RECURSION SOFTWARE, Inc.

Software for Software Developers™

A Distributed Knowledge Network for the Secure Border Initiative SBI*net*

By Greg Cowin

Recursion Software, Inc.

March 2006
V1.3

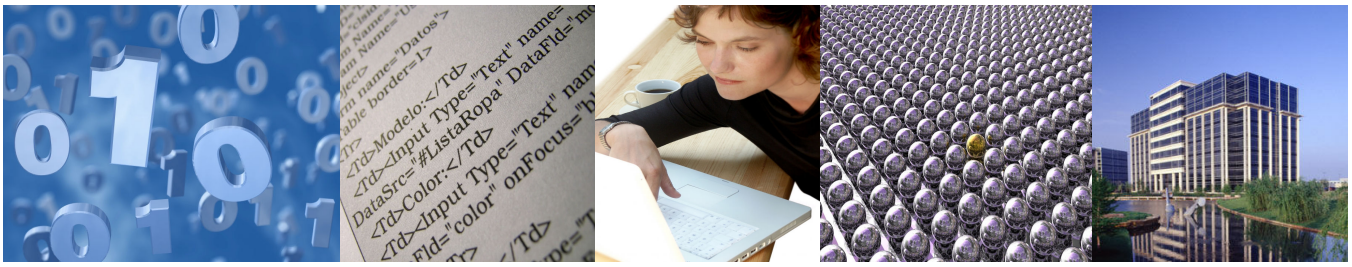


TABLE OF CONTENTS

A Distributed Knowledge Network for the Secure Border Initiative SBI*net*

By Greg Cowin

Introduction

The emergence of the Secure Border Initiative (SBI) as a comprehensive approach of the federal government's Department of Homeland Security approach to secure the United States borders identifies the need to fulfill two strategic goals:

> ***Border control:*** *to detect and respond to all cross-border crime; to end "catch and release" of non-Mexican illegal aliens; and to deter cross-border crime*
>
> ***Interior enforcement:*** *to identify and remove incarcerated aliens, immigration fugitives, and violators; to build strong compliance and enforcement programs for law-abiding employers; and to uproot the infrastructure of illegal immigration*

SBI*net* will provide the system capabilities to meet the needs of the SBI by integrating technologies, infrastructure, a rapid response capability and personnel into a comprehensive border protection system.

The foundation of such a system requires the ability to intelligently integrate surveillance data from all available sources. The integration of sensor data is the first and foremost challenge to developing a model and the ultimate product for the SBI initiative. The integration of separate and distinct sensors is actually the association or the fusing of data from heterogeneous sources to provide the user information from which to derive knowledge. The first step in solving this challenge is to architect a network to accommodate various sensors providing both homogeneous and heterogeneous data to distributed sites for the derivation of knowledge of the environment under surveillance. Providing the end user with discrete contact information of possible violators and their locations begins with the assembly and dissemination of intelligence information to the right people. With that information and with the doctrine of standard operating procedures for the day, personnel can then begin intelligent surveillance based on predictive data. This predictive data then provides the initiation and the prioritization of sensor data required to accomplish the detection of potential intruders. Computer applications developed for this network must also be easily configurable and low in maintenance. The implementation of this type of surveillance network will require the deployment of a large-scale, intelligent, autonomous, and self-configuring network with associated computer applications.

A key technology prevalent today in sensor networks and network and system management is the use of intelligent software agents. This type of network, with large-scale sensor arrays, planned for deployment, as part of the SBI, will require the use of intelligent mobile agents to cope with the complexity and sheer number of devices and sensors necessary to protect U.S. borders.

BACKGROUND

Recursion Software is participating in the following programs, demonstrating the required capabilities for the Secure Border Initiative through consultation and/or deployment of Recursion's Voyager® intelligent mobile agent technology.

- United States Joint Forces Command Joint Warfighting Center, Joint Development Integration Facility's Decision Support Tool
- United States Joint Forces Command, Joint After Action Review Toolset
- Partnering with Spec Ops, Inc. on The Department of Defense Small Business Innovation Research awards providing communications and mobile agent framework for:
  - SBIR CR3-2202 Automated Assessment of Joint Training and Education
  - SBIR AF06-040, F061-040-3683 Distributed Methods for Assessing the Readiness of Coalition Workgroups, and Teams

In addition to these programs, Recursion Software supports professors and students from over 85 universities around the globe through their University Center by providing:

- Full software package with all the standard features
- Professional software development tools used by thousands of programmers worldwide
- Help from Java, C++, C# (,NET) experts
- Free individual Education License for one semester
- Free individual support for one semester
- On-line product documentation
- Subject matter expert support as a guest lecturer or project mentor

Recursion Software has several patents on communications and mobility of agents in a networked distributed computing environments. Voyager is the first platform to seamlessly integrate fundamental distributed computing with mobile agent technology, and was designed from the ground up to support communications between mobile objects and autonomous agents. The Voyager philosophy is that an agent is simply a special kind of object that can move independently, can continue to execute as it moves, and otherwise behaves exactly like any other object. Voyager enabled objects and agents can send standard Java messages even as they are moving as well as allowing you to remote-enable any Java class, even a third-party library class without modifying the class source in any way. In addition, Voyager offers flexible security options such as firewall tunneling, secure socket layer communications over encrypted and authenticated channels with pluggable SSL socket factories and support for the latest PHAOS and RSA SSL Toolkits and pluggable security services via the Voyager Administrative Console.

The Challenge

Similar to network and system management operations, sensor networks are highly distributed, and agent architectures are prevalent in these domain areas. Network management has several functional management areas including fault management, configuration management, accounting management, performance management and security management. Sensor networks also have these functional areas, but require more automation and autonomy in the field. As a result, intelligent software agents are needed to decentralize decision-making and give more autonomy at the device level.

Intelligent software agents localize intelligence, reduce network traffic, enable self-configuration, and make the overall system more resilient to failure and delay. When Voyager agents are utilized on sensing devices in a distributed network, the agents can detect a change in state at the device and respond immediately rather than relying on a centralized monitoring function to scan each device from a centralized location and report back any change in status prior to a response being activated. Local intelligence is used to detect, track, warn and deter. With more autonomy at the edge, less communication is required and less attention and fewer personnel are required to monitor the system.

System Description

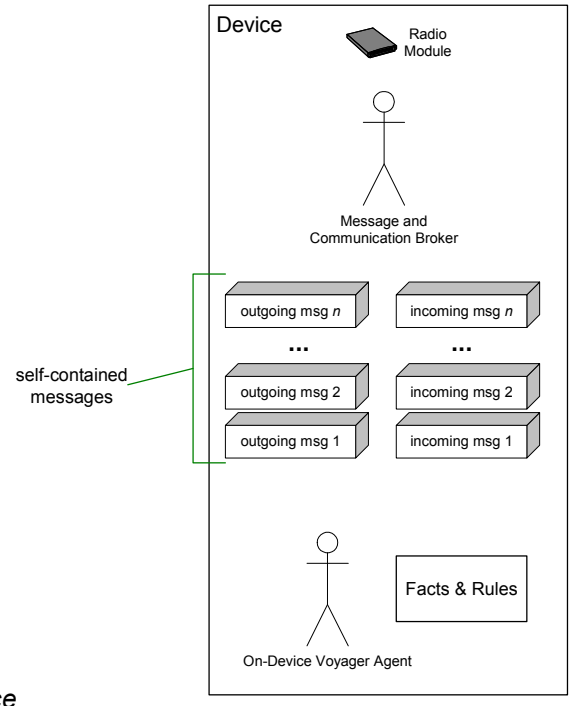
Deployment of a large-scale surveillance system using sensor arrays not only requires the right hardware and software infrastructure, but also a set of technical capabilities to enable successful network configuration, management and message delivery.

Technical Capabilities

The technical capabilities requirements for the Secure Border Initiative are the ability to localize intelligence, guarantee message delivery, tolerate faults, auto-configure and reduce bandwidth. The following architecture blocks enable these capabilities:

- Intelligent On-Device Agent
- Message and Communication Agent
- Asynchronous Messaging
- Store-and-Forward Messaging
- Command Center Agent

Figure 1: Device-Centric Viewpoint



Intelligent On-Device Software Agent

Intelligent On-Device Agents use rules to make decisions and to take actions based on local knowledge (or facts). The more sophisticated the device, the more it should delegate to additional intelligent software agents that make decisions and take actions based on their local knowledge. The Intelligent On-Device Agent is also responsible for the following:

- Registration
- Self-configuration
- Provisioning requests
- Providing health status

What is Software Intelligence?

Consider the definition of Intelligence from a *Signals Intelligence* perspective. Signals Intelligence is a product of the National Security Agency that extends the classic separation of Data, Information, and Knowledge.

The NSA represents Signals Intelligence as a stack [2]:

Intelligence:	Applied Knowledge
Knowledge:	Facts and relationships
Information:	Discrete facts
Data:	Bits and streams
Signals:	Electrical signals

Where *intelligence* is applied knowledge.

Using the NSA definition, agents are intelligent—they apply knowledge; in other words, Voyager agents use rules to take action and make decisions based on knowledge (facts and relationships). Applied and actionable knowledge is necessary for localized intelligence. Localized intelligence is necessary for devices to be more autonomous and to make decisions in the field. Devices also need to be autonomous to help operators cope with the complexity and size

of the sensor network that will be deployed along the northern and southern borders.

Message and Communication Agent

The Message and Communication Agent is responsible for managing the incoming and outgoing messages. In addition, it is responsible for establishing communication and transmitting and receiving messages. See Figure 1 for a depiction.

Asynchronous Messaging

When developing technology for wireless devices, it is immediately apparent that asynchronous messaging is imperative for critical field applications. Asynchronous messaging is the concept that self-contained messages can be routed, transmitted or stored for later transmission. Latency and connection failure is regularly experienced when using a sophisticated cellular device with synchronous transmission, for instance when the cellular device user takes a couple steps and loses the data connection. Another circumstance where this occurs is during peak service hours. This is why synchronous messaging is not an acceptable method of signaling for critical applications such as sensor reading, command or alert, where synchronous connections might simply fail. Even with wired connections, latency and failure is a common reality.

For critical field applications, transmitting important data such as that from devices hooked to sensors and actuators and from PDAs in the field, asynchronous messaging is necessary.

Store-And-Forward Messaging

As stated before, a key mechanism in machine-to-machine communications is the self-contained message. With wireless sensors and actuators, a store-and-forward mechanism on a device is imperative to ensure that messages are delivered when the wireless connection is unavailable. This simple mechanism can provide reliable messaging.

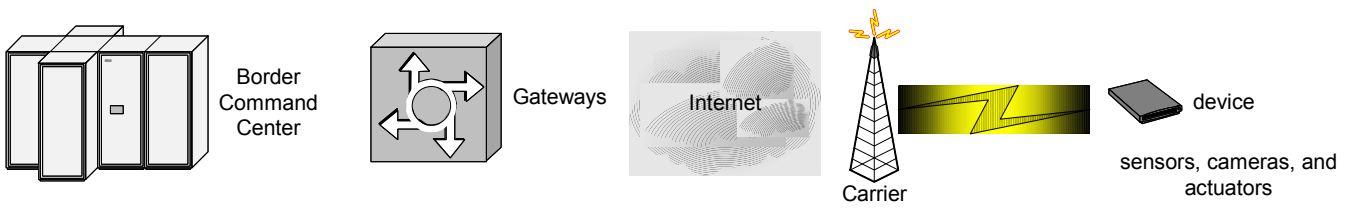
Command Center Agent

A highly available Intelligent Agent at the command center for each device will execute enterprise rules. The On-Device Agent provides local intelligence. The Command Center Agent provides highly available enterprise intelligence.

Infrastructure Required

The infrastructure required to support and enable a large-scale sensor network, such as the one planned for the Secure Border Initiative includes a command center, data center, gateways, agent technology, radio modules, sensor arrays, remote surveillance, actuators, and security. Communication flows to and from the command center to devices, as depicted in Figure 2. Self-contained messages are stored-and-forwarded on the device and at the Border Command Center.

Figure 2: Communication Flowing through the Infrastructure



Command Center

A Command Center provides operators with access to the enterprise system that houses the border security system. The Command Center includes interfaces to alarm management, sensor network health, situational awareness and account management and logging. In addition, enterprise knowledge and rules can be modified.

Gateways

For wireless devices, a gateway to possibly multiple carriers is required. Depending on coverage and the need for redundancy, multiple carriers are often required - especially in rural areas.

Agent Technology

Agents are used to provide truly intelligent and autonomous sensor networks. This helps reduce the cognitive load for operators. In addition, they provide the communication and message delivery.

Radio Modules

Radio Modules come in basically two types including radio only module with an interface, usually rs232, and radio plus computing environment such as J2ME. Wireless devices require a radio module. There have been over 250 million Java phones shipped. These mass produced all-in-one modules are cheap and capable. The numbers make them cheap and Java makes them powerful.

Sensor Arrays

Sensor Arrays deployed along the northern and southern borders of the U.S. include devices such as camera systems, motion, weight and other sensors.

Remote Surveillance Camera Systems

Remote Surveillance systems can use infrared cameras to identify, track, alert and deter criminal activity. The on-device agent can use rules to determine when to record and transmit video since the data rates of video can roughly range from 1.5 Mbps to 19.2 Mbps.

Security

Security is not only needed for commands sent to devices and actuators, but for data from sensors. False readings can lead operators and enterprise intelligent agents to make the wrong decision, so security is imperative, but what kind of security? Devices need to be authenticated and communication secured. Both of these can be accomplished with asymmetric encryption.

Conclusion

Recursion software can provide the software development environment, tools and foundation structure upon which to develop the needed Distributed Knowledge Network required to satisfy the goals of the SBInet. Utilizing our industry and government proven technologies the SBInet can accomplish its goals of Border Security through implementation of an extensible system utilizing intelligent agent technology as a foundation to achieve the goals of the SBInet large-scale intelligent, autonomous and self-configuring sensor network.

The ability to provide actionable knowledge to autonomously detect, track, warn and deter calls for a solution that intelligent computer agents can provide to maximize the effect of the limited force of border patrol agents to more effectively deter and prioritize criminal activity at America's borders.

Bibliography

1. Press Release. “Secure Border Initiative”, Homeland Security. http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0794.xml. 2006.

2. NSA. “Signals Intelligence”, National Security Agency. http://www.nsa.gov/sigint/index.cfm.

3. Voyager® 4.7 Documentation, Recursion Software, Inc. 2003.

About the author

Greg Cowin served as Director of Emerging Technologies at Recursion Software, Inc. from 2005-2006. Prior to joining Recursion Software, Greg was the Chief Architect & VP of Development for SensorLogic. Selected at SensorLogic’s inception, Greg was responsible for the development of a radically intelligent service oriented architecture for the monitoring and control of remote machines via satellite, GPRS, CDPD, SMS, Reflex and the Internet. During his tenure, Greg was responsible for building the development team, architecture, technical direction, intellectual property, and is credited with authoring key patents.

As Chief Architect for Netfolio, a fully automated agent-based financial trading website that created a new way to invest called the personal fund industry, Greg co-authored patents for trading personal funds via the web and was responsible for the enterprise architecture as well as providing critical technological and development direction.

At ParcPlace, a spin-off of the Xerox Palo Alto Research Center, Greg deployed important software applications for Lawrence Livermore National Labs, Lucent, AT&T, McKesson and Texas Instruments.

Greg has a BS in CS from the University of Oklahoma. engineering@recursionsw.com

Recursion Software, Inc.
2591 North Dallas Parkway
Suite 200
Frisco, Texas 75034
1.800.727.8674 or 972.731.8800
www.recursionsw.com

RECURSION SOFTWARE, Inc.