

APPLICATIONS OF NETWORKING CAPABILITIES TO ASSIST IN SITUATIONAL AWARENESS

Jason M. Hunter
Timothy Matlack
Kevin G. Schweer
Myong S. Sung
Thomas E. Ward
Altaf S. Bahora
Steven C. Davis

Dr. Barry M. Horowitz
Department of Systems and Information Engineering
University of Virginia
Charlottesville, Virginia

David Drescher
Daniel Park

RoamSecure, Inc.
Arlington, Virginia

Daniel Spar
Michael Sullivan

Institute for Defense Analyses
Alexandria, Virginia

ABSTRACT

Situational awareness is a primary concern in emergency response and military urban operations. The need for situational awareness in emergency response applications can be addressed through the use of RoamSecure Alert Network (RSAN) servers utilizing peer-to-peer technology for inter-jurisdictional integration. Linking RSAN servers from different jurisdictions will enable them to communicate with each other more effectively, automatically synchronize group lists and manage messaging permissions. In military urban operations, the application of wireless technologies will allow the military to provide soldiers with mission-critical information gathered from distributed sensors. The implementation of a secure peer-to-peer network over commercial wireless technology will provide the military with a secure ad-hoc solution for urban operations. The use of peer-to-peer networking in emergency response and urban operations can provide pertinent information to users in order to improve situational awareness.

1 INTRODUCTION

Making good decisions can often mean the difference between life and death. In order to make critical decisions, people must be able to assess their current situations and have access to pertinent information that addresses variables upon which these decisions are based. By increasing situational awareness, individuals are able to make decisions faster and more effectively. This is especially important in emergency response and military operations, where time and quality information are of the essence.

Through the use of peer-to-peer networking protocols, such as HyperCast and wireless networking technologies, situational awareness can be improved in these areas. These technologies can facilitate the creation of dynamic and mobile networks. However, these networks are only useful if implemented with security in mind. Security can be achieved through proper authentication, encryption, and network monitoring.

The ad-hoc nature of urban operations may limit deployment of physical infrastructure. Wireless technology addresses this problem by allowing for the transmission of data without a physical connection. Therefore, wireless technology enables increased information-sharing on the battlefield and allows for the integration of distributed data management among wireless alerting servers.

2 EMERGENCY RESPONSE APPLICATION

2.1 Wireless Alerting Problems

Emergency response departments throughout the D.C. metropolitan area utilize the RoamSecure Alert Network (RSAN) to distribute wireless alert messages. RSAN is a system used to facilitate the sending of wireless alerts to mobile devices (cell phones, pagers, etc). Currently, RSAN is capable of sending out text-based alerts to the wireless devices of user-defined groups over the system. The system, however, does not allow for any communication between independent RSAN servers. For example, the Arlington Emergency Response department groups cannot access alerts sent out from the Fairfax Emergency Response department. As more jurisdictions adopt the RSAN

system, there will be issues of scalability, configuration, and management of the system.

2.2 Initial Solution Design

RoamSecure proposed to implement a client-server architecture to integrate user groups and alert messages across RSAN servers in different jurisdictions. This design uses encrypted email to store and transmit the alerts between jurisdictions. The primary disadvantage to this setup is the lack of automated group management. When a new RSAN server wants to send wireless alerts to other jurisdictions, a user must manually configure all the group information on the RSAN server that he or she wants to communicate with, as well as enter that group's information on those remote servers. As the number of RSAN servers increases, this task becomes increasingly difficult. The process of manually updating servers is initially time consuming, and the cost of automating this process will outweigh the benefits as more RSAN servers are added in the future.

2.3 Peer-to-Peer Approach

In relation to this project, a peer-to-peer solution has many advantages over a client-server model. In a true peer-to-peer system, no single authority has total control over all aspects of the system. Table 1 explains the pros and cons of both possible architectures for a new system.

Table 1. Pros and Cons Comparison

Peer-to-Peer		Client-Server	
Pros	Cons	Pros	Cons
<ul style="list-style-type: none"> • Highly scalable • Robust to failures • Dynamic re-configuration of network 	<ul style="list-style-type: none"> • Evolution cannot be reproduced • Security more difficult to ensure and control 	<ul style="list-style-type: none"> • Evolution can be reproduced • Single-point administration • Easy data collection / analysis • Easier to maintain security 	<ul style="list-style-type: none"> • Less scalable • Has a single point of failure

The major drawback to a client-server architecture is that it lacks scalability. Since RoamSecure has a growing client base, utilizing this architecture could create a bottleneck in the future and slow down RSAN integration until a new solution is adopted.

HyperCast, a peer-to-peer communication framework developed at the University of Virginia, builds and maintains logical overlay networks for multi-casting information between members of that overlay. An overlay network is a virtual network that is implemented on top of a network of routers and links. Each logical link of the virtual network consists of a complete end-to-end unicast route. Examples of overlay networks in the Internet are the MBone, virtual private networks (VPNs), and peer-to-peer networks. Nodes in the overlay network can be hosts,

routers, servers, or applications. HyperCast also provides support for data transmission between applications in the overlay. Applications self-organize into a logical overlay network, and transfer data along the edges of the overlay network using unicast transport services. Each application communicates only with its neighbors in the overlay network. Using the overlay, services for one-to-many transmissions ("multicast") and many-to-one transmissions ("incast") are relatively simple to provide (*HyperCast Website*). HyperCast will also soon include the ability for fully encrypted point-to-point, multicast, and incast communications.

HyperCast utilizes a light-weight Delaunay Triangulation (DT) server to construct and maintain the structure of a logical overlay. The DT server maintains the network by restructuring it when nodes enter or leave; it plays no part in the actual transmission of messages. The use of a single DT Server for overlay maintenance imposes minimal resource constraints on the network.

A major concern in adopting a peer-to-peer approach for RSAN integration is the usage of open ports on the individual servers. Typically, a larger number of open ports means increased security risks. A basic solution for RoamSecure would be to open a port for each overlay on the network; however, in a large scale system, this could result in hundreds of open ports. This issue raises the need for an architecture that can utilize one central overlay, such that only one port on each server needs to be opened.

In a peer-to-peer approach, both servers and groups can be added or removed dynamically from the system. The system also allows for complete automation of background functions and can utilize a visual interface since it will be integrated into the existing RSAN application. The system is scalable and will remain stable even with the addition of large numbers of RSAN servers.

There were several different architecture designs that were considered in creating a network of RSAN servers with group subscription and group management capabilities. The following sections describe the advantages and disadvantages of each of these architectures.

2.3.1 Architecture 1: Peer-to-Peer Group-based Design

In this design, every RSAN server runs a separate DT server for each group that wants to use the remote messaging feature. A remote group that wants to receive messages from a local group subscribes to that group's HyperCast overlay. If a group wants to receive messages from three groups, it must be a member of three overlays. Messages from a given group are then multicast out on that group's overlay. Because only remote groups wanting to receive messaging from that group are subscribed to the overlay, only the intended recipients receive the message.

Administration of the various overlays is handled through an all-inclusive overlay.

There are four major advantages to this architecture. First, because all communication is done via multicast, there is no wasted bandwidth. Secondly, groups only receive messages specifically intended for them. This addresses a serious security concern wherein potentially sensitive alert messages are received by unauthorized users. The system also supports both adding and removing groups dynamically and has no single point of failure due to its decentralization.

The major drawback to this plan is the large number of overlays it requires. Because each overlay requires an open port on both the DT server host and all subscribing computers, there could potentially be hundreds of open ports on RSAN host computers. Additionally, these ports need to be opened and closed dynamically, which may be unacceptable to security administrators at most companies or government agencies using firewalls. Also, using a small number of nodes on each overlay is does not take advantage of the scalability of HyperCast.

2.3.2 Architecture 2: Server-based Peer-to-Peer and Client-server Hybrid Design

This design combines a peer-to-peer messaging network with a client-server-based group management system. Each RSAN server hosts a single DT server, and a remote group wanting to subscribe to a given RSAN server's local groups subscribes to that server as a whole. As before, all administrative traffic is sent through a separate, all-inclusive overlay hosted by RoamSecure, but unlike Architecture 1, overlay subscriptions are done at the server level instead of the group level. RSAN servers receive messages from the various overlays to which they are subscribed and distribute the messages internally to the intended groups.

Group management is handled by the client-server part of the system. A master list of all RSAN servers and their groups is kept in a database on a central server maintained by RoamSecure. This server is connected to the all-inclusive overlay, which it uses to collect and distribute changes to the database.

This architecture was designed to address some of the problems raised by the previous design. First, because each RSAN server only hosts a single DT server, it is only necessary for one port to be open to incoming traffic. Also, since the server-level overlays are not created dynamically, the port does not need to be opened and closed dynamically. These improvements were made while still maintaining the benefits of Architecture 1. Servers and groups can still be added and removed from the network dynamically, and because HyperCast 3.0 includes support for encryption, there is no concern for unauthorized message distribution. The centralized group management database does provide a single point of failure but at the same

time creates an easily accessible master list of all servers, groups and the various remote messaging permissions associated with them. Also, it provides a convenient means of compiling a history of all alerts sent via the remote messaging system.

The primary drawback to this design is its complexity. Multiple overlays are difficult to manage, particularly in regard to DT server redundancy. The centralized group management system is a tradeoff between the benefits described previously and the drawback of introducing a single point of failure. However, the centralized design can easily be replaced with a distributed one that does not have such a weakness.

2.3.3 Architecture 3: Single-overlay Peer-to-Peer and Central Server Hybrid Design

Architecture 3 uses a single HyperCast overlay for all communications, including both message and administrative traffic. Like the all-inclusive administrative overlay in the previous designs, Architecture 3's single DT server for this overlay is hosted on a RoamSecure computer, with optional redundant backups. Overlay subscriptions are once again done at the server level instead of the group level, so if any group on an RSAN server wants to participate in remote messaging, that whole server joins the overlay. As in Architecture 2, messages are sent between servers using HyperCast and then distributed locally by the receiving server. Group management is the same as in Architecture 2, including the option to make it centralized or distributed. Essentially, this design is the same as the previous except without the unnecessary complexity of separate overlays for each RSAN server.

This architecture has a number of positive features. First, because there is only one DT server for the entire system, only one port needs to be open. This is an improvement over both the previous architectures. In this case, the RSAN servers do not have to host any DT servers so there is no concern about overusing system resources. Additionally, having a large number of nodes on a single overlay is consistent with HyperCast's original design. Furthermore, messages can be sent using either the point-to-point transfer to assure only the intended recipient receives the message or multicast with encryption.

The only drawback to this design is the central DT server used to maintain the overlay. However, as before, creating backups for this server solves this problem.

2.3.4 Architecture 3 Variation

A variation on Architecture 3 was considered in which overlay subscriptions are done at the group level instead of the server level. This eliminates the need for RSAN servers to distribute messages received from HyperCast but in-

creates the number of HyperCast nodes that must be running on each RSAN server.

2.4 Proposed RSAN Network Architecture

The proposed design closely follows Architecture 3, including the option to use a distributed group management system. The primary program logic was developed in Java because the HyperCast API is also written in that language. However, because the program will eventually be integrated with existing RSAN software, the rest of the project was modeled after that system. The group management and permissions database uses MySQL and builds off tables in the existing RSAN database, and the interface for remote messaging is written in HTML.

2.5 Software Logical Design

Adding a new RSAN server to the HyperCast remote messaging network requires a multi-step process. First, the new RSAN server connects to the central DT server, which incorporates it into the HyperCast overlay. It then multicasts its group list to all other servers on the overlay, which respond by sending point-to-point messages containing their respective group lists. The existing servers then add the new server's group information into their databases, and the new server creates and populates its own database. Figure 2 is a representation of how all the RSAN servers are connected over a single overlay hosted by the central DT server.

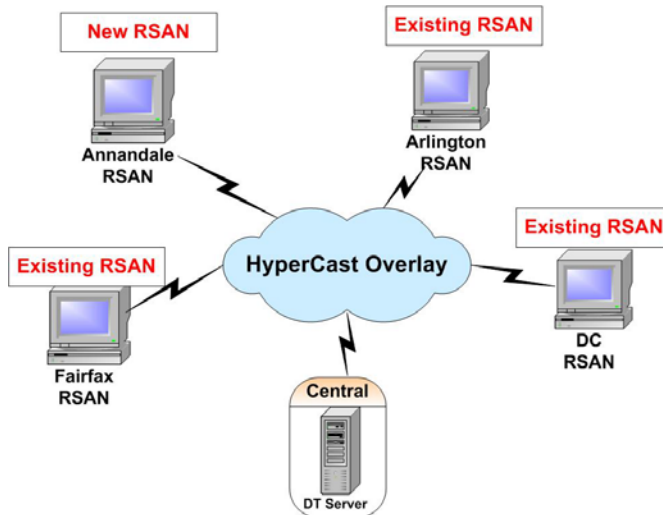


Figure 1. RSAN Overlay Diagram

Each RSAN server maintains a MySQL database with a list of all remote groups on the remote messaging network and each of these groups' relationships with that server's local groups. Whenever a change is made to any server's database, an update is sent as a multicast to the

other servers on the network via HyperCast to synchronize group access information.

2.6 Interface Design

The code behind RSAN is written primarily in PHP and Perl. These languages do not provide support for access to pre-defined Java classes. Since the HTML interface must interact dynamically with my MySQL databases and Java functions, it must be coded in a language that allows these interactions. Thus, the interface must utilize JavaScript functions that are created directly from Java classes that access the database.

Servlets are well-suited for integrating Java interfaces with HTML. The proposed interface will make calls to a Java servlet, which will allow communication between the interface and the MySQL databases.

The visual interface, shown in Figure 3, will give the user all information necessary to subscribe to alerts sent from other groups. It displays information such as the currently selected local group, remote server, and the available groups for the remote server. From here, the user can select the groups he/she wishes to subscribe to, and can then click a button to subscribe to the groups.

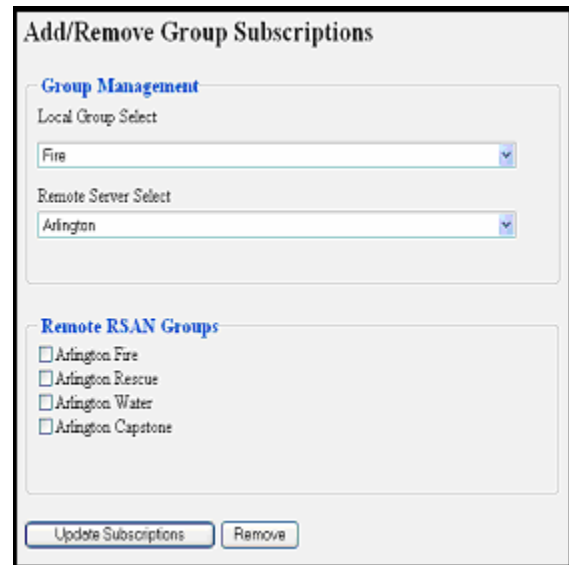


Figure 2. Group Subscription Interface

Some groups may not want other groups to have access to the alerts being sent. For this reason, the software needs to have the capability to set access permissions for their own groups. Since these functions are similar to those of the subscriptions page, a very similar page can represent the access settings. The user can simply check the boxes of the remote groups he/she wishes to provide access to.

2.7 Peer-to-Peer RSAN Network

RoamSecure proposed that utilizing an integrated central server would facilitate inter-jurisdictional communications. The client-server architecture's reliance on a central database to facilitate all inter-jurisdictional communication provided a convenient way to store the alert messages from each jurisdiction in a central location. Security was a major issue with this design due to the storage of potentially sensitive data on the central server. This introduced the need for a new networking protocol that will allow data to be sent securely, without anything being stored on a central server.

Using HyperCast as a framework to create a group-management feature for RSAN will allow users to view alerts from other RSAN servers. Using the proposed interface as the front-end, all current RSAN users will have the ability to add, remove and manage subscriptions to remote group messages. This is a scalable solution because HyperCast can service a large number of RSAN servers.

The improved remote messaging and group management capabilities in this solution enhance RSAN's ability to improve situational awareness for both government agencies and the general public. With this system, groups can share information across jurisdictional boundaries that would not otherwise be available to departments of other counties. This sharing will be done over an encrypted HyperCast network to ensure the security of potentially sensitive messages.

3 URBAN OPERATIONS APPLICATION

3.1 Problem Definition

Situational awareness is an ever-present problem in military operations. For years, the scope of battle has revolved around the traditional battlefield. In recent years, however, the focus has turned to the urban terrain.

Military operations on urban terrain are complex. The urban environment is located in areas where the enemy is often unknown, can be hidden, or where the soldiers' view is often obstructed. Operations in this scope involve more than just fighting – they involve peacekeeping and support operations as well. Therefore, any additional insight into situational awareness may help to prevent casualties and collateral damage.

United States and Coalition Forces are presently being killed and/or injured almost daily in Iraq. Since the beginning of the war, over 500 soldiers have died from accidents and hostile fire. As seen in Table 1, nearly two-fifths of the deaths that have occurred in Iraq have been the result of several different types of hostile attacks. While the statistics do not include all of the deaths that have occurred, there are two intriguing statistics located in the table: the

deaths caused by improvised explosive devices (IED) and the deaths caused by ambushes. These two statistics reflect a lack of situational awareness in the urban environment.

Table 2. U.S. Casualties in Iraq [Source: lunaville.org]

Item	Total	Percent
Hostile - hostile fire - IED attack:	96	17%
Hostile - hostile fire:	71	13%
Hostile - hostile fire - ambush:	38	7%
Hostile - hostile fire - RP grenade:	27	5%

Situational awareness of the common soldier can be increased with new sensors for helping soldiers recognize dangerous situations. With the assistance of wireless networking technology, soldiers will be able to obtain the relevant information from the sensors. Therefore, by exploring scenarios and developing alternatives utilizing wireless technology, future casualties and collateral damage may be reduced.

3.2 Distributed Sensor Networks

A smart sensor network is an ad-hoc network of sensors spread across a geographical area. These networks are used in surveillance systems, detection systems, and monitoring systems. According to the National Institute of Standards and Technology (NIST), there are four common applications for which smart sensor networks are used. These applications are to determine the value of a parameter at a given location, to detect an event, to classify an object, and to track an object.

Through the use of distributed sensor networks, the military will be able to collect sensitive data pertinent to mission critical applications. This data can be fed to a centralized source or to an analyst for further evaluation. Once this data is analyzed by an outside source, the source will be able to alert the appropriate military personnel to situational developments in their geographical area.

3.3 Wireless Technology

In order to use the data collected by distributed sensor networks, a method of transmitting information to an outside analyst must be established. This is accomplished through the implementation of wireless networking technology. Wireless networking allows for the transmission of data through radio frequencies.

There are several protocols and standards that currently exist for wireless networks, and these include the 802.11 standards, Bluetooth, and infrared technology. While Bluetooth and infrared technologies are implementations of wireless, there is limited support and structure

available for them. The 802.11 standard, developed by The Institute of Electrical and Electronics Engineers (IEEE), provides the basis for all structured wireless technologies. By making use of transmission, security, and bandwidth protocols, this standard is the most acknowledged standard for wireless networking. However, current wireless security implementations are not sufficient for military use. These implementations lack the necessary security required for military operations.

3.4 Wireless Security

Since wireless security is a paramount concern for the military in any solution that is developed, a thorough analysis of current commercial technologies must be performed. Wireless security products can be broken down into three categories: (1) authentication/access control, (2) monitoring and intrusion detection, and (3) encryption. Therefore, a successful evaluation into existing commercial solutions will be representative for the above categories.

3.4.1 Analysis of Authentication

Authentication ensures that only authorized users gain access to a network and prevents potential intruders from tampering with the system. IEEE's 802.1x is the standard for authentication within a wireless network. It supports several commercial authentication methods for the authentication of a network. Most of the protocols fall in the Extensible Authentication Protocol (EAP) family, including the Protected EAP (PEAP), Lightweight EAP (LEAP), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), and Simple Password Encrypted Key Exchange (SPEKE). Of these technologies PEAP and TTLS are stronger because they provide for an additional layer of security through tunneling, and they allow for fast re-authentication.

3.4.2 Analysis of Intrusion Detection

Monitoring and intrusion detection are important characteristics for a secure wireless network in order to make sure that the network remains secure. Monitoring and intrusion detection ensure that security policies remain in use and alert system analysts to potential attacks occurring on their network. Important features of wireless overlay monitoring systems are to detect the presence of a rogue network, to detect ad-hoc networks being established, and to enforce authentication and VPN use. Also, it is important that these monitors actively detect possible Denial of Service attacks, authentication attacks, and MAC address spoofing.

3.4.3 Analysis of Encryption

Encryption ensures data privacy and integrity. By encrypting data, outside users are unable to read or alter the contents being passed through a network. NIST has chosen AES as its standard encryption algorithm. Its 128, 192, or 256-bit encryption key makes it a longer key than many of its competitors. The increased complexity of the algorithm makes it harder to crack than other encryption algorithms. It has strong integrity checking, more encryption rounds, and filters out weakly-encoded packets to help prevent replay attacks.

3.5 Key Findings

Authentication, monitoring, and encryption are the foundation of commercial security. This foundation allows for the development of solutions that make use of third-party components and standards. However, commercial security solutions that are currently available are often based on centralized systems. These systems are not flexible or scalable enough for urban operations deployment. Many commercial solutions are based on positioned access points and are intended to work over a small geographical area.

While wireless security has significantly improved over the last few years, and new solutions are on the horizon, current commercial solutions are not easily applicable to ad hoc networks. Since most solutions depend on centralized administration with centralized directories of access permissions for distributing information, these solutions do not allow the mobility required for urban operations. However, through building new ad hoc configurations with peer-to-peer protocols such as HyperCast, a standards-based solution can be developed to secure ad hoc wireless networks. The use of HyperCast will allow for authentication to be controlled by the members of the peer-to-peer networks. This control will eliminate the need for centralized authentication servers. Additionally, HyperCast configures fast dynamic networks, which is useful in urban operations. By developing security configurations and applying them on top of ad hoc networks, security can be provided for the urban environment.

3.6 Operational Scenarios

Once security has been ensured, wireless applications can be used in urban terrain. The following problems arise from the urban environment that work to limit situational awareness:

- Limited sight into the battlefield
 - Short ranges of intervisibility
 - Presence of manmade structures
 - Multidimensional terrain
 - Dense Vegetation

- Limited ability to communicate among units within the battlefield
- Limited ability to shoot into the urban terrain
 - Difficult Target identification in engagement areas
 - Presence of non-combatants
 - Restrictive Rules of Engagement

Thus, the following example scenarios were developed and evaluated in order to address situational awareness for the common soldier.

3.6.1 Scenario 1: Excess Number of Civilians in a Target Identification Mission

In this scenario, a group of Special Ops forces are assigned to detain and capture a suspected terrorist individual. They are given intelligence pinpointing a precise location where the suspected terrorist is located. Once arriving at that location, the soldiers notice that there is a peaceful demonstration with nearly 100 people occurring in the street. Additionally, the building where the terrorist is located is filled with people.

The above situation presents the Special Ops forces with a few hurdles. Due to the large number of innocent non-combatants in the area and the possibility for combatants to be present, the soldiers need assistance in locating the terrorist and ensuring the safety of others as well as their own safety. To increase the situational awareness of the environment, they immediately set up a wireless network and disperse miniature cameras throughout the street/building. These cameras can either be placed out in the open or in non-descript locations.

In a separate location, central command analysts will watch the video feed and any other information being fed to them. These analysts will assist the soldiers in identifying the target and/or alerting them to possible hostile situations.

3.6.2 Scenario 2: Movements through a highly vegetative, poor line-of-sight area

A new uncontained area is about to be explored within the city. This area is one of the most vegetated in the city and contains many large buildings and obstructions that could house potential combatants. Therefore, approximately 30 to 40 minutes before the forces are to arrive in the city, central command authorizes the drop of a distributed sensor network into the new area. This drop is done by unmanned aerial vehicles (UAVs) and other aerial craft.

There are several types of sensors that may be dropped including unmanned ground scout vehicles (UGV), explosion sensors, cameras, audio sensors, and toxic industrial material (TIM) sensors. The chemical and explosion sensors would work to assess the total environment and the

location of possible weapons within the area. The purpose of the cameras and audio would be dual – working to assess the presence of combatants before their arrival and helping with situational awareness when the forces enter the area.

In addition to the uses of wireless technologies in these scenarios, other applications such as a global positioning system (GPS), infrared cameras, and audio recording devices can be incorporated into a wireless sensor network. These devices could assist in peace-keeping operations, joint operations, and subterranean access missions.

4 CONCLUSION

Through the use of peer-to-peer networking protocols, such as HyperCast, and wireless networking technologies, situational awareness can be improved in emergency response and urban warfare applications. Improved situational awareness will allow people to have more information about their current surroundings, which could lead to better decision making.

The use of HyperCast facilitates alert message management and distribution. The developed system for emergency responders allows for automatic group and database synchronization and distribution of wireless alerts across jurisdictional boundaries. By allowing informational sharing across jurisdictional boundaries, emergency response groups will be able to receive information pertinent to their own jurisdiction. This information sharing will increase shared situational awareness and will help to reduce latent communications in critical emergency response situations.

In urban operations applications, the use of wireless networking technologies will provide assistance by increasing situational awareness of the common soldier. These soldiers will be able to gain access to pertinent information in real time, in order to aid in decision-making. Distributed sensor networks will provide outside analysts with the information necessary to make these mission critical decisions. Additionally, the integration of HyperCast networking and ad hoc security with commercial wireless technologies can create a secured solution for increased situational awareness in urban operations.

REFERENCES

- Army Science Board. Group Presentation. November 2003.
- Boristov, Nikita, et al. "Security of the WEP Algorithm" Available Online via www.isaac.cs.berkeley.edu/isaac/wep-faq.htm [Accessed November 20, 2003]
- Multimedia Networks Group. HyperCast. University of Virginia Department of Computer Science. Available

online via <www.cs.virginia.edu/HyperCast> [Accessed October 15, 2003]

Iraq Coalition Casualties. Available Online via <www.lunaville.org> [Accessed December 4, 2003].

Molta, Dave. "Wi-Fi vs. Bad Guy". Network Computing. 4 March 2004. Vol. 15, pp.36-58.

National Institute of Standards and Technology. Project: Wireless Ad-hoc Networks. Available online via <w3.antd.nist.gov/wctg/manet/> [Accessed March 19, 2004]

Stanek, William (1996). Peter Norton's Guide to JAVA Programming. United States of America: Macmillan Computer Publishing.

U.S. Army. Army Field Training Manual 3-06. 2000.

U.S. Army. "5-3. FOC-05-03: Operations in Urban and Complex Terrain." Manuscript.

BIOGRAPHIES

JASON MICHAEL HUNTER is a fourth-year majoring in Systems and Information Engineering at the University of Virginia, specializing in Computer and Information Systems. Additionally, Mr. Hunter has minored in Computer Science. He is from Fairfax, VA. For this project, he worked on developing the interface for the HyperCast system. Mr. Hunter will be working for Capital One in McLean, VA upon graduation.

TIMOTHY MATLACK is a fourth-year majoring in Systems and Information Engineering at the University of Virginia and concentrating in Economic Systems, with a minor in Economics. Mr. Matlack is from Yardley, PA. In this project, he worked on analyzing commercial security products to recommend a secure wireless solution. After graduation, Mr. Matlack plans to return to Pennsylvania to work.

KEVIN GREGORY SCHWEER is a fourth-year majoring in Systems and Information Engineering at the University of Virginia, specializing in Computer and Information Systems. Additionally, Mr. Schweer has minored in Computer Science. He hails from Stafford, VA. For this project, he worked on developing alternative scenarios for urban warfare and analyzed the security flaws associated with current wireless standards. Mr. Schweer will be working for Solers, Inc in Rosslyn, VA upon graduation.

MYONG SUNG is a fourth-year majoring in Systems and Information Engineering at the University of Virginia and specializing in Computer and Information Systems. Mr. Sung is originally from Richmond, VA. For this project, Mr. Sung created the HyperCast DT server infrastructure and aided in the development of Java servlets. Next year, Mr. Sung will be completing his master's degree in Systems Engineering.

THOMAS EDWIN WARD is a fourth-year majoring in Systems and Information Engineering at the University of Virginia and concentrating in Computer and Information Systems. Mr. Ward is from Arlington, VA, yet used to live in Tokyo, Japan. For this project, Tom developed the back-end database work. Next year, Tom will be working for CGI-AMS in Fairfax, Virginia.

ALTAF SHABBIR BAHORA is a graduate student in Systems and Information Engineering at the University of Virginia pursuing a Master of Science degree. Mr. Bahora received his B.S degree in Systems and Information Engineering with an emphasis in Computer and Information Systems at the University of Virginia in 2003. Mr. Bahora is from Nashville, TN.

STEVEN CLARENCE DAVIS is a graduate student in Systems and Information Engineering at the University of Virginia, pursuing a Master of Science degree. Mr. Davis received his B.S degree in Systems and Information Engineering with an emphasis in Computer and Information Systems at the University of Virginia in 2003. Mr. Davis is from Elkton, VA.

DR. BARRY HOROWITZ is a Professor of Systems and Information Engineering at the University of Virginia. He joined the faculty in 2001, after an industrial career involving the application of systems engineering to many large and complex systems. From 1969 through 1996 he was employed in a variety of positions at the Mitre Corporation, including the last five years as President and CEO. Dr. Horowitz received an MSEE and PhD from New York University in 1967 and 1969 respectively, and a BEE from the City College of New York in 1965. He can be reached at <barrymhorowitz@virginia.edu>.