MASTER OF SCIENCE
IN
COMPUTER SCIENCE

A PRO-ACTIVE ROUTING PROTOCOL FOR CONFIGURATION OF SIGNALING CHANNELS IN SERVER AND AGENT BASED ACTIVE NETWORK MANAGEMENT (SAAM)

Hasan Akkoc-First Lieutenant, Turkish Army
B.S., Middle East Technical University, 1994
Master of Science in Computer Science-June 2000
Advisor: Geoffrey G. Xie, Department of Computer Science
Second Reader: CDR Deborah R. Kern, USN, Department of Computer Science

As networks are upgraded to provide services for streaming applications, the current way of routing is not satisfactory. Server and Agent based Active network Management (SAAM) introduces a novel network architecture that provides guaranteed quality of services to real-time traffic. In SAAM, the server and routers need to establish two-way, robust, and efficient signaling channels for exchange of control and management information. Any change in network topology must be determined and handled as they occur in order to support guaranteed services. Local detection of topological changes and hop-by-hop dissemination of knowledge of these changes is not optimal for SAAM architecture. A reactive method of updating routing tables takes longer time than tolerable for real-time traffic. Therefore, a pro-active approach that re-reconfigures the signaling channels in real time and without degrading services to user traffic is mandatory. This thesis presents such a pro-active routing protocol for configuring the signaling channels of a SAAM region.

DoD KEY TECHNOLOGY AREAS: Command, Control and Communications, Computing and Software

KEYWORDS: Routing Protocol, Signaling Channel Configuration, Soft-State Approach, Pro-Active Approach, Networks

SUPPORTING A TRUSTED PATH FOR THE LINUX OPERATING SYSTEM

Scott A. Bartram-Ensign, United States Navy
B.S., Oregon State University, 1999
Master of Science in Computer Science-June 2000
Advisors: Cynthia E. Irvine, Department of Computer Science
Paul C. Clark, Department of Computer Science

The existence of Trojan horses, viruses, and other malicious software has motivated the computer security industry to invent mechanisms that protect against malicious software. One such mechanism is called the Trusted Path. The Trusted Path provides a way for the system to authenticate itself to the user. Once invoked, the Trusted Path provides an environment in which the user can perform trusted operations such as login, logout, and change password.

This thesis provides a high level design for a Trusted Path and an in depth analysis of how a Trusted Path can be implemented in the Linux operating system. Research of process family creation and keyboard handling has led to the implementation of a Secure Attention Key that can be used to invoke a Trusted Path in Linux.

This research is meant to be used in combination with other efforts to enhance the Linux operating system as an inexpensive platform for instruction on computer security policies.

DoD KEY TECHNOLOGY AREAS: Other (Secure Computer Systems, Computer Security, Information Assurance)

KEYWORDS: Trusted Path, Secure Attention Key, Computer Security, Linux, Policy Enhanced Linux

DEMONSTRATION OF A CONCURRENTLY PROGRAMMED TACTICAL LEVEL CONTROL SOFTWARE FOR AUTONOMOUS VEHICLES AND THE INTERFACE TO THE EXECUTION LEVEL CODE

William D. Carroll-Lieutenant, United States Navy
B.S., Oregon State University, 1993
Master of Science in Computer Science-June 2000
Advisor: Man-Tak Shing, Department of Computer Science
Second Reader: CDR Michael J. Holden, USN, Department of Computer Science

The desire for use of autonomous robotic vehicles has undergone tremendous growth in the past decade. One of the greatest challenges to the successful development of truly autonomous vehicles is the ability to link logically based high-level mission planning with low-level vehicle control software, without a labor intensive programming effort for each mission.

This challenge can be effectively achieved through the use of tri-level control software architecture, as described in the Rational Behavior Model. The control software (in the tactical level) must de-couple the high-level mission planning from the low-level vehicle control software to reduce the programming effort for each mission. This report describes an object-oriented, modular architecture for the middle (tactical) level that uses concurrent programming techniques and multi-language interfacing. This design enables the control software to handle the intense data management effort required to operate in an autonomous fashion and interface with code already perfected for use in the strategic (top) and execution (bottom) levels.

The design was evaluated by providing the tactical level with a simple execute order statement that was then used to drive the actions of the vehicle. The software package demonstrates the validity of the design and provides the framework for full implementation on an actual vehicle.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Surface/Under Surface Vehicles - Ships and Watercraft, Other (Autonomous Vehicle Control Software)

KEYWORDS: Autonomous Vehicle, Robot, AUV, Rational Behavior Model, RBM, Concurrency, Ada 95, Control Software

TARGET IDENTIFICATION ALGORITHM FOR THE AN/AAS-44V FORWARD LOOKING INFRARED (FLIR)

Jessica L. Herman-Ensign, United States Navy
B.S., Stanford University, 1999
Master of Science in Computer Science-June 2000
Advisor: Neil C. Rowe, Department of Computer Science
Second Reader: Wolfgang Baer, Department of Computer Science

Accurate identification of unknown contacts is a crucial issue in military intelligence. In order for this task to be accomplished by human observers, each one must be specially trained and regularly re-qualify. Even with training, their decisions are subject to human error: bias, expectations, or even a lack of sleep may compromise their accuracy. If an automated system could quickly and accurately determine the identity of a contact, it would be a great benefit. This thesis explores some of the problems which must be addressed in producing such a system. We detail an approach to an algorithm which compares a picture of an unknown ship to an established database and determines its most likely classification. In particular, we use infrared images from FLIR video taken at sea, and obtain classification results for a small test set. We tested eighteen images with success rates varying between seventy-three and eighty-nine percent.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Image Recognition, Ship Identification, Hough Transform, Edge Detection

DEVELOPMENT OF DIGITAL DATA ACQUISITION MODULE AND INTERFACE FOR ANALOG BEARTRAP MISSION DATA

Richard N. Massie-Lieutenant, United States Navy
B.S., United States Naval Academy, 1993
Master of Science in Computer Science-June 2000
Advisors: Michael K. Shields, M.K. Shields Company
J. Bret Michael, Department of Computer Science

This work is part of an ongoing effort to integrate the separate BEARTRAP post mission analysis tools into a system residing in a Microsoft Windows NT environment. This new integrated system will contain software modules designed to replace the array of diverse processing systems currently being used for BEARTRAP post mission analysis. While current BEARTRAP mission analysis requires a timescale of weeks, this new solution will enable actual tactical use of the data by units at sea. This thesis develops the module and user interface responsible for digital data acquisition of BEARTRAP mission data from multi-track analog sonobuoy tapes as well as a module to access buoy indexing information from the Orion II maritime surveillance software. This work describes the development process as well as the integration and testing of the interface, acquisition, and indexing functionality for the BEARTRAP Post Mission Processing System 2000 (S2K) using Microsoft Visual C++ as the implementation language.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Sensors

KEYWORDS: Acoustics, BEARTRAP, DSP, Sound Pressure Level

A SOCKETS APPLICATION PROGRAMMING INTERFACE FOR THE PETITE AMATEUR NAVAL SATELLITE

Fernando J. Maymí-Captain, United States Army
B.S., United States Military Academy, 1989
Master of Science in Computer Science-June 2000
Advisor: Gilbert M. Lundy, Department of Computer Science
Second Reader: Jim Horning, Space Systems Academic Group

The Petite Amateur Naval Satellite (PANSAT) is an operational communications microsatellite designed at the Naval Postgraduate School (NPS). PANSAT's communications software was intended to be developed after orbital insertion and transmitted to the satellite.

The Sockets Application Programming Interface (API) developed at the University of California, Berkeley is the de facto standard API for network applications. It provides a strong and flexible platform on which to develop a wide variety of programs. It accelerates the development of new applications by providing a standard set of features and isolating the program from the underlying networking mechanisms.

This thesis studied the viability of implementing of a Sockets API for PANSAT based on the Berkeley Sockets. PANSAT's Sockets API was built on BekTek's Spacecraft Operating System (SCOS). Because SCOS source code was not available, network protocols had to be implemented in user mode. SCOS is optimized for multiple small tasks, not the complex processes required for Internet programming. Because of SCOS' limitations in memory management, the development of this protocol stack and API was not successful. SCOS does not have the features required for an implementation like this.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Space Vehicles

KEYWORDS: PANSAT, Internet, TCP/IP, Sockets

STATIC-TASK SCHEDULING INCORPORATING PRECEDENCE CONSTRAINTS AND DEADLINES IN A HETEROGENEOUS-COMPUTING ENVIRONMENT

Michael D. Niedert-Lieutenant, United States Navy
B.S., United States Naval Academy, 1990
Master of Science in Computer Science-June 2000
Advisor: Neil C. Rowe, Department of Computer Science
Second Reader: CDR Deborah R. Kern, USN, Department of Computer Science

Distributed systems have grown in popularity due to the rapid increase in networking of personal computers. A mixture of computers consisting of different architectures can be more powerful, reliable, and scalable than a single supercomputer. The problem of optimally scheduling jobs on a cluster of heterogeneous machines to minimize the time at which the last machine finishes is NP-complete. Nonetheless, the choice of a heuristic algorithm greatly affects the speed of solution. This work evaluates a greedy algorithm, an A* algorithm, and a simulated annealing algorithm applied to the heterogeneous scheduling problem with deadline and dependency constraints. Tradeoffs of speed and schedule quality were noted between the algorithms. The greedy algorithm produced results quicker than the A* and simulated annealing algorithms, but with a lower schedule quality. Because of these offsetting performance criteria, an analysis was conducted to determine which algorithms should be used for which input cases.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Scheduling, Algorithms, Artificial Intelligence, Distributed Computing

TRANSPARENT DETECTION OF QOS VIOLATIONS FOR CONTINUOUS APPLICATIONS

Kendal V. Polk-Captain, United States Army
B.S., United States Military Academy, 1990
Master of Science in Computer Science-June 2000
Advisor: Cynthia E. Irvine, Department of Computer Science
Second Reader: Timothy Levin, Anteon Corporation

Resource Management Systems have the task of determining the structure, resource allocation, and scheduling of applications within their scope. One such system is the Management System for Heterogeneous Networks (MSHN) which uses its Client Library to gather knowledge of its environment. The Client Library is wrapped around each application to gather application status and resource usage information by intercepting and interpreting system calls. In previous work, the Client Library was utilized to provide status of an application at the end of the application's execution. This research focuses on a method to gather QoS information on continuous applications within mission-critical systems, while applications are running rather than after execution, without modification to the application's source code.

The Client Library has been modified to provide application execution information that is evaluated and compared against user-defined specifications. Any QoS violations result in a notification. This is an indicator for MSHN's scheduler to take corrective action such as adapting to use different resources or data formats.

When wrapped applications are used in conjunction with continuous monitoring, overhead is increased, which may be acceptable if transparent QoS monitoring is essential.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Command, Control, and Communications

KEYWORDS: Quality of Service, Resource Management System, MSHN, Desiderata Wrapper, QoS Violations, Client Library, Resource Monitoring

THE APPLICATION OF A VIEWPOINTS FRAMEWORK IN THE DEVELOPMENT OF C4I SYSTEMS

Sheila A. Smith-Lieutenant, United States Navy
B.S., Illinois State University, 1994
Master of Science in Computer Science-June 2000
Master of Science in Systems Technology-June 2000
Advisors: J. Bret Michael, Department of Computer Science
William G. Kemple, Command, Control, Communications, Computers, and Intelligence Academic Group

In the development of large distributed systems, both the detection and resolution of inconsistency in policy, requirements, and specifications pose major challenges. The purpose of this thesis is to examine the inconsistencies in policy, requirements, and specifications in the development of information/Joint Command, Control, Communications, Computers, and Intelligence (C4I) systems. This thesis explores the application of a "viewpoints" framework to aid in the development of distributed information systems.

A viewpoints framework methodology that was developed to aid in the development of distributed systems is the Reference Model of Open Distributed Processing (RM-ODP). This thesis is concerned with the application of the five viewpoints of RM-ODP and the translation of policy into requirements and specifications. In this thesis, the Ballistic Missile Defense (BMD) system is used as a case study to explain how RM-ODP can be used to develop distributed information systems. It was found that identifying inconsistencies regarding interoperability amongst the subsystems of BMD necessitated the use of multiple viewpoints and that firm conclusions could not be made until the system was viewed at the lower levels.

DoD KEY TECHNOLOGY AREAS: Command, Control, and Communications, Computing and Software

KEYWORDS: Ballistic Missile Defense, C4I, Interoperability, Policy, Reference Model of Open Distributed Processing, Requirements Engineering, Viewpoints

AUTHENTICATION IN SAAM ROUTERS

Luis E. Velazquez-Captain, United States Marine Corps
B.S., Jacksonville University, 1992
Master of Science in Computer Science-June 2000
and
Peter J. Szczepankiewicz-Lieutenant, United States Navy
B.A., Boston University, 1994
Master of Science in Information Technology Management-June 2000
Advisors: Geoffrey G. Xie, Department of Computer Science
Rex A. Buddenberg, Information Systems Academic Group

Server and Agent based Active network Management (SAAM) is a network protocol developed at the Naval Postgraduate School to address the router software requirements for the Next Generation Internet (NGI). A working prototype has existed for over nine months to materialize abstract research ideas in the field of active networking.

Authentication is particularly important because SAAM uses mobile code, called resident agents. These resident agents are loaded onto SAAM routers dynamically, and execute on the destination SAAM router. Mobile code in the SAAM system requires an authentication scheme to prevent an outsider from sending a malicious resident agent. Two issues explored are time synchronization and authentication. This thesis focuses on authentication.

With authentication, SAAM can be used as the technical network infrastructure to support Network Centric Warfare (NCW) as described in JV2010. The NCW network must allow mobile code to securely execute on the fly. The prototype developed in the thesis authenticates new nodes that join a SAAM network using Kerberos. Signaling data, also called control traffic, is certified with a dynamic signature key that changes every two minutes. Once a SAAM node is authenticated, its identity is protected

throughout the battle. In the same way that Allied forces use Identification Friend or Foe (IFF) traffic today, SAAM authentication could support NCW.

The NCW network must also be self-healing. Auto configuration is already integrated into the SAAM prototype. Network failures are detected within 500ms. Probing agents are also deployed to investigate suspicious activity within the network. Future probes could fingerprint a specific group of hackers while on-line, using genetic algorithms.

The effects of SAAM on the organizational behavior of a tactical Information Warfare (IW) organization are explored in this thesis.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Authentication, Encryption, Routing, Java, Key Distribution, Kerberos, Secure Time Synchronization

APPLICATION OF FAULT-TOLERANT COMPUTING FOR SPACECRAFT USING COMMERCIAL-OFF-THE-SHELF MICROPROCESSORS

Kimberly Davenport Whitehouse-Captain, United States Marine Corps
B.S., University of Florida, 1990
Master of Science in Computer Science-June 2000
and
Susan E. Groening-Lieutenant, United States Navy
B.A., University of Florida, 1989
Master of Science in Computer Science-September 2000
Advisors: J. Bret Michael, Department of Computer Science
Alan A. Ross, Navy Tactical Exploitation of National Capabilities (TENCAP) Chair

Low availability, high cost, and poor performance of radiation hardened (rad-hard) equipment has driven the market to rely on commercial-off-the-shelf (COTS) equipment for the computing needs of today's spacecraft. This thesis describes the tailoring of a COTS embedded real-time operating system and design of a human-computer interface (HCI) for a triple modular redundant (TMR) fault-tolerant microprocessor for use in space-based applications. One disadvantage of using COTS hardware components is its susceptibility to the radiation effects present in the space environment, and specifically, radiation-induced single-event upsets (SEUs). In the event of an SEU, a fault-tolerant system can mitigate the effects of the upset and continue to process from the last known correct system state. The TMR basic hardware design used for this research is an acceptable fault-tolerant design candidate for the main processor for space-based applications. We found that a COTS embedded real-time operating system could be tailored to support the TMR hardware. The HCI accepts serial data from the TMR, correctly identifies the source of the error, allows for processor mode selection and provides system- and board-level reset capabilities. The tailored operating system combined with the HCI is a viable software implementation to support hardware-based fault-tolerant computing in a space environment.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Space Vehicles, Human System Interface

KEYWORDS: Fault Tolerance, Embedded Operating System, Human Computer Interface, Triple Modular Redundant Hardware, Spacecraft Design

A TRUSTED CONNECTION FRAMEWORK FOR MULTILEVEL SECURE LOCAL AREA NETWORKS

Jeffery D. Wilson-Lieutenant Colonel, United States Marine Corps
B.A., Bluefield College, 1982
Master of Science in Computer Science-June 2000
Advisors: Cynthia E. Irvine, Department of Computer Science
Second Reader: Timothy Levin, Anteon Corporation

The Naval Postgraduate School is developing a Multilevel Secure Local Area Network (MLS LAN) that incorporates commercial-off-the-shelf client workstations to provide multiple users with simultaneous secure access to stored data of different sensitivity levels. The MLS LAN uses a Trusted Computing Base Extension (TCBE) in the LAN's client workstations to extend the TCB from the trusted server across the network to these workstations. Connections between elements of the LAN are under TCB control and are conducted by way of several new communications protocols.

Using a realistic System Requirements Document and a High Level Protocol Analysis, this thesis presents a framework of communications protocols that will enable the components of the MLS LAN to securely interact. The framework first presents a communications channel protocol that protects all data transmitted on the network. Following this, three other protocols are described that enable MLS LAN users to safely login and negotiate a secure session, access Application Protocol Servers that provide services such as e-mail or WWW services, and to use typical LAN-based office automation services. Finally presented is an analysis of both TLS and IPSec, which provides evidence that IPSec is best suited to provide MLS LAN communications protection.

DoD KEY TECHNOLOGY AREA: Other (Computing and Networks)

KEYWORDS: Multilevel Security, Trusted Path, High-Assurance, Network Client-Server

HELICOPTER URBAN NAVIGATION TRAINING USING VIRTUAL ENVIRONMENTS

George T. Wright, Jr.-Major, United States Marine Corps
B.S., University of West Florida, 1984
Master of Science in Computer Science-June 2000
Advisor: Rudolph P. Darken, Department of Computer Science
Second Reader: Barry Peterson, Department of Computer Science

Helicopter missions are never defined as "…successful navigation to and return from a location." Navigation, in and of itself, is not the mission – it is, however, a skill that all helicopter pilots are expected to master in order to function as pilots. *Navigation is a means to an end*.

Helicopter operations, being inherently expensive and unforgiving of mistakes, are prime candidates for such innovative training techniques as virtual (3-D) fly-throughs. This thesis, as a logical extension of previous research, seeks out ways to enhance current training methods for urban helicopter navigation using state-of- the-art-technology. Using empirical data from pilot surveys and controlled experiments, principles can be formulated to determine the level of computer graphics fidelity necessary for helicopter crews to conduct a virtual flight in an urban setting that is a credible, effective tool in preparation of an actual flight.

This research does not seek a replacement method of training helicopter terrain navigation – pilots must still be taught the fundamental skills of map interpretation and terrain association using conventional training techniques. However, it is the intent of this research to explore methods of enhancing and supplementing site-specific helicopter navigation training through the transfer of spatial knowledge from the virtual world to real-world applications.

DoD KEY TECHNOLOGY AREAS: Air Vehicles, Computing and Software, Manpower, Personnel, and Training, Modeling and Simulation

KEYWORDS: Helicopter, Urban Terrain, Virtual Environments, Navigation Training, Mission Rehearsal, Spatial Orientation, Situational Awareness

IMPLEMENTATION AND EVALUATION OF A NETWORK ACCESS PROTOCOL

Joseph A. Wronkowski-Captain, United States Marine Corps
B.S., University of Southern Illinois, 1992
Master of Science in Computer Science-June 2000
and
David I. Odom-Lieutenant, United States Navy
B.S., Norfolk State University, 1994
Master of Science in Computer Science-September 2000
Advisor: Dennis Volpano, Department of Computer Science
Second Reader: J. Bret Michael, Department of Computer Science

Traditional Ethernet networks are wired networks. There is now an increasing need, however, for hosts on the network to be mobile without losing network connectivity. This is where wireless technology comes in. The basic idea is to allow a portable device, equipped with an Ethernet transceiver, to relocate while "connected" to the network. Connected here means being within radio range of another transceiver, called an access point, which acts as a relay for the portable device. Its relocation is entirely transparent.

Currently, there is a standard that defines how wireless devices communicate within a Local Area Network. This standard is called IEEE 802.11. The standard, however, is not scalable due to the level at which security is handled.

This thesis examines an alternative security solution, the Network Access (NA) Protocol, developed by Professor Dennis Volpano. It runs on mobile devices and designated hosts called bridges and has the potential to scale up to meet the demands of mobility while ensuring secure network access.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Mobile IP, Wireless Computing, IP Mobility Support, IP Encapsulation, IpSec, IPChains, Home Agent, Mobile Host, Foreign Agent, Tunneling, Care-of-Address, MAC, IEEE 802.11, Route Optimization, Intra-Subnet Roaming