

# MASTER OF SCIENCE IN COMPUTER SCIENCE

---

## WEB PORTAL DESIGN, EXECUTION, AND SUSTAINABILITY FOR NAVAL WEBSITES AND WEB SERVICES

**Sandra L. Amsden-Lieutenant Commander, United States Navy  
B.S., University of Montana, 1988**

**Master of Science in Computer Science-December 2003**

**Advisors: Don Brutzman, Department of Information Sciences**

**Curtis Blais, Modeling, Virtual Environments, and Simulation Institute**

**Second Reader: Barb Helfer, Modeling, Virtual Environments, and Simulation Institute**

With the rapid evolution of Web-based technologies, keeping up with the latest trends is a complicated process. The newest “Web Service” is the development of Web Portals. Portals allow the design of Web Services in such a way as to allow the users to define their needs, and create a home of their own within a site. As users become more proficient, knowledgeable and demanding, this technology will expand due to the demand of users.

As with all new technology, it includes significant benefits and pitfalls. Determining where to best use Web Services and Portals is important. The plethora of tools being promoted for the development of portals is significant, and choosing the right tool to accomplish the task while ensuring compatibility is critical. Already, considerable work has been accomplished by Task Force Web and the Fleet Numerical Meteorology and Oceanography Center. An important factor in the decision process is meeting the demands of an ever increasing technology literate environment. Reaching the goal of a fully connected Navy will require significant expenditure of money and manpower, but will reap large benefits from the long-term value of improved training and access to knowledge.

This research looks at Web Services and Web Portals, examining the design of portals and an evaluation of their use.

**KEYWORDS:** Web Services, Web Portals, NEP, Navy Enterprise Portal

## THE THERMINATOR: CONFIGURING THE UNDERLYING STATISTICAL MECHANICS MODEL

**Daniel W. Ettlich-Lieutenant, United States Navy**

**B.S., B.A., University of San Diego, 1994**

**M.B.A., University of Arizona, 2001**

**Master of Science in Electrical Engineering-December 2003**

**Master of Science in Computer Science-December 2003**

**Advisors: John C. McEachen, Department of Electrical and Computer Engineering**

**CDR Chris S. Eagle, USN, Department of Computer Science**

The rapid increase in sophisticated Internet attacks has left the security industry lagging far behind. In an attempt to improve network security, Therminator, a patternless intrusion detection system, was developed in 2001 by NPS in conjunction with NSA. The Therminator model uses statistical mechanics to analyze network traffic as a system of exchanges. Being highly configurable enables Therminator to be adapted for any network configuration. Until now, however, no exploration had been conducted on the configuration parameters of the underlying statistical mechanics model. It is important to understand the effects of these parameters to optimize anomaly detection. Thus, the current study explored these parameters using HTTP traffic generated in a controlled test environment. Results were as follows: equations were developed for state counting to determine bucket state space sizes; bucket state space size was found to be symmetrical about the midpoint of the boundary conditions; proper display period was based on traffic rate; and lastly, the more orthogonal anomalous traffic was to the normal traffic, the larger the perturbation was in the state graph. These results provide needed insight into properly configuring Therminator for optimal anomaly detection, ultimately affording the Department of Defense greater network security.

**KEYWORDS:** Network Security, Network Assurance, Information Protection, Intrusion Detection, Patternless Intrusion Detection, Network Anomaly Detection, Real-Time Network Monitoring, Statistical Mechanics

**EVALUATION OF A MULTI-AGENT SYSTEM FOR SIMULATION AND ANALYSIS OF  
DISTRIBUTED DENIAL-OF-SERVICE ATTACKS**

**Saw Tee Huu-Captain, Republic of Singapore Army**

**B.E., Nanyang Technological University, 1999**

**Master of Science in Computer Science-December 2003**

**Advisors: J. Bret Michael, Department of Computer Science**

**Mikhail Auguston, Department of Computer Science**

Distributed Denial-of-Service (DDoS) attack is evolving at a rapid and alarming rate. An effective solution must be formulated using an adaptive approach. Most of the simulations are performed at the attack phase of the DDoS attack, thus the defense techniques developed focus mainly on filtering and isolating the attack. In order to develop and verify the effectiveness of a defense strategy, a robust and flexible simulation tool is needed. The Multi-Agent System Development Kit (MASDK) provided a means to generate DDoS attack in a safe experimental environment for testing and validating security solutions, starting from the implantation phase: this allows researchers to develop new defense strategy even before the DDoS attack is launched. The paper begins with the study of the characteristics of DDoS attacks, the types of detection-and-response techniques, and the available DDoS attack simulation tools. The result generated by the MASDK simulation tool was used to evaluate the performance of the tool in simulating the DDoS attack over the networking environment.

**KEYWORDS:** DDoS, MASDK, Simulation Tool, Attack Tool, Computer Network

**SIMULATING DISTRIBUTED OBJECT ORIENTED SERVERS**

**Kwok Chee Khan-Civilian, Singapore Ministry of Defense**

**B.S., National University of Singapore, 1995**

**Master of Science in Computer Science-December 2003**

**Advisor: William J. Ray, Department of Computer Science**

**Second Reader: Man-Tak Shing, Department of Computer Science**

Distributed object oriented (OO) computing such as RMI, COBRA, and SOAP, etc., is fast becoming the de-facto standard for software development. Distributed OO systems can consist of multiple object servers and client applications on a network computer, as opposed to a single large centralized object server.

The aim of the system designer is to determine the optimal deployment strategy for the system to perform efficiently. This is an enormous task, especially when multiple object servers are fielded on hardware of different specifications. The number of possible deployment strategies of object servers to hardware grows exponentially with increased numbers of object servers and machines. For example, with three machines and ten object servers there are 59,049 possible deployment patterns. Eventually, the number of possible deployments makes it impossible for system designers to setup test beds to determine the optimal deployment strategy.

The main goal of the simulation model is to analyze the object server deployment, verify an existing optimization model, and determine the optimal deployment strategy that will reduce the client response time. In one of the experiments conducted with the simulation model, in an environment with three machines and ten object servers, it will take 53 years to attempt all deployment patterns in the lab environment. The simulation model will take only 13 days, which is an improvement of 1480%.

**KEYWORDS:** Distributed Object Oriented Architecture, Simulation, OMNet++, Optimization

---

# COMPUTER SCIENCE

---

## SCENARIO SELECTION AND STUDENT ASSESSMENT MODULES FOR CYBERCIEGE

**Teo Tiat Leng-Civilian, Republic of Singapore**

**B.S., National University of Singapore, 1991**

**M.Tech., National University of Singapore, 1999**

**Master of Science in Computer Science-December 2003**

**Advisor: Cynthia Irvine, Department of Computer Science**

**Second Reader: Michael Thompson, Department of Computer Science**

CyberCIEGE aims to provide an Information Assurance (IA) teaching/learning laboratory in the form of an interactive, entertaining, commercial-grade, PC-based computer game. Each game plays as a single scenario that serves to teach a particular IA concept. However, more synergy can be gained if there is higher-order organization of these scenarios, such as by grouping around a set of desired concepts to be taught, or by increasing the complexity of the scenarios built around a common theme. This thesis aims to provide an instructor tool for this purpose.

In addition, by tapping the CyberCIEGE event log files generated at the end of each game, the game's progress can be reconstructed to support After Action Reviews (AAR) to assist the instructor and student in analyzing game decisions and the student's progress. This provides a constructive follow-up to review and reinforce the concepts being taught.

**KEYWORDS:** Information Assurance, Security Education, After Action Review

## A METHODOLOGY FOR DEVELOPING TIMING CONSTRAINTS FOR THE BALLISTIC MISSILE DEFENSE SYSTEM

**Michael H. Miklaski-Commander, United States Navy**

**B.S., National University, 1987**

**Master of Science in Systems Technology-December 2003**

**Master of Science in Software Engineering-December 2003**

**Joel D. Babbitt-Captain, United States Army**

**B.S., Brigham Young University, 1995**

**Master of Science in Computer Science-March 2004**

**Advisors: Man-Tak Shing, Department of Computer Science**

**J. Bret Michael, Department of Computer Science**

The Department of Defense (DoD) is developing a Ballistic Missile Defense System (BMDS) based on a layered defense that employs complementary sensors, weapons, and C2 elements, integrated by software into a system-of-systems to engage and destroy threat ballistic missiles through all phases of flight. Inherent to the ultimate success of the BMDS will be the timely execution of the kill chain process against threat ballistic missiles.

In this thesis, the Unified Software Development Process (USDP) is applied, utilizing the BMDS as a case study to investigate a means to identify and validate timing behaviors and constraints of system-of-systems. In particular, the information exchange needed for processors to share, collaborate, fuse, and distribute sensor information in a distributed sensor network is examined, and modeling and simulation to provide insight into the timing aspects of interactions among subsystems comprising a system-of-systems is utilized. The case study will involve deriving and documenting system and software requirements, developing a test-ready model for representing the timing requirements, and then validating this model through the use of an OMNET++ simulation. The simulation will then be used to provide feedback to further refine the system requirements and the functional specifications of the subsystems.

**KEYWORDS:** Software Engineering, System-of-Systems, Ballistic Missile Defense System, BMDS, Sensor Fusion, Collaborative Fusion, Modeling, Simulation, OMNeT++, UML-RT, Real-Time Constraints, Software Requirements, Kill Chain, Timing Requirements, Unified Software Development Process, USDP

---

# COMPUTER SCIENCE

---

## **FREE SPACE OPTICS COMMUNICATION FOR MOBILE MILITARY PLATFORMS**

**Soo Sim Daniel Neo-Civilian, Defence Science and Technology Agency, Singapore**

**B.S., Nanyang Technological University, 1996**

**M.S., Nanyang Technological University, 2000**

**Master of Science in Computer Science-December 2003**

**Advisor: Bert Lundy, Department of Computer Science**

**Second Reader: Wen Su, Department of Computer Science**

Free Space Optics (FSO) is widely regarded as the next-generation high-speed wireless communication technology. FSO has demonstrated its capability to deliver data faster than any other state-of-the-art wireless communication technology. Today, terrestrial FSO links are able to reach 150 kilometers; unmultiplexed data rates of 2.5 Gbps have been achieved; Acquisition, Pointing, and Tracking (APT) systems have been successfully deployed between communication satellites; and carrier-class availability is being offered by FSO vendors. However, FSO has not seen widespread use in the military. This is attributed to the fact that military platforms are largely mobile, while the progress in the commercial arena has largely been confined to links between fixed sites.

This thesis analyzes the features of FSO technology while being mindful of how these apply to the military. These features include the bandwidth, spectrum use, bit error rates, communications security, free-space loss, and power consumption. The limitations and challenges presented by atmospheric effects, directional precision, line-of-sight obstructions, and laser safety are also studied. A final section looks at the acquisition, pointing, and tracking mechanisms that are necessary for deploying FSO on mobile platforms.

**KEYWORDS:** Free Space Optics, FSO, Laser Communications

## **INTEGRATION OF THE NAVY TACTICAL ENVIRONMENTAL DATABASE SERVICES WITH THE JOINT EFFECTS MODEL**

**Victor B. Ross, III-Lieutenant Commander, United States Navy**

**B.S., Florida Institute of Technology, 1990**

**Master of Science in Computer Science-December 2003**

**Advisor: Neil C. Rowe, Department of Computer Science**

**Second Reader: Carlyle H. Wash, Department of Meteorology**

The Oceanographer of the Navy is responsible for the maintenance and distribution of the “4-D cube” of environmental data, the Virtual Natural Environment, using an object oriented database and distribution system, Tactical Environmental Database Services (TEDServices). The new military dispersion modeling capability within the military is called the Joint Effects Model (JEM), and has to have an interface created to allow inclusion of weather data in JEM. This thesis utilizes TEDServices using web protocols to query for available data, and then retrieves the required meteorology data. The software creates a specifically formatted file to be used in JEM. It is now fully functional and submitted to Space and Warfare Command for inclusion in JEM. Much of the testing was to ensure that the data are available and within the reasonable meteorological standards. The thesis also suggests additional changes that should be made to TEDServices to make it more capable of storing and serving environmental data.

**KEYWORDS:** REA, JEM, Dispersion Model, TEDServices, HPAC, Mesoscale Model

---

# COMPUTER SCIENCE

---

## **DEFENDING IEEE 802.11-BASED NETWORKS AGAINST DENIAL OF SERVICE ATTACKS**

**Boon Hwee Tan-Major, Republic of Singapore Navy  
B.E., Nanyang Technological University, 1997**

**Master of Science in Computer Science-December 2003**

**Advisor: William J. Ray, Department of Computer Science**

**Second Reader: Man-Tak Shing, Department of Computer Science**

The convenience of IEEE 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial, and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. In addition to widely publicized security flaws in IEEE 802.11's basic confidentiality mechanisms, the threats to network availability presents an equal, if not greater, danger to users of IEEE 802.11-based networks. It has been successfully demonstrated that IEEE 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols.

Computer simulation models have proven to be effective tools in the study of cause and effect in numerous fields. This thesis involved the design and implementation of a IEEE 802.11-based simulation model using OMNeT++, to investigate the effects of different types of DoS attacks on a IEEE 802.11 network, and the effectiveness of corresponding countermeasures.

**KEYWORDS:** IEEE 802.11, WLAN, Wireless LAN, Protocol, Computer Security, Denial of Service, Simulation, OMNeT

## **CONFRONTING CYBERTERRORISM WITH CYBER DECEPTION**

**Kheng Lee Gregory Tan-Lieutenant Colonel, Singapore Army  
B.E., University College London, 1990**

**Master of Science in Computer Science-December 2003**

**Advisor: Neil C. Rowe, Department of Computer Science**

**Second Reader: Dorothy E. Denning, Department of Defense Analysis**

This thesis concerns the possibility of deceiving cyberterrorists using defensive deception methods. As cyberspace today is a battleground for a myriad of cyber attacks and intrusions, it may only be a matter of time before terrorists choose to advance their deadly cause in cyberspace. Some of the questions raised regarding the threat of cyberterrorism are explored by examining different perspectives, motivations, actors, targets, and how they may be confronted. One way is to draw from the lessons of deception and apply them against cyberterrorist attacks. Cyber deception applies in cyberspace just as well as deception in military battles. From the different categories of attackers that could perpetrate cyberterrorism, the ways in which they may be deceived are examined. Many of the methods and tools that cyberterrorists would use are similar to those used by other less malicious hackers, so specific deceptions to use against them in advance can be planned.

**KEYWORDS:** Cyberterrorism, Terrorism, Deception, Cyber Deception, Intelligent Software Decoys, Software Deception, Information Warfare, Cyber Attacks

## **EFFECTIVE DISTRIBUTION OF HIGH BANDWIDTH TO THE LAST MILE**

**David Kwok Vi-Keng-Civilian, Defence Science and Technology Agency, Singapore  
B.E., National University of Singapore, 1995**

**Master of Science in Computer Science-December 2003**

**Advisor: Bert Lundy, Department of Computer Science**

**Second Reader: Wen Su, Department of Computer Science**

Since the mid 1990s, the Internet has been revolutionizing the way business is conducted around the globe. Bandwidth-intensive graphics, video, and audio applications are becoming more popular and the desire for fast access to information places a huge demand on high bandwidth in metro networks. The primary bottleneck in the quest for delivering high bandwidth to the customers is the last mile. The last-mile of today primarily relies on infrastructures that were not designed for the transport of digital data. The current

infrastructure of twisted pair is very close to its upper limits. As a result, consumers are unable to enjoy the full potential of the Internet, and generally do not have access to enhanced services such as enriched multimedia services, converged voice, video, and data services, and high-speed Web browsing.

This thesis assesses a broad spectrum of wired and wireless last mile technologies available - Optical Fiber Technology, Digital Subscriber Lines, Free Space Optics, Wireless Local Loop, Wireless LAN, and Cellular Technology. Besides discussing the basic concepts and principles, this thesis highlights the current limitations of these technologies for last mile implementation. An innovative and state-of-the-art methodology for linking building with optical fiber to achieve high bandwidth through sewer systems is presented.

**KEYWORDS:** Last Mile Technologies, Optical Fiber, Digital Subscriber Line, Free Space Optics, Wireless Local Loop, Wireless Local Area Network, Cellular Technology, Fiber in Sewer