This software/hardware suite provides situational awareness, planning, and command and control functions for disaster relief and crisis management using mobile ad hoc networking techniques on a wide variety communications gear and protocols. SentryPoints also assists in interoperability by bridging external systems via standard protocols and message formats, as well as providing data transport services for other applications to use. The use of mobile ad hoc networking techniques allows for peer-to-peer self configuration making the network fully operational with minimal coordination by users.

A disaster can create an infrastructure poor communications environment. Unlike the military, commercial and municipal agencies may not have the resources to set up and sustain communications if the established infrastructure is destroyed. SentryPoints is designed to use a wide variety of existing commercial and military communications gear so that in a disaster whatever infrastructure has survived or has been brought in as part of the relief effort may be used to rapidly reform a network among disaster responders. This allows for quick deployment during or after a disaster, using whatever part of the infrastructure has survived or been restored.

The SentryPoints team has been developing interoperable systems since the late 1980’s. Their focus has been to define an architecture to support interoperability, and then to build systems using that architecture to solve the interoperability problem by connecting
systems that had not been designed to work together, to connect those systems without modifying them, and to display a common operational picture from all interconnected systems.

There are two key facets of this interoperable architecture

(1) **Data networking over existing communication channels in a peer-to-peer mobile ad hoc manner, and**
(2) **Interoperability with the existing systems of the day without modifying the existing system.**

The interoperable system component then appears to an external system just as another node of that system. It exchanges data with that system using the external system’s native communication channels, formats, and protocol. If it is just linking two external systems of the same type, the data passes through unchanged. However, if it is connecting different types of systems, it transforms the data into its own internal representation, either for local use or to transfer to another system. It could interface with any number of different systems in this way, and then present that data to command staff to create a common operating picture from disparate systems.

The SentryPoints team discovered there were five core functional areas that had to be implemented to interoperate between these disparate systems and to present a common operating picture. These are:

1. Databases
2. Communications
3. Graphics
4. User Interface
5. System (authentication, access controls, threading, etc)

In addition there were three key patterns of processing that took place in all C2 systems:

- Transforms – data was transformed from one format to another
- Updates – the change in state of some data in the state caused another data item to change state, or an action to occur
- Relationships – one data item in the system would be related to other data item(s)

By implementing the five key functional areas as independent building blocks, and by implementing the three key processing patterns, the core functionality was built that allowed for the rapid creation of systems to interoperate with disparate external systems. These building blocks were assembled by high level code that expressed concepts in the user’s terms. These core components are assembled into maps, plans, messages, units, logs, etc, for the user to manipulate.
Creating an interoperable application then is just a matter of gluing these components together using the key processing patterns of transforming data from one format to another, updating data on state changes, and relating data items together. By implementing these patterns, and by creating independent core components, developers can work independently on specific code without interfering with each other, allowing for the rapid development and deployment of new capabilities.

As previously noted, one of the impediments to interoperability is that each agency typically has their own communications equipment, and that equipment is often incompatible with another agency’s equipment. Building a software system for interoperability is pointless if basic voice and data communications cannot be established between the systems they were attempting to interconnect. To overcome this roadblock a radio interface device is used that communicates with a wide variety of radios and crypto gear while presenting a common and simple Application Programming Interface (API) to applications desiring to communicate over radios. A prototype device, known as the Micro InterNet Controller (MINC), was originally developed by Command System, Inc of Fort Wayne, IN, and is now owned and sold by General Dynamics.

The first MINCs were voice only devices that allowed two dissimilar voice radio networks to be connected. The MINC would relay and buffer if necessary voice traffic between the nets. It was an effective, low-cost, and simple means to bridge voice networks. MINCs were then enhanced to support data traffic. MINCs are available in one or two channel configurations, and any number of MINCs may be connected to a host application via a serial or USB port.

MINCs currently support analog radios, in which case the MINC converts digital application data to modem tones using an internal modem. MINCs also support digital data for radios that provide an RS-232, RS-422, or MIL-STD-188-114 interfaces.

A typical configuration is shown in Figure 1 below.
As shown in a typical military configuration, the MINC provides to the application a common interface to both the low bandwidth analog squad radio network (often a lightweight handheld walkie-talkie type radio with typical bandwidth of 2400 bps), and to the higher bandwidth platoon command network (more often a standard military digital radio such as SINCGARS with a bandwidth of 16 Kbps). MINC models also contain embedded GPS receivers, allowing them to be used as a single device to provide communications and location reporting. The MINC was designed to support rapid, low cost interoperability between different radio networks. This design goal drove decisions on the processing contained in the MINC versus in the host computer application code.

The MINC contains almost no network protocol code. It simply keys the radio and transmits when instructed to by the host computer application code. This has several advantages:

- since the MINC is an embedded processing device, this makes MINC firmware development easier in the difficult environment of an embedded device with limited processing and memory resources.
- the code in the MINC is simpler and more reliable.
- the code in the MINC is longer lived; the MINC firmware rarely needs to be changed to support new radios.
- likewise the interface between the MINC and the application is long lived. The interface is exactly the same for a 25 year old 300 baud voice grade radio and the very
latest high bandwidth digital radios. In fact, the MINC to host computer API has not changed in over 10 years.

These factors all work together to support rapid deployment of interoperable data communications over dissimilar communications gear.

**SentryPoints next generation interoperability**

This interoperable system architecture was developed and thoroughly tested via multiple DOD ACTD events and by numerous military users world-wide. The concept of an interoperable command and control and situational awareness application based on mobile ad hoc networking has been proved viable. In 2002 SentryPoints set out to factor in lessons learned and to re-architect the system specifically for crisis management systems used by municipal and other agencies based on these same principles of interoperability.

The original system was designed for interoperability and ad hoc networking for military applications. While the architecture proved successful for that environment, it still required development effort to interoperate on different communications equipment and with different systems. This was all right in the military environment where planning for operations is rigorous and well-defined. However, in the civilian world there isn’t the tradition or resources to plan for “what your enemy might do.” A system to be used in a civil disaster response environment must provide interoperability without extended development. Interoperability has to be achievable on the ground after a disaster by support personnel, not by skilled developers at the home office.

**Key tradeoffs in the SentryPoints interoperable architecture**

**a. Separable components:** While a single monolithic executable simplifies the development of the application, it means unplanned for configurations can only be created by rebuilding the application. The SentryPoints system is assembled from separate components at runtime, using a platform independent plug-in architecture. This means that if all you need is a map display all you load is the map component, and that’s all you get. Or if all you need is a Comm relay, then all you load is the Comm component and you then have the communications capability and nothing else to get in the way. This can all be done at deployment, there is no need for additional development work to fit a specific situation.

**b. Service interoperability:** Object interfaces through means such as COM or CORBA have been used to provide service interoperability between applications. However, this often results in a finer level of granularity than needed. To do something as conceptually simple as “send a message” may require a deep understanding of the application’s data model and will require implementing a specialized COM client to do it. This works against the rapid deployment of interoperable applications. SentryPoints presents service based APIs for external applications to use. Services exist at the conceptual levels that
years of working with providing services for external applications have told us are the right ones. For example, there is a Comm service that allows you send and receive messages and configure by exchanging messages in a simple XML schema.

c. **Data interoperability**: As with services, data interoperability for external applications can be achieved through object interfaces such as COM and CORBA. This is very powerful, but also very difficult to use. An external application developer has to acquire a deep understanding of the other application’s architecture to use it. Furthermore, any changes to that application’s internal data model potentially affects these object clients. This makes for significant versioning problems, and hinders the rapid deployment of separately developed components. SentryPoints provides message interfaces for interoperability. This is primarily through XML documents exchanged with services as described above. Using XML makes these interfaces simple and resilient, as well as allowing the use widely known techniques and tools such as DOM parsers and XSLT for manipulating them.

d. **Mesh routing**: As noted by [Campen] “The information age has turned every individual with a wireless device into a potential communications repeater node—an element in a ubiquitous and infinitely expandable and self-healing network.” To exploit this potential, SentryPoints implements a tailored version of the Optimized Link State Routing (OLSR) [RFC 3626] for automatic network discovery and routing. OLSR allows SentryPoints to determine which nodes are repeaters on the same network or onto different nets, and to keep connectivity and routing data up to date without user action as the network topology changes. Sentry Points supports mesh networking over wired and wireless LANs, as well as radios.

e. **Commercial/industry protocols and formats**: Standards, protocols, and techniques such as XML, SOAP, SMTP and HTTP have achieved a near ubiquitous nature. SentryPoints has been designed to exploit these widely accepted techniques and to use them when appropriate. This allows for rapid deployment and interoperability of separate systems that were not designed with each other in mind.

However, it should be noted that these sorts of technologies often rely on high bandwidth communications and a solid infrastructure of networks, servers, etc. In a disaster situation this sort of capability and infrastructure is often not available. SentryPoints can bridge that gap by communicating using just single channel, half-duplex, voice grade radios if that is all that is available. In a disaster situation it is likely that while parts of the communication infrastructure will collapse, other parts will remain intact. And that as relief efforts are underway, a variety of communications gear will become available. See for example [Kenyon], [Lawlor], and [Ackerman]. By being designed to exploit a wide variety of commonly available protocols and formats, the SentryPoints system can be rapidly deployed in a disaster on whatever communications are available.

f. **Scripting**: SentryPoints is using Python, a platform independent, interpreted, interactive, object-oriented programming language to combine core components into applications. This allows applications to be created or changed very rapidly from the
separable and independent components described earlier to respond to a situation.

g. **Non-military command and control:** Military personnel are well-trained in command and control and planning. There are well-defined processes in place to prepare for, plan, evaluate, and execute a mission. However, as noted in [Campen] in the commercial or municipal world there is no such tradition of a unified command structure. SentryPoints is implementing a NIMS Incident Command System planning module to support multi-agency planning and command and control for disaster situations.

**Next generation MINC**

The current MINCs were created to provide the same interface to the application, regardless of the type of radio being used, allowing applications to be deployed rapidly on any radio network and to bridge dissimilar networks. SentryPoints is currently building the next generation of devices to bring this type of capability for municipal and commercial communications. Like the previous MINCs the next generation device will provide a communications interface and GPS in a single device, allowing a simple solution to provide situational awareness.

The next generation device includes interfaces for analog and digital radios (including Hayes modem interfaces to satellite and other phones), as well as IP based radios, and standard 802.11 series wireless. Additional communication capabilities include the ability to embed a cellular transceiver. This combination of capabilities - radio, wireless IP, and cellular - provides interfaces for the application for most of the data communications infrastructure likely to be encountered in disaster relief. In addition to the communications and GPS capabilities, it also includes the option to embed an RF Id reader. As asset tracking by RF Id becomes increasingly common, this allows a simple way of locating and tracking assets and reporting that information.

**VI. Data protocol interoperability via SentryPoints software/hardware**

Interoperability has two distinct components:

(1) Communications interoperability – using whatever communications are available to move data between systems, and
(2) Applications interoperability – exchanging data between different applications.

SentryPoints is designed to use whatever communications are available to transport data, and to make it easy to exchange that data with other systems. The underlying communications infrastructure, radios, cellular networks, and wired or wireless LANs, is generally transparent to the end user. The system automatically discovers and uses the appropriate interfaces. However, the user can control which interface is used to transmit data if desired. For example, assume the destination of a particular message is reachable both over an 802.11 wired LAN, and over a SATCOM radio. Clearly, the message should not be transmitted over the expensive and limited resource of a SATCOM radio if a faster alternative is available. The system should correctly choose the “best” path, but
the user can override that choice if desired.

Each type of network interface is discussed below. SentryPoints automatically and transparently routes data within the same network or across different types of networks.

1. Radios: The application can interface with radios by a number of means. If the radio provides a standard serial (e.g. RS-232), PPP, or IP interface the application can be connected directly to the radio. If the radio provides a specialized serial interface, (e.g., a close-to-ground Push-To-Talk line) a MINC can be used to interface between the application and the radio.

The protocol used over the radio network also depends on the capability of the radio. SentryPoints optionally compresses and encrypts the data. AES is used for encryption by default. The data is encoded for forward error correction, and then packetized to a size appropriate for the speed and error rate of the network.

A sliding window protocol with a selective acknowledgement is used to provide reliable delivery of data.

The OLSR protocol, as described earlier, is used over the radio networks to provide a mobile ad hoc network. OLSR has been modified on the radio interfaces to account for non-IP addressing, and the lower bandwidth and higher error rates (relative to an 802.11 wireless LAN) of the radios. For radios that provide no media access control, SentryPoints is currently upgrading its simple CSMA MAC protocol to reservation based TDMA approach specifically tailored for mobile ad hoc networks on single channel half-duplex radios.

2. LANs: For wired or wireless LANs a variety of protocols and formats can be used, depending on the configuration and infrastructure. For messaging on a local network with no routers, gateways, firewalls, etc to deal with, either TCP or UDP is used using IANA unassigned ports. UDP is used for short, unreliable messaging such as network discovery messages or position reporting. TCP is used for user messaging where reliability is desired.

SentryPoints uses the OLSR protocol as described earlier over wireless LANs to form a mobile ad hoc network. Over a wired LAN, SentryPoints also uses OLSR to discover other nodes and route data. The wired LAN is treated like a mobile ad hoc network. In a disaster situation a wired LAN will be subject to frequent changes and additions. By using its mobile ad hoc techniques, SentryPoints requires no preplanned configurations or network administration during operation to interoperate with changing configurations. SentryPoints mobile ad hoc protocols are tuned for the wired environment to not consume unnecessary bandwidth since the rate of change to the network is slow, at least compared to a mobile wireless network.

For networks that extend through routers, firewalls, DMZ’s and the like, it is often difficult or unfeasible to get non-standard ports opened up and to get UDP or TCP
packets routed through. In these configurations SentryPoints can be configured to act as a HTTP server on port 80 (unsecure) or port 443 (secure) and route data for other SentryPoints instances that act as HTTP clients.

In this case, although it is set up like a client/server network, the network behaves like an ad hoc peer to peer network. The clients discover the server automatically, and the server routes on behalf of the clients using the OLSR mechanism. No special setup or configuration is required of the user.

Additionally standard SMTP/POP3 email may be used. Data may be routed between SentryPoints instances via email, and SentryPoints may send and receive data from external applications or users via email. Although email may be slow and can be unreliable compared with many other communication means, if it is available, SentryPoints can use it to exchange data. Command and control and situational awareness data is simply transformed to and from MIME multi-part messages and emailed. Since SentryPoints uses standard XML for streaming its internal data model, the receiving station, (if not another SentryPoints node) can easily transform the data, using XSLT or other techniques. Data may optionally be encrypted for security.

SOAP/XML can be used for interfacing with external services over LANs with SentryPoints typically acting as a client of a web service. Interfaces include simulation/training systems and image collection systems.

3. Cellular and Satellite Phones: Cell and satellite phones may be used as communication devices in a number of ways depending on their capabilities. If a cell or satellite phone has a Hayes modem type of interface, SentryPoints applications may exchange data by dialing each other to establish a connection and then transfer data. In the typical configuration each application is set up to auto answer a call initiated by another SentryPoints application.

If the cell phones are Java capable they can be downloaded directly with a handheld version of the SentryPoints application. This application will report the position of the cell phone, if GPS enabled, and allow the cell phone user to exchange data with other SentryPoints applications, whether cell phone or computer based. As noted in [Lawlor], cell phone text messaging would often work in the Katrina relief efforts when other communications means failed. SentryPoints can use short text messages to pass situational awareness information (i.e., location and status), as well as basic command and control information.

4. Services: Finally, external applications may use the SentryPoints service APIs over a LAN. Services may be discovered dynamically or configured to exist on “well-known” ports. External applications send and receive SOAP/XML documents to invoke services and receive results. While interacting directly with the SentryPoints services provides the most power and performance for interoperation between different applications, it also requires some development work to make it happen. Clients for the services have to be implemented to the service APIs.
Once implemented, however, service providers and clients can be deployed in an ad hoc fashion. The loose coupling and auto discovery of services means the SentryPoints services can be used by any number of different clients without requiring any special configuration during deployment.

SentryPoints provides services for:

1. **Comm** – sending and receiving data and configuring comm interfaces
2. **Mapping** – getting map tiles from the SentryPoints map tile cache or renderer, displaying symbols on the SentryPoints map such as units, individuals, or geometries such as lines and areas of interest, and getting information about symbols on the map.
3. **Planning** – Extracting data from or adding data to the ICS planning data, including ICS form data, archived plans, and incident logs.
4. **User interface** – tightly integrated external applications may want to place data on the SentryPoints user interface or add their own forms and controls to the interface to provide a seamless appearance to the user. The SentryPoints user interface service allows external applications to add an independent subsystem to the user interface, for example, a finance application could add a menu item or tab that leads to that system’s detailed forms for tracking personnel and equipment costs. Or existing forms may be manipulated by external applications, for example, a weather reporting system could use the user interface service to automatically populate the weather forecast field of an ICS 202 form that would otherwise have to be manually entered.

**VII. Potential multi-agency network architectures supported by SentryPoints**

Figure 2 shows a sample network configuration for bridging a mobile wireless team to a command post server to browser at crisis center.

Figure 2. Disaster relief bridging search and rescue team on wireless LAN via SATCOM to Incident Command Post.
In this configuration a mobile team (e.g., a search and rescue team) is equipped with 802.11 wireless devices. Those devices form a mobile ad hoc network that allows the team members to exchange situational awareness and other data. One team member also has access to a satellite radio terminal (either satellite telephone or data terminal). SentryPoints seamlessly bridges the high speed mobile network onto the low speed satellite link. On the other end of the satellite link another SentryPoints node bridges the satellite link to the wired LAN of an Incident Command Post. This provides seamless connectivity from the mobile team to the command post, allowing situational awareness and command and control.

Figure 3 shows a multiple agency municipal deployment connecting, for example, police, fire, and public works to a command center.

In a municipality police and fire units often use 800MHz radio systems and have at least some level of voice interoperability. As shown above, a SentryPoints system can be connected to that 800MHz system and bridge data to a crisis center. Likewise, public works vehicles, such as dump trucks and snow plows may be equipped with GPS capable cell phones. These too are bridged to the crisis center. During a crisis this allows coordination of the multiple agencies from a single center.
Figure 4 shows connecting a user on the ground at a disaster site to the World Wide Web.

Relief workers on the ground at a situation may have cell phones with GPS and wireless data capabilities. These cell phones report the position and status of the workers over the cellular data network. A SentryPoints system takes that information and bridges it onto a satellite link to another SentryPoints system located where Internet connectivity is available. This SentryPoints system also acts as a web server, so that authorized users may connect to it and see the situational awareness data provided from the workers on the ground.

VIII. Pros/Cons of potential SentryPoints use in disaster relief/Homeland Defense crisis scenarios

This paper has attempted to summarize the myriad issues surrounding the thorny issue of how to rapidly achieve voice and data interoperability in disaster and crisis response scenarios. Significant field testing of the basic concepts behind the SentryPoints application repeatedly demonstrated the ability to link widely disparate radio systems into a common network with any node able to communicate with any other node regardless of the type of radio used.
This is achieved through the insertion of SentryPoints software where applicable and the addition of next generation MINC devices where needed. The result is a homogenous mixture of multiple voice and data paths supporting data exchange in widely varying formats. SentryPoints pulls this together at the command center level, either at static Emergency Operations Centers activated in response to crisis, or at mobile ad hoc command centers operated by the first responder units to arrive on scene.

The flexibility of the SentryPoints approach allows all responding agencies to continue to operate their existing communications infrastructure, but with the addition of some small code insertions and MINC devices where required based on radio types. This does not mean that all agencies would have to have SentryPoints/MINC capability in their “tool bag”. It does mean that at some level, perhaps at state or federal emergency response teams would have some pool of these devices to issue when required to allow all units to interoperate.

Pro’s of such a configuration:

1. Agencies would continue to use existing communications infrastructure.
2. Insertion of SentryPoints/MINC capability is easily achieved at deployment.
3. Agencies could use only what components they need without having to purchase the “full package”.
4. Cost of SentryPoints/MINC deployment is several orders of magnitude less than complete restructuring of communications infrastructure.

Con’s of such a configuration:

1. A decision would need to be reached as to who and where such a repository of such devices would exist. Should this be at the local, state or federal level, or some combination?
2. Institutional resistance to “one more solution”.
3. Cost of providing this capability to “everyone” may be more than some local budgets allow.

Our experience over the past ten years with this developing technology can be summed up in the simple phrase “it works”. This has been demonstrated in military field exercises in very complex communications environments that eventually linked the following components into a common data network:

- HF radios
- VHF/UHF Line-of-sight radios
- SATCOM radios
- Squad Tactical Radios (handhelds)
- Wired LAN’s
- Wireless (802.11) LAN’s
- Wired phone (modem connection)
- Cellular phone (modem connection)
- Satellite phone (Iridium modem connection)

There are few other systems in operation today that can immediately link all these disparate communications paths into a common network such that any node using one type of communications device can rapidly exchange data with any other node using other communications devices. This is true interoperability at the transport to application layer. It is already in use in a limited fashion by the State of Indiana and is immediately ready for consideration for use on a wider basis for crisis response.

Therefore we believe SentryPoints and its associated next generation MINC device offer a ready solution to the three main issues raised at the beginning of this paper. They are:

1. Provide adequate spectrum for first responders: The SentryPoints/MINC solution actually extends the available spectrum for first responders by allowing all users to maintain their existing RF systems while linking them together. This provides significant cost benefits against considering total infrastructure reconfiguration.

2. Establish a Unified Incident Command System: SentryPoints is already in the process of automating the message formats in the National Interagency Incident Management System. This would allow all users to instantly exchange data in NIIMS formats recognized by all. It also would allow these NIIMS formats to be translated quickly into other existing C2 systems and delivered in that native format. The end result is a unified interoperable data exchange infrastructure.

3. Allocate homeland defense funds based on risk and vulnerability: We believe the SentryPoints/MINC option offers a cost effective way to rapidly achieve functional interoperability across the total spectrum of crisis response communications while avoiding massive budget outlays for full infrastructure replacement.

References


