Hypercast Implementation for PTDS
- Final Report

R. Jones, J. Wang, B.M. Horowitz
University of Virginia
December, 2006

1. Introduction

The convergence of current and emerging technologies presents the opportunity to provide innovative, intelligently tailored role-based communication architectures allowing information exchange between personnel, sensors, and databases. This is driven in large part by the evolution of the Internet, the continuing commoditization of highly portable computing devices (laptops and PDAs), and growing industry support of open source software and standards (SOA, XML, UDDI, etc.). This has and continues to enable the creation of complex and highly customizable systems utilizing inexpensive components. These changes, coupled with advances in wireless communication and Peer-to-Peer (P2P) technologies, provide a foundation for the development of a flexible, reconfigurable, and relatively low-cost infrastructure to support information exchange in rapidly changing environments.

In this document we present the UVA efforts towards the development of the Persistent Threat Detection System (PTDS) according to the requirements in the document "Statement of Work (SOW) for Hypercast Implementation for PTDS" (See Appendix). The discussion of UVA efforts includes the concept of operation and architecture to enable dynamic and flexible information acquisition and sharing among all participants, as well as the development of a prototype system that facilitates the construction of information sharing groups over a heterogeneous network environment based on user selected variables, such as rank, job, geographic location, etc.

The proposed concept of operation addresses the challenge of how to develop a dynamic system for creating and managing the sharing of information among various units: including sensor networks, databases, commanders, Tactical Operation Centers (TOC), and CONUS personnel. In addition information exchange should not be hindered by differences in facilities, equipment, protocols, or procedures of the parties involved. To address these problems an information management architecture will be discussed which addresses the information needs of disparate Army units in a way that transcends their inherent organizational, procedural, and technical differences while allowing for rapid adaptation to changing circumstances. Figure 1 shows the scenario of desired information exchange.

The proposed architecture aims at achieving the following goals:

- Facilitate the creation and management of groups of users and information services to support the transparent sharing of information among those users with common information needs.
- Allow omni-directional information flow: recognizing that every actor in the system should be capable of serving as both a consumer as well as a provider of information to others.
- Permit the heterogeneous communication infrastructure to be rapidly deployed, expanded, and contracted as needed.
- Provide flexibly designed information services to meet the needs of users with dissimilar levels of technical skill, analytical capabilities, and requirements.

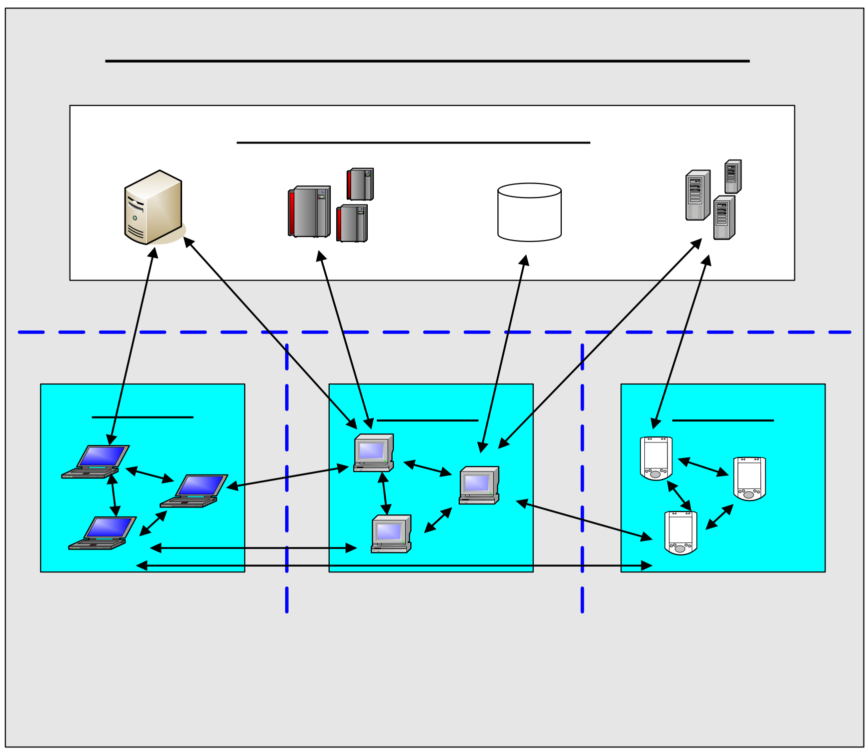

Figure 1. Flexible information exchange

2.Technology Components

Hypercast

Hypercast is a networking software for building large-scale P2P networks containing thousands of members. Hypercast, developed at the UVA, aims at fast deployment of ad hoc P2P networks or overlays. Hypercast is an application layer protocol that works on top of different physical networks such as Local Area Network (LAN), mesh networks, or an 802.11 wireless network. Hypercast also supports dynamic joining and leaving of entities/users and self-recovery from partitions. Hypercast protocol accomplishes this by constructing a logical network topology: Delaney Triangulation (DT), Hyper Cube (HC) or Spanning Tree (SPT) topology. In wired networks, DT protocol is mostly used. In wireless networks, SPT protocol is more suitable due to the radio range limits of the devices. For detailed information on Hypercast please refers to [1] [2] [3] [4].

Service Oriented Architecture

Service Oriented Architecture (SOA) is an industry driven software design and development concept that emphasizes the reusability, interoperability and flexibility of software, is adopted into our system design. The integration of SOA and P2P networking technology, such as Hypercast, creates a new methodology for building rapidly reconfigurable systems over heterogeneous networks. This new methodology (1) allows easy integration of systems constructed on dissimilar hardware and software platforms; (2) enables the inoperability between users with different capabilities and authorities in a standardized way; (3) fills the gap between existing and upcoming new commercial and enterprise technologies.

XML message

All the messages exchanged in the system, except the messages sent in raw formats due to performance reasons (e.g. video and audio streams), are sent as XML (Extensible Markup Language) messages. XML is a platform independent language and is widely accepted by the commercial and industry world. Using XML message makes it possible to unify the interfaces of entities and standardize the creation and processing of all messages. In addition, it reduces the efforts on integrating existing commercial software.

2. System Architecture

The architecture proposed in this section is for building an autonomic system, which has clearly defined tasks and runs independently over heterogeneous networks. Multiple autonomic systems can form a hierarchy of information sharing through their management components using the technology described here. In such an autonomic system, the following components are defined:

Administration Component

Each autonomic system contains an administration component that is in charge of the management of the system; the authentication of users, including service providers and service subscribers; and the intercommunication with other autonomic systems. It is well known to all components in the system.

In the system all services are registered by service providers to the Administration Component, becoming available to all participants. In the cases of information exchange groups constructed based on rank, job, or geographic location, each player is a service provider and subscriber simultaneously. The first player coming to the system executes the service registration task.

Information Exchange Groups (IXGs)

An IXG is a logical grouping of information providers and consumers that facilitates the flow of information among the members of an IXG. Specifically, it is a P2P communication group established over heterogeneous networks (fiber, Ethernet, 802.11, etc). Each autonomic system will use IXGs for organizing its users and information services. For example, if there exists a database of information (e.g. geographical information of a city) and there are several soldiers, all of whom may or may not be utilizing the same communication equipment and all of whom desire to access the information stored at the database, than the Administration Component would set up an IXG to provide the soldiers with access to that database: even if all of the soldiers have different communication equipment.

As such each autonomic system will have a suite of tools to assist in the creation and management these IXGs. Such tools will allow the architecture to be flexible in allowing end users to also create and join IXGs on-demand.

The Universal Information Exchange Group (UIXG)

In order to facilitate the creation of IXGs a mechanism is needed to coordinate the various users and communication infrastructures involved. The mechanism for this will be the Universal Information Exchange Group (UIXG). This is a special IXG that will be used as the default communication channel for all users operating within the purview of a particular autonomic system. All users will know how to join the UIXG, and once a connection has been established to the UIXG, users can then join specialized mission and task-specific IXGs for tactical information exchange. Finally, users will be continuously connected to the UIXG.

The Information Service Registry (ISR)

The ISR is an important entity in the autonomic system. It will serve as a central repository of metadata about the information services available to users within the UIXG. The ISR will contain all of the information needed by a user to make use of available services, such as:

- The computer address of the information provider
- Protocols or applications required
- Security restrictions
- Device capabilities and bandwidth requirement
- User-customizable features of the service.

Customizer

Participants of the autonomic system will posses a myriad of capabilities and responsibilities, which add constraints on the quality and contents of the services they can consume. To bridge this gap between information service providers and information subscribers, the concept of Customizers is introduced. Customizers are located at the border of two networks formed with different physical medias or administrative domains. They not only execute the information conversion between different networks, but also fulfill the conversion/customization of service contents between service providers and subscribers based on the capabilities and responsibilities of the subscribers. This allows for increased flexibility in service providing and information sharing group organization.

For example, when new users or new sub-groups with customized communication hardware and software want to join the autonomic system, it will determine the function of the Customizer that will serve them, based on their system parameters and capabilities (processing power, memory, bandwidth, etc.), and automatically fulfill the construction and distribution of needed software to satisfy their requirements.

Information Service Provider Tool (ISPT)

The ISPT will assist service providers in preparing and publicizing their information service in a manner that conforms to a common set of information service protocols. Specifically, it allows the provider to restrict access to their information service to certain users or groups, and would provide standardized service metadata templates for specifying information about the service, such as which client applications and protocols are required to access the information.

System Overview

Figure 2 shows an instance of autonomic system configuration. The instance shown in Figure 2 has a main information exchange group (referred to as an overlay (Layer 1)) on which the Administration Component and ISR reside. The Customizers are located on the overlays that connect service providers to the Layer 1 overlay or to the overlay chain connecting service subscribers.

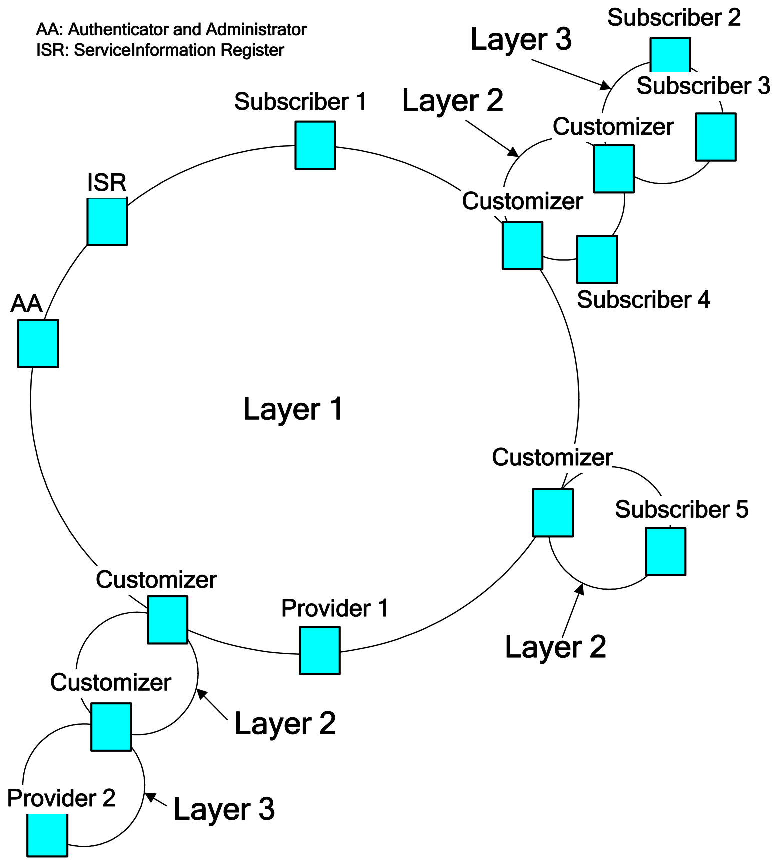

Figure 2. An instance of autonomic system

3. Work Flow

The proposed system is a rapidly reconfigurable system and adapts to the dynamics of the networks and customized sub-systems. All the service providers, customizers, and subscribers become part of the system only when they are necessary for the implementation of services. A service provider joins the system with its customizers (if needed) dynamically when it wants to provide the service to the entire system. In addition, a service subscriber with its customizers (if needed) joins the system when it is interested in a service provided within the system. At the system level, the services are organized based on common interests among the participants, such as job and rank through authentication and service information advertisement.

In the following parts of this section, we discuss several basic work flows in the lifetime of an autonomic system that give deeper understandings to the proposed system design concept and architecture.

Joining the UIXG

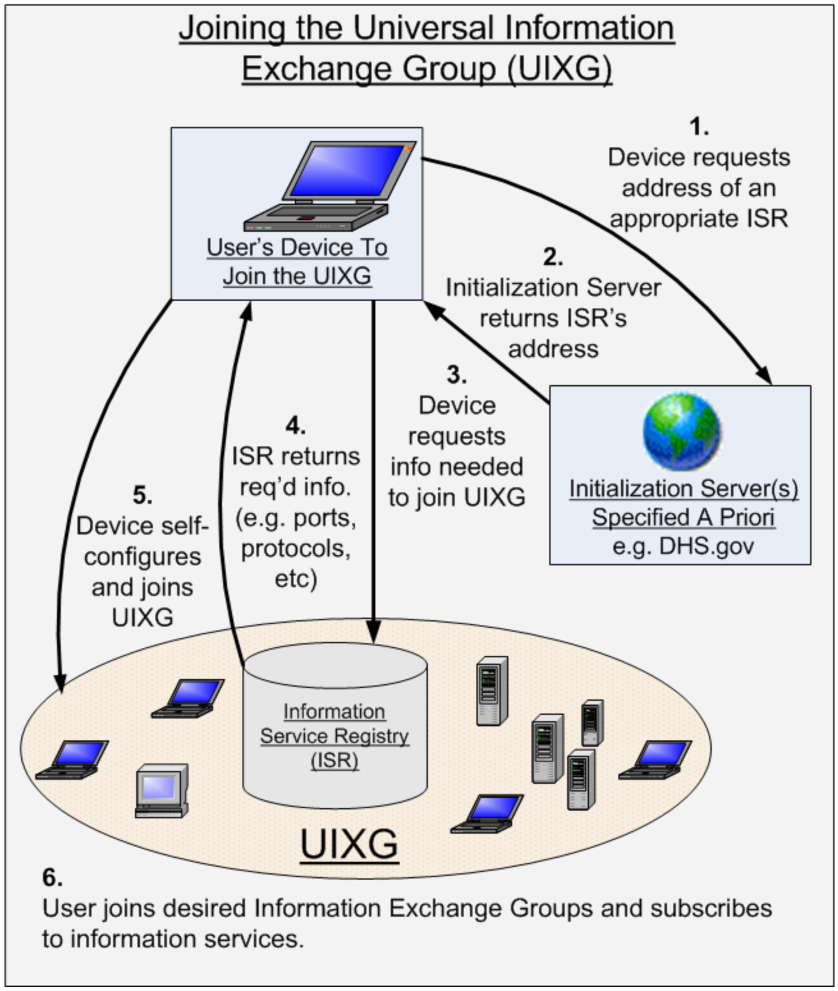

Figure 3. Joining UIXG

As previously stated, all users within an autonomic system must establish a connection to that system's Universal Information Exchange Group (UIXG) before information exchange can occur, thus the procedure for establishing this connection to the UIXG should be specified in advance in order for users to integrate themselves into the system as rapidly and effortlessly as possible when the need arises. To this end, the following procedure is proposed:

Prior to any service providing and subscription, all participants will agree upon a set of known, fixed, Initialization Servers which are redundant data sources containing the information needed by a user's device in order to begin establishing a connection to the appropriate UIXG. This information would be the address of the UIXG's ISR. Thus, all devices needing to join the UIXG will first query one of the Initialization Servers and retrieve the address of the ISR for the UIXG they wish to join. The user's device will then query that ISR, and the ISR will provide the device with the detailed configuration information needed to establish a connection with the UIXG. After retrieving this information, the device will configure itself appropriately and establish a connection to the UIXG. Once a user has joined the UIXG he may look up available information services in the ISR and subscribe to those services to which he has authorization.

The address of ISR can alternatively become available to all participants through off-line methods such as e-mail or phone message.

This process is shown in Figure 3.

Adding New Information Service Providers
As components offer to provide information services, those offers will be handled as follows:

- The new information service provider uses the Information Service Provider Tool provided by the system to prepare their information service for access by service subscribers, which will include such things as specifying authentication information required by interested users, and defining any applications that may be necessary to receive the information service.
- The new information service provider joins the UIXG through the procedure described in previous section.
- The new information service provider sends authentication request to the Administration Component and gets authenticated.
- The new information service provider will use the software tool to publish the metadata about their service to the ISR where it will be available to interested users.

New Service Request Fulfillment
As information service requests are received from participants, they are handled in the following way:

- A participant wishing to subscribe to an information service, or to communicate with another user or group, but who is unable to do so due to missing software or inadequate authentication information, may submit a request to the system administration component.
- The Administration Component will use the IXG Information to fulfill the user's request and push the new configuration and authentication information to the appropriate users.
- The involved devices configure themselves based on their newly provided configuration and join their desired UIXG through the procedure described in the previous section.
- The participant with service requests authenticates itself to the Administration Component and gets service information from ISR.
- The participant with service requests subscribes services from the providers (through customizers when it is in the different network of the providers).

4. The Development of Prototype Systems

Consistent with the requirements in the SOW, two prototype systems have been developed. One is the implementation of an autonomic system under Overlay Based SOA (OBSOA) concept; another one is a multi-tier system implementation showing the management and interactions among different autonomic systems.

Prototype OBSOA Autonomic System

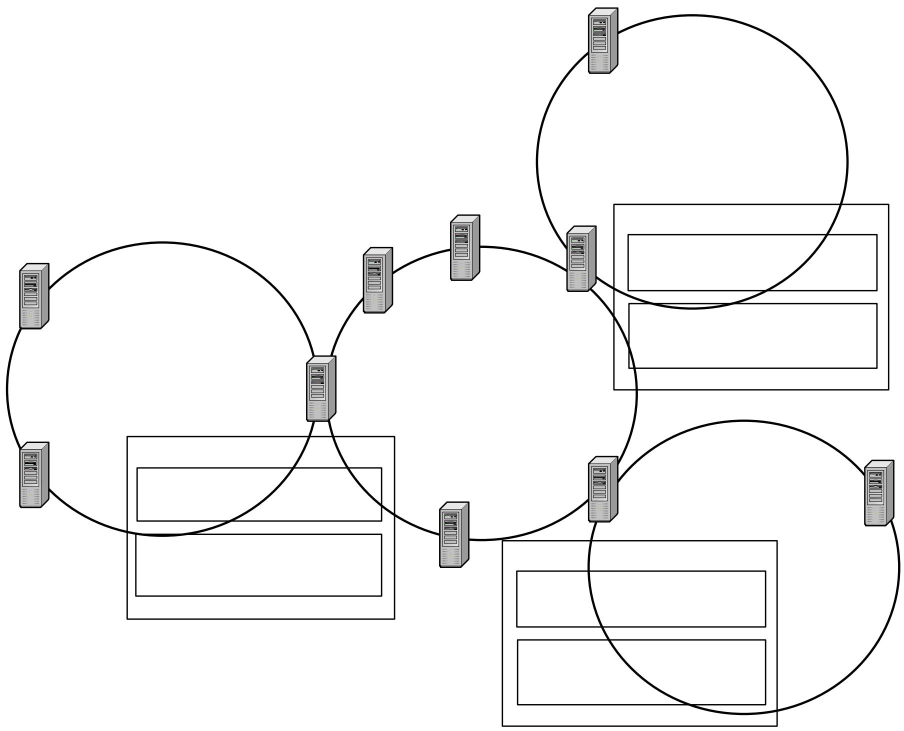

Figure 4. A prototype of OBSOA autonomic system

Figure 4 shows the configuration of the prototype of OBSOA autonomic system that has the following main features:

- It is built over heterogeneous network environment, which includes different network platforms such as the CHEETAH optical network (a high speed Gigabit network), Internet, Ethernet LAN and 802.11.
- Multiple services, including image file download, TV stream and WebEOC, are provided to different subscribers through different customizers based on the requirements and capabilities of the subscribers.
    - WebEOC is a commercially available software system provided by ESi. It provides real-time emergency information management to Emergency Operation Centers through a web-based interface over the Internet through the concept of boards. Boards can be in the form of maps (to which additional information can be added), messages, forms, or other information exchange. (More information can be found at http://www.esi911.com/esi/products/webeoc.shtml). In our prototype

system we have utilized Customizers to provide customized WebEOC boards to PDA users located on an 802.11 wireless network (the 802.11 network was NOT connected to the Internet).

- The locations of Customizers are flexible and are determined by the system designer. For example, the Customizer that connects the two service providers (RAW image download and Live TV Stream) located on a server in Georgia through the CHEETAH network to Internet (Layer 1 overlay). This customizer converts RAW image files into JPG image files so that the participants in the system only know and subscribe to JPG format image files. Meanwhile, two service subscriber Customizers resize or cut JPG images to satisfy the different requirements of PC and PDA subscribers (PDA subscribers ask for smaller size image files due to bandwidth constraint). The Customizer connection the PDA to the Layer 1 overlay converts HTTP messages provided by the WebEOC Web server to XML format messages so that PDA users, which possesses no Web browser functionality, can participates in the discussion with other PC users which can access the WebEOC server directly.
- All service providers and subscribers are authenticated by the Administration Component before they take part in the service activities.

The prototype system has an open architecture that permits new services to be easily added into the system. Due to the space constraint in Figure 4 not all service providers and subscribers nor all the possible cases of service activities are shown. Principally, there is no limit on the amount of participants (service providers and subscribers) and their locations. In the prototype implementation, another service called Whiteboard is also available to help users exchange non-text information. Whiteboard is a session-based group communication application in which each user is both service provider and subscriber, and joins the group through the procedure described in previous sections. A Whiteboard application represents a common interest group: such as a battalion in which the commander needs to brief his entire unit on an up coming battle strategy.

Prototype Multi-tier Information Exchange System

Figure 5 shows the configuration of a prototype multi-tier information exchange system. The Blueforce Database and Web Server are not part of the system. They are accessed through normal HTTP protocol by the Blueforce Manager. Below are its main features:

- Multiple network platforms, including Internet, NovaRoam radio wireless network and 802.11 wireless network, are employed to build the system.
- Each member in tier 2 each group dynamically joins the group through authentication procedure and receives all messages to this group. The messages can be sent from other members in the same group or from other group.
- The manager in a group can subscribe the service (or messages) in another group through the Manager group. Once subscription is accepted, the manager in another group will forward all messages in its group to the subscriber group.

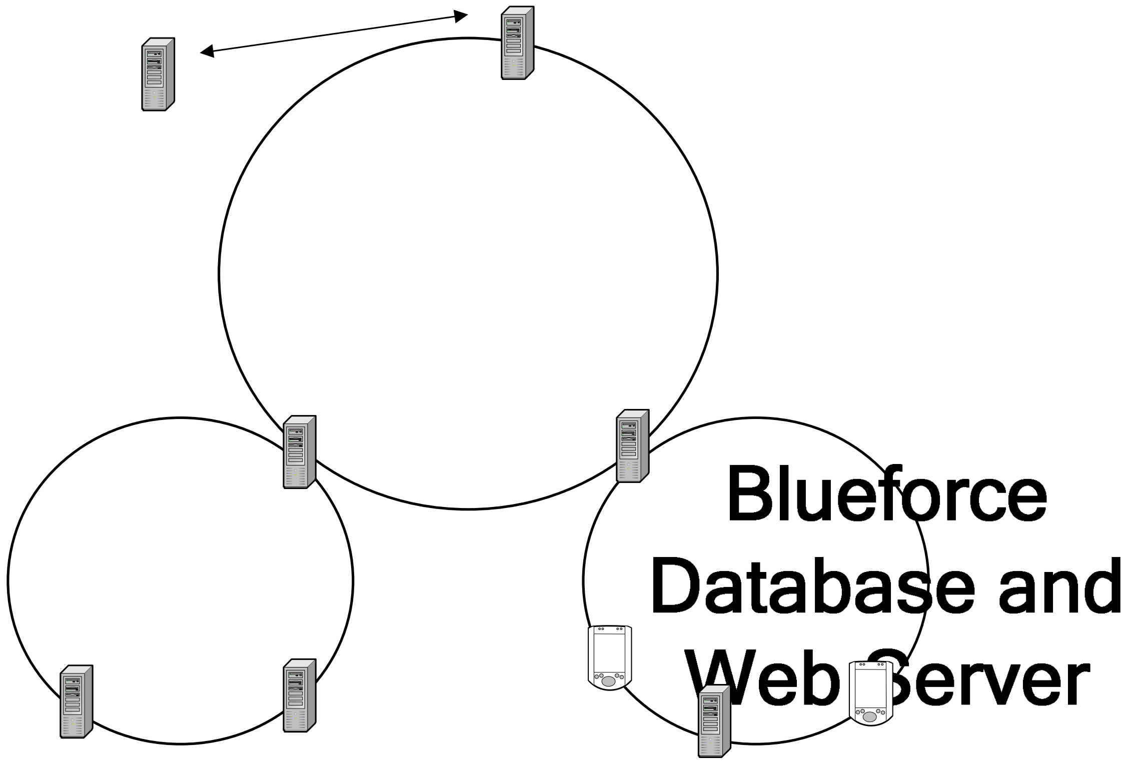

Figure 5. A prototype of multi-tier information exchange system

5. Conclusion and Future Work

In this document, we have discussed a new methodology for developing rapidly reconfigurable information exchange systems over a heterogeneous network environment. The proposed methodology is based on SOA concepts and Hypercast P2P technology and has been tested with prototype system implementations. The experience from the prototype systems shows that Hypercast is a suitable technology to bridge devices or sub-systems with different capabilities to form a complex information system over heterogeneous networks. Fused with SOA concepts a system design that maximizes flexibility, reusability, and adaptability is obtained. In addition SOA concepts provide a way to integrate with existing commercial and open source standards. Therefore more standards, such as J2EE, UDDI, JBoss and SOAP, will be examined and integrated into our system implementation to further increase the services available and reduce system development cost.

Finally, large-scale system experiments will be performed to test the proposed system construction technology. It is an important and necessary step before it is actually applied in practice. As such, several experiments on system performance are planned to provide quantitative measurements on the prototypes performance.

Appendix

Statement of Work (SOW)
for
Hypercast Implementation for PTDS

Overview

Hypercast is a software middleware project being conducted by the University of Virginia (UVA) for quickly and easily building information sharing groups out of nodes on an existing communications network. UVA shall adapt this hypercast technology to provide the US Army's Persistent Threat Detection System (PTDS) the capability to provide intelligent tailored role-based information exchange between personnel, sensors, and databases as part of the on-going combat evaluation process. As a result, distributed sensor nets will share detections, times, speeds, directions, etc., with appropriate databases, commanders, Tactical Operations Centers (TOC), and CONUS personnel automatically and in parallel. This unclassified effort shall mature and harden the Hypercast technology, integrate it into existing PTDS technology and sensors and provide interface with emerging Army communications media in a rapid prototyping environment.

Sub Task 1.0 Information Sharing from Humans and Databases. UVA shall conduct research and development to integrate and support a prototype Hypercast-based PTDS-like communications network for small unit operations using PDA's that will provide reporting, mapping, imagery access and databases containing tactically relevant information such as Patrol briefings and Imagery. This Hypercast-based approach will create information sharing groups by rank, job, geographic location, etc., and automate the sharing of information between heterogeneous groups of humans and databases. The UVa effort will establish automation aids for creating, controlling and integrating group communications. UVA shall develop the necessary types of information sharing groups as listed to demonstrate the flexibility of the Hypercast middleware to support user needs (e.g., imagery, GIS information). Communications systems will include, as available, the use of the CHEETAH test-bed to emulate the fiber optic-based GIG. UVA shall demonstrate and deliver Hypercast middleware tailored as follows: The prototype will be designed to display…

- Two Maneuver Units – each with its own hierarchical permissions structure consisting of 10 members each, with 2 commanders and two battalions of 4 members each.
- Four databases – two imagery databases, one blue-force tracking database and one "sensor detections" database.
- The imagery databases will reside on the fiber optic GIG in two separate geographic locations (such as UVA and another university).
- The software must be able to demonstrate five knowledge sharing groups in each maneuver unit – one each based on: (1) job, (2) geographical location, (3) battalion membership and (4) two user specified (i.e. subscribed by interest).

This prototype capability will be demonstrated through a series of quarterly unclassified progress reviews and an end of contract demonstration of a entire prototype system.

References:

[1] Hypercast project, http://www.hypercast.org.

[2] HyperCast: A Protocol for Maintaining Multicast Group Members in a Logical Hypercube Topology, J. Liebeherr, Tyler K. Beam, July 1999. Proc. First International Workshop on Networked Group Communication (NGC '99), in: Lecture Notes in Computer Science, Vol. 1736, pp. 72-89, 1999.

[3] Application-Layer Multicast with Delaunay Triangulations, J. Liebeherr, M. Nahas, W. Si, IEEE Journal on Selected Areas in Communications, Special Issue on Network Support for Multicast Communication, 40(8):1472–1488, October 2002.

[4] Programming Overlay Networks with Overlay Sockets, J. Liebeherr, J. Wang, and G. Zhang, NGC 2003 proceeding, Munich, Germany, September 2003.