# AN INTEGRATED APPROACH FOR SECURITY ON DEMAND

# IN HIGH SPEED, SHARED USE NETWORKS

by

Henry J.(Jerry) Schumacher

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy



ARIZONA STATE UNIVERSITY

May 1999

AN INTEGRATED APPROACH FOR SECURITY ON DEMAND

IN HIGH SPEED, SHARED USE NETWORKS

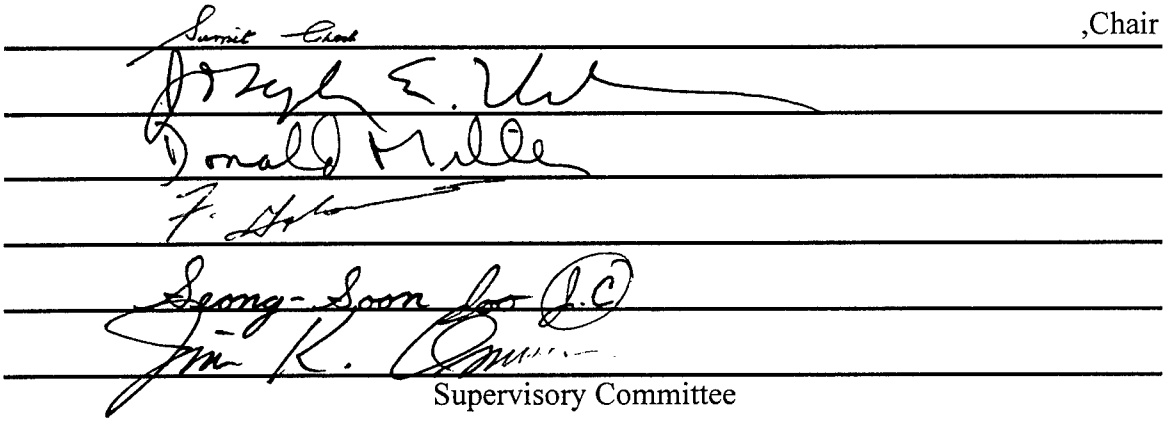
by

Henry J.(Jerry) Schumacher

has been approved

September 1998

APPROVED:



,Chair

Supervisory Committee

ACCEPTED:

Department Chair

Dean, Graduate College

## ABSTRACT

This dissertation presents a user level security on demand system, resulting from an integration of a fundamental framework for network security with the fundamental and unique characteristics of Asynchronous Transfer Mode (ATM) networks. The framework offers a conceptual structure encapsulating the fundamental knowledge and set of relationships in network security, permitting systematic and scientific reasoning about network security. The changing nature of networks from a set of unconnected entities, controlled and used by a specific class of users, to an increasingly interconnected and integrated, "mixed use", set of networks, simultaneously shared by different classes of users, requires a mechanism to enable these "mixed use" networks to meet the diverse security requirements of all users. The framework, developed as a part of this dissertation, provides the ability for all user groups, such as the military, government, industry and academia, to define their security requirements within its context and enable the framework, when integrated into an ATM network, to provide a template for matching network security resources to individual user requirements.

The user level aspect of the security system is unique and is enabled by the ATM network's call setup process. In this approach, during the call setup phase, the security posture of every node and link is computed, utilizing the security framework. When the system configures a virtual path from source to destination, every node and link is verified to meet the user specified security, in addition to bandwidth and other quality of service (QoS) requirements. Traffic is launched when the call setup succeeds, otherwise, the call fails. Thus, the approach is consistent with the basic characteristics of ATM

networks, offering comprehensive security while viewing security as a distributed network resource, allocating it to each user efficiently, based on demand and dictated by the need. This approach was modeled for representative, 50, 40 and 32 node ATM networks and the model is successfully implemented through an asynchronous distributed simulation. Analysis of the behavior, obtained utilizing stochastic, representative input traffic, scientifically validates the security on demand system and reveals negligible performance impact on an ATM network's operation and advantages over the status quo.

TABLE OF CONTENTS

CHAPTER Page

LIST OF FIGURES

Figure Page

Figure Page

Figure Page

# CHAPTER 1

# INTRODUCTION

## Overview

The principle contribution of this dissertation is the design, modeling, implementation through simulation, scientific validation and behavior analysis of the integration of a novel security on demand approach into the operation of an Asynchronous Transfer Mode (ATM) network. This system enables, at the user level, tailorable security for data transmission. The ability to provide security on demand down to the user level, in an ATM network, facilitates the integration of the previously isolated, secure, military networks for Top Secret, Secret and Confidential traffic, along with the public commercial network infrastructure, consisting of a single, "mixed use" network which provides user tailorable security for transporting traffic. The mixed network provides increased performance over the previously isolated military networks as well as greater potential for distributed security resource allocation to reduce overall costs and achieve higher efficiency.

The security on demand system is achievable through the integration of a framework for network security into the call setup process of an ATM network. A literature search and the author's extensive experience in the Army, Department of Defense, the Executive Branch and with civilian corporations reveals the lack of a

comprehensive definition for network security. In response, a comprehensive network security framework was developed by the author, published in the literature and principles of the framework integrated into a draft of a National Security Agency paper (National Security Agency 1996) on their Network Rating Methodology.

The comprehensive framework has several uses, one of which is providing the basis for a user level, security on demand system in an ATM network. The design and model for the security on demand system concentrated on the need for the system's integration into the normal operation of an ATM network to mitigate the performance impact. Security has a history of being an afterthought for most networks and is generally implemented through the addition of software and hardware devices after a network has been created resulting in degraded performance. ATM network's economies of scale through distributed resource allocation, in addition to ATM's unique characteristic of establishing virtual paths, provides a necessary and unique opportunity for a user level security on demand system. Coupled with the network security framework, ATM's virtual path selection can be used to build, in effect, a virtual network for a particular user's data which provides the user's required level of security. The system developed by the author is an integral part of the call setup process in an ATM network, modifying the method for the call setup message route selection. Since the behavior of the system follows that of current ATM networks, the expectation is the implementation would be successful and the performance impact would be minimal.

To scientifically validate and study the behavior of the security on demand system, the system was implemented through a simulator consisting of over 15,000 lines of C/C++ code and executed on a testbed of 25+ Pentium processors under the Linux operating system to collect system behavior data. Three representative networks were also developed to study the behavior of the system under differing and realistic conditions. A scientific evaluation of the impact of the integration of the military's isolated, secure networks with the public, commercial ATM infrastructure was one goal in developing and studying these networks. Different methods for determining the call setup message path were also modeled and implemented to analyze and compare behavior.

The result of the successful design, modeling and implementation through simulation is a user level, security on demand system which was scientifically validated and shown to have minimal impact on performance as compared to a baseline ATM network. The creation of the security on demand system enables networks to be established which combine all types of users to include the military, government, industry and academia while providing tailored security for their data. The traditional method of certifying isolated, closed networks for a particular level of security is transcended and a new paradigm created which is one of risk management where data is sent over a "mixed use" network and the data stream is protected according to the originator's security requirements.

## Statement of Problem

Current methods for implementing security in high speed networks do not provide comprehensive security, do not provide for optimal use of the security resources at the user level and are not well integrated into networks. The growing importance of security, and need for interconnection of military, industry, and government networks and the high cost of security resources has prompted the need for a security on demand system which can be used by all groups: military, industry, government and academia. Such a system must be integrated into the operation of a network and not as an after the fact, add-on system. Integration into the operation of a network insures minimal performance impact. Offering the system down to the user level optimizes the use of security resources, by enabling the connection of previously isolated networks with the public, ATM infrastructure, reducing costs as well and enabling the combination of previously isolated networks. The author has proposed such a system in the literature, modeled and implemented, through simulation, its operation to scientifically validate and study the behavior of the system.

## Organization

The remaining chapters are organized in the following manner. Chapter 2 reviews related work, detailing the history behind network security and the work done on ATM network security. The outcome of the literature search was a confirmation of the absence of a comprehensive framework resulting in the creation of one by the author. Chapter 3 describes the network security framework developed by the author and uses of the

framework. Chapter 4 develops the user level, security on demand system approach integrated into an ATM network. Chapter 5 presents the three representative ATM networks: military, civilian and "mixed use", as well as the three models used in the behavioral analysis studies: baseline, security on demand and a refinement to the security on demand approach called Node Status Indicator (NSI). Chapter 6 characterizes the input traffic used in the behavioral analysis studies and presents the results and analysis of a stability study conducted to determine a high call rate for the studies which does not cause instability. Chapter 7 presents the results and analysis of the scientific validation of the security on demand approach, comparative performance analysis of the security on demand approach to a reference baseline ATM network approach and the comparative performance analysis of the military and civilian networks to a "mixed use" network. Variations on the security on demand approach through refinements to the generation and flooding of network topology information were also analyzed and compared. Chapter 8 presents conclusions and future research.

# CHAPTER 2

# RELATED WORK

## Introduction

Current research can be broken down into two areas. The first being research into the general area of network security and the second being specific research on security in ATM networks. Research into network security is broad and has its roots in communications cryptography from World War II. ATM network security is relatively new with published work appearing no earlier than 1995 and mainly concentrated on encryption techniques.

The objective of this dissertation research was to establish a security on demand system at the user level for a high speed computer network. A natural starting point was finding a comprehensive definition for network security which includes all areas related to network security and applicable to all types of users, military, government and industry. An extensive literature search revealed the lack of a comprehensive framework for network security. Reasons for this lie in the fact that different classes of users developed their own frameworks which include their own security concerns, but are not universally applicable to other classes of users. These separate definitions of network security proved to be adequate when the networks were closed and isolated from other classes of user's networks, however, networks today are increasingly being

interconnected, as well as new networks being created which are "mixed use" for many classes of users. Without a common framework for network security, users cannot protect their data according to their requirements when networks are interconnected. The need for a common framework has recently become apparent and the National Security Agency started an initiative to create a common definition which has led to the adoption of the framework approach published by the author (Schumacher and Ghosh 1997a, 1997b) and described in detail in Chapter 3.

It is appropriate to review the past history of network security to understand how the current numerous and diverse definitions of network security were developed. It is also important to note that the framework and definitions for network security are methods of organizing and categorizing actual implementations of network security. The framework does not provide implementations of network security rather it offers a method and map for organizing and discussing how network security is provided. For example, a particular type of encryption device can encrypt and decrypt data on a communications link and this would be considered an implementation for a level of communications security. The framework developed by the author defines the area as communications privacy and this device would fall into that element of the framework.

## History Behind Network Security

The military was the first to recognize the need for network security because of its experience in World War I (WWI) and World War II (WWII) with communications

security. Encryption was used extensively during WWII to protect the communications lines over which messages were being sent. Later, when the military built data networks, the practice of encrypting the data was carried over to these networks and became the backbone for computer network security in the military. The military started out with the idea of securing each individual computer and later expanded the concept to securing a network of computers and devices. However, it is not the only organization that requires and has implemented some form of security. Network security has evolved over the years and other departments of government and government networks, including the US Treasury (Edfors 1996), FBI (Edfors 1996), and the Federal Reserve banking network, as well as commercial institutions and commercial networks such as the banks, financial institutions, and credit card transaction networks (Geer 1995), have embraced the idea of developing a secure network.

Recently, the commercial industry has become very interested in security of networks since, now, a favorable cost benefit can be associated with security. The Internet's growing popularity and potential for commerce (Tenenbaum et al. 1995) has increased the amount of money and effort devoted to produce and enforce security for the privacy and non-repudiation attributes (Geer 1995). Corporations such as General Electric, that have lost money as a result of intrusion, can justify increased attention and spending on network security. The vulnerability of the power grid possibly leading to catastrophic loss of electric power in the country, has raised deep concerns about the reliability of networks.

The computer driven integration of the fields of (i) communications and (ii) automation and control, are primarily responsible for the proliferation of today's networks. Computer networks have grown from a simple time sharing system - a number of terminals connected to a central computer - to large, complex environments that provide the infrastructure to many critical and economically valuable components of the economy. Many of the large-scale real-world systems in the government, military, and civilian sectors consist of a number of geographically dispersed hardware and software entities that are interconnected through a network that facilitates the exchange of both data and control traffic. Examples include the Federal Reserve banking network, the power grid, the proposed intelligent vehicle highway system network, the US Treasury network (Edfors 1996), the FBI network (Edfors 1996), and the proposed community health care network. While the successful demonstration of remote surgery by the US Army attests to the capability of today's networks, it also underscores the critical need for network security.

There is an increased reliance on computer networks today that is not widely known to the general public. In fact, most US residents, do not realize that they rely on hundreds of computer networks during the normal course of the day and the proper functioning of these networks is critical to our well being and survival. As a result, the risk to the economy, infrastructure and well being of the population, has not necessarily been widely reported and has only been recently in the spotlight (Schwartau 1996) (Report by the President's commission on critical infrastructure protection 1997). Such

complex systems, however, are often vulnerable to failures, intrusion, and other catastrophes. Backhouse and Dhillon (1995) estimate the yearly damages to the vulnerable finance and banking sectors in the US at $2 billion. With the growing use and ubiquitous reliance on such computer networks, an increasing emphasis is being placed on security. Both industry and government are engaged in developing new ways to ensure that the networks are more reliable, survivable and secure. This increased reliance on networks has caused industry to pay more attention to security requirements. The Report by the President's commission on critical infrastructure protection (1997) was created to spotlight the vulnerabilities and address the issue of security from all perspectives: military, industry and government.

## Definitions of Network Security

Fundamentally, the reason underlying network security is the value of the information riding on the network. As reprinted in Madron's book (Madron 1992), Admiral Grace Hopper pointed out in the 1970s, that the industry is engrossed only in the processing aspect of the information processors, and lacks a basic understanding of the "value of the information." Even though computers and networks have been around for decades, there appears to be the lack of a community wide agreement on adopting a framework to define, describe, and evaluate network security.

A framework is defined (*The American Heritage Desk Dictionary* 1981) (*Webster's Third New International Dictionary of the English Language* 1993) as a

conceptual structure that encapsulates the fundamental knowledge and the set of relationships of a discipline. A framework permits systematic and scientific reasoning about the discipline and is therefore essential to the advancement of the discipline. This dissertation research motivated the development of a framework for network security and added that the framework must be comprehensive, especially since the nature of networks is changing from a set of interconnected entities, controlled and used by a specific class of users, to an increasingly interconnected and integrated network which is simultaneously shared by different classes of users, and utilizes a language which is common between industry, government, academia and the military.

In the literature, definitions of network security terms are influenced heavily by the respective researcher's affiliation and background - industry, government, or military. Each of the three sectors continue to maintain their individual vocabulary which is built around the perceived threat and cost benefit. However, the distinction is increasingly being blurred by overlapping networks as is highlighted by a recent fact - 90% of the DoD's electronic traffic runs over the public networks (Baggett 1996). The lack of a common language to describe network security and the consequent inability to discuss network security hampers progress in the field and threatens the livelihood of millions of people and hundreds of corporations and government agencies. It is therefore imperative for all involved parties to agree on a common framework and revitalize the efforts towards evaluating network security. Recognizing this problem, the National Security Agency, the nation's proponent for computer and network security, organized the First

Network Rating Model (NRM) conference in Williamsburg, VA, on March 20-22, 1996 (National Security Agency 1996). The goal was to develop a comprehensive model to rate the security of networks that would be acceptable to government, industry, defense, universities, and other relevant organizations. As a result of the author's participation, the NSA adopted his framework approach and have acknowledged the published work in this area in the NSA draft NRM document. NSA's NRM is expected to draw upon the agency's vast expertise in the security products and certification fields to provide definitions, ratings and scopes of the individual framework element fields.

The development of security in automation and control over the years has been ad hoc, led primarily by the available technology and the goals of the funding agency. During World War II, the focus was on cryptography which aimed to protect written traffic between encoding and decoding machines. This is defined as communications security. With the proliferation of computers and the birth of networks, the role of cryptography also expanded into military networks. However, cryptography is only one attribute of a secure network and it, alone, cannot guarantee comprehensive security, particularly with today's and tomorrow's sophisticated computer literate population.

The US military methodically categorizes security attributes in the Orange Book (Department of Defense 1985) and the Red Book (Department of Defense 1987). While the concepts of COMmunications SECurity" (COMSEC) and "INFOrmation SECurity" (INFOSEC) are well understood within the Department of Defense, they mean little to most of industry and many civilian government agencies. A comprehensive literature

search was carried out that culminated in a detailed listing of the attributes of network security, as used by the military, and the specific terms used to describe them in industry and government. The common terms are grouped together and the best fit term was selected to describe the respective issue. As an example, consider the term, "classification," which the military uses to describe whether a network is restricted to a particular person, group, or class. This is further subdivided into the categories of - unclassified, for official use only, confidential, secret, and top secret. In contrast, the term, "private" or "proprietary" in industry restricts the use of a network to a specific person, group or class and therefore corresponds to the military's "classification." Motorola's POPI classification is based on whether failure to protect data may disrupt business, provide undue economic advantage to the receivers, cause embarrassment, permit access to other classified data, provide undue advantage to a competitor in the marketplace or in its negotiations with a mutual customer or in its market strategy or access to technology, or lead to legal problems including liability. A detailed discussion of network security vocabulary is contained in Chapter 3.

There are many specific examples of definitions of network security or lists of network security attributes. Schwartau (1996) sites many sources and creates many different lists of ways to subvert network security which by supposition, define what network security entails. These definitions include protecting the originality of data, encrypting data, reliability of the network, privacy of data, physical security of the network and its links. Unfortunately, the definitions are not comprehensive and are

presented as separate definitions, as lists of ways of corrupting the security of a network and range from the DoD's perspective to that of other government agencies and industry. Simonds (1996) cites several examples of what he calls security standards such as the DoD's Orange Book, OSI security services by ISO model layer, as well as listings of areas of network security such as authentication, access control and encryption. These standards and areas of network security are not comprehensive in and of themselves and are presented from the viewpoints of the different sectors which developed them. Winkler (1997) gives numerous examples of how security is violated in the corporate arena, but does not provide a comprehensive definition of network security. Efforts such as the Common Criteria (White 1997) are also focused on combining many of the security attributes into one unified standard. However, the criteria is yet to be standardized and argued as comprehensive. The framework described in Chapter 3 provides a basis to address, fundamentally, every weakness in a given network. None of these sources provides a comprehensive framework for network security which could be employed on a shared use (government, industry and military) network to address each group's security concerns.

A key difference between the industry, government, and defense perspectives has traditionally hovered around threats and their sources. This difference is also becoming blurred. To the military, the traditional threat has been the enemy, typically a hostile government or terrorist, whose efforts were aimed at stealing valuable information from the network. Today, however, a new kind of threat, termed "information warfare" (Power

1995), is gaining notoriety. It consists of disabling or rendering useless the enemy's key networks including the command and control (Power 1995), power grid (Baggett 1996), financial, and telecommunications networks. In addition, the threat of economic espionage, i.e., stealing secrets from industry and government networks, is on the increase. There is increasing evidence that insiders - disgruntled and recently fired employees, constitute the most significant threat (Edfors 1996). Malfeasants are another threat capable of causing mischief or serious harm to networks.

## Summary of Definitions of Network Security

In general, the definitions of network security in the literature are not comprehensive or universally applied. They are focused on the particular class of users perceived threat to their networks and security measures employed in the past. These definitions from the various classes of users (military, government and industry) are usually in the form of lists and in numerous cases use different vocabularies to describe the same aspect of network security. None of the definitions include all of the aspects of network security found in the literature by the author. The following section discusses the individual areas the different groups considered to be important for network security, as well as the divergent terms used to describe similar areas of network security. This information is used to develop the comprehensive network security framework discussed in Chapter 3.

## Development of a Comprehensive Network Security Framework

A comprehensive framework for network security did not exist in the literature when the author began this research in 1995. In a mixed use (military, government and industry) network, such a framework is a necessary element for providing a user level, security on demand system. The absence of a comprehensive framework compelled the author to develop one. Since that time, the author has published a fundamental framework for network security (Schumacher and Ghosh 1997a, 1997b) which fills this void and can be used in a user level, security on demand system in a high speed, shared use network. The author initially investigated the different views of network security by the several different classes of users discussed in the previous subsection. These views, along with the author's background in network security and working group meetings with the National Security Agency helped to develop and validate the comprehensive framework. Numerous sources which developed their own language and terms to describe network security were collected during the investigation of the area and development of a common framework. The framework allows discussions between these various groups using a common language and framework. The sources for the attributes and perspectives of network security as well as the differing terms used to describe them are discussed below.

Madron (1992) presents a generalization of the DoD's network security vocabulary of such terms as INFOSEC and COMSEC and provides the following definitions. Information security (INFOSEC) is defined to consist of procedures and

actions designed to prevent, for a given level of certainty, the unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional, of information in a network. Information includes data, control, voice, video, images and FAX. In contrast, communications security (COMSEC) refers to the protection resulting from the application of cryptosecurity, transmission security, and emissions security measures to telecommunications and from the application of physical security measures to communications security information.

Numerous authors provide additional vocabulary to describe aspects of network security. The following is a review of publications found during the literature search in this field. Abrams and Joyce (1995) review the trusted system concepts and reference validation mechanism and explores a new computer architecture to generalize the concepts for distributed systems. Nessett (1989) reviews the difficulties in authentication and notes the security advantages of centralized authentication during logon in distributed systems. Lin and Lin (1996) note that in enterprise networks, the principle security "areas" include confidentiality, integrity, data-origin authentication, non-repudiation, user authentication, and access control. They review public-key and secret-key cryptographic techniques for confidentiality and kerberos for third-party authentication. They also suggest the use of centralized security management over distributed schemes to reduce overhead and security risks. Cryptography has continued to play a major role in security. To Janson and Molva (1991), network security involves the tasks of controlling access to objects, enumerating the access rights of subjects, the threats that must be considered

during access control design, and mechanisms to enforce access control. They describe the role of cryptography as central to both authentication and access control. In addition, they propose tracking resource usage by authorized users at least for accountability and for subscribers to identify themselves to each other to fend off masquerading intruders.

Power (1995) introduces the notion of information warfare and notes that its scope includes (i) the electronic battlefield, i.e. disruption of enemy command and control, (ii) infrastructure attacks, i.e., failing key telecommunications, financial systems, and transportation, (iii) industrial espionage, i.e., covert operations aimed at stealing proprietary secrets or sabotage of company information network, and (iv) personal privacy, i.e., stolen private information such as credit card or driver's license or social security numbers. The security services required in Electronic Commerce (EC) networks (Geer 1995) include authentication, authorization, accountability, integrity, confidentiality, and non-repudiation. Geer (1995) also identifies two kinds of possible attacks on EC networks - (i) passive or pure listening and (ii) active or insertion of modified packets. To defeat such attacks, the goals of security must be aimed at preventing traffic analysis attacks, preventing release of contents attacks, detection of message stream modification attacks, detection of denial of service attacks, and detection of spurious association initiation attacks. Hosmer (1995) remarks that the desired goal in the current computer security paradigm is absolute security. This requires logical and mathematical precision while, unfortunately, precision and complexity are inversely

related. A related complication is that the future may witness other new types of threats to network security.

According to Hill and Smith (1995), the risks in the corporate world include personnel, property, information, and liability. Today's corporations are concerned with (i) protecting financial resources, personnel, facilities, and information, (ii) access control for facilities and management information systems, and (iii) recovery from disaster and continuity of operations. Chambers (1995) underscore the difficulty in detecting intrusion and notes that although the FDA network was successfully penetrated in 1991, the logging and monitoring tools, left running for weeks, revealed no signs of unauthorized access. Wolfe (1995) underscores the value of the information contained in the hardware by pointing out that for many likely events that arise from the lack of security, such as virus attacks, there is neither a widely accepted measure of risk nor is it likely to obtain insurance. Oliver (1995) traces the concept of "privacy" of computer users and individual-related data to the US Constitution and notes that it is provided by a third party as far as distribution, publication, and linkage of the information to the individual is concerned. Oliver also addresses the debate as to whether computer users making anonymous statements may be held accountable. Hitchings (1995) stresses the need to examine the human issues - cultures of people involved, attitudes, morale, and differences between personnel and organization objectives - relative to network security.

The literature on the use of audit trails to realize accountability, detect anomalous behavior of users, and possibly flag intrusion, is rich. Vaccaro and Liepins (1989)

describe their experiences with recording and analyzing anomalous behavior in computer systems at Los Alamos National Laboratory immediately following an intrusion. Helman and Liepins (1993) present a stochastic foundation for and analysis of audit trail analysis. They also suggest several criteria for selecting attributes. Janson and Molva (1991) proposes the tracking of system resource usage by authorized users for accounting as well as intruder detection. They enumerate the need to (i) identify objects access to which must be controlled, (ii) identify subjects whose access must be controlled, (iii) identification of the possible threats that must be defeated, and (iv) cataloging of enforcement mechanisms. Lunt and Jagannathan (1988) enumerate several discrete and continuous intrusion detection criteria and state that their system maintains system usage profiles of users which in turn, are periodically updated based on the a priori known user behavior. Kumar and Spafford (1994) encode the knowledge of known attack procedures through specialized graphs in their system and use of a pattern matching scheme to detect network penetration. Soh and Dillon (1995) present a Markov model of intrusion detection and devise a "Secure Computation Index" measure to quantify the intrusion resistance of a system. Their results, however, are limited to a single computer system. In her survey of intrusion detection techniques, Lunt (1993) notes that they are primarily based on maintaining audit trails and observes a few key controversial issues. They include the appropriate level of auditing, the voluminous amount of audit information, the comprehensibility of detailed audit information, the possible performance degradation as a result of audit, and the invasion of privacy of computer users. A variation of the audit

trail concept has been proposed for the electric power industry. Weerasooriya and colleagues (1992) present a neural-network solution to the problem of security assessment in large-scale power systems. They use neural nets for fast pattern matching of the state of the power system immediately following a "contingency" with historical trends. Their results are, however, limited to static-security.

Recently, many computer network experts (Edfors 1996)(Baggett 1996) have joined the electric power system researchers in sharing the latter's long-held belief of system availability (Billington and Khan 1992)(Computer Sciences Corporation 1994)(Klein and Menendez 1993) and transient stability (Pecas Lopes et al. 1987) as primary security concerns. Fitzpatrick and Hargaden (1994) argue that the design of complex networks must take into account scenarios where the network may be rendered unavailable by enemy action. They point out that in military command and control networks, units may need to continue fighting while out of contact with the higher headquarters and adjacent units, acting out of their own initiative within the framework of the commander's intent.

An analysis of the current literature reveals the following. First, the nature of the security concerns differs for each of the sectors - military, government, and industry. This has led to problems since many of these sectors are forced, for efficiency and economy reasons, to use each others networks. Third, there is the lack of a common framework and vocabulary to describe security and intrusion resistance of networks, an important issue that had dominated the Network Rating Model workshop. Fourth, the

traditional security criteria have already been transcended and it is critically important to address the issues of stability of networks, intrusion resistance, privacy, and other high-level security issues which will be elaborated in Chapter 3.

## Review of High Speed Network Security Research

Security in ATM networks is a recent and rapidly evolving phenomenon. The current literature is sparse and reveals two principal thrusts -- the use of cryptography to encrypt ATM cells and links and the use of digital signatures in authenticating end-to-end signaling. No work has been done on providing a truly user level, security on demand system which is comprehensive or implementing such a system in an ATM network simulator to study its viability and behavior. In June 1996, Cylink and GTE (Cylink 1996) were the first to demonstrate a commercial cell encryptor for ATM networks. Spanos and Maples (1996) have proposed a MPEG video compression algorithm to achieve security of multimedia traffic in ATM networks. Chuang (1995) proposes access control for secure multicast in ATM networks. Wilcox (1996) describes the experiences with the ATM testbed -- ATDNet, and reports that the four coupled areas of interest include ATM interoperability, distributed computing, information security, and high speed network connections. Deng, Gong, and Lazar (1995) propose mutual end-to-end authentication in signaling, cryptographic key distributions, and data protection, towards security in ATM networks. Stevenson, Hillery, and Byrd (1995) propose the use of cryptography to achieve data privacy and digital signatures to authenticate the end users

during the setup procedure. Cohen (1995) describes the ATM encryption process and the challenges and issues of encrypting cells and links. The encryption of ATM cells or links and the authentication in signaling, however, are only two elements of the much broader ATM network security.

In their presentation of the ATM Forum's approach to network security in ATM networks, Peyravian and Tarman (1997) propose the use of authentication, key exchange, and negotiation of security options, in an end-to-end manner as in the case of the Internet. Thus, their proposal inherits the basic difficulties of the peer-level, end-to-end approach. A fundamental limitation of data networks, including the Internet, is that the actual intermediate nodes through which packets propagate, are unknown a priori. Thus, security in the Internet is forced to assume the form of encoding the data packets through cryptographic techniques coupled with peer-level, end-to-end authentication mechanisms, such as Kerberos, at the transport or higher layers of the OSI model. Conceivably in the world-wide Internet, a data packet, though encoded, may find itself propagating through a node or a set of nodes in an insecure region of the world where it may be intercepted by a hostile unit. While there is always a finite probability that the hostile unit may successfully break the cryptographic technique, even when the coding is un-compromised, the hostile unit may simply destroy the packet thereby causing the end systems to trigger retransmissions which, in effect, slows down the network and constitutes a performance attack. Furthermore, the lack of confidence in the lower levels of the network OSI model forces Peyravian and Tarman to require, even after the virtual

circuit is established and the propagation of traffic packets is initiated, that some form of message authentication code be appended to every ATM packet. This results in high overhead and loss of efficiency. An additional serious difficulty is that the end-to-end network security approach may not be engaged until a virtual path has first been successfully determined by the call setup process. Peyravian and Tarman (1997) acknowledge this requirement while discussing ATM Security Messaging. For, there is always a chance that a call setup process may not succeed. However, once the virtual path has been determined, the intermediate ATM nodes have already been committed and it may already be too late in that many of the potential security considerations may no longer be available. The principal reason for the difficulty with the ATM Forum's proposal is the blind desire to follow the security techniques that have been developed for data networks and a disregard for the fundamental characteristics of ATM networks.

Fundamentally, in data networks, there is little control over the intermediate nodes through which packets propagate. This translates into a distrust of the intermediate nodes and a reliance on the slow, high-level end-to-end mechanisms. Fortunately, the ATM network is immune to this limitation. Therefore, the ATM network principles mandate a radically new approach to network security, one that may exploit the key characteristic of ATM networks namely, the control over the choice of the intermediate ATM nodes.

Current research in security for ATM networks follows the pattern set previously for other types of networks. The focus is on individual security implementations which are added on, after the network has been established or the methodology for

implementing and organizing security does not allow user level selection of security features. Recently, the author published an approach which employs the fundamental framework discussed in Chapter 3 in a user level, security on demand system integrated into a high speed computer network (Schumacher and Ghosh 1998a, 1998b, 1999) which is unique in that a security system which is comprehensive in its scope is provided at the user level, for more efficient use of security resources in a shared use network. This approach is discussed in Chapter 4.

# CHAPTER 3

# A FRAMEWORK FOR NETWORK SECURITY

## Introduction: The Need for a Security Framework

This chapter presents a fundamental framework for network security which describes a unified and comprehensive view of security among civilian, military, and government networks. It also offers a unique set of principles, inherent in the framework, to enable the realization of the dynamic risk assessment approach across different types of networks for any type of user -- civilian, military, or government. Under dynamic risk assessment, security is viewed as a resource and the network security problem is mapped into a resource allocation problem which takes into consideration, dynamically, the risks, threats, resource availability, cost, and other parameters. Thus, this approach reflects a pragmatic, cost effective, and best effort approach to provide a user on demand network security system. It also derives a part of its momentum from the increasing trend towards the merging of civilian, military, and government networks. The framework, developed by the author, consists of eight perspectives and nine attributes. The perspectives, termed pillars, individually provide orthogonal views of network security and collectively constitute a comprehensive stable structure that supports the total network security. The attributes refer to the inherent characteristics of a secure network. The framework provides a basis to address, fundamentally, every weakness in a given network.

Furthermore, it applies to every level of the network, starting at the highest network of networks level and down to the single computing node that maintains connections with other nodes. Thus, the framework enables the understanding of the security posture of an individual network, in a comprehensive manner, the comparative evaluation of the security of two or more networks, and the determination of the resulting security of a composite network that is formed from connecting two or more networks with known security. These uses of the framework can be extrapolated to establish a user level, security on demand system in an ATM network. Such a system is discussed in detail in Chapter 4.

As part of the development of the comprehensive network security framework, the author participated in work the National Security Agency initiated on developing a Network Rating Model (NRM). This chapter presents information on the development of the NRM leading up to its draft definition document, arrived at by consensus, at the National Security Agency's NRM conference in March 1996 and a subsequent NRM author's group workshop in July 1996. The framework approach proposed by the author was adopted at the NRM author's group workshop.

The analysis of the current literature in Chapter 2 revealed the following. First, the nature of the security concerns differs for each of the sectors - military, government, and industry. This has led to problems since many of these sectors are forced, for efficiency and economy reasons, to use each others networks. Third, there is the lack of a common framework to describe security and intrusion resistance of networks, an

important issue that had dominated the Network Rating Model workshop sponsored by the National Security Agency. The framework developed is comprehensive in the sense that it includes all of the different sectors concerns and definitions for network security. Such a comprehensive framework can be used by all parties to describe their own network's security as well as compare their network's security to other networks.

## The Changing Paradigm of Network Security

The definition of network security has evolved over time. The general concept of security in message communications may be traced to the advent of human civilization. In contrast, however, security in automation and control is a recent phenomenon, originating with the computer age and is rapidly gaining importance with the proliferation of networks. With computer networks integrating the dual functions of (i) communications and (ii) automation and control, computer network security must address the security issues inherent in both communications and automation. Until recently, research and development in computer security was strongly linked with cryptography including encryption and decryption of electronic messages. However, as computer networks have started to proliferate into large, complex, real-world systems, such as electronic banking, the power grid, and the proposed intelligent vehicle highway system, the author believes that computer network security has transcended the traditional definition and has migrated to a higher, logical level. In current and future networks, the information riding on the network may control parts of the network while the control, in

turn, may ensure the correct propagation of information from the source to the intended destination. Thus, networks constitute complex, multi-dimensional entities that require security at different levels of both network hardware and network software.

Threats to network security have also evolved resulting in changes to how network security is defined and viewed. In contrast to the classic threats, e.g., the military espionage of the former Soviet Union, hostile governments, and terrorist organizations, the new threats include information warfare (Power 1995) and, more recently, the threat of liability law suits, stemming from failure to protect information. While there are outside threat sources, Edfors (1996), Madron (1992) and Simonds (1996) reveal that the greatest threat has always and continues to be "insiders." Madron estimates that as high as 75% of possible attacks on a network emanate from one or more sources inside the network establishment. In response, both government and industry are emphasizing internal threats. Threats may be leveled at a network from several different aspects of that network. That is, while a hacker may infiltrate applications and divert financial transactions to a fictitious account, another intruder may attack the performance of the network and render the network virtually unusable. The following is a list of the key threat sources:

- Outside threats including terrorism, hackers, malfeasants, ex-employees, foreign espionage, economic espionage by foreign governments or foreign or domestic corporations, and liability law suits.
- Inside threats including employees, hackers, mischief, legal, and uneducated users.

The literature records the use of audit trails, cryptography, and authentication techniques to ensure network security. However, these techniques are essentially confined at the lower level and are ad hoc. Hitchings (1995) strongly believes that a new approach to information security is needed. This chapter theorizes the need for a logical, high-level approach towards comprehensive network security and argues that the networks and algorithms, underlying the high level applications, must integrate the security concerns into their design. The overall approach must continuously monitor the exchange of data between sites and within a site to detect or defeat intrusions and unauthorized activities as well as a fail-safe method for detecting system faults before they become catastrophic. The approach must anticipate the presence of malicious and ignorant users everywhere and not take the validity of any data for granted. Further discussion of such an integrated security scheme is contained in Chapter 4.

Increasingly, experts in computer systems are recognizing the vital role of system availability or stability, a concept that has long been recognized in the electric power community. If an enemy succeeds in degrading the command and control network sufficiently, none of the sophisticated cryptographic schemes are useful since no messages will get across the networks. The nation's well being is at risk if an enemy is capable of rendering the telecommunications network unavailable, without engaging the traditional defense forces or firing a single shot.

The phenomenal growth of distributed networked systems coupled with their enormous future potential marks a new era in the information age. On the other hand,

their ubiquity and the near total dependence for day to day activities, coupled with their complexity and vulnerability to stability raises a deep concern. The algorithms that underlie the distributed systems are complex and are susceptible to external and environmental disturbances. The well known incidents of unexplained system failures in IBM mainframes despite smooth running for decades, the discovery of previously unknown errors in AT&T network software, and the numerous unreported telephone system failures across the country, all attest to the complexity of the underlying algorithms. A researcher from a major manufacturer of Automated Teller Machines acknowledges that the nation's ATM network is a collection of patchwork and it is a miracle that it works. The perturbations, even if transient, may degrade the system performance, either lightly or severely, or cause catastrophic failure. It is therefore imperative that the research community undertake serious efforts to understand the issue of stability in depth and synthesize performance metrics. These changing threats have caused a shift in the network security paradigm from one of certification to one of risk assessment.

## The National Security Agency's Network Rating Model (NRM)

Given the wide scope of today's networks and their enormous future potential, the goal to achieve comprehensive network security is challenging. The overall goals of the NRM workshop were to determine the degree of protection that should or could be provided, synthesize a measure of protection and a methodology for evaluation, and

determine the cost and performance tradeoffs. The workshop was organized to first arrive at a definition of network security, acceptable to the government, military, industry, and academia. Next, the potential threats were enumerated and the key attributes of a secure network identified. Logically, one must bound what one is protecting before one can analyze how well one is protecting it. Thus, the attributes serve as potential weak points in a network. It is increasingly evident that the vulnerability or security of a network may be viewed from different conceptual points of view, termed perspectives by the author. Although this idea is referred to as "disciplines" in the literature, the term "perspectives" appears to capture the underlying meaning more accurately. Therefore, the total security of a network requires its detailed evaluation, relative to every perspective. While one organization, building on its assumption of a specific set of threats, may find one subset of the perspectives important, another organization may find a different subset of the perspectives critical based on its own perceived threats.

The consensus definition of a Network Rating Model is: "A consistent, cost-effective methodology based upon a defined set of characteristics for assessing the total security of any network or combinations of networks, either in operation or development; to define what exits, determine what is needed, identify what could affect security, and provide a universally acceptable assessment report."

In the definition, the term "consistency" stresses the need for the security rating of a network to apply uniformly across different sectors. Furthermore, a rating must be

valid for a reasonable length of time into the future despite rapid advances in networking technology. The cost effectiveness criteria underscores the need to balance the cost of the threat against the cost of implementing security. The defined set of characteristics is currently under consideration. The total security refers to the different dimensions of a secure network while the phrase "network or combinations of networks" reflects the increasing blur between network boundaries. Since the report must be universally acceptable and useful, it must record the security measures currently in place in the network which, in turn, will facilitate identifying what more is required to ensure total security.

In order to define the characteristics or attributes of a given secure network, it was agreed at the workshop that one must focus on the relevant set of network security perspectives to yield security services that satisfy stated concerns. The comprehensive list of perspectives include (a) systemic, (b) communication, (c) physical, (d) personnel, (e) operational, (f) application, and (g) performance. The services were enumerated as (a) access control, (b) confidentiality, (c) integrity, (d) authentication, (e) traffic flow security, (f) assured service, (g) non-repudiation, (h) anonymity, and (i) intrusion detection. The concerns included (i) accountability, (ii) availability, (iii) liability, (iv) reliability, (v) audit-ability, (vi) interoperability, (vii) confidentiality, and (viii) integrity. These perspectives, services, and concerns are corroborated in (Edfors 1996).

At the first NRM workshop, given the limited time available for a thorough discussion, security services and concerns were separated into two distinct lists. This

split is driven by the divergent views of the representatives of industry, government, and military, which, in turn, stems from differing perceptions of the threat sources. Upon careful analysis, it is increasingly evident to the author that a unified approach to total network security, i.e., across the military, government, industry, and university, sectors, requires the recognition of two fundamental components of network security. First, any secure network must possess a few inherent characteristics, regardless of the sector to which it belongs and independent of any specific threat. The characteristics are referred to as attributes of a secure network and is the result of unifying security services and concerns. Second, a network's security may be viewed at different conceptual layers, each view reflecting a threat, being relatively orthogonal of others, and thereby permitting independent development and evaluation.

The NSA's NRM work is important because it validates the need for a common framework across all sectors - military, government, industry, as well as the author's own work on developing a network security framework. The author's work and participation was instrumental in the NRM adopting the framework approach.

## A Comprehensive Network Security Framework

As a result of the author's research into current literature, work with the NSA's NRM and the author's own background with network security in the military, a comprehensive network security framework was developed. Figure 1 presents a representation of the author's framework through a matrix. Conceptually, network

security may be viewed as one where the attributes permeate each of the pillars that, in turn, collectively hold up network security. The relative strengths of the pillars may vary, depending on the perceived threats in a given scenario. Thus, network security is only as strong as the weakest pillar. The concept provides an organized framework for the network security evaluation information, which may be utilized to improve security or to evaluate the resulting security from interconnecting two or more networks. Ideally, a fully secure network would require every attribute to be strongly protected in all pillars, subject to some standard threat, relative or absolute. However, this may be neither cost effective nor practical due to limited time and resources. Network security related decisions are based on the perceived threat to a particular pillar and/or attribute and the level of risk that the security management is willing to assume.

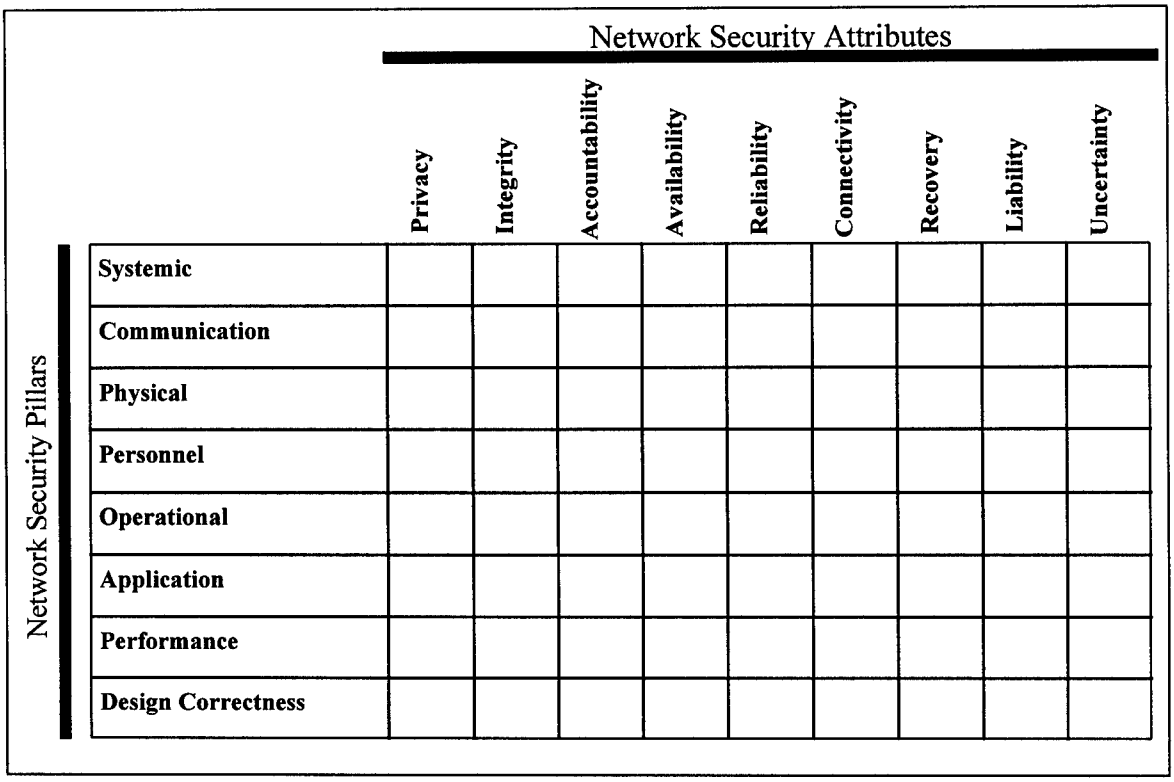



Figure 1. Comprehensive network security framework.

The list of attributes include (1) privacy, (2) integrity, (3) accountability, (4) availability, (5) reliability, (6) connectivity, (7) recovery from disaster, (8) liability, and (9) uncertainty, and they constitute a superset of the attributes proposed in the literature. The list of pillars include (a) systemic, (b) communication, (c) physical, (d) personnel, (e) operational, (f) application, (g) performance, and (h) design correctness.

## Pillars of Network Security

The choice of the term pillars reflects the eight foundation blocks, each of which may be under attack, either independently or collectively, and they cumulatively support

a network's security. Thus, each pillar corresponding to the seven perspectives, reflect the seven foundation blocks that individually describe an orthogonal conceptual view of network security and may be developed and evaluated independently, based on the degree of importance assigned to the appropriate threats. Consequently, the pillars may exhibit different relative strengths. Should new types of threats emerge in the future, requiring additional views of network vulnerability, additional pillars may need to be incorporated into the framework. The scope of the seven pillars are elaborated as follows:

- Systemic encompasses the software that operates the network and constitutes the basic infrastructure of the high-level application software.
- Communications encompasses the links and devices that interconnect the computers to constitute the network.
- Physical encompasses the equipment, material, and documents associated with the network.
- Personnel encompasses the people associated with the operation or use of the network.
- Operational encompasses the procedures, policies, and guidelines that constitute the security posture of networks.
- Application encompasses the high-level software that executes on the network.
- Performance encompasses the normal range of operating parameters and throughput of the network.
- Design correctness encompasses the correctness of the total system. The complex interactions between the different components of the system will, in general, result in a

very large number of states and state transitions. Without ensuring that every state and state transition is correct, the threat of the system entering an unstable state which then triggers catastrophic failure, is very real.

## Attributes of Network Security

Each of the attributes will bear a specific degree of relationship to each of the nine perspectives or pillars, defined by the network and the current understanding of security attacks. While most of the relationships are readily understood, a few are unclear at the present time, while all are subject to evolution as our understanding of network security matures. For instance, the Privacy attribute bears a strong relationship to the Personnel pillar. In contrast, consider the relationship between the Performance pillar and the Liability attribute. At the present time, the relationship is weak since it is difficult to prosecute a hacker for degrading a network's performance and even more difficult to quantify the degradation and, therefore, determine a commensurate punishment. However, as society acquires a better understanding of the responsibilities and consequences, the relationship will be greatly refined. The relationships may be evaluated, objectively or subjectively, through mechanisms, some of which are well known while others are yet undefined. As an example, the use of background checks may help strengthen the Privacy attribute and the Personnel pillar. Similarly, the strength of the relationship between the Systemic pillar and Privacy attribute for a given network may be evaluated through the access controls implemented. While the dependencies

between the (i) "Design correctness" pillar and the attributes and the (ii) "Uncertainty" and "Liability" attributes and the pillars, are clear, the exact relationships and the corresponding mechanisms to evaluate them are yet to be defined. The attributes are elaborated as follows:

- Privacy (Power 1995) (Oliver 1995) is defined as intended for or restricted to the use of a particular person, group or class. It applies to data, control signals, and traffic flow. Synonymous and associated words in the literature include confidentiality (Janson and Molva 1991) (Geer 1995) anonymity (Oliver 1995), classification (Department of Defense 1985), proprietary, TRANSEC, cryptosecurity, EMSEC, and encryption (Madron 1992).
- Integrity (Klein and Menendez 1993) (Geer 1995) is defined as ensuring that information held in a system is a proper representation of the information intended and that it has not been modified, created, destroyed, or inserted by an unauthorized entity. Integrity also refers to the processes, process sequences, and other system assets. Synonyms and associated words include soundness, incorruptibility, completeness, and honesty.
- Accountability (Oliver 1995) is defined as a statement or exposition of reasons, causes, or motives to furnish a justifying analysis or explanation which can be documented or traced and ownership established. Synonyms and associated words include non-repudiation (Klein and Menendez 1993), audit-ability (Lunt 1993), audit trail (Lunt 1993), answerable, authentication (Geer 1995), signature, and responsibility.

- Availability (Janson and Molva 1991) (Klein and Menendez 1993) is defined as qualified and present or ready for immediate use by authorized users and worthy of acceptance or belief as conforming to fact or reality. Synonyms and associated words include access control (Janson and Molva 1991), authentication (Geer 1995) and confirmation.
- Reliability is defined as generating consistent results during successive trials. Synonyms and associated words include assured service, assuredness, certainty, and dependability.
- Connectivity (Guidoux 1995) is defined to consist of the devices that constitute the network including the computers and links between them, and the intelligence that supports the seamless and transparent integration of a wide variety of different protocol driven terminals and host computers. Synonyms and associated words include interoperability, traffic flow, logical flow, associations, relationships, emissions control, and TEMPEST.
- Recovery (Hill and Smith 1995) is defined as returning from a disaster and continuity of operations. Synonyms and associated words include self healing and contingency planning.
- Liability (Hill and Smith 1995) is defined as having to do with legal obligation and responsibility that may affect property and information. Synonyms and associated words include responsibility, due process, ethical responsibility, open, and exposure,

i.e., lack of protection or powers of resistance against something actually present or threatening.

- Uncertainty reflects the lack of complete knowledge of the system security as a result of previous penetrations, with known and unknown consequences, that may degrade future network security. This attribute may be viewed as a generalization of the concept of anomaly detection (Lunt and Jagannathan 1988) in a user's behavior through audit trail analysis.

## Uses of the Network Security Framework

The framework provides a basis to address, fundamentally, every weakness in a given network. Furthermore, it applies to every level of the network, starting at the highest network of networks level and down to the single computing node that maintains connections with other nodes. Thus, the framework enables the understanding of the security posture of an individual network, in a comprehensive manner, the comparative evaluation of the security of two or more networks, and the determination of the resulting security of a composite network that is formed from connecting two or more networks with known security. These uses of the framework can be extrapolated to establish a user level, security on demand system in an ATM network which is discussed in detail in Chapter 4.

The value of the proposed framework is in that it stimulates the network designers to examine the vulnerabilities of all eight pillars even when they may appear inconsequential. For instance, while a credit card network, operating on the Internet, may successfully address the Privacy attribute and feel secure, malicious agents may penetrate the network and reduce the availability such that customers are denied from making purchases. An examination of the Performance pillar may be advisable under these circumstances. In a different scenario, while the military assigns resources to ensure the Privacy and Connectivity attributes, a disgruntled employee may send out an unauthorized message, under an assumed id, to the finance and accounting military pay program, take advantage of a weakness in the Accountability attribute, and deny hundreds of thousands of soldiers their pay on time.

The procedure for determining a rating of a network consists of the following. For a given standard threat level, relative or absolute, and a given environment, the strengths of the intersection points in the matrix are obtained through evaluating the corresponding mechanisms. The evaluations may assume the form of numerical values, narratives, or graphs, subjective or objective. To improve the security posture of the network, either (i) the individual values along a row that constitute an evaluation of the corresponding pillar, may be examined against a perceived threat level, or (ii) the values along a column that reflect an evaluation of the strength of the corresponding attribute, may be compared against a desired measure for the attribute. Clearly, the desired measure will reflect a cost-benefit analysis, i.e., the level of risk that the security

management is willing to assume. As indicated earlier, the matrix provides a meaningfully organized framework for the network security evaluation information, in terms of its fundamental characteristics. Thus, to compare the security postures of two or more networks, either (i) the individual values along a row of the corresponding matrices may be examined against each other, or (ii) the values along a column of the corresponding matrices may be contrasted.

To understand the operation of the framework, consider that the military perceives the primary threat to its networks and data from hostile governments. Clearly, to the military, the Communications and Physical pillars are vulnerable. This, in turn, points to the Connectivity attribute. Furthermore, the desire to protect data riding on the network requires focus on the Privacy attribute. In contrast, consider a financial network's concern that a malicious agent may disrupt its financial services. Clearly, the Systemic pillar is vulnerable which in turn, points to the Connectivity attribute. In addition, the Privacy attribute may also be flagged due to the confidential nature of the financial transactions.

Assume that a defense agency plans to send Top Secret traffic through a network. Initially, it will insert the highest value, say 0, in the entire privacy column and communication row, of the matrix associated with the corresponding call request. To successfully propagate the traffic through the network, the call setup process must first determine a route, if possible, where each and every ATM node along the route offers a privacy value of 0 in every pillar and 0 in every attribute of the communications pillar.

The values assigned to the elements of the security framework matrix of the node reflect the strengths of the security in the respective domain. The values of the individual elements may differ over a wide range, with some elements possibly being nine, implying the absence of security in that element area. Examples of three matrices, corresponding to three military traffic types -- Top Secret, Secret, and Confidential, are presented in figure 2 along with the relevant element values.

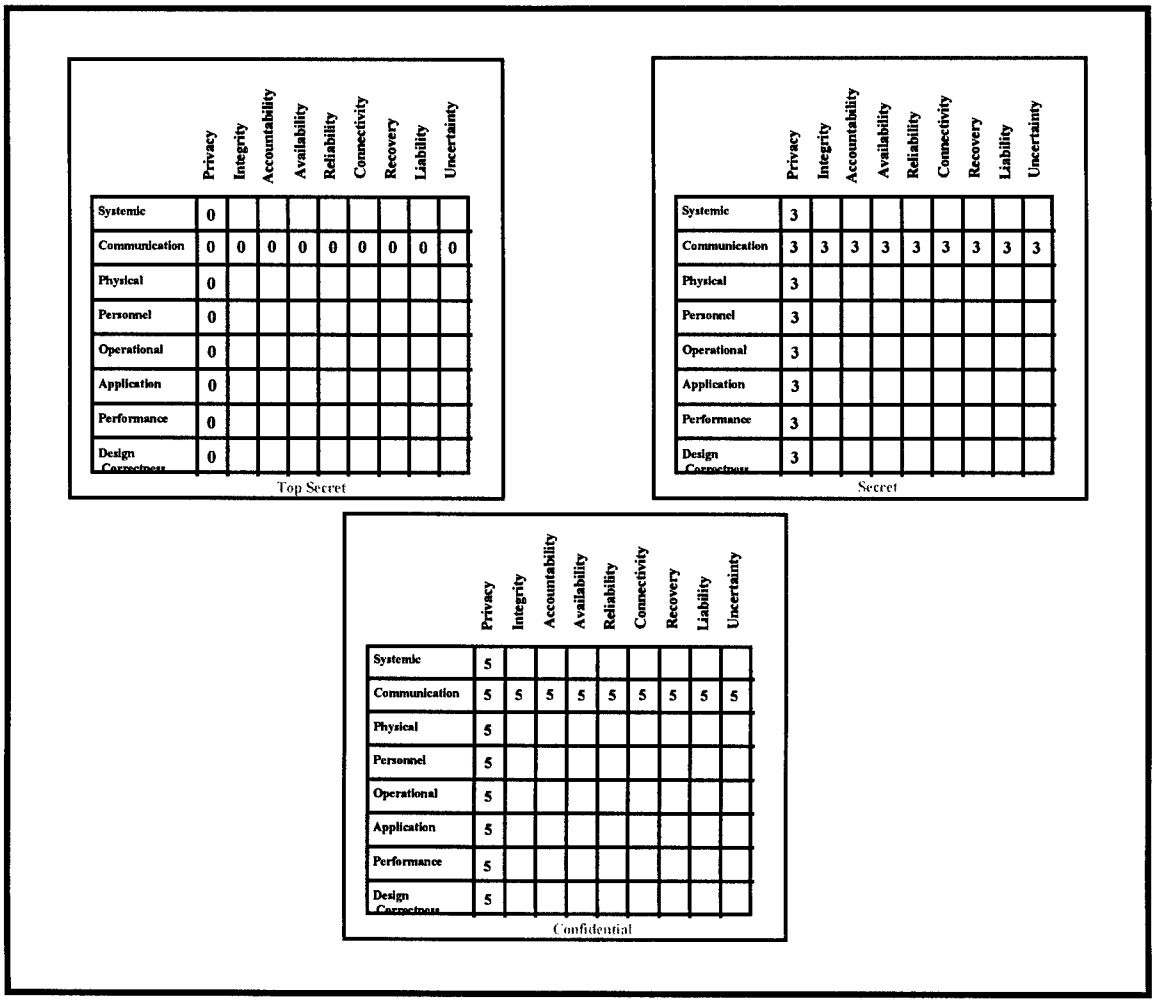



Figure 2. User specified security matrices for military traffic.

It should also be noted that network security is a continuous process and must be exercised periodically. With time and as the roles of networks evolve, security breaches may appear in previously unsuspected areas.

The framework's second use is in computing the resulting security of the composite network, AB, formed from connecting two networks -- A and B, with known security and shown in figure 3.

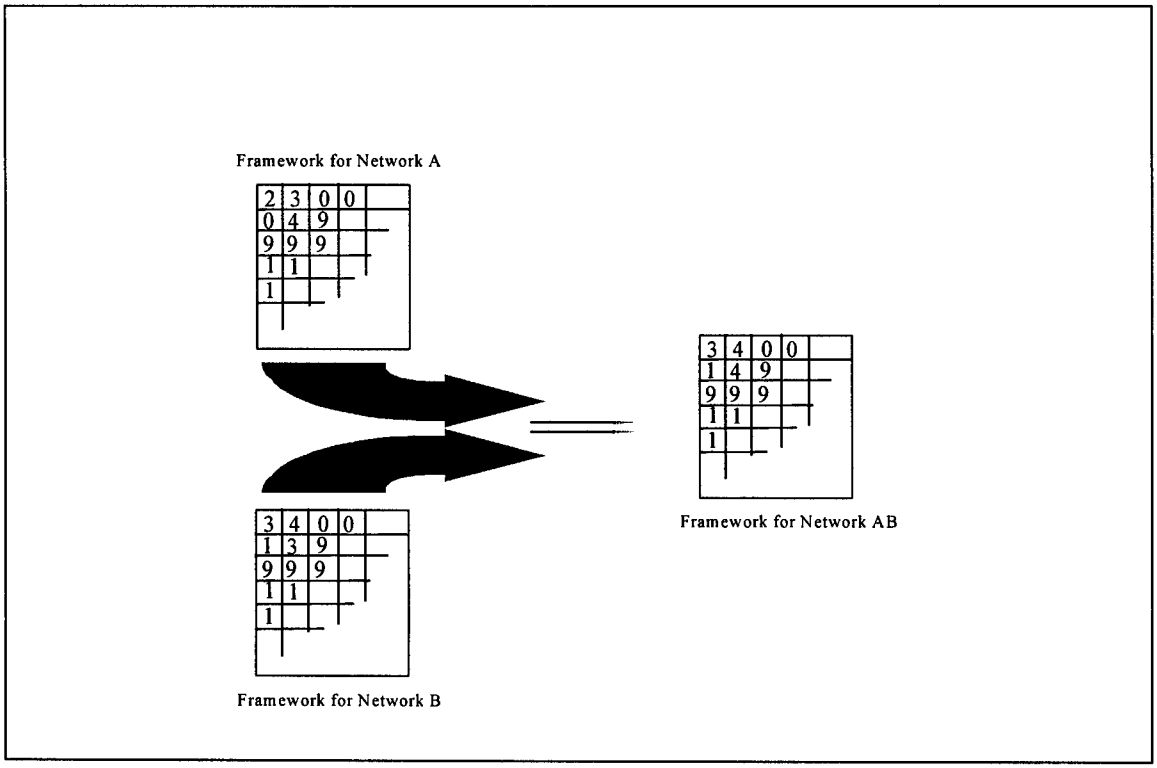



Figure 3. Comparing two network's security.

By design, the framework applies to every level of the network, starting at the highest network of networks level and down to the single computing node that maintains connections with other nodes. A key goal of the framework is to provide a template for organizing the different aspects of network security to permit the military, government and industry to start their connectivity discussions from a common baseline. Whether they choose to use or ignore some or all of the elements of the framework is their decision and is based on the amount of risk they wish to assume. In any case, they will all be aware of the total framework and all of its elements. The perspectives, termed pillars, individually provide orthogonal views of network security and collectively constitute a comprehensive stable structure which supports the total network security. The attributes refer to the inherent characteristics of a secure network.

The framework's third use is in a user level, security on demand system. The author hypothesizes that key attributes of specific networks may be exploited to reduce the potential performance impacts that may arise from implementing security measures. To achieve security in ISDN networks, Fernandez and Subbarao (1994) claim to implement Rivest-Shamir-Adleman (RSA) encryption algorithm for authentication and Data Encryption Standard (DES) algorithm for encryption, transparent to the user and without any software upgrades to the switch, through embedding the schemes in the ISDN Customer Premises Equipment (CPE). Given the growing popularity of ATM networks, their future potential, and the lack of comprehensive high-level security characteristics, the author modeled and implemented a user level, security on demand

system in an ATM network simulator. Details of the implementation, results and analysis are presented in the following chapters.

The advantages of an ATM network include its high speed, small packet size, point to point connection, and virtual path-oriented transmission of messages. Other issues important towards developing security mechanisms include whether the ATM nodes are physically secure, whether the network will be statically configured or permit dynamic reconfiguration, whether routing will be primarily limited to domestic nodes or exploit the less heavily used international nodes, whether commercial carrier links will be utilized, whether the dropped cells, if any, are destroyed thoroughly, and whether the commercial networks will be capable of implementing levels of security. Where the network is dynamic, the procedure for adding and deleting nodes including the authenticity of the control message to add or delete a specific node will impact on security. Where routing occurs through foreign countries, perhaps with different communications eavesdropping laws, countermeasures must be designed to protect the information riding on the network.

## Summary

This chapter presents the definition of the network rating model, arrived at by consensus, at the National Security Agency's Network Rating Model (NRM) conference in March 1996 and a subsequent NRM author's group workshop in July 1996. It proposes a comprehensive, fundamental framework for network security which consists of eight

perspectives of network security and nine attributes of a secure network. The author's framework approach was also adopted at the NRM author's group workshop. The perspectives of the framework, termed "pillars" in this chapter, individually provide orthogonal views of network security and collectively constitute a comprehensive stable structure that supports the total network security. The attributes reflect the inherent characteristics of a secure network. The author's framework fills a need within the community which had previously been left unfulfilled. The uses of the framework are threefold. The framework enables the understanding of the security posture of an individual network, in a comprehensive manner, the comparative evaluation of the security of two or more networks, and the determination of the resulting security of a composite network that is formed from connecting two or more networks with known security. The framework can also be used as a basis for a user level, security on demand system in an ATM network. A discussion of such a system follows in the next chapter.

# CHAPTER 4

# SECURITY ON DEMAND IN AN ATM NETWORK: A DYNAMIC ALLOCATION STRATEGY

## Importance of Security on Demand

The traditional, certification based approach attempts to guarantee the security of a network through risk analysis that involves the static analysis of the risks, threats, resource availability, cost, and other parameters. Certified networks are generally confined to a limited domain and, as a result, they are isolated, costly, and under-utilized. In data networks including the Internet, security assumes the form of encoding the data packets through cryptographic techniques coupled with peer-level, end-to-end authentication mechanisms, such as Kerberos, at the transport or higher layers of the OSI model. While the high-level, end-to-end mechanisms are slow, conceivably in the world-wide Internet, a data packet, though encoded, may find itself propagating through a node or a set of nodes in an insecure region of the world where it may be intercepted by a hostile entity. While there is always a finite probability that the hostile unit may successfully break the cryptographic technique, even when the coding is not compromised, the hostile entity may simply destroy the packet thereby causing the end systems to trigger retransmissions which, in effect, slows down the network and constitutes a performance attack. In ATM networks, while cryptography is utilized to

encrypt ATM cells, the ATM Forum proposes the use of authentication, key exchange, and negotiation of security options, in an end-to-end manner as in the case of the Internet.

Due to military security requirements, a "mixed use" network consisting of all types of users such as the military, industry, government agencies and academia cannot be created without a user level, security on demand system. Currently, the military keeps its secure networks isolated from nonsecure civilian networks. In addition, even within the DoD, the secure networks are organized into three totally separate networks to carry traffic at (1) Top Secret - (2) Secret - (3) Confidential - levels (Department of Defense 1987). Due to the obvious risks and the unknown resultant security from combining networks, the U.S. military is unwilling, to date, to mix their secure traffic on commercial networks and continues to build and operate costly, separate and totally isolated networks for their secure traffic. Some of the risks the military is trying to avoid include the misrouting and/or possible interception of classified data by unauthorized parties, unauthorized use of encryption devices, malicious disruption of unprotected network resources through physical destruction, or denial through remote software bombs or viruses. The current state of the DoD regulations relative to network integration stems from the lack of a sound theoretical basis and a proven practical approach. The security on demand approach, developed in this dissertation, allows the military to integrate all of its networks along with the commercial networks and still address all of its security requirements and concerns. The framework described in Chapter 3 and integrated into the security on demand system provides a method to indicate the type and level of

protection of all of the military's possible security requirements as well as any other user group's security requirements. While a security on demand system would enable the military to combine its three types of classified networks in addition to its unclassified networks, the ability to offer the security on demand system down to the user level enables all types of user groups such as the military, government agencies, industry and academia to use the same, "mixed use" network.

Security must be universally understandable, applicable and agreeable to all user groups before a true, "mixed use" network can exist and function to all user groups security expectations. The comprehensive framework discussed in Chapter 3 provides the ability for all user groups to define their security requirements within the context of the framework. The framework, when integrated into an ATM network, provides a template for matching network security resources to user requirements.

The user level aspect of the security on demand system is possible in an ATM network due to ATM's unique call setup process. The integration into an ATM network of the user level, security on demand system enables a "mixed use" network to be created and offered at the user level, enabling the military to use the public ATM network backbone to augment its newly combined network of networks to effectively manage limited and costly security resources. Such a combination of networks would provide additional routes for unclassified traffic, thereby relieving congestion on links with costly security resources. Currently, the DoD does not permit the mixing of commercial traffic on DoD nodes and links. However, the future may witness significant improvement and

economy in security resources and commercial traffic that desires secure transfer may be permitted, in a limited manner to use the DoD resources.

This chapter presents a user level, security on demand system, that results from an integration of the recently introduced fundamental framework for network security presented in Chapter 3 with the fundamental and unique characteristics of ATM networks. The concept of a virtual path in ATM networks (Sato, Ohta and Tokizawa 1990) which was introduced because of its efficiency and favorable economic impact, can also be used to create an efficient and cost effective security on demand system. In this approach, the security capability of every node and link is determined, utilizing the framework. Under call setup, the ATM network allows the system to configure, i.e., first project and then verify through propagating a setup message which includes a Designated Transit List (DTL) packet, a route from the source to the destination, including every intermediate ATM node and link, that meets the security requirements of the user. Every user specifies the appropriate elements of a security matrix that represents the desired security requirements, in addition to the usual bandwidth and other Quality of Service (QoS) requirements. This ability of the network to provide, personalized, security on demand service to every user reflects a unique and the most desirable method of utilizing and distributing the security resources. Traffic is launched when the call setup succeeds, otherwise, the call fails. Thus, the approach is fundamentally the most logical approach to comprehensive security in ATM networks. It also views security as a distributed network resource and allocates it to each user efficiently, based on demand and dictated

by the need. This approach has been integrated into the Call Admission Control (CAC) algorithm of the ATM Forum proposed Private Network-Network Interface (PNNI) specification (ATM Forum Technical Committee 1996), modeled for a representative, 50-node ATM network, and an asynchronous distributed simulation which is discussed in detail in Chapter 5 and was executed on a testbed of 25+ Pentium workstations under Linux, configured as a loosely-coupled parallel processor. The success of the implementation validates the approach and the asynchronous distributed simulation closely resembles an operational ATM network. Performance results obtained utilizing stochastic and representative input traffic, presented in Chapter 7, reveal that the overhead of integrating security into CAC is negligible.

## Call Setup in an ATM Network

ATM networks are ideal for implementation of the proposed user level, security on demand system because the route the user's data will follow is known a priori and can be manipulated during the call setup. In ATM networks, when a user launches a call, the ATM node that intercepts the call, termed source node, is responsible for organizing a route or virtual path up to the destination node. For geographic, geo-political, and other reasons, the nodes of an ATM network may be organized into groups where the intra-group connectivity information is strictly local to every group. However, information on the inter-group connectivity is contained within every group, thereby enabling any node within a group to compute a path, in terms of other group identifiers, to the destination

group that contains the destination node. Clearly, the path within a group may be computed in terms of the nodes, while the detailed paths within the intermediate groups are computed locally by the corresponding groups. The ATM Forum specifies a skeleton protocol, termed Private Network-Network Interface (ATM Forum Technical Committee 1996), to characterize the route determination process. Under PNNI, in the determination of the route, a source node may utilize any function of the relevant parameters including physical propagation delay of the ATM links, processing delays of the ATM nodes, etc. Once the route is computed by the source node, the ATM networking model requires the source node to launch an actual setup message including the Designated Transit List (DTL), that is required to traverse through each of the actual ATM nodes in the appropriate groups, reserving the corresponding bandwidth, where available. In the event that the setup message fails to reserve the user required bandwidth, the message returns as unsuccessful and the call fails. Where the setup message succeeds in reserving the bandwidth all along the virtual path, up to the destination node, the call processing is viewed as a success and the user traffic is then launched on the switching network.

Consider, for example, the ATM network shown in figure 4. The network consists of five nodes in the greater Baltimore/Washington metropolitan area located in Baltimore, downtown Washington, D.C., the White House, Alexandria and Norfolk. Except for the links between the nodes in downtown D.C. and Alexandria and Norfolk, the physical propagation delays for all links are under 1 millisecond. A possible scenario

would be a call from the president's staff, located at the White House node, requesting to establish a connection to Norfolk for a live television interview with a local TV station.

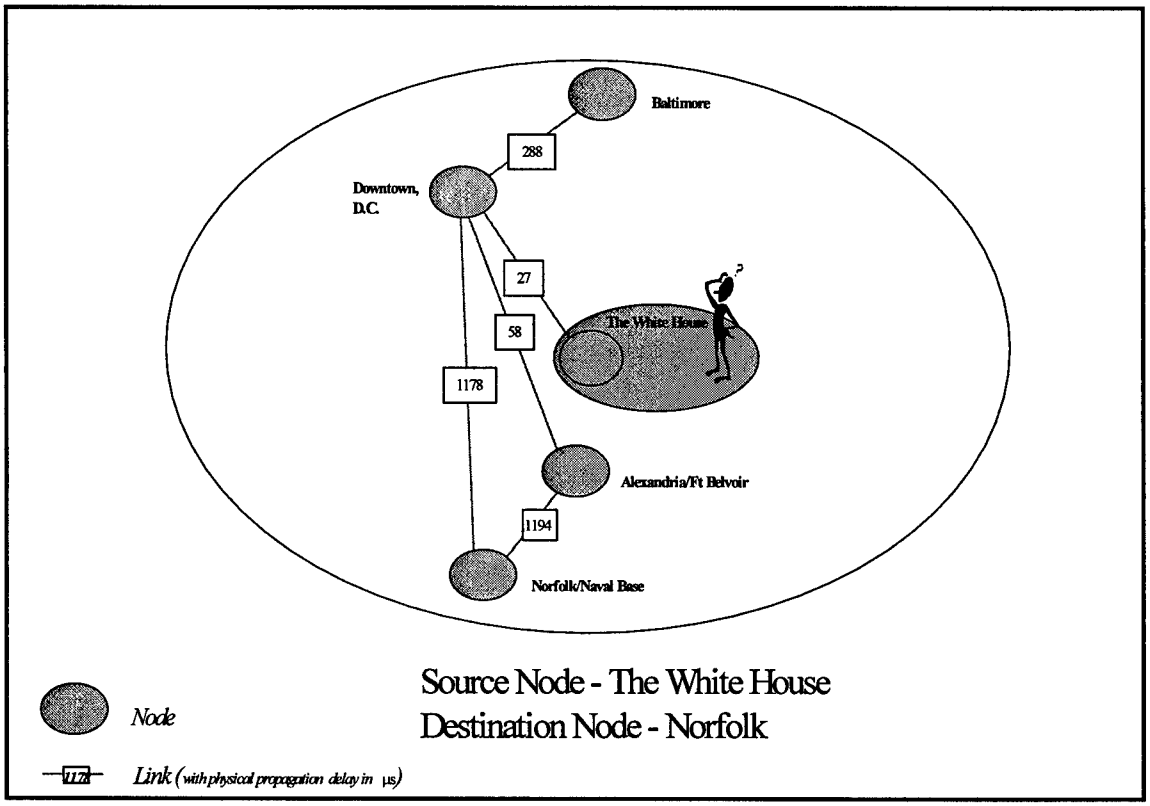



Figure 4. ATM call setup between the White House and Norfolk.

For the given topology in figure 2, there are two possible routes. One would traverse through the downtown D.C. node, to Alexandria and on to the destination at Norfolk. The other would also go through the downtown D.C. node and then directly to Norfolk. If latency delays are used in conjunction with a bandwidth availability check,

the route selected would be through the downtown D.C. node straight to Norfolk as shown in figure 5.

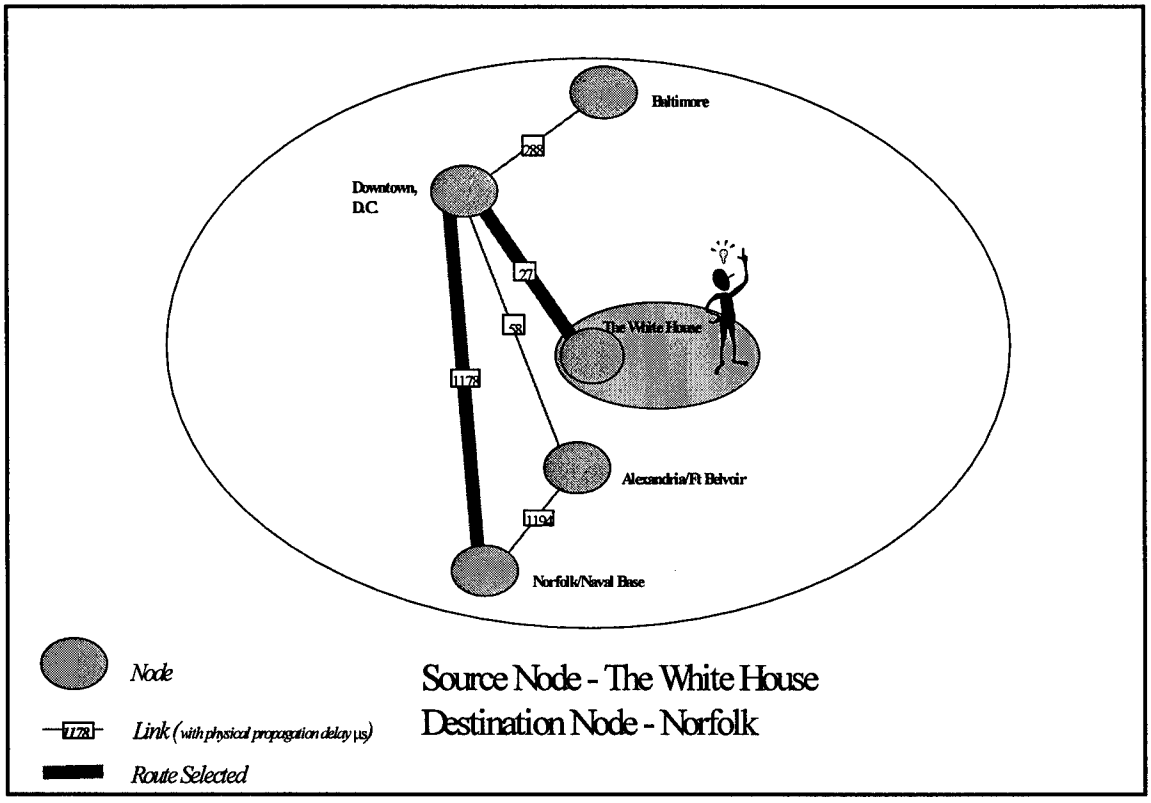



Figure 5. ATM route selection based on bandwidth.

**Call Setup in an ATM Network with a Security on Demand System**

In an ATM network with a security on demand system at the user level, the system is integrated into the call setup process when the route is determined. The user level, security on demand approach consists of three key elements. First, every ATM node and its corresponding links must be characterized by a matrix that reflects a

comprehensive view of the security posture of the node, from the perspective of the fundamental framework. Second, every call request must be accompanied by a matrix that represents the user's desired security characteristics for the call. Third, under call admission control, in the source node's computation of the virtual path, the user specified matrix for the call and the security matrices of the nodes play a predominant role. While the PNNI does not prescribe any cost function in the determination of the virtual path, conceivably a number of functions may be utilized and the issue is elaborated further in Chapter 8. In addition, the call setup message which includes the DTL packet, carries with it the user specified matrix and compares it against the security matrices of the nodes along the virtual path. Should every ATM node and link along the computed virtual path meet the user specified security requirement and have available bandwidth, a secure path is successfully determined from the source to the destination node and ATM traffic cells may be transported over the switching network. Otherwise, when any of the intermediate nodes, including the source and destination nodes, fail to meet the user specified security requirement, the call fails. Thus, the fundamental framework for security constitutes the basis for integrating comprehensive security into the operational model of the ATM network down to the user level and the approach generates, where possible, a secure path for the transport of ATM cells, with a degree of security commensurate with the user's request. Following the completion of transport of the ATM cells through the network, the virtual path is torn down, releasing the network resources for use by future call requests. In essence, the security on demand approach realizes the dynamic creation and

tear down of routes of different security criteria and the simultaneous existence of multiple routes in the network, each rated at different security levels.

Consider a similar scenario to the one previously presented in figures 4 and 5 and shown in figure 6. Here, the network contains several additional nodes including one at the Pentagon which has the only link to the White House node. In this ATM network the Pentagon node is also connected to the downtown, D.C. node and the Alexandria node which are both connected to the node at Norfolk. Additional, military nodes, are located at Ft Meade, Andrews Air Force Base and the Naval Academy.

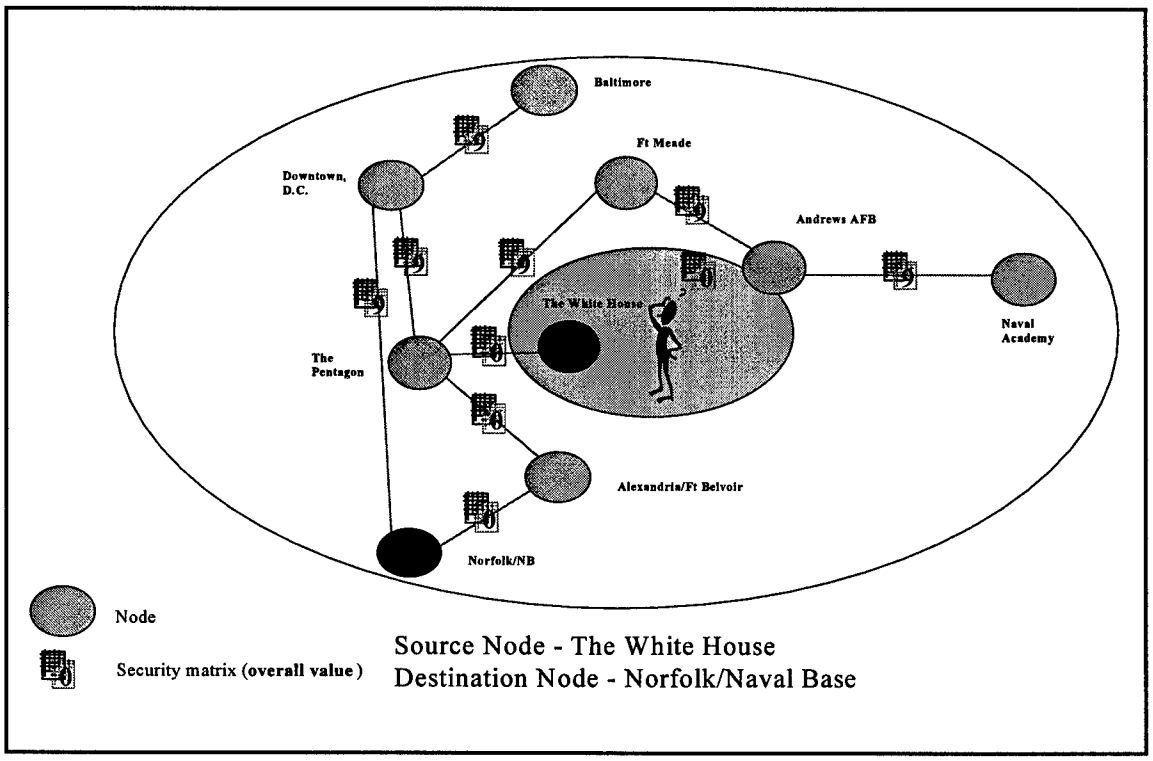



Figure 6. Secure ATM call setup between the White House and Norfolk.

The network also provides a user level, security on demand system which associates a security matrix with each link in the network. The graphical representation of each link's security matrix shown in the figure also contains a number between 0 and 9 which is the highest value of any of the 72 matrix elements. It represents the worst security offered in any of the 72 elements of the security matrix associated with the link. Top Secret security is represented by a value of zero in the security matrix elements. The absence of security is represented by a value of 9. In this scenario, assume that the president, located at the White House node, desires to send a Top Secret message to the Commander in Chief (CinC) of Atlantic Command, located in Norfolk. If the routing function, used to determine the path, is based on the most secure links with a check to see if bandwidth is available on those links, the only possible route which provides the required, Top Secret security includes the nodes at the Pentagon and Alexandria. This route, shown in black in figure 7, is selected by choosing the links which provide the security level of 0 on the path from the White House to Norfolk. This scenario exemplifies the method for call setup used by the security on demand system integrated into an ATM network and is different from the path selected in the example shown in figure 5, which shows how a path is selected without a security on demand system.

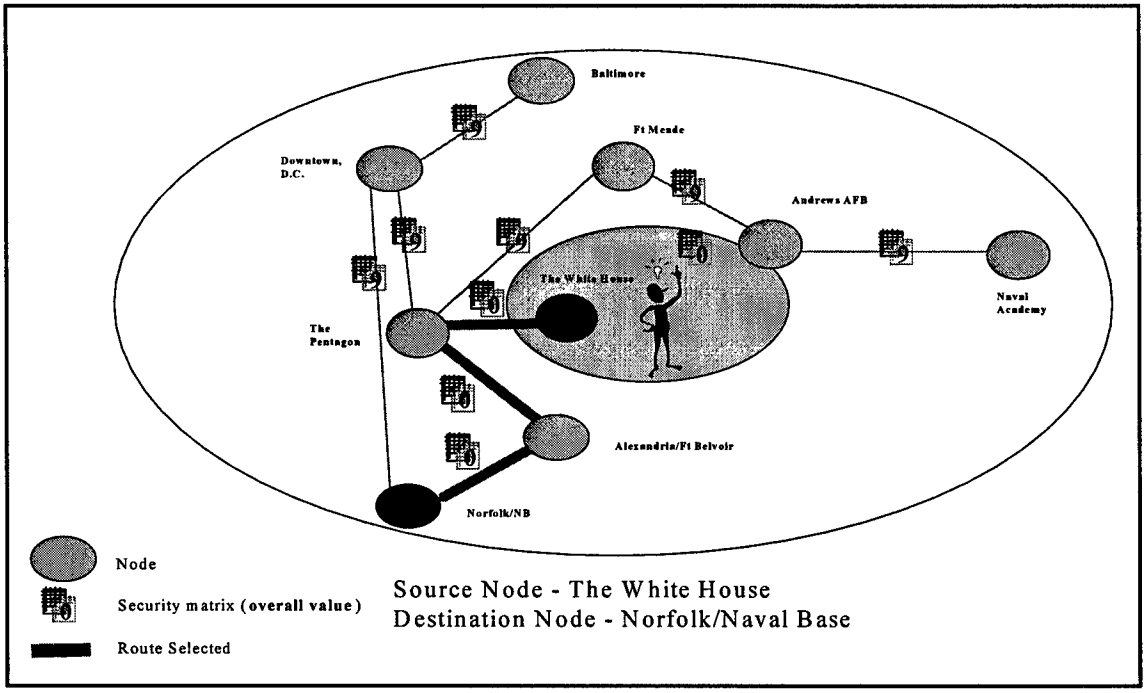



Figure 7. Secure ATM route selection between the White House and Norfolk.

### Call Setup in an ATM Network Using a Node Status Indicator (NSI)

CAC with security on demand could be based solely on the security resources associated with each node and link, along with a check for available bandwidth as discussed in the preceding section or it can be based on a combination of security, level of available bandwidth, and latency to more closely fit the possible route selection to the user's requirements and available resources. These factors are combined formally in a function, called a Node Status Indicator (NSI) to produce one number for each link of the proposed route selection contained in the call setup message. The hypothesis being that if a link is coded with a value, including its security value, latency and level of bandwidth availability, a better determination of a possible path could be made for a successful call

setup message. While available bandwidth or buffer occupancy could be used to indicate the link usage levels, bandwidth is chosen because its availability fluctuations are more stable over time making it a better gauge of link usage and matches the scale of the flooding intervals for network topology information.

In essence, the NSI views bandwidth as a dynamic security resource which influences the path prediction of a call setup message. The amount of bandwidth available, link security value and physical propagation delay impact the route selection for the call setup message. As bandwidth is allocated or deallocated and passes certain thresholds, the NSI value associated with the link is raised or lowered, impacting the route selected for the call setup message. A more detailed discussion of how the security, level of available bandwidth and physical propagation delay factors are computed and scaled in relation to each other is contained in the Chapter 5 section titled: Refinement of the Security on Demand Model: NSI Function.

Information is propagated by every node to every other node in the network through flooding. In flooding, each node propagates its knowledge of network topology information to its immediate nodes and so on. At each flooding interval, this action takes place until ultimately, all nodes within the network are aware of every other node and their topology information. Although all connected nodes will eventually receive new information on other nodes in the network, the exact times at which the nodes receive the information will differ. This time interval between the receipt of information at a node and the propagation from the original node is referred to as data latency. It causes

uncertainty and is one potential cause of a call setup message to fail. Of course, the further away a node is located from the original node, the later it will receive the node's topology information which causes a loss of accuracy, in the sense of timeliness. Flooding can also overload a network if it occurs too frequently. The NSI value can be flooded or all available information to include the 72 element security matrix can be flooded to every node which in turn produces its own NSI table depending on the network signaling bandwidth and/or desire to keep the security, level of available bandwidth and physical propagation delays hidden.

### Advantages of a User Level Security on Demand System

In addition to the advantage of allowing mixed users such as the military and industry to share the same network, a key advantage of utilizing the user level, security on demand system is its effective resource allocation strategy which, in turn, precludes the need to provide the highest security to every node; a costly requirement. This is unlike the traditional approach where all nodes and links must have identical security resources. In essence, this approach constitutes a new paradigm, one that views security as a distributed network resource and allocates it to each user call based upon demand and dictated by the need.

Currently, the DoD does not mix traffic of different security levels and all traffic in a particular network is designated as system high according to the classification level of the network (Department of Defense 1990). A key advantage of the security on

demand system in ATM networks is its ability to successfully support multiple user traffic, each with its unique security requirements, simultaneously over the same network and to do so down to the user level. This, in turn, implies that in a network with secure and non-secure resources, users who do not require security may be provided non-secure resources, thereby relieving the burden on the generally scarce security resources. Consider a "mixed use" network with nine nodes in the greater Baltimore-Washington metropolitan area with nodes at the Naval Academy, Andrews Air Force Base, Ft. Meade, the Pentagon, Baltimore, downtown D.C., Alexandria, Norfolk and the White House. The security associated with the links between these nodes is mixed at two levels: Top Secret (0), Unclassified (9). Two military users -- A and B, both at the White House and shown in figure 8, are interested in propagating traffic to Norfolk Naval Base.

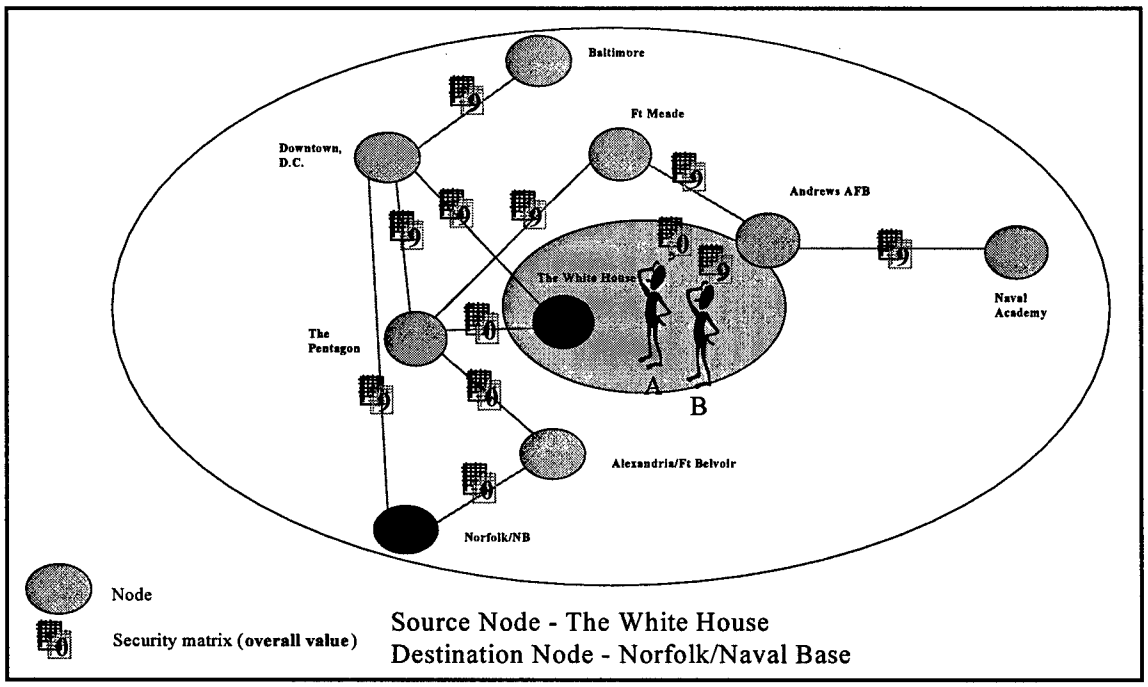



Figure 8. ATM call setup between the White House and Norfolk Naval Base.

While A insists on a secure route from the White House to Norfolk Naval Base, B does not require any security. The routes chosen for the two different call requests travel on different paths in the network based on their security requirements. The secure traffic passes through the Pentagon and Alexandria nodes on its way to Norfolk while the traffic which does not require security travels through the downtown D.C. node on its way to Norfolk. Figure 9 presents the results of call processing wherein the route for A, shown in dark, proceeds along the secure nodes – the Pentagon, Alexandria/Ft. Belvoir and Norfolk. In contrast, the route for B, shown in gray, proceeds along a path of non-secure nodes – downtown Washington, D.C. and Norfolk. The advantage of such a system being that security resources are not required to be the same at every node, as the military

currently requires, enabling better use of costly, security resources. Without the efficiency of a security on demand system, all nodes within the network would be required, under DoD standards to have the same security resources, increasing the cost of the network.

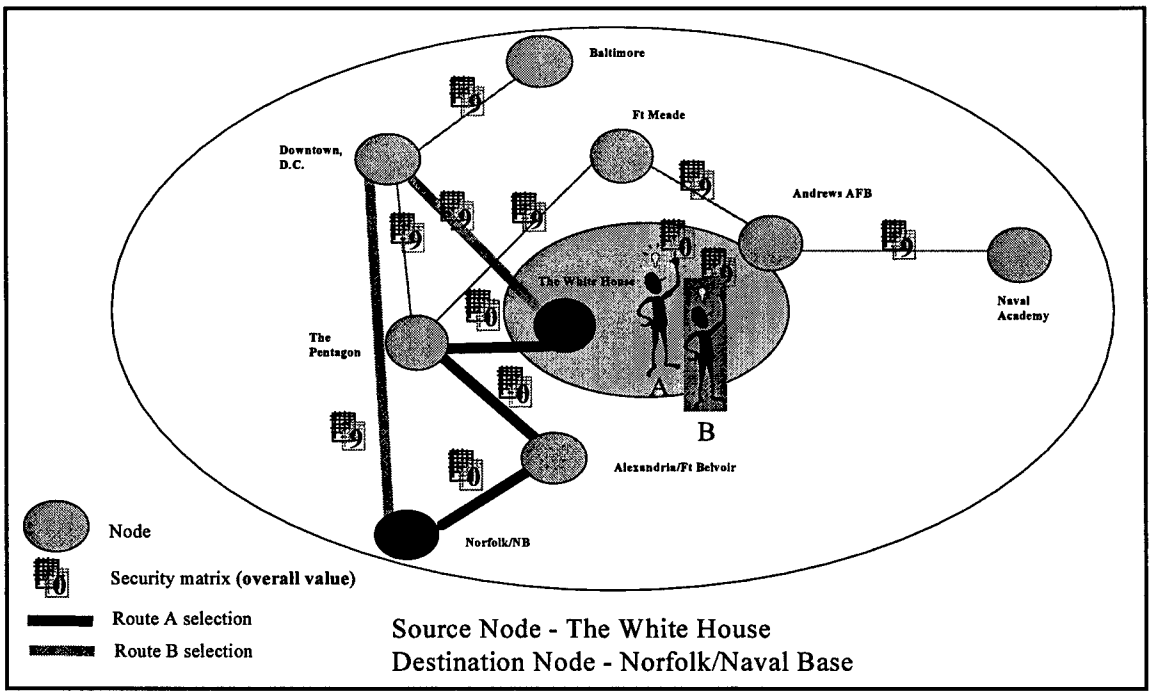



Figure 9. ATM route selection with security on demand system.

Figure 10 shows the same network as before, but with the military's current requirement of having the same security resources at every link and node of this network. This requirement adds security resources to 7 links and their associated nodes. In addition to the increased cost, both users A and B could be forced to compete for the same security resources - nodes the White House, Pentagon and Norfolk, causing an

inefficient use of security resources or possible failure of one of the calls. If user B's request precedes user A's then user A's call could fail unnecessarily. This competition, is the result of the military's current requirements for its secure networks and is, in essence, unnecessary since the traffic for user B does not require any security.

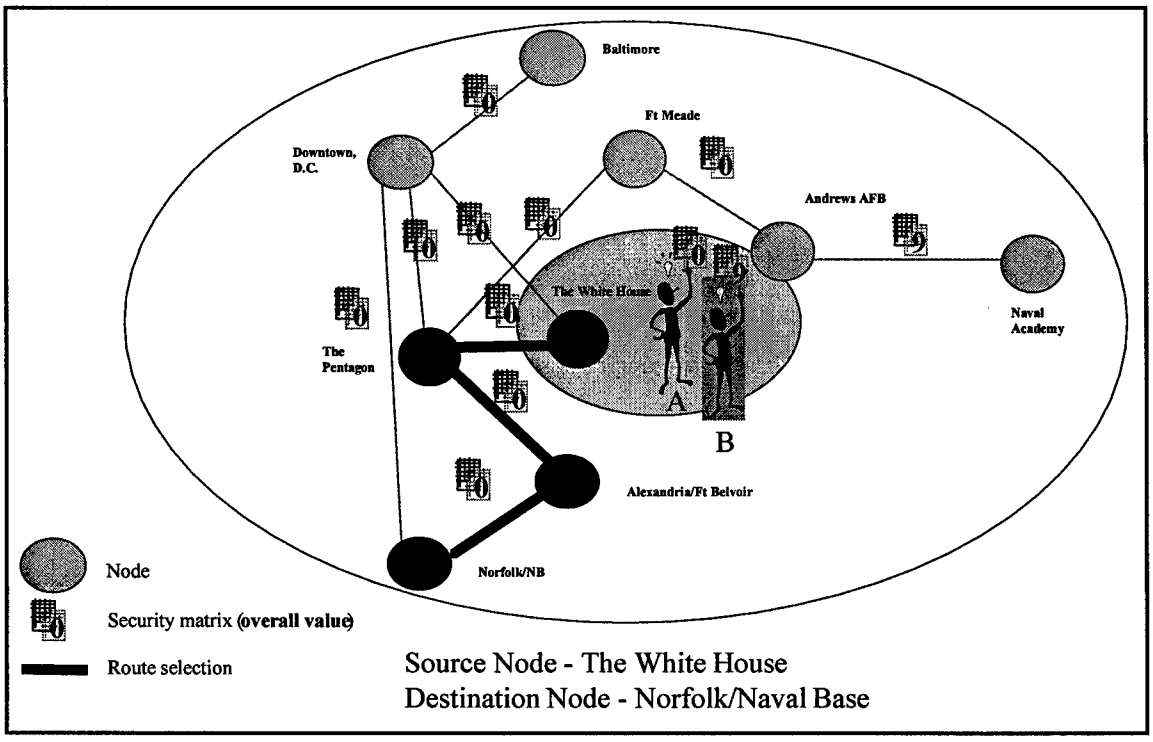



Figure 10. ATM route selection using the military's current security resource scheme.

## "Mixed Use" ATM Networks

The advantage of providing a user level, security on demand system in an ATM network is that it enables previously unconnected networks to be connected in a logical and systematic manner enabling a larger, "mixed use" resultant network with its

resources available to all participant users. A "mixed use" network is a new concept introduced in this dissertation. In it, the conventional military and commercial ATM networks which have deliberately been kept totally isolated, are integrated into a single, uniform network whose combined resources may be utilized by all participant users - military, government, industry and academia, while ensuring the security of every traffic type. For example, the military does not now connect its classified networks to commercial networks due to security concerns. The military also keeps its secure networks separate from its nonsecure networks. Additionally, the secure networks in the military are divided up into three separate networks rated to carry traffic at Top Secret, Secret and Confidential levels (Department of Defense 1987). These required divisions create isolated networks with excess capacity of bandwidth and duplication of some security resources.

A "mixed use" network combining the commercial and all the military networks would enable the military to effectively manage limited and costly security resources while satisfying the military's requirements for security in addition to providing increased security for commercial traffic at reduced costs.

Consider the representative commercial ATM network depicted in figure 11 which is composed of 32 nodes and 40 links. There is no security at any of the nodes or on any of the links. This 32 node network and associated links was developed using information on AT&T's (AT&T 1998) and MCI's (Chaffee 1988) ConUS commercial backbone networks.

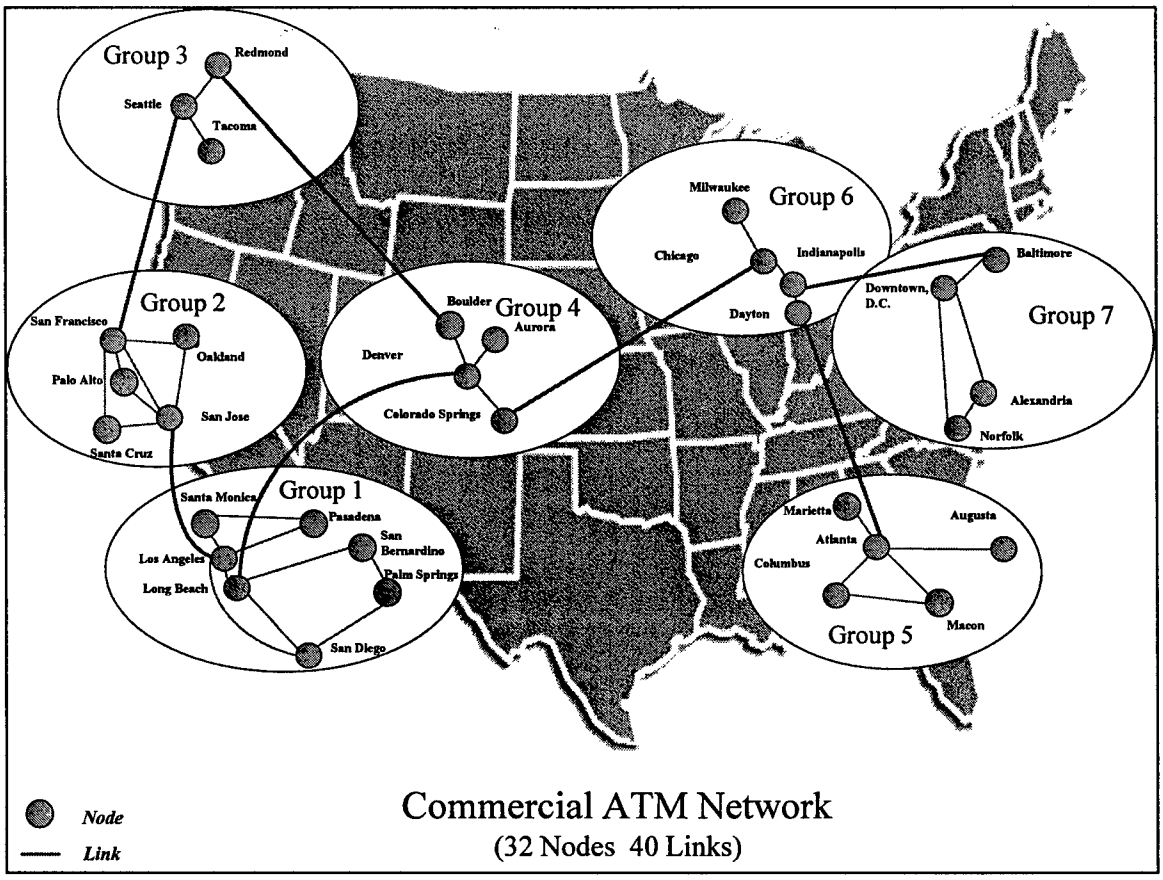



Figure 11. A 32 node ConUS commercial ATM network.

Consider another representative network consisting of 40 nodes and 48 links shown in figure 12. Security resources are the same at every link and node and rated at the highest security level of zero. This network is representative of a classified military network spanning the continental United States (ConUS) and was developed from actual locations of major defense installations and processing centers and is representative of a military, ConUS ATM network for secure traffic.

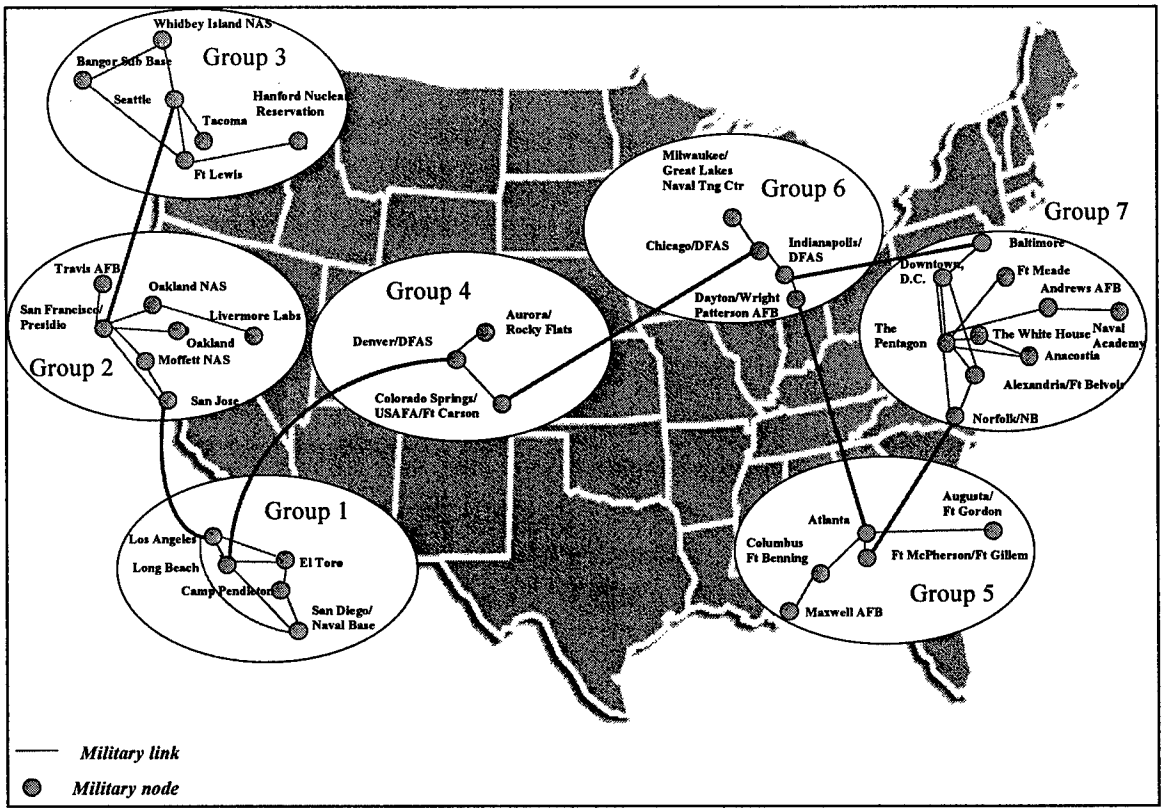



Figure 12. A 40 node ConUS military ATM network.

These previously unconnected networks can be combined into a 50 node network (figure 13) where some of the nodes and links which occur in duplicate locations in the commercial and military networks are combined. This "mixed use" network is possible as a result of the integration of the user level, security on demand system into the network's operation. Link and node security resources are of mixed levels where the security values of the links in the 50 node network are a combination of the two smaller networks. Those links and nodes which existed in the military, 40 node network retain their security resources while all remaining links and nodes have no security resources.

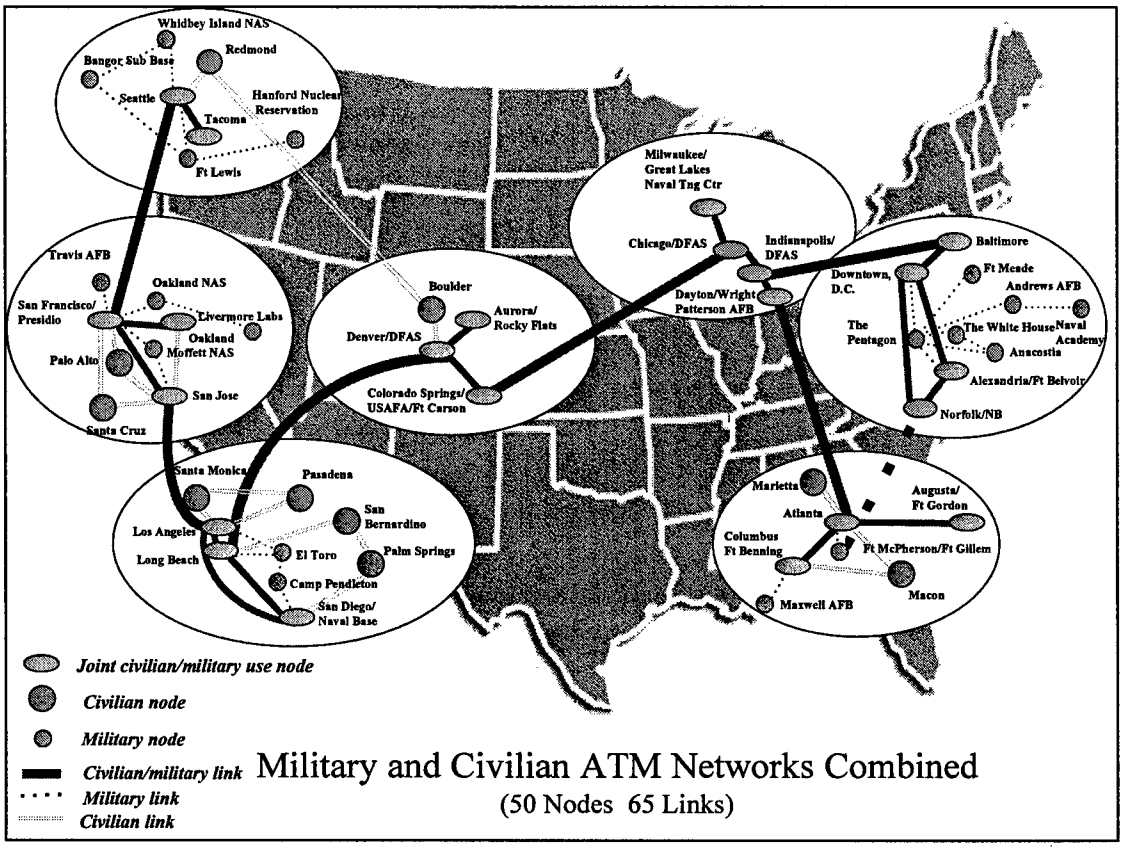



Figure 13. A 50 node "mixed use" military and commercial ConUS ATM network.

The military's requirements for security for its classified data are satisfied as a result of the integration of the user level, security on demand system. The military could route its secure traffic through its links and nodes which already offer the required security resources. Any unclassified traffic which previously was routed over secure links and nodes could be routed onto commercial links and nodes, relieving congestion on secure nodes. Such a network can offer higher call success rates due to the increased number of possible paths to a destination. The network could also offer, in the future, civilian users the ability to send data over secure paths.

# CHAPTER 5

# MODELING SECURITY ON DEMAND IN A REPRESENTATIVE ATM NETWORK

## Introduction

The user level, security on demand system for ATM networks discussed in Chapter 4 was integrated into the call setup process of a distributed ATM network simulator. The goal of modeling and simulating the user level, security on demand system is threefold. First, the scientific validation of the approach through simulation demonstrates the successful integration of the security on demand system, as well as how and where the system is integrated into the ATM Forum's PNNI. Second, the results collected from the study enable a comparative performance analysis between representative ATM networks with and without the security system. Third, refinements to the security on demand approach were studied to determine methods to improve the overall network performance.

The ATM simulator used in this study is unique in that it is distributed and closely resembles an operational ATM network. The distributed simulation permits large scale networks to be simulated accurately and fast, thereby enabling a systematic study of the performance impact of security on demand for different choices of network parameters and input traffic.

This chapter is organized as follows. An introduction discussing the simulator, networks used for the study is provided followed by a more detailed discussion of the series of three networks developed for the study's different scenarios. The three models: baseline, security on demand and NSI function are then described. Consistency checks for duplicate executions of the simulation are analyzed and presented at the end of this chapter. The methodology used to generate the traffic and its parameters is presented in Chapter 6 in addition to a discussion of the network stability study conducted in order to test the input files and their effect on the simulated networks.

The integration into the ATM Forum's PNNI specification of the security on demand system, discussed in the "Mixed Use" ATM Networks section of chapter 4, is modeled for 50, 40 and 32 node representative Contiguous United States (ConUS) ATM networks. The three representative ATM networks presented in Chapter 4 (figures 11, 12 and 13) are modeled and used in the behavioral study of the security on demand system. While the 50 node "mixed use" network is organized into 7 groups with a total of 65 links, the 40 node military network consists of 7 groups and 48 links and the 30 node commercial network is organized into 7 groups with a total of 40 links. The 50 node, "mixed use" network is made possible as a result of a successful integration and implementation of a user level security on demand system.

While the distributed simulation yields high throughput, the modeling and simulation closely resembles an actual operational ATM network. Key elements of the PNNI, including call requests, are modeled. The model utilizes Dijkstra's (1959) shortest

path algorithm to compute the routes corresponding to call requests. The shortest path algorithm utilizes the physical propagation delays of the links, based on the speed of light in fiber (Ferguson and Huston 1998), in addition to available bandwidth in its cost function. During the forward propagation of a call setup message from the source towards the destination node, bandwidth is reserved, where available, at the intermediate nodes. The reservation, however, is confirmed during the return pass of the call setup message, only if the call setup succeeds, i.e., in reserving bandwidth up to the destination node. While the available bandwidths of the links, following a successful call request, are reduced for the duration of the call, they are recovered after the call terminates. With the integration of the security on demand system, in addition to carrying with it the user requested bandwidth and other quality of service parameters, every call setup message includes the DTL and the user specified security matrix. In addition to the maximum and available bandwidth of each of its links, a security matrix is associated with every node link. This security matrix defines the level of security for that particular link. When the bandwidth is reserved on the return pass of the call setup message, a check is also made to determine if the user required security levels are met. If the security or bandwidth requirements cannot be met, the call will fail and any reserved resources are released.

Modeling of the representative ATM networks is done in the following manner. Each ATM call processing node is described behaviorally and executed on a processor. The ATM links are represented through TCP-IP connections and ATM cells transport is expressed through guaranteed messages. The distributed simulation accurately represents

the ATM network operation through the use of the conservative, null message based, asynchronous distributed simulation algorithm (Lee and Ghosh 1994).

### Three Representative ATM Networks: Military, Civilian and "Mixed Use"

Three representative ATM networks were developed for the series of simulations. The 40 node network and associated links previously shown in Chapter 4 was developed from actual locations of major defense installations and processing centers and is representative of a military, ConUS ATM network for classified, secure traffic. Due to the large number of installations requiring connectivity and the many alternate types of backup networks, the general rule followed was to limit the number of alternate paths between nodes which reduces cost. The 32 node network and associated links also presented in Chapter 4 was developed using published information on AT&T's (AT&T 1998) and MCI's (Chaffee 1988) ConUS commercial backbone networks. These commercial networks generally allow for a rich topology of alternate paths between nodes and the 32 node commercial network is representative of this fact.

These military and civilian networks are subsets of a larger, 50 node, 7 group, "mixed use" network. This 50 node network is a proposed joint use network for use by all types of users to include the military, government and industry. It is shown in figure 14 with the node and group IDs labeled as well as the commercial links which have no security and the joint and military links which have maximum security.

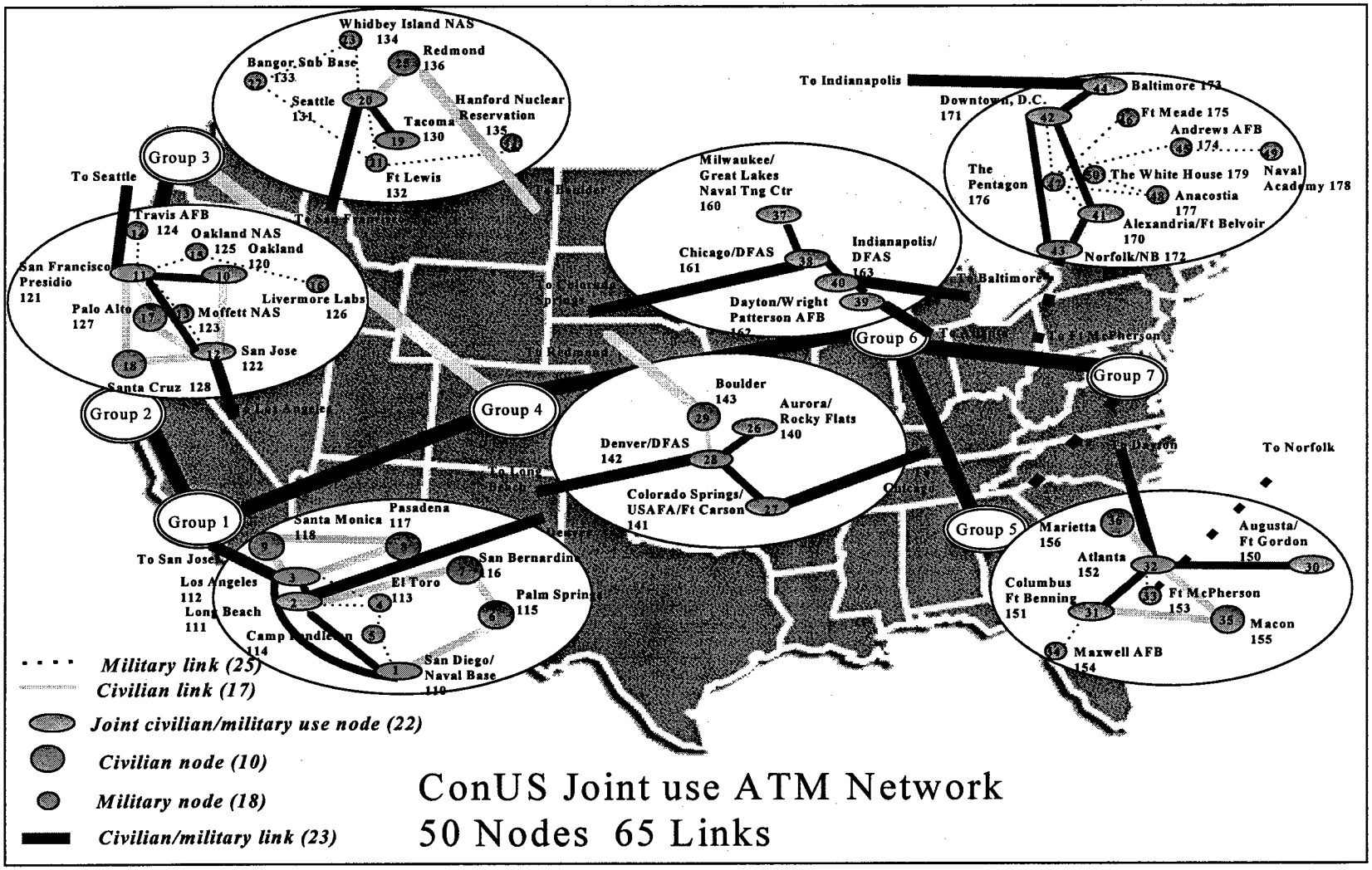



Figure 14. Labeled 50 node "mixed use" military and commercial ConUS ATM network.

Of the 50 nodes in the "mixed use" network, 40 are tied to military users and 30 are tied to commercial users. As a result, a smaller subset of 22 nodes and 23 links exist at duplicate locations for both the military and civilian networks. These 22 nodes and 23 links are jointly used by the military and civilian users in the 50 node, combined use network.

The links between nodes in the 40 and 32 node networks are 77.5Mb between the jointly used nodes and 155Mb between the sole use military or civilian nodes. All links in the 50 node network are 155Mb. Straight line distance is used to calculate the physical propagation delay on the links, which is based on the speed of light in fiber of 194,865 km/sec (Ferguson and Huston 1998).

The modeling and simulation of the user level, security on demand system enables a "mixed use" network with different security levels to be tested. Such a network enables the military to combine its classified networks, as well as its unclassified networks, with the public ATM network backbone to effectively manage limited and costly security resources while satisfying the military's requirements for security. Additionally, it also provides for the increased security for commercial traffic.

Security values associated with the links are set according to their use. In the military network of 40 nodes, the security associated with all the links is "0" representing the highest level of security. The security value of the links in the commercial, 32 node network is "9", equivalent to no security. The security values of the links in the 50 node network are a combination of the two smaller networks. Those links which existed in the

military, 40 node network are given a value of "0" and all other links are given the value of "9".

**Baseline and Security on Demand Models**

Two approaches are modeled and implemented in an ATM network simulator to study their behavior and scientifically validate the security on demand system. One additional model is developed to refine the security on demand approach and is discussed in the next section. Each approach is based on the ATM Forum's PNNI specification with two of the three approaches adding modifications to the call setup process to integrate the user level, security on demand system. In every one of the three ATM network models a timestep has a granularity of 2.74μs. This value is determined from the fastest link in the network simulated which is 155Mbps. The 53bit packet size in an ATM network multiplied by an 8bit/byte is divided by 155Mbps to determine the timestep. Each simulation is executed for a total of 1,200,000 timesteps using the same machine configuration (Pentium 90 or 200 MHz processor with 64 MB of memory). The duration of the longest simulation required a total wall clock time in excess of 90 hours, i.e. all of the processors complete execution within 90 hours. Each of the three models has a corresponding simulator code version which is composed of over 15,000 lines of C/C++ code.

The flooding rate for updating the topology information such as bandwidth and the security matrix was an interval of 25,000 timesteps. The call processing delay of each ATM switch of 800 timesteps is based on Fore Systems, ASX 1000 ATM switch

specifications as reported in Network Computing (Conover 1997) where a test of the switch produced a top routing speed of 437 calls per second, equivalent to approximately 1 call every 800 timesteps or 2.192ms.

Call setup time is a function of the network link delays, signaling buffer occupancy and the Call Admission Control (CAC) delay of 2.192ms. The switch at each node can only process one CAC request at any one time, therefore, it takes a node 2.192ms to process one request. Any requests which arrive while the switch is processing a call will be queued until the switch has completed processing the call. All calls are processed in the order received. Call success rate is equal to the number of successful calls originated at that node divided by the total number of calls originated at the node. The intergroup call setup routing prediction is based on the shortest number of hops which minimizes the number of groups traversed and is the same intergroup method used for all models.

The first model is called the baseline model and follows the ATM Forum's PNNI specification (ATM Forum Technical Committee 1996) with the algorithm used for the intragroup call setup routing prediction based on physical propagation delay influenced by that node's most current bandwidth information if the bandwidth requested is not available on that particular link. The choice of using physical propagation delay for the value supplied to Dijkstra's algorithm is based on its simplicity as well as the desire to keep the list of multiple independent link parameters to a minimum. The PNNI specification does not require a particular type of path selection algorithm. It states that

"efficient QoS-sensitive path selection is still a research issue." The PNNI also states that multiple independent link parameters are "expensive computationally" which led the author to develop the refined, NSI model. The example algorithm used in the PNNI specification is Dijkstra's shortest path algorithm (Dijkstra 1959) and is the algorithm was used in all three versions of the ATM network simulator.

The second model, called security on demand, follows the ATM Forum's PNNI specification with the addition of the security on demand system. The addition of this system requires that a 72 element matrix be associated with every network link and each user's call setup request. The values supplied to the shortest path algorithm used in the simulator in the straight security version for intragroup routing is based on the largest security value of a link security matrix, influenced by that nodes current bandwidth information if the bandwidth requested is not available on that particular link.

**Refinement of the Security on Demand Model: NSI Model**

The third model includes the Node Status Indicator (NSI) function introduced in Chapter 4. The model for the security on demand version and this NSI function version are the same except the algorithm used for the intragroup call setup routing prediction is based on the NSI for a particular link as well as being influenced by bandwidth if the bandwidth requested is not available on that particular link. The NSI function model of the simulation code views bandwidth as a security resource which influences the path prediction of a call setup message and distributes the calls between a source and

destination evenly across all possible paths. The NSI is a combination of numerical representations of the link security level, level of available bandwidth and physical propagation delay.

NSI = link security factor + scaled available bandwidth + scaled physical propagation delay

The security factor used in the NSI function is computed by using the numerically highest element, representing the lowest available security, of the 72 element security matrix associated with the link and node in the range: $0 \leq$ security factor $\leq 9$. Level of available bandwidth is converted to a scale on par with the security factors, as follows. The scaled level of available bandwidth is a value in the range of 0 to 10 and is computed using a step function which compares the raw available bandwidth (Mbps) on a particular link to five ranges of bandwidth resulting in the NSI factor: $155 \leq$ available bandwidth $\geq$ 77.5, NSI available bandwidth factor = 0, 77.5 < available bandwidth $\geq$ 38.75, NSI available bandwidth factor = 1, 38.75 < available bandwidth $\geq$ 19.375, NSI available bandwidth factor = 3, 19.375 < available bandwidth $\geq$ 9.6875, NSI available bandwidth factor = 6, available bandwidth < 9.6875, NSI available bandwidth factor = 10.

This step function puts the bandwidth available on a scale nearly equal to that of the security values. These scales are similar in range and importance because the security and level of available bandwidth factors are critical to the success of a call. The scaled propagation delay values are deliberately converted to a scale half the range of the

security and level of available bandwidth scales. The scale is half the range of the others due to the less critical nature of the physical propagation delay to call success. The conversion is as follows: (physical propagation delay * 2.74) / 100. The physical propagation delays for the intra-group links in the 3 representative networks used in the behavioral studies, when scaled using this conversion, have values of 0, 1, 2, 3 or 4.

## Consistency of Data

A gauge of the consistency of the results produced by the simulation is performed by executing the same 50 node, NSI code version of the simulator code twice and computing the standard deviation of the average call success rates and call setup times (figures 15 and 16). The results show a majority of nodes have zero standard deviation in the data for both average call success rate and average call setup. Those nodes which showed a standard deviation of the average call success rates at each node were less than 0.0085 and those nodes which showed a standard deviation of the average call setup times at each node were less than 36 timesteps. An absence of a bar at a node id in the plots indicates the standard deviation of the data was zero for that particular node.

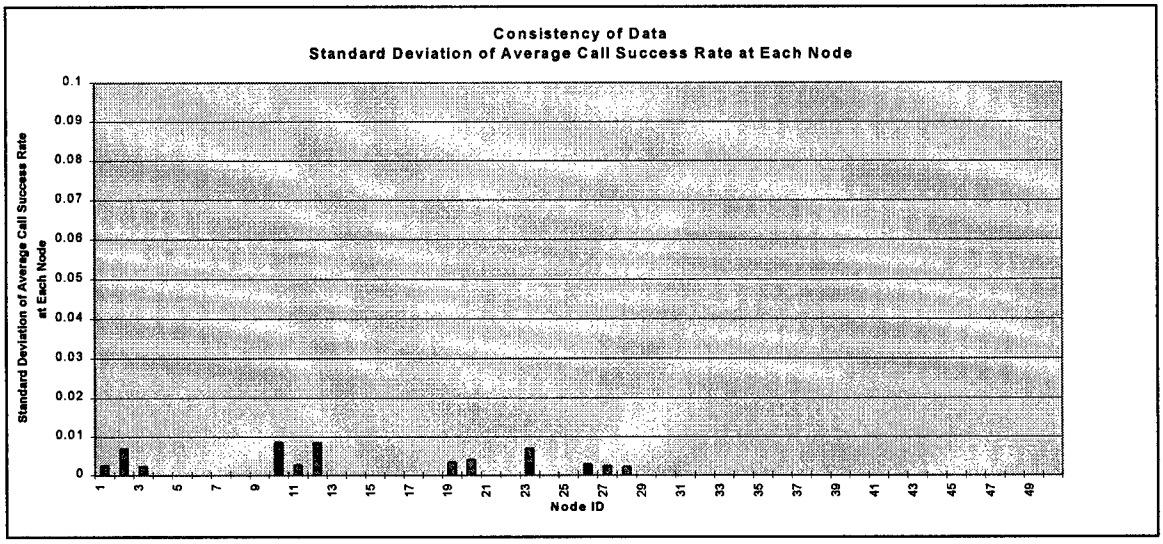



Figure 15. Standard deviation of average call success rates at each node for data from two identical behavioral studies.

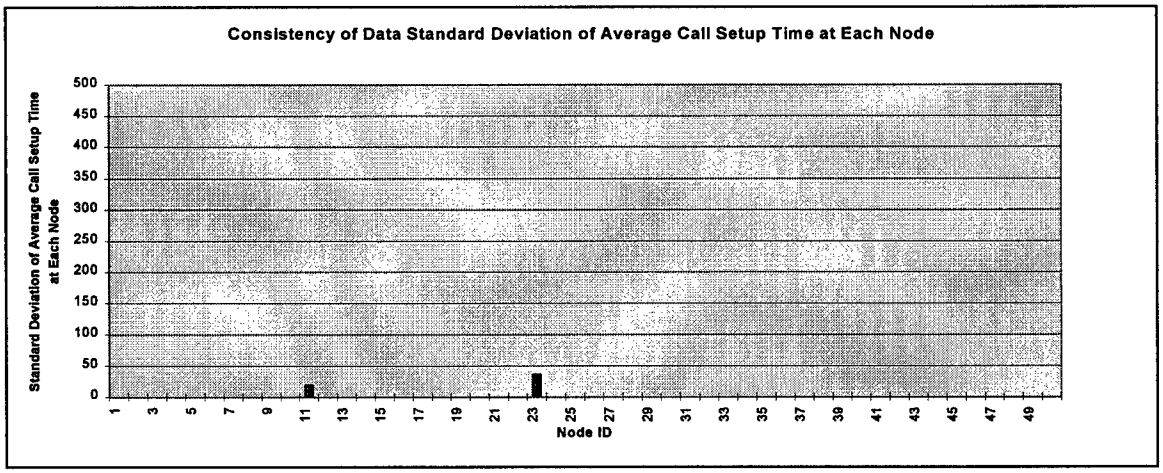



Figure 16. Standard deviation of average call setup time at each node for data from two identical behavioral studies.

# CHAPTER 6

# CHARACTERISTICS OF THE INPUT TRAFFIC

## Input Traffic

Input files used to generate traffic during the simulation are created with the intent to stress the network by generating a large number of calls without destabilizing the operation of the network. This large number of calls would represent a worst case scenario of traffic which the network could sustain without failure. The parameters utilized for the stochastic input traffic distribution may be described as follows. While traffic modeling can be found in the literature, there is a lack of information on the distribution of user launched call requests, their duration, bandwidth, security requirements and quality of service distributions. In the simulations conducted, the assertion of call setup requests, their duration, and the distribution of the bandwidth, are all generated through stochastic techniques. While a great deal of thought and effort was involved in creating a realistic level and types of calls, there are no ATM traffic models to follow for commercial or military ATM networks with switched virtual circuits (SVCs). The simulation scenarios and resulting analysis are not intended to provide an absolute measure of performance for a particular type of ATM network. Instead, the average call setup times and call completion rates are used to compare the performance impact of the security on demand system integrated into an ATM network to a baseline

ATM network. As a result, the nature of the composition of the input file parameters is not critical. In the future, when SVC ATM networks are created and actual traffic data is collected, the performance comparisons drawn from these simulations will still be valid since identical input files are used for each simulation, except for the addition of a security matrix, and the results collected are used for a comparative analysis.

A number of factors are considered when generating the input traffic: call interarrival rate, call duration, bandwidth requested, intra/inter group call rates, security level requested. These factors are discussed in the following sections.

### Call Duration and Bandwidth

Calls are organized into two categories. Call duration for 95% of the calls is selected stochastically with a uniform distribution within the range of 300 to 900 ms. The remaining 5% of the calls, once initiated, last the duration of the simulation. The 95% of the calls with a range of 300 to 900ms reflect the assumption that with increasing ATM link bandwidths, the call durations are likely to shrink while a small representative portion of all calls will be of a longer length. This range is equivalent to 109,490 to 328,467 timesteps.

Call duration for the remaining 5% of the calls last from the time they are initiated through the length of the simulation and also have destinations which are also chosen stochastically with a uniform distribution over all nodes. These calls represent the possibility of a small number of calls which could last longer than the 300 to 900ms

duration range. There will be fewer calls total and the network will not be as stressed if the call duration is increased. While the cost of having calls lasting longer than 900ms in today's commercial market is expensive, there still exists a possibility that some customers will require, and pay for, a small number of such connections which accounts for the 5%. The studies are conducted to look at the performance of the network under stress. Therefore, the assumptions made are highly conservative and rigorous.

For each call, the user requested bandwidth is assumed to range from 1 Mb/s to 10 Mb/s based for an average of 5 Mb/s. Therefore, in 900ms call duration is equal to the total number of ATM cells: 0.9 * 5Mb = 4.5Mb; (4.5Mb x 10^6) / (53 * 8) = 10,000 ATM cells. Each node generates approximately 100 calls for a total of 5000 calls generated by all nodes in the 50 node network within the wall clock time for a 50 node simulation of 3.288 seconds.

### Distribution of Intra- and Inter-Group Calls

For a call generated at a node, the destination is selected stochastically, with a uniform distribution across all nodes within a group and with a 75% probability that the destination is an intra-group node and a 25% likelihood that the destination lies in a different group. This rate is chosen to reflect the fact that groups are chosen logically and one method of logically grouping nodes is based on commonalties and calling patterns. An analysis of the data contained in the "Utilization of the U.S. Telephone Network" report (Mitchell and Donyo 1994) is also used to select the rates. According to the Rand

study, it was determined that in 1991 the number of long distance (toll) calls per capita was 15.35% of the total number of all calls made. The total number of minutes as a percentage of all calls was 30.35% for combined inter/intrastate toll calls.

In one scenario analyzed, the performance of the two smaller, 40 and 32 node networks, are compared to the 50 node network to determine if performance is enhanced when these networks are combined. To enable the comparison with the 50 node network, call intervals and the resulting number of calls generated at joint nodes in the 40 and 32 node networks are ½ the rate of the same nodes in the 50 node network. This enables the calls for joint nodes in the 50 node network to be created from combining the military and civilian input files while maintaining network stability.

The separation between calls initiated at a node are an average of 7745 timesteps with a range of +/- 245 timesteps. Once the calls are started they are generated at this specified interval throughout the simulation duration of 1,200,000 timesteps unless a node is used by both military and civilian traffic. In this case, the input files related to the common military or civilian nodes have a call separation average of 15,490 timesteps with a range of +/- 245 timesteps. This increased separation enables the civilian and military input files to be combined and used in a 50 node simulation while maintaining network stability. The issue of network stability is discussed subsequently. The topology information is flooded within the network at a rate of every 25,000 timestamps. This interval was determined by executing the simulation on the 50 node network to determine

the lowest flooding interval without overwhelming the network with signaling information.

## Security Levels of Traffic

The security of the ATM nodes and the corresponding links range from 9 (unknown or no security) to 0 (highest security) with the ranges for security (0,3,5) corresponding to the military's classification levels: Top Secret, Secret and Confidential. A security matrix value of 9 can be interpreted to be Unclassified under the military's classification system. For every call originating at a node, the security matrix associated with that call may never exceed the matrix of the origin node.

The ability to estimate how much traffic on commercial or government ATM networks which will need to be protected with some type of security is difficult to predict. When the proposed security on demand system is implemented and users become familiar with its capabilities, usage will increase. Currently, there is no definitive source for the amount of traffic generated which requires security. In the government, there are no sources which describe the amount of data traffic on government or military networks which require some type of security. In the early 1970s, several Congressional hearings were held on the subject of how much government information is classified and the methods used to determine its worthiness of protection. One of the more famous and widely reported hearings was on the Pentagon Papers in 1973. Commenting on the hearings, Dorsen and Gillers report it is "clear that no one really knows just how many

classified documents there are in any Federal agency." (1973) It is reported by Horton and Marchand (1982) that Federal agencies generate the equivalent of 10 billion sheets of information a year. In a 15 year period, Dr. Rhoads, the Archivist of the U.S., testified before Congress that the Archives contained 470 million pages of classified documents (Dorsen and Gillers 1973). This averages to 31.3 million a year or the equivalent of approximately 1% of all the paper documents in the U.S. archives are considered classified. Horton and Marchand (1982) reported that as a part of the federal budget, money spent on classified federal information industries ranged from 14.5 to 20.5% of the total information budget from 1961 to 1970. It appears from the sparse information on the volumes of government data requiring security that the Federal government produces classified information at a rate anywhere from 1 to 20% of the total of all information produced by the government based on the percent of the number of pages in the U.S. Archives which are classified and the percentage of the information budget devoted to classified purposes. Further clouding the situation is the fact that the figures for the amount of classified traffic for each government agency or department are different. Each will produce differing amounts of protected information dependent on many factors. For example, in 1991 the DoD generated more protected information due to the Gulf War as a result of the need for increased security.

Of the total calls generated in the simulation, utilizing Dorsen and Gillers' figures for the information security budget and the number of pages in the Archives which are classified (1973) a figure of 20% of those calls from military (secure) nodes, are assigned

a security value of 0. The remaining 80% of the calls on military nodes, are non-secure and assigned a value of 9. In the civilian 32 node network all calls are assigned a security value of 9. These values are assigned to all 72 elements of the security matrix.

### Network Stability and the Choice of Input Traffic

The parameters utilized are derived through a novel, "indirect" mechanism, wherein the choice of the input traffic intensity is limited by the requirement that the network must be operationally stable. That is, the time interval to establish a successful call for a given pair of source and destination nodes, must not increase monotonically with advancing simulation time. Another key indicator of an unstable network is the call success rate at each node over time, a factor which is influenced by the available bandwidth. The objective of this stability study was to initiate the greatest number of calls in the shortest period of time with the call success rate remaining uniform and not monotonically decreasing. Available bandwidth influences the call success rate. While a high call success rate is desired, maximum utilization of the available bandwidth is also a goal. Finding a call arrival rate which maintained a stable call setup time, high call success rate and maximized utilization of the bandwidth is the goal of the stability study. Extensive trial and error simulation executions determined the chosen minimum interval between two successive call requests generated at the same node to be 7500 timesteps. The network becomes unstable at higher rates due to an increasing call setup time and a low success rate due to the complete utilization of the available bandwidth.

In order to determine the minimum duration between calls generated at a particular node without creating an unstable network, a series of network stability simulations were performed by decreasing the interval between calls in each successive simulation execution. The network used is the nine node, group 1 of the 50 node network shown in figure 17. This is one of the largest of the seven groups in the 50 node network and also contains the most intragroup links and is representative of a diverse group of solely commercial, military and joint nodes with a rich topology.

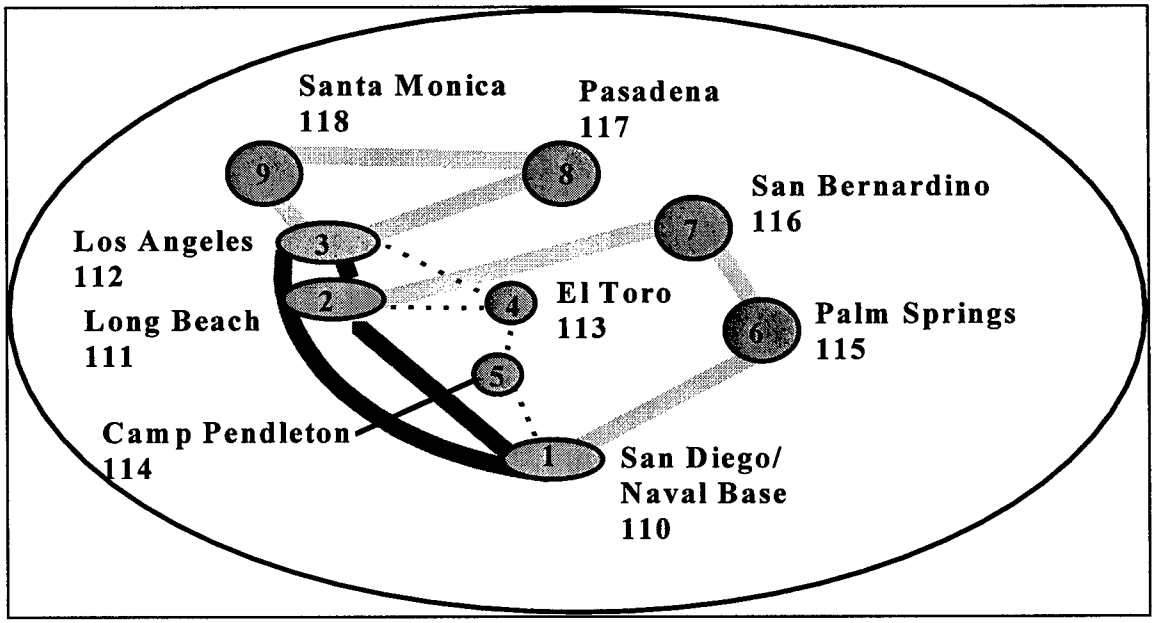



Figure 17. Nine node network used in network stability study.

The security on demand model used for the study which has a routing algorithm based on the security value of a link influenced by bandwidth only if the requested bandwidth was not available. The input files are generated using the previously discussed

constraints. After the calls were initiated they continued for 903,000 timesteps, through the end of the simulation. The results are analyzed by focusing on one node, node 8, and those calls at that node initiated to node 1. Calls from node 8 to node 1 are selected for study because the stochastically generated input files produced one of the larger samples of repeat calls between nodes. These two nodes are also selected because alternate paths existed between them. The call setup times for the successful calls are plotted over time and are shown for the call interarrival times of 5000, 7500, 10000 and 15000 in figures 18, 19, 20 and 21 with trend lines for the scatter plots also plotted. An analysis of the results shows the call setup time increases for a call interarrival rate of 5000 timesteps while the rates of 7500, 10000 and 15000 are flat or decreasing.

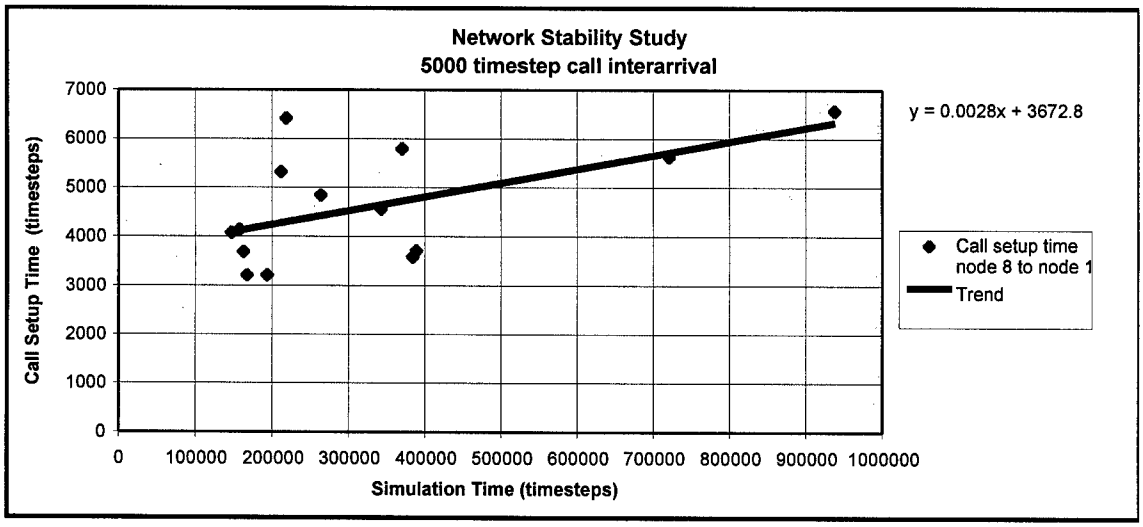



Figure 18. Scatter plot of node 8's call setup times to node 1 with a 5000 timestep call interarrival time.

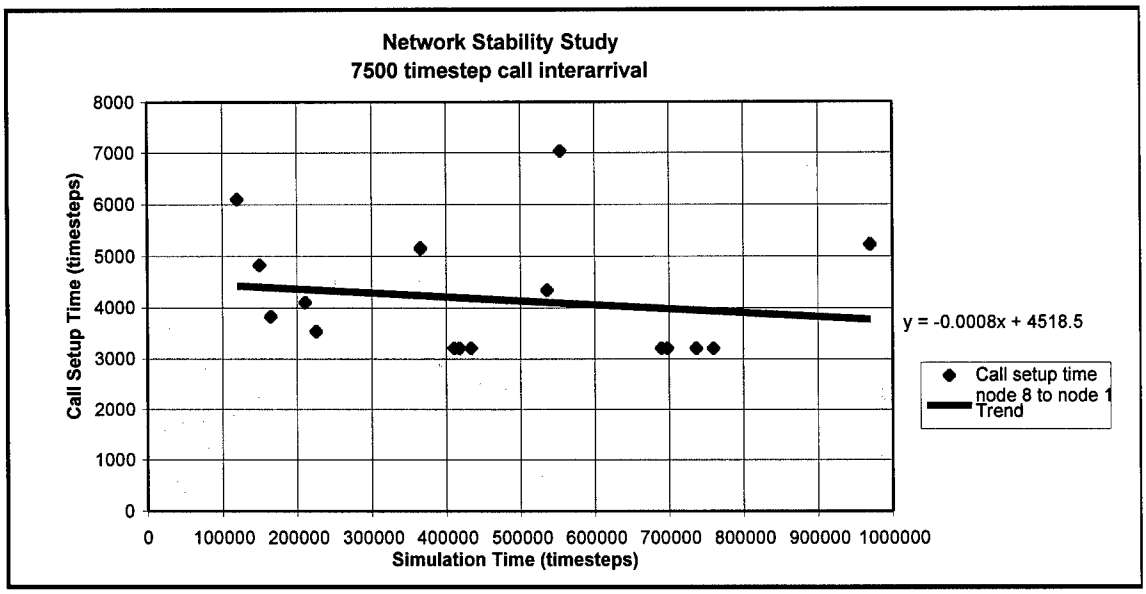



Figure 19. Scatter plot of node 8's call setup times to node 1 with a 7500 timestep call interarrival time.

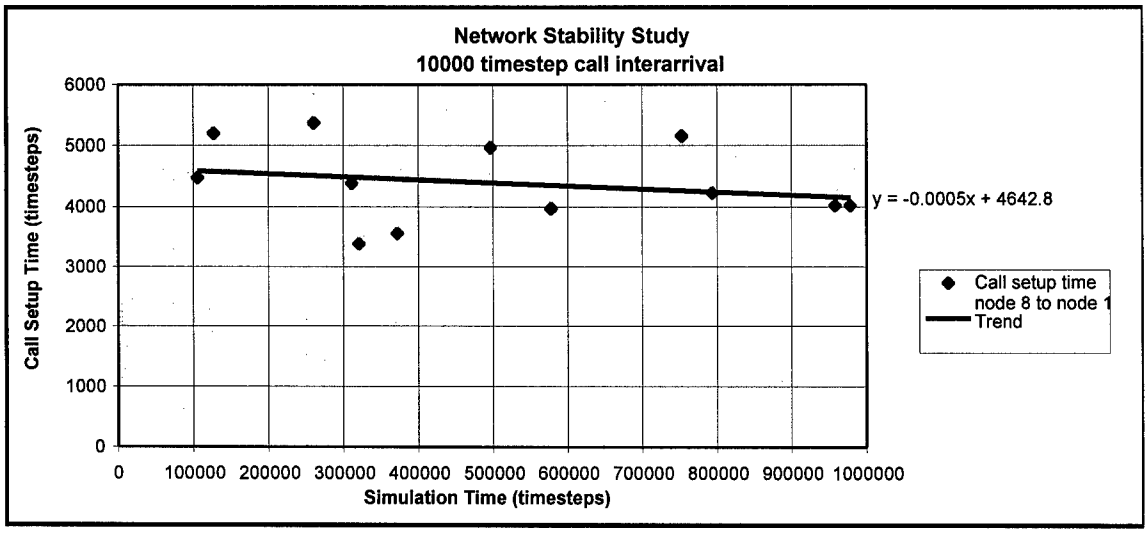



Figure 20. Scatter plot of node 8's call setup times to node 1 with a 10000 timestep call interarrival time.

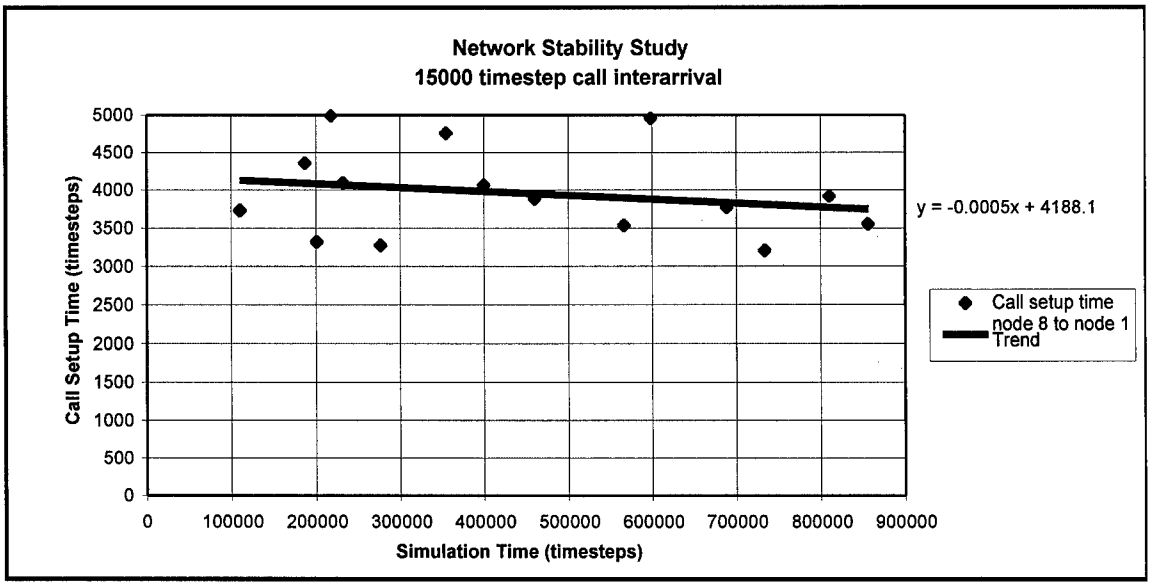



Figure 21. Scatter plot of node 8's call setup times to node 1 with a 15000 timestep call interarrival time.

An additional set of simulations is necessary to corroborate these results because the previous plots, figures 18 through 21, focus on a select number of calls which occur at random and are few in number. New input files for node 8 are generated which produced calls to node 1 every 15,000 timesteps. The input file used in the previous study is merged with the new calls to node 1. An old entry for a call is deleted for every new call inserted in order to maintain the required call interarrival rate. The results of this series of simulations corroborate the previously discussed results. Call setup time for a call interarrival rate of 5000 timesteps increase over time while the call setup times for the 7500, 10000 and 15000 rates are essentially flat. The results for the call interarrival times of 5000, 7500, 10000 and 15000 timesteps are plotted in figures 22, 23, 24 and 25 in

addition to a trend line. The standard deviation of the call setup times, average call setup time and equation for the trend line are also noted on the figures.

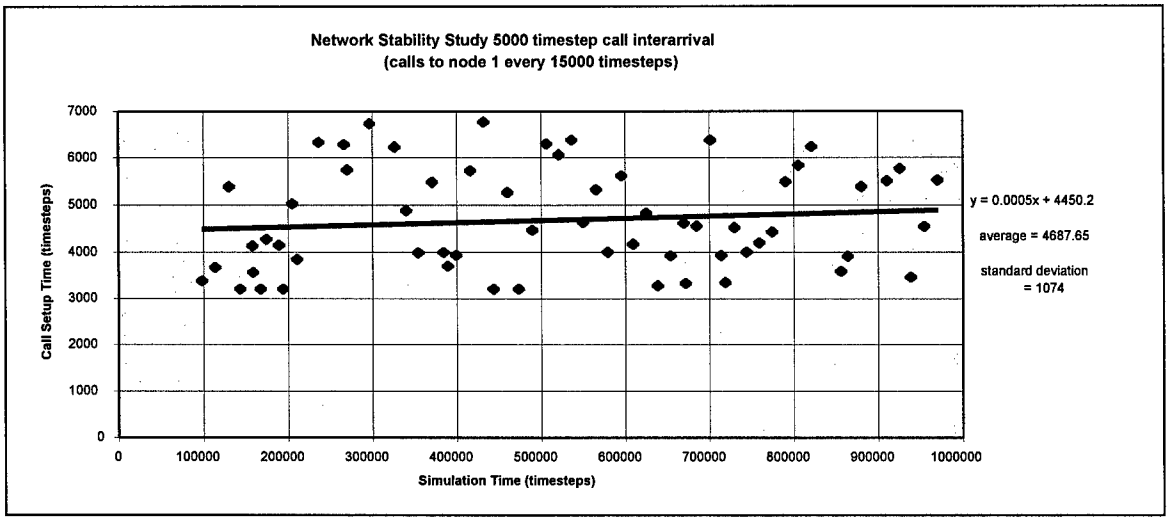



Figure 22. Scatter plot of node 8's call setup times to node 1 with a 5000 timestep call interarrival time (modified input file).

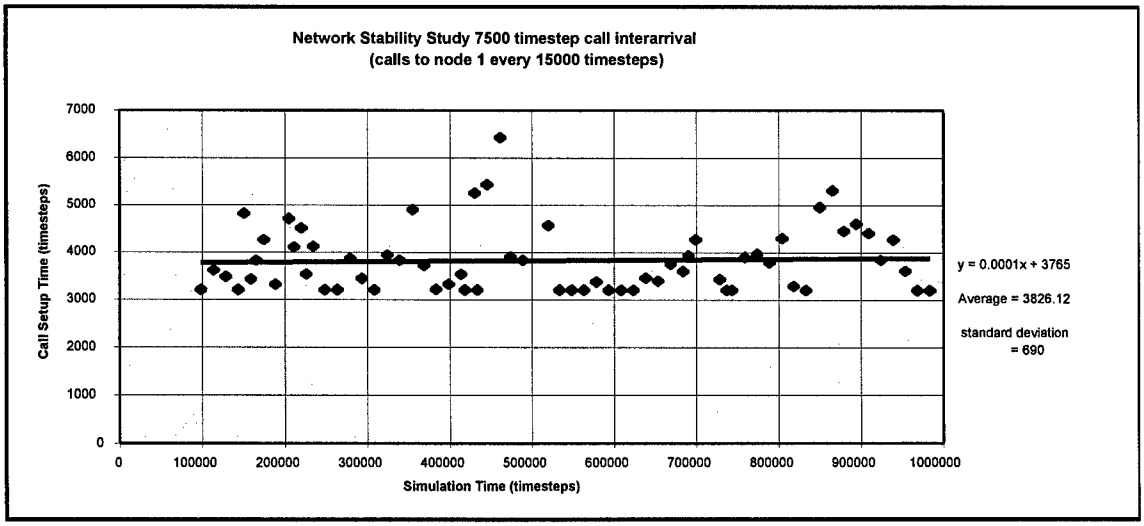



Figure 23. Scatter plot of node 8's call setup times to node 1 with a 7500 timestep call interarrival time (modified input file).

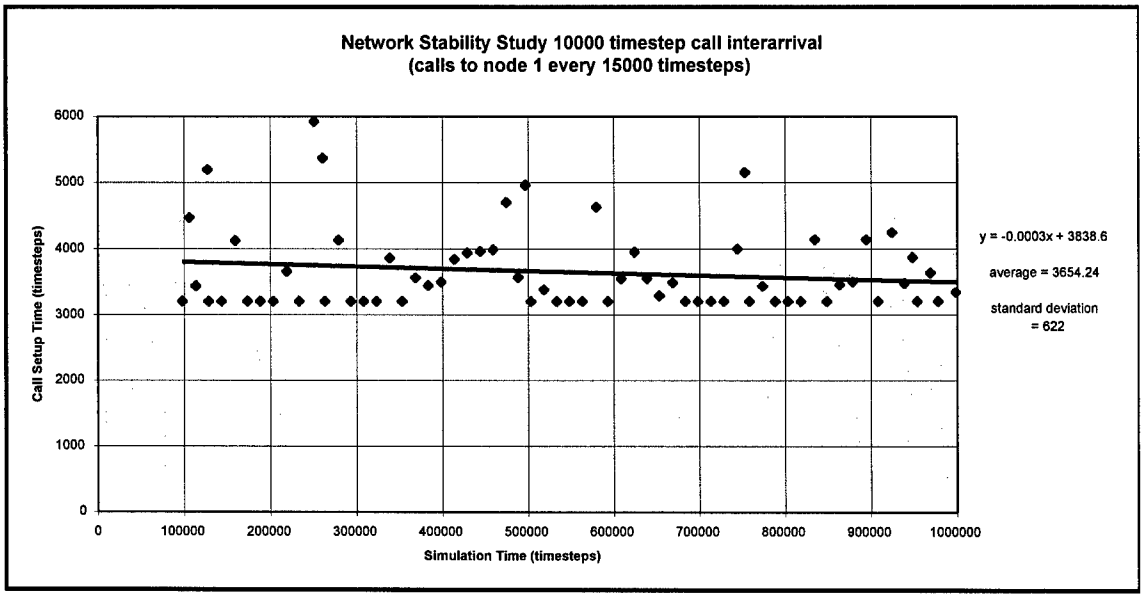



Figure 24. Scatter plot of node 8's call setup times to node 1 with a 10000 timestep call interarrival time (modified input file).

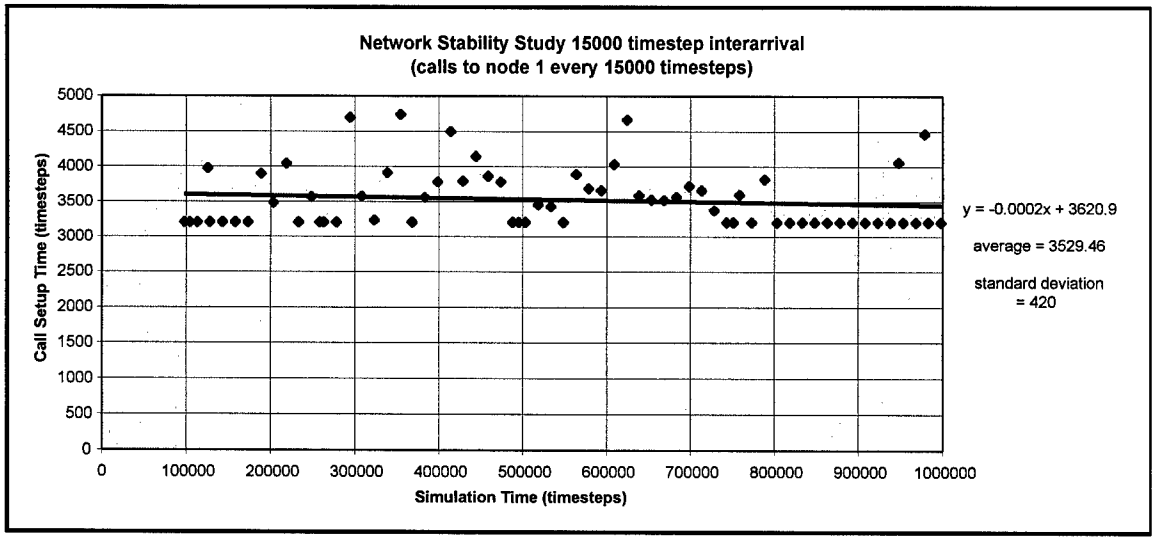



Figure 25. Scatter plot of node 8's call setup times to node 1 with a 15000 timestep call interarrival time (modified input file).

The overall objective of the stability study was to determine a call interarrival time which enabled each node to generate the maximum number of calls possible while maintaining the overall stability of the network. The most appropriate call interarrival time is determined to be 7500 timesteps by looking at the call success rate and the trend of the call processing times for a set of calls originating at node 8 with a destination of node 1. As the time between calls generated by nodes decreases, the call success rate goes down and the call processing time goes up. The network reaches a certain point where the trend in call processing time is increasing while the call success rate decreases, creating an unstable network. In the case of a call interarrival rate of 7500 timesteps, the call setup time did not increase over time and the call success rate remained above 80% as shown in figure 25. The call success rates for the call interarrival times of 10000 and 15000 timesteps are nearly 100% are also plotted in the figure. Bandwidth usage affected the call success rate. These interarrival times are not selected because the network would not be operating under enough stress and the objective is to generate input files for a worst case scenario.

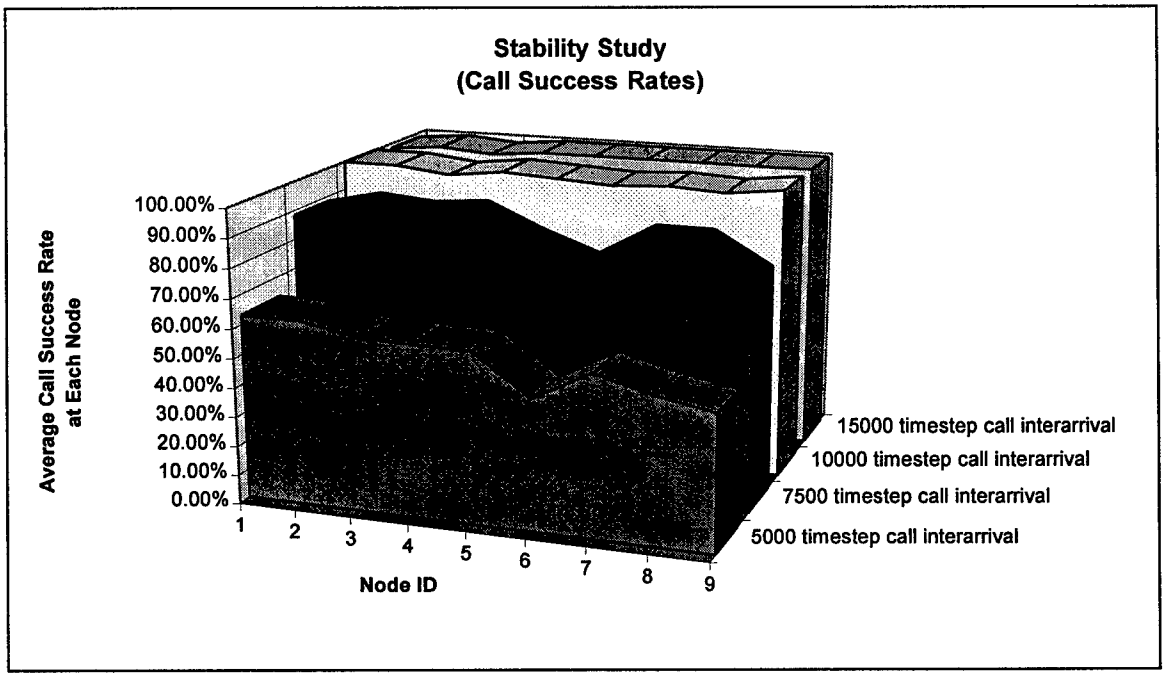



Figure 26. Call success rates for the four call interarrival times.

Using the 9 node network described, at a call interarrival rate of 5000 timesteps, the bandwidth usage on a link on the favored path between node 8 and 1 drops to zero within 300,000 timesteps and oscillates in a decreasing range of less than 30Mbps to zero for the remainder of the simulation and shown in figure 27. When the call interarrival rate is increased to 7500 timesteps, the first time the link available bandwidth drops to zero is not until more than twice the time previously noted and the rate of decrease in the amount of available bandwidth is not as steep, shown in figure 28, suggesting that the call interarrival time of 7500 is an appropriate rate which will utilize the maximum amount of available bandwidth without destabilizing the network. For the call interarrival rates of 10000 and 15000 timesteps, shown in figures 29 and 30, the available bandwidth remains above zero and appears to level out after an initial decline.

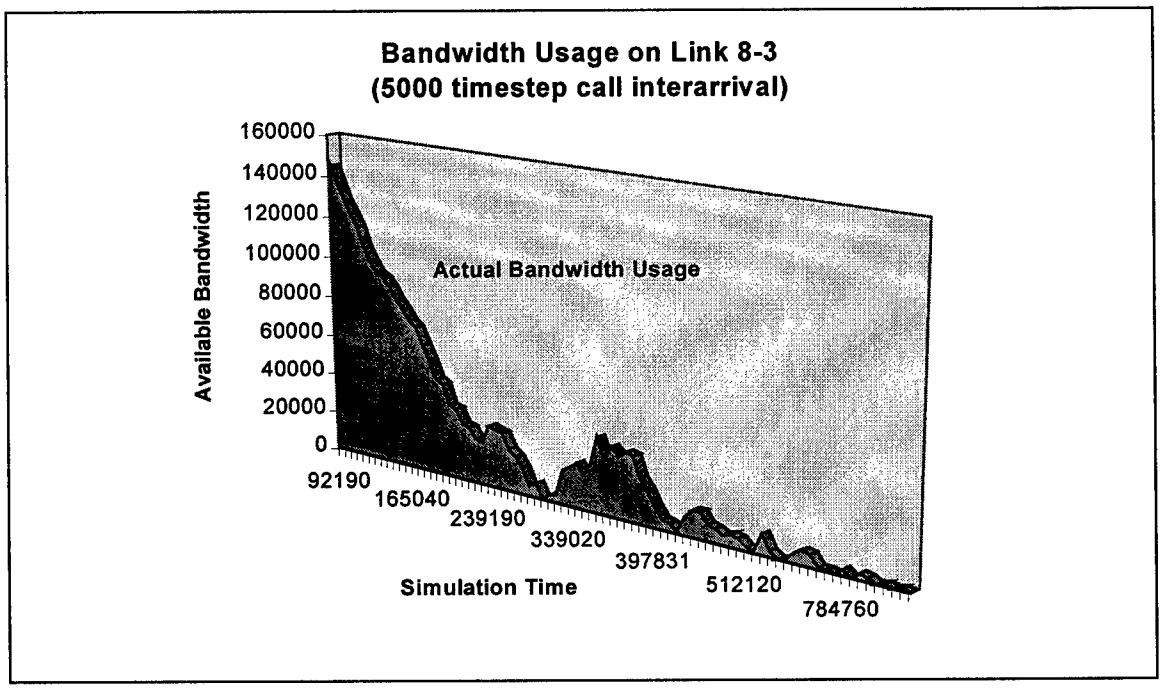



Figure 27. Bandwidth usage on link 8-3 with a 5000 timestep call interarrival.

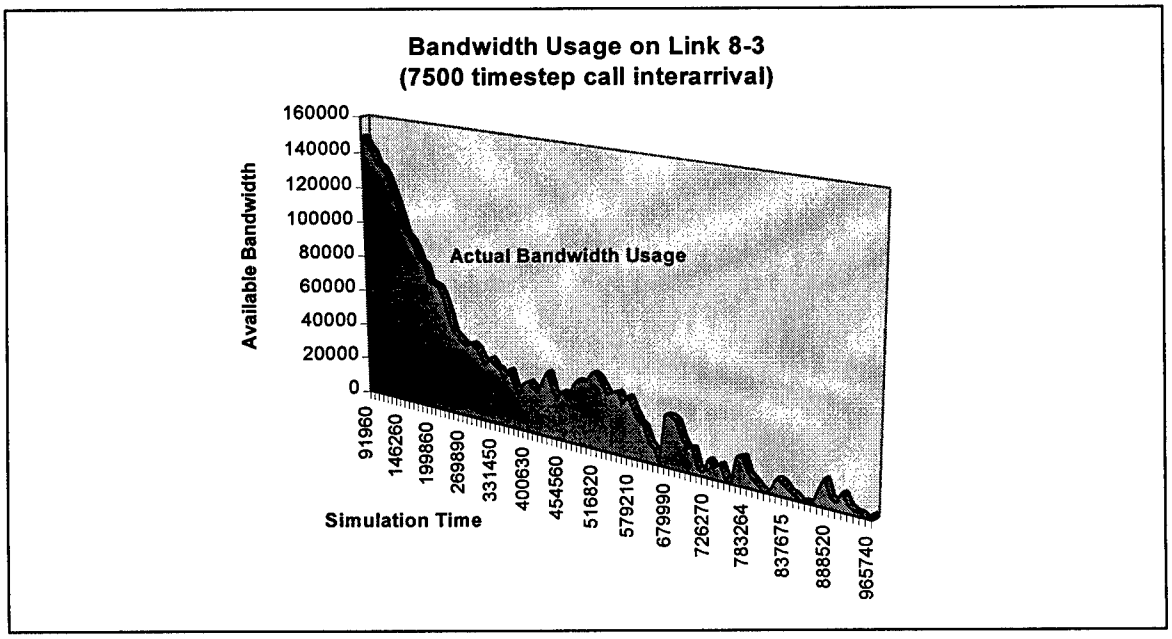



Figure 28. Bandwidth usage on link 8-3 with a 7500 timestep call interarrival.

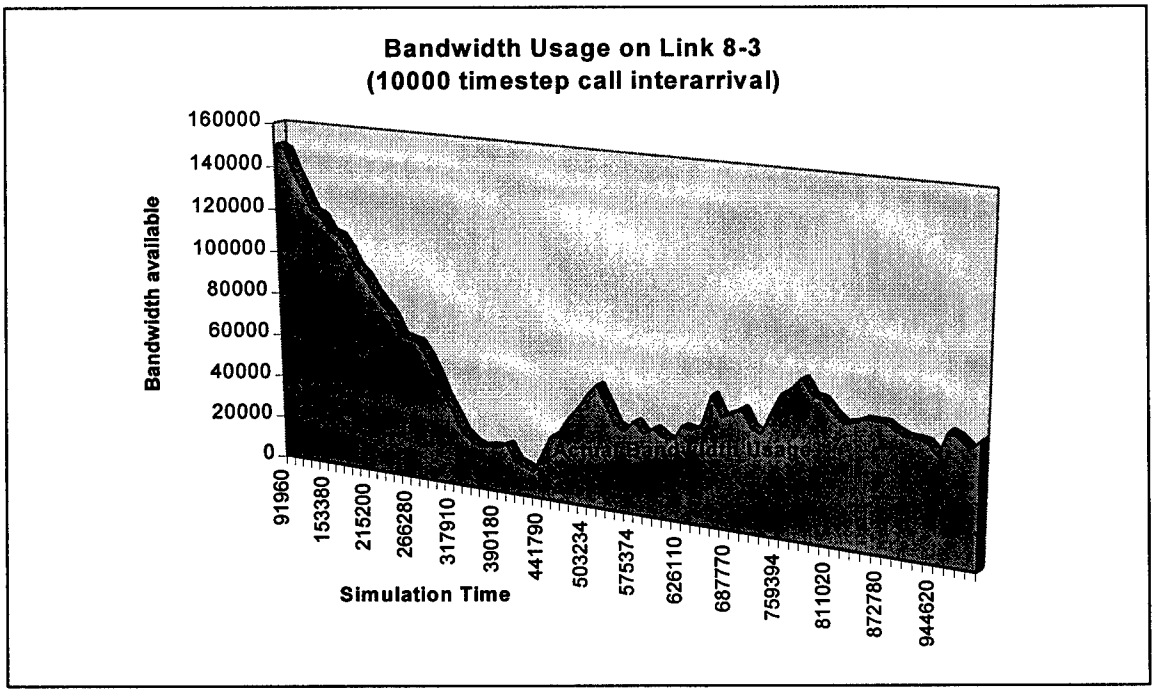



Figure 29. Bandwidth usage on link 8-3 with a 10000 timestep call interarrival.

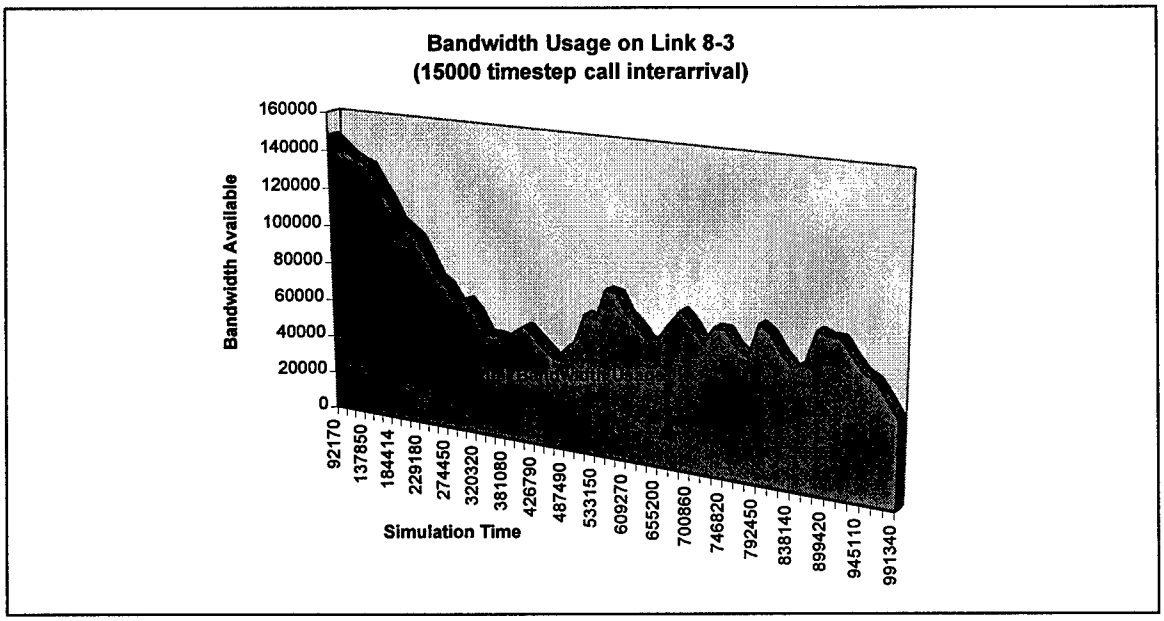



Figure 30. Bandwidth Usage on Link 8-3 with a 15000 timestep call interarrival.

# CHAPTER 7

# DISTRIBUTED SIMULATIONS OF BASELINE AND SECURITY MODELS, SIMULATION RESULTS AND PERFORMANCE ANALYSIS

## Introduction

Performance comparisons between an ATM network based on the ATM Forum's PNNI specification (ATM Forum Technical Committee 1996) and one with the security on demand system integrated into the network's operation were made possible by executing a series of simulations utilizing the three networks and input files described in Chapter 5. Three versions of the ATM network simulator code were used in the scenarios - (1) the current ATM PNNI specifications: baseline model, (2) the user level, security on demand system integrated into the PNNI: security on demand model and (3) the security system integrated into the PNNI with a highly refined routing algorithm utilizing the available security on the links, physical propagation delay of the links and a range factor reflecting the level of available bandwidth, encapsulated through a function termed Node Status Indicator: NSI model.

The objective of the simulations was threefold. First, the successful modeling and simulation validates the approach proposed here, namely the ability to integrate the security on demand system into the ATM Forum's PNNI specification. Second, the simulation results enable a comparative evaluation of the representative ATM networks, in the presence and absence of the security on demand system. Third, refinements to the

model were designed and results collected and compared to determine what refinements, if any, serve to improve the performance of the security on demand for a class of users.

It is well known that the addition of security into a system has generally been ad hoc and that the penalty is serious performance degradation. Since the elements of the author's fundamental security framework are integrated into the basic ATM principles, minimal performance impact on the network's operation is reasonable to expect. Three logical performance metrics were used - (1) the number and percentage of calls successful at each node and the overall number and percentage of calls successful for all nodes, relative to the total number of calls inserted at the node and at all nodes, (2) the total and average time required for call processing at every node as well as for all nodes combined and (3) the percentage of calls successfully processed at every node, relative to the total number of calls processed at the node in addition to the total and percentage for all nodes combined.

**Successful Integration of the "User Level Security on Demand System"**

The successful modeling and simulation of an ATM network with the user level, security on demand system integrated into an ATM network's operation demonstrates the security on demand system can function in an ATM network and be successfully integrated into the ATM Forum's PNNI specification. The call success rates for the security on demand model are shown in figure 31.

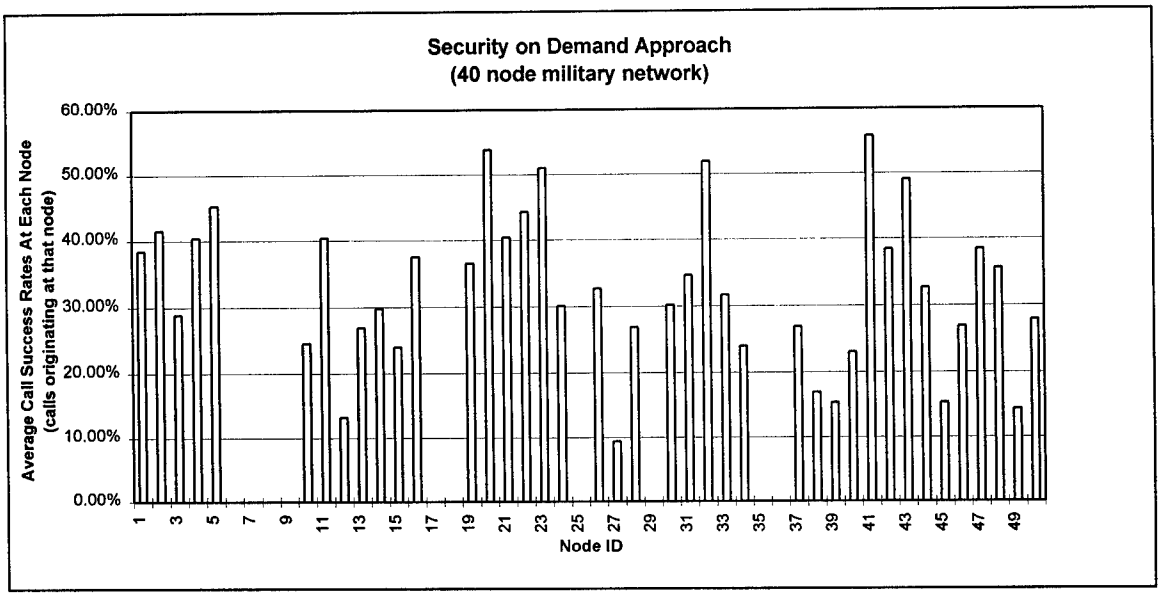



Figure 31. Average call success rates at each node for the security on demand approach using the 40 node military network.

Every node in the network has a unique identification number which is the basis for the x axis in figure 31. Since the military network is used for the collection of results, there are only forty nodes which have information plotted by the corresponding node id. The 10 node ids without results belong to the solely commercial nodes which only appear in the commercial and mixed use networks. There are a total of 22 nodes which jointly appear in both the commercial and military networks. The number of calls generated at these nodes are approximately ½ the rate of solely military or commercial nodes. In this study, the number of calls generated at joint nodes is 54 and at solely military nodes, 104. The call success rate across each node for calls originating at that node is plotted on the y axis and is determined by dividing the total number of successful calls by the total

number of calls attempted at the originating node throughout the duration of the simulation.

The overall network call success rate for the 40 node military network is 32.56% with a total of 984 successful calls. The overall average network call setup time is 4234.7 timesteps. The average call setup time at each node is shown in figure 32. The x axis represents the unique node identification number of the node and the y axis represents the average call setup time at each node for calls originating at that node. The scale of the y axis is in timesteps.

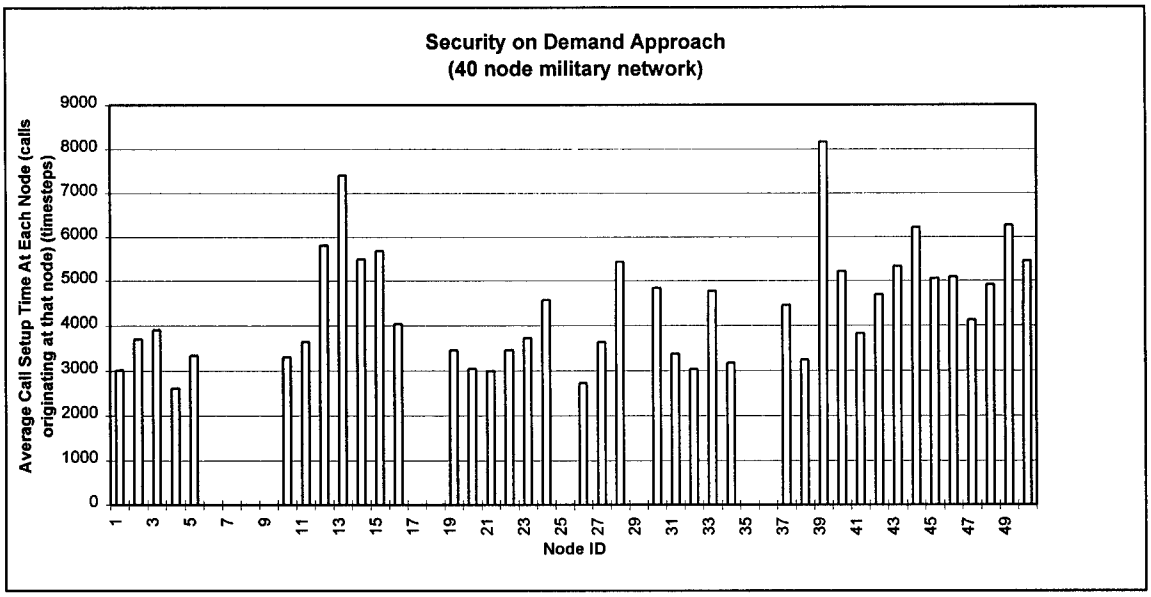



Figure 32. Average call setup time at each node for the security on demand approach using the 40 node military network.

Examination of the results show an average call setup time range from 2610 timesteps on node 4 to 8167 timesteps on node 39. The low average call setup time on

node 4 is due to a high number of short hop routes to other nodes within the group. Out of a total of 42 successful calls from node 4 there are 30 successful calls requiring only one hop and 11 successful calls requiring only two hops to reach their destinations. Node 4 has three direct links to other nodes within the group. The short number of hops for the successful calls implies reduced cumulative physical propagation delay for the routes and number of nodes required to process the call resulting in a low, average call setup time for node 4.

The higher average call setup time on node 39 is due to 1 successful call of the 8 total which were successful at this node. One call to node 21, required a total call processing time of 35748 timesteps and the path included a total of 11 hops. The small number of successful calls at this node in addition to the 11 hop call to node 21 resulted in the high average call processing time for node 21.

### Overview of the Performance Impact of Security on Demand

Following its scientific validation, the second objective of the performance study focuses on the ATM network's operation. A baseline reference model was created and results collected on an ATM network operating under the ATM Forum's PNNI specification for the comparative analysis.

The initial metrics used for comparing the performance of the baseline to the security on demand model, overall call success rate and overall average call setup time,

are broad measures of the general behavior of the two models. The baseline results show an overall call success rate of 31.5% for a total of 952 successful calls across all 40 nodes.

The baseline model's results reveal the overall average call setup time is 4246 timesteps for the 40 node network. The broad measures of overall call success rate and overall average call setup time across all nodes for the baseline and security on demand results show only a factor of 1.06 difference in the overall call success rates or a total of 32 additional successful calls using the security on demand approach and the overall average call setup time for the security on demand model was only 11.3 timesteps shorter than the baseline reference model. The baseline results for the average call success rate and call setup times for each of the 40 nodes in the military network are shown in figures 33 and 34.

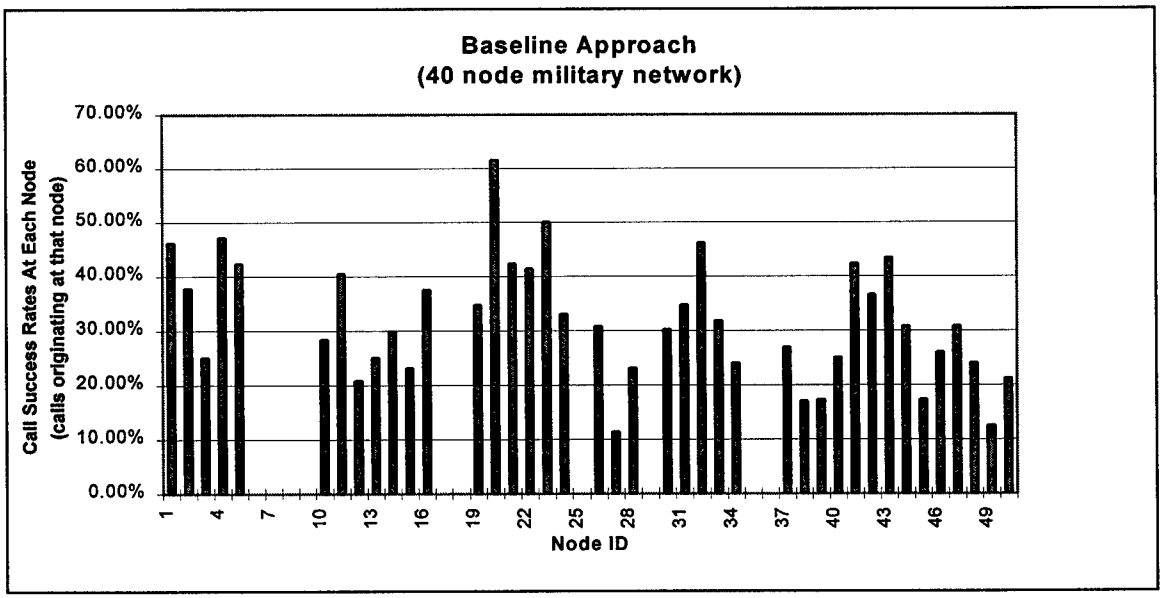



Figure 33. Call success rates at each node for the baseline approach using the 40 node military network.

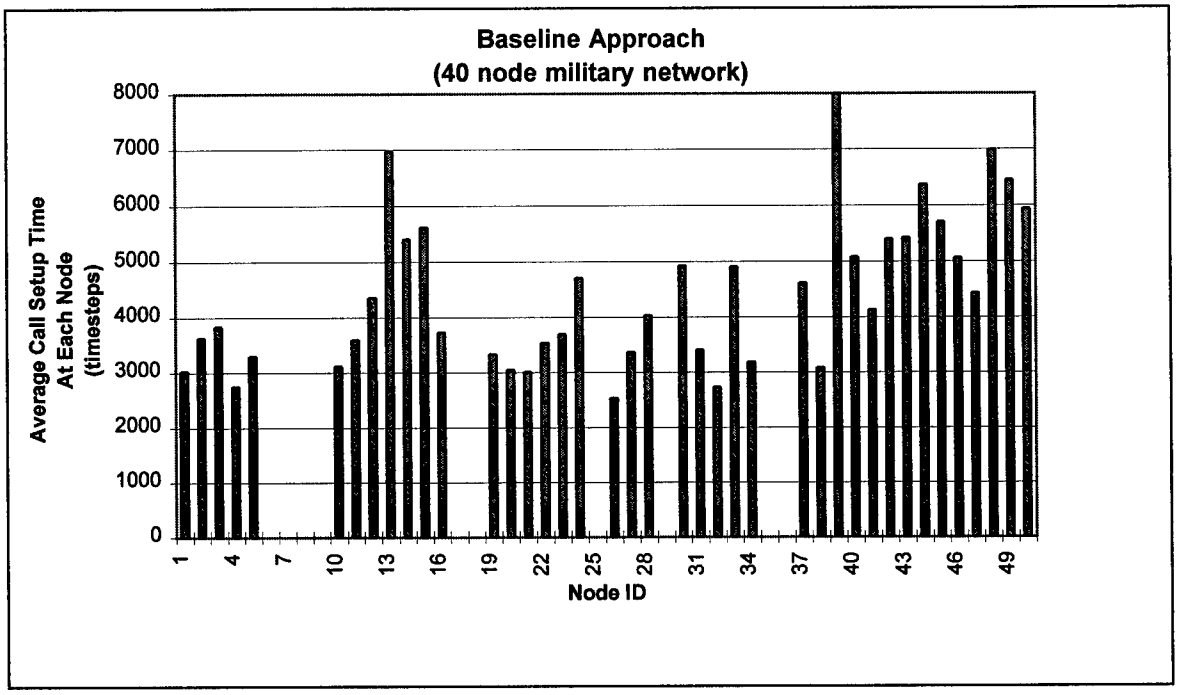



Figure 34. Average call setup time across each node for the baseline approach using the 40 node military network.

The results for the call setup times and call success rates at each of the forty nodes, for both the baseline and security on demand models, as well as the overall call success rate and overall average call setup time across all nodes, were used in the comparative analysis of the two approaches. A comparison of the average call success rates and call setup times for each node are plotted in figures 35 and 36 and show the range between the two sets of successful call rates to be small, supporting the hypothesis that a user level, security on demand system can be successfully integrated into the operation of an ATM network with minimal performance impact.

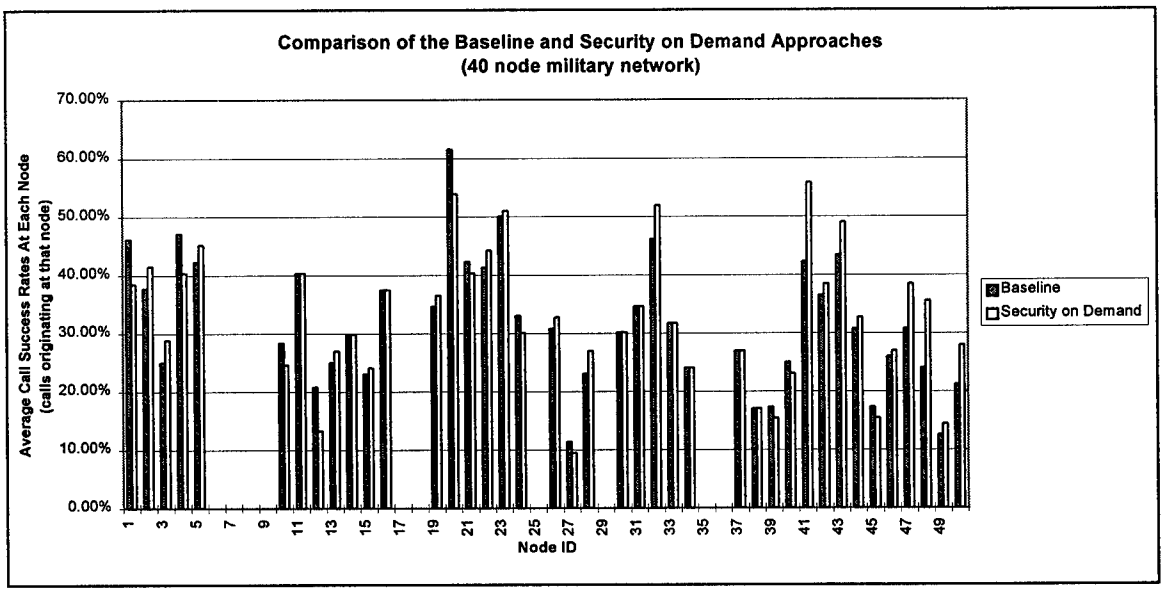



Figure 35. Comparison of average call success rates at each node between the baseline and security on demand approaches using the 40 node military network.

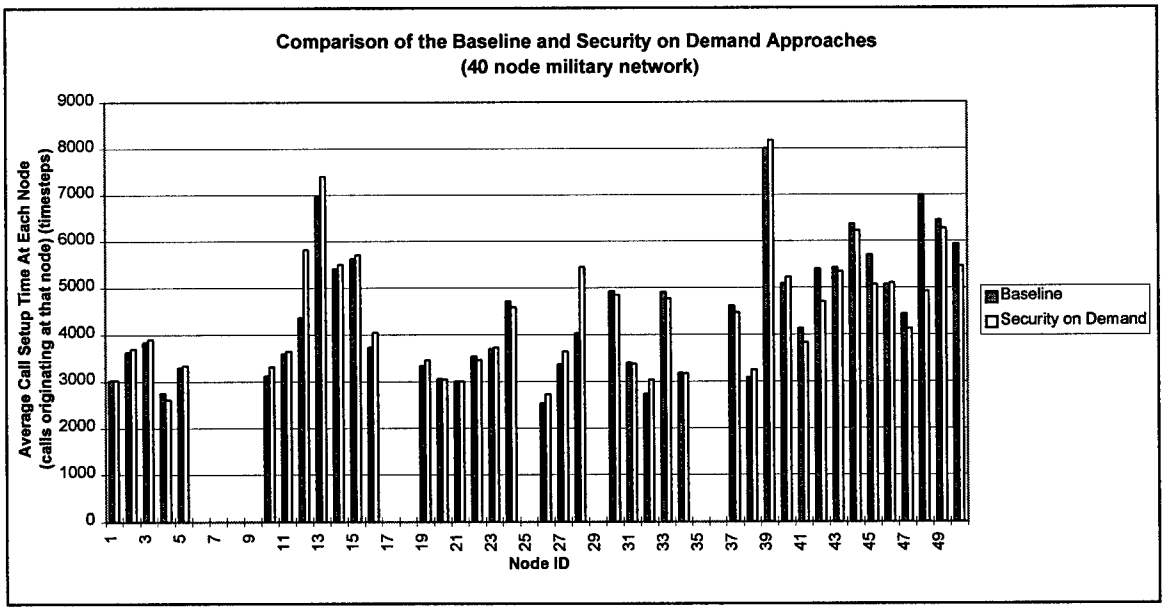



Figure 36. Comparison of the average call time at each node between the baseline and security on demand approaches using the 40 node military network.

Further analysis of the security on demand results reveal that group seven's node's, nodes 41 through 50, call success rates are higher on 9 of the 10 nodes in that group. The higher rates on those nodes caused the overall call success rate for the security on demand model to be higher than the baseline model. This may appear counterintuitive, but when the results from group 7 are removed, the overall call success rate across the remaining nodes for the baseline approach is 33.57% compared to 33.21% for the security on demand approach. This is as expected.

The reason for the difference in group seven's performance lies in the method used to select a path for the call setup message, the rich topology of the group and the differences in the topological data used for route selection in the baseline and security on demand approaches. In the baseline approach, the path selection is determined by the shortest path between the source and destination based on the link physical propagation delay value. These values are different for all 12 links within group 7 causing the path chosen to have the smallest total physical propagation delay time but not necessarily the shortest number of hops.

In the security on demand approach, the path selection is based on the shortest path between the source and destination as determined by the security value of the link. All links in the military network have the highest security value of "0". With all link values equal, the path selected for the call setup message will be always characterized by the shortest number of hops but not necessarily a path with the least total physical propagation delay. This explanation of the difference in path selection techniques for the

call setup message is also applicable to the comparison of the security on demand and more refined approach using the NSI in the next section.

In order to better understand what is occurring, an example using actual call setup request results is given tracing four successful calls under both the baseline and security on demand approaches. In the baseline approach, for the 4 successful call requests to node 48, two different paths are selected and shown in figure 37. One is from Alexandria through the Pentagon and White House nodes ending at Anacostia requiring 3 hops for 3 of those calls, call id numbers 1, 29 and 39. The other path selected is from Alexandria through the Pentagon node to Anacostia requiring 2 hops for the remaining call, call id 73. In contrast, under the security on demand approach only one path from Alexandria through the Pentagon node to Anacostia is used for all 4 calls, call id 1, 29, 39 and 73. All of the 4 call requests are successful on this two hop path depicted in figure 38.

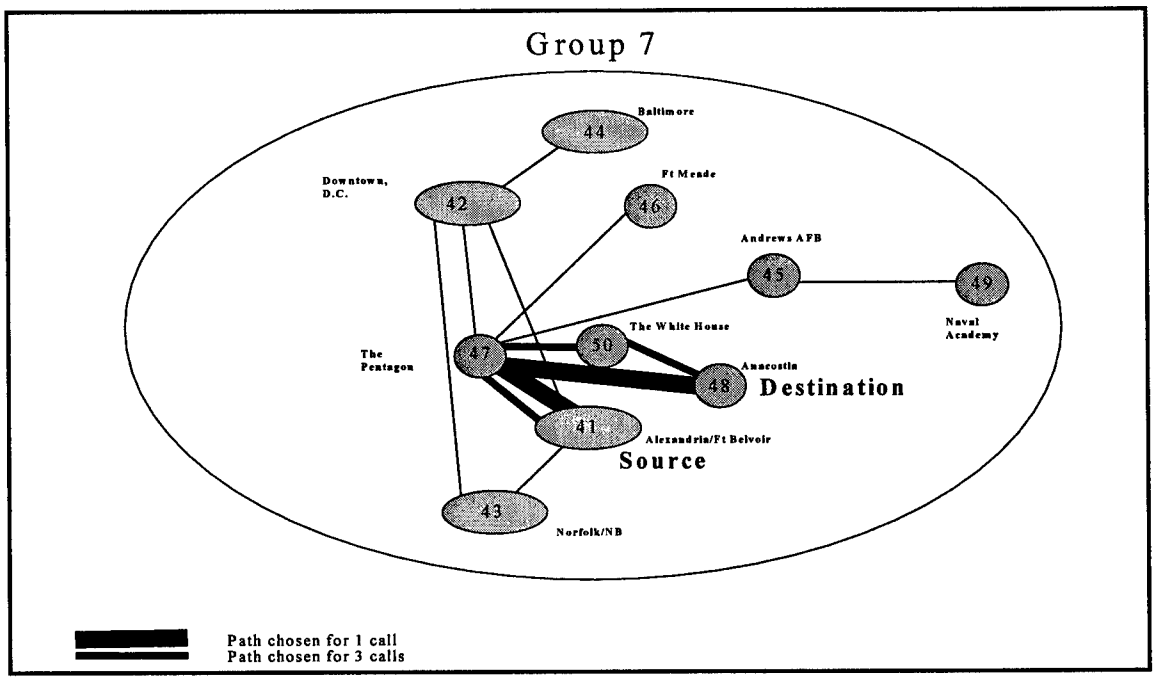



Figure 37. Path selection for the 4 calls made from Alexandria to Anacostia under the baseline approach.

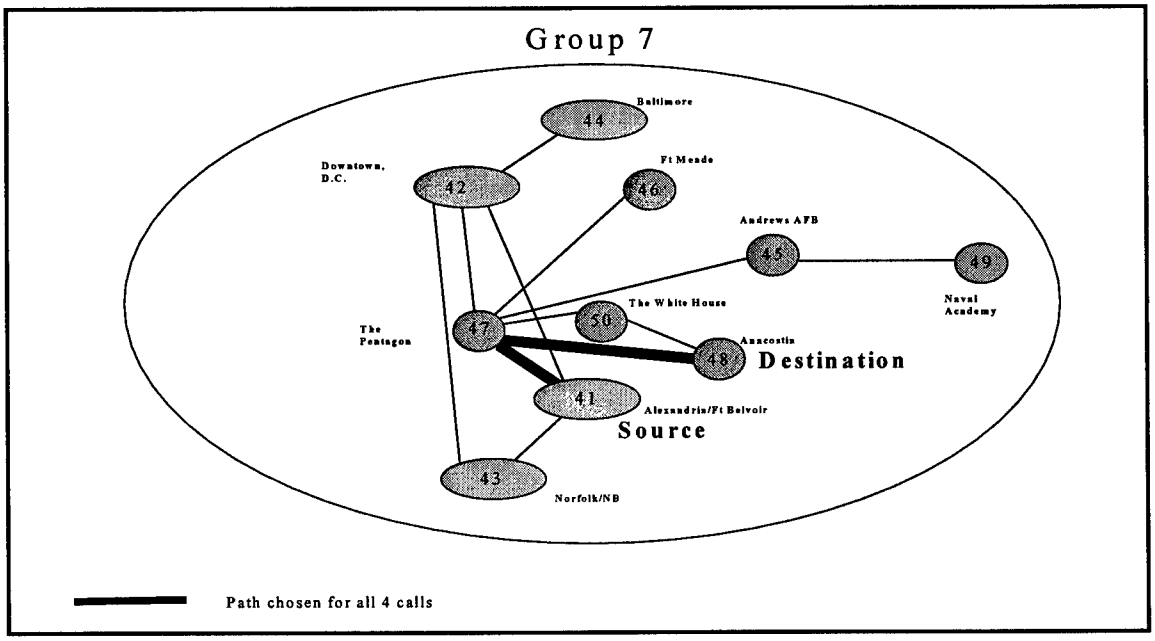



Figure 38. Path selection for the 4 calls made from Alexandria to Anacostia under the security on demand approach.

The results of call successes and failures reveal the tendency for the baseline approach to select paths requiring more hops than the security on demand approach. These differences between the two approaches, combined with the large number of call attempts in the network produces an environment which benefits an approach favoring path selection based on the minimum number of hops. The smaller the number of hops, the less likely the call is to fail due to bandwidth not being available, resulting in a higher call success rate. The fewer number of hops in a path the less number of nodes traversed. Since each node through which a call travels adds to the overall processing time of a call, the less number of nodes traversed, the lower the average call setup time which accounts for the slightly higher average call setup times for the baseline approach. While the differences between the two models is most pronounced in group 7 due to the multiple paths between nodes, there is little difference with respect to average call setup time in groups 4, 5 and 6 due to the sparse topologies of these groups which limits the number of paths between nodes.

Thus, the result of these comparisons show the performance impact of integrating the user level, security on demand system into the PNNI call setup process of an ATM network is negligible. The most significant contribution of this study is the successful realization of the user level security on demand paradigm, through modeling and asynchronous, distributed simulation. Another contribution of this research is that since the asynchronous, distributed simulation of the representative ATM networks under

security on demand closely resembles the actual operational networks, the code developed here may be transferred to actual ATM networks with little effort.

## Analysis of NSI Model's Impact on Performance

Thus far, the choice of routes, a key issue in security on demand, has been confined to the available security on the links and associated nodes and the physical propagation delay of the links. A refinement is introduced here wherein the available bandwidth of the links is considered along with the other two components. These three components are combined in what is called the NSI function. The use of the NSI function to refine performance is a result of viewing bandwidth as a dynamic security resource and refining its use in the route selection process for the call setup message. The available bandwidth is encapsulated through a factor determined from one of the five levels described in the section in chapter 5 titled, Refinement of the Security on Demand Model: NSI Model. The objective of using available bandwidth is to "spread" i.e., disperse the routes selected throughout the network instead of confining to a few routes. The hypothesis being that if a link is coded with a NSI value a better distribution of resources is possible conditional on the existence of more than one path to a destination with the requested bandwidth. As bandwidth is allocated or deallocated and the available bandwidth exceeds or falls below certain thresholds, the NSI values associated with the links are increased or decreased, thereby impacting the route selected for the call setup messages.

Figure 39 presents the call success rates of each of the 40 nodes in the representative military ATM network under the original security on demand model and the refined approach, NSI model. On 31 out of 40 nodes, the call success rate for the NSI model is either identical or lower than the security on demand model.

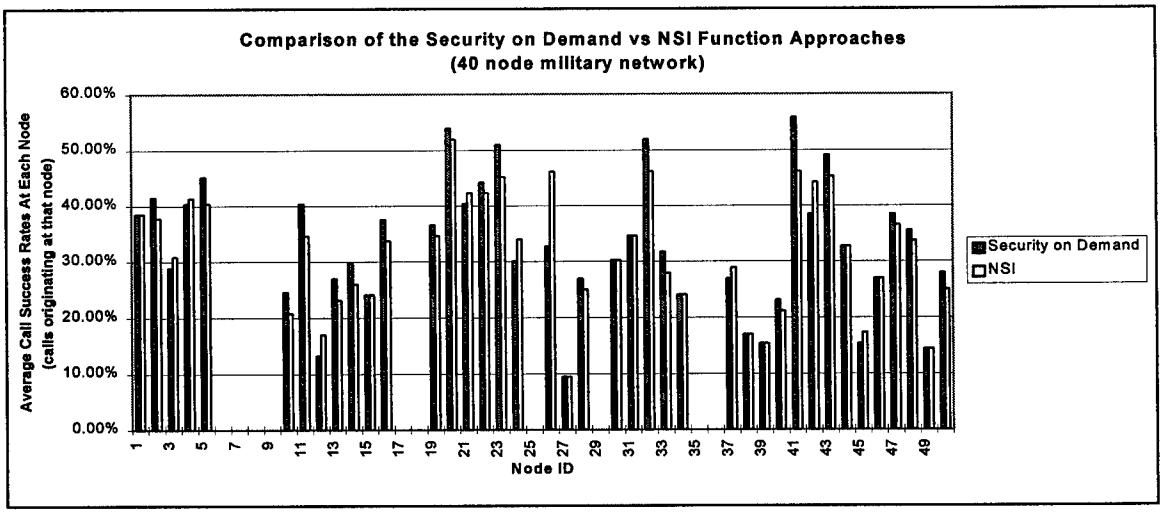



Figure 39. Comparison of the average call success rates at each node between the security on demand and NSI function approaches on the 40 node military network.

The call success rate is higher for 9 nodes, especially node 26. The reason the call success rate is higher for that node is due to a combination of the call success rate being lower for other nodes, resulting in a new pattern of intergroup calls that are routed through node 28. This pattern at simulation timestamp 694617, shows the available bandwidth on the link between nodes 28 and 26 is 100 times greater under the NSI model. This frees up bandwidth on the links connected to node 28 so that 5 of the 9

additional successful calls made from node 26 under the NSI model can be successfully routed to and through node 28.

The average call setup times for each of the nodes in the security on demand and NSI function models are shown in figure 40. The slightly higher average call setup times for the security on demand approach as compared to the NSI approach are due to the high volume of traffic, low available bandwidth and network topology as is the case with the comparison between the baseline and security on demand approaches discussed in the previous section.

The longest difference in the average call setup time occurs at node 13. This node has four fewer successful calls then the security on demand approach for a total of 24 successful calls with one of the successful calls being an intergroup call to node 46 with a call setup time of 33380 timesteps. This call is not successful in the security on demand approach. The resulting differences in the total call setup time causes the average call setup time for node 13 to spike under the NSI function approach. If node 13 results are removed and the two approaches are compared, the resulting overall average call setup time for the security on demand approach is 4142 timesteps and 4187 timesteps for the NSI function approach a difference of only 45 timesteps as compared to the difference of 65 timesteps with the node 13 results.

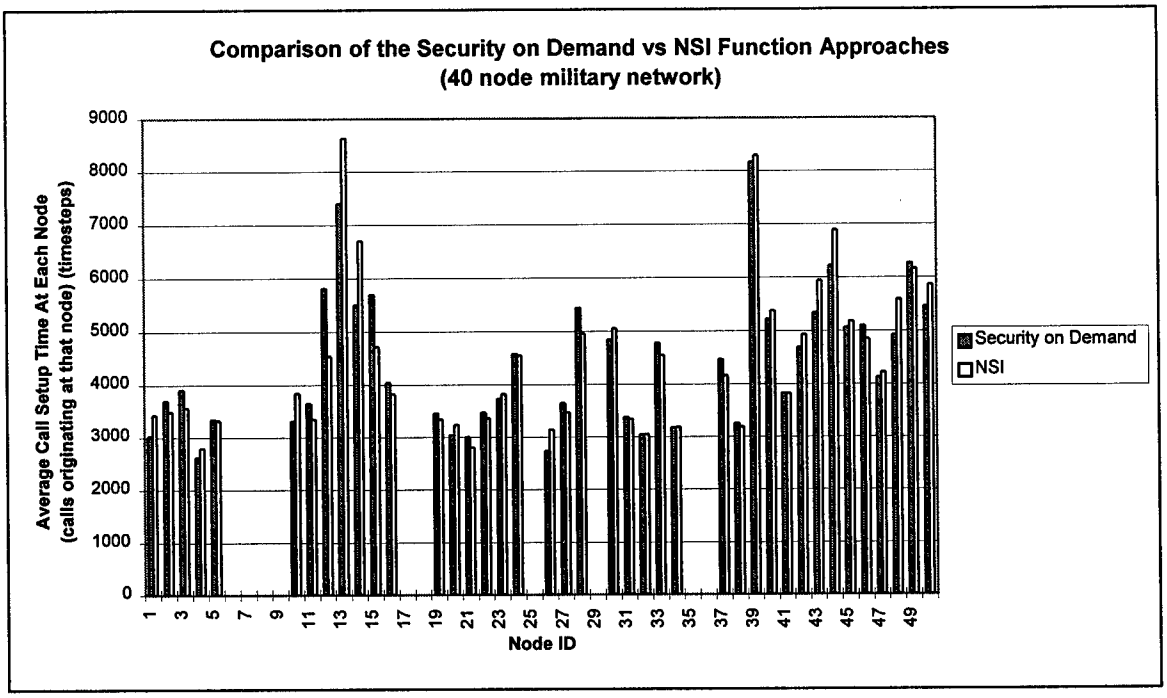



Figure 40. Comparison of the average call setup time at each node between the security on demand and NSI function approaches using the 40 node military network.

So, both the average call success rates and call setup times are slightly worse in the NSI model as compared to the original security on demand approach. The real benefit of the NSI approach is the manner in which the calls are distributed across possible paths to a destination. This even "spread" across alternate paths can be advantageous to a network provider who desires to distribute the network calls across all available resources evenly. It can also be an advantage to a user or group of users such as the military who do not want to rely on a primary path between a particular source and destination which can become a target for the enemy. Spreading calls across the network has the additional security advantage of masking network activity.

Under the NSI approach, the calls will have a tendency to be spread evenly across possible paths between the source and destination. The constant, high level of traffic causes the bandwidth to have a low availability rate causing a larger number of calls to fail due to limited bandwidth availability. Since the NSI approach increases the number of hops on some paths chosen, the likelihood of a call failing on a link due to bandwidth not being available is greater then under the security on demand approach.

Analysis of actual call data between a particular source and destination for the security on demand and NSI function approaches illustrates the distribution of the load or "spread" through the network. When the series of 19 attempted calls between Whidbey Island Naval Air Station (NAS) and Fort Lewis are compared, the differences in the path selection methods of the two approaches are clear. There are two possible paths to Ft. Lewis from Whidbey Island going through either Bangor Submarine Base or Seattle shown in figure 41. The physical propagation delay of the two routes is exactly the same and the initial bandwidths of each of the links is 155Mbps.

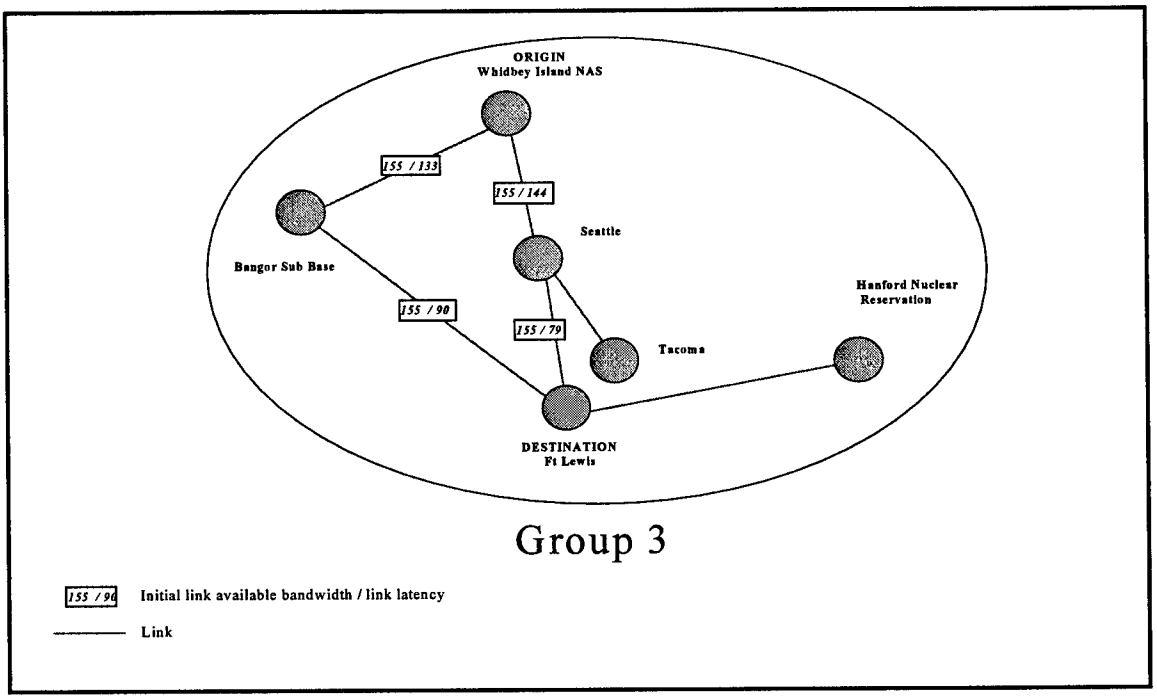



Figure 41. Group 3 topology.

Under the security on demand approach, the first eight successful calls follow a path through Seattle based on the fact that the link between Whidbey Island NAS and Seattle appears first in the database and since the security of all links and number of hops is equal, the path through Seattle is chosen and is shown in figure 42. When the 9th successful call is made, the available bandwidth on the link between Whidbey Island NAS and Seattle drops to zero and so the alternate path through Bangor Sub Base is chosen. When the 10th successful call appears, bandwidth is freed on the Whidbey Island NAS - Seattle link and the favored path again is through the Seattle node. Three other successful calls will be routed through Bangor Submarine Base, but only after the

available bandwidth on link(s) between Whidbey Island NAS and Seattle or Ft Lewis and Seattle have dropped to zero.

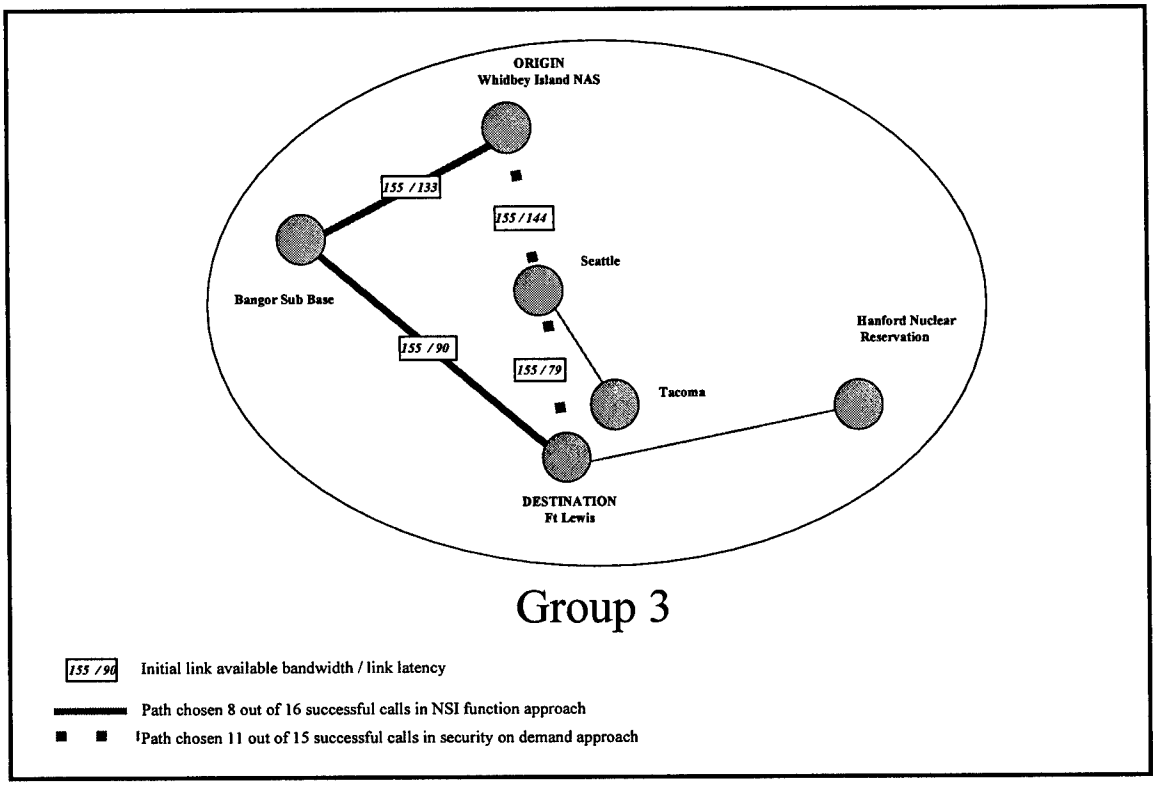



Figure 42. Path selection for calls made between Whidbey Island NAS and Ft. Lewis.

Under NSI function approach the initial path chosen is through Seattle since all other variables for the NSI function are the same and this path appears first in the list of possible paths. When the 6$^{th}$ successful call is processed, the bandwidth on the Whidbey Island NSA - Seattle link passes the set available bandwidth threshold of 77.5Mbps and the NSI function associated with this link becomes greater than the Whidbey Island - Bangor Sub Base link causing the path chosen to be routed through the Bangor Sub Base

node shown in figure 42. The next series of calls are routed alternately between Seattle and Bangor Sub Base as the bandwidth of links in the two paths is filled and the available bandwidth thresholds have been reached, the NSI value increases. The final outcome is an even distribution of calls between the two possible paths causing an even "spread" of calls on the two possible paths as opposed to the security on demand approach of favoring one particular path until all available bandwidth is exhausted.

While the tendency to spread the calls evenly across possible paths can be an advantage in some cases, when the network is stressed with a high call load and the bandwidth on links becomes full, the extra hops incurred on some of these alternate routes can become possible failure points during the call setup process. Extra hops result in additional possible failure points due to an increased chance of bandwidth unavailability.

Another example of results which illustrate a disadvantage of the NSI approach in a highly stressed network is also worth discussing. When the call data for node 41 in group 7 is analyzed, the disadvantage of the NSI function approach, in a highly stressed network, becomes apparent. An intergroup call is made to Ft. McPherson in group 5, early in the study when bandwidth is available on most links. The path chosen under the NSI function approach goes through downtown, D.C., Norfolk and then Ft. McPherson shown in figure 43. The same call, under the security on demand approach, follows a more direct path through Norfolk to Ft. McPherson also shown in figure 43. The extra

hop in NSI function path did not affect the success of the call since bandwidth was generally available on all links early in the simulation.

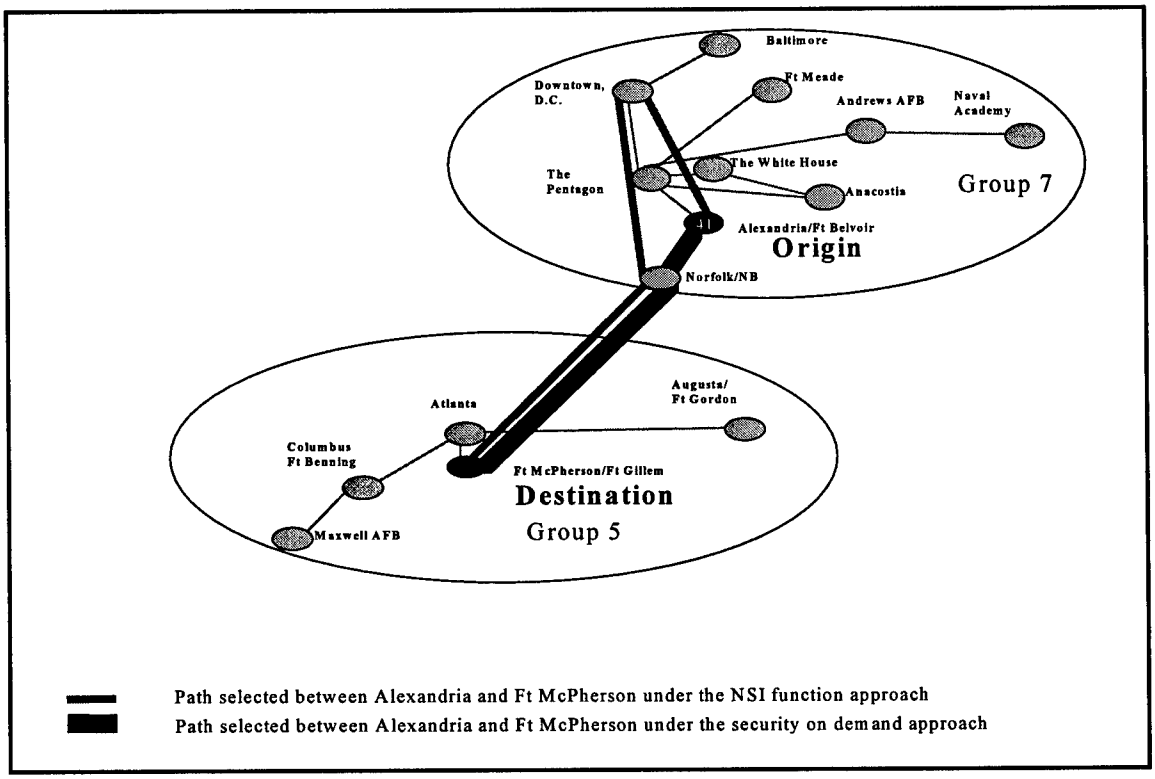



Figure 43. Path selection for calls made between Alexandria and Ft McPherson under the NSI function and security on demand approaches.

After this call, 4 calls are initiated from node 41 to node 49. On the first two call attempts, the NSI function approach chose a path through downtown, D.C., the Pentagon, Andrews AFB and finally the Naval Academy shown in figure 44. Both calls failed due to a lack of bandwidth on one of the links. The third call attempt from node 41 to node 49 under the NSI function approach which chooses the same path as before and is

successful. The fourth call attempt chooses a path through the Pentagon, Andrews AFB to the Naval Academy which proved to be unsuccessful. The security on demand approach chooses the same path for all 4 calls which included the Pentagon, Andrews AFB and finally the Naval Academy shown in figure 45.

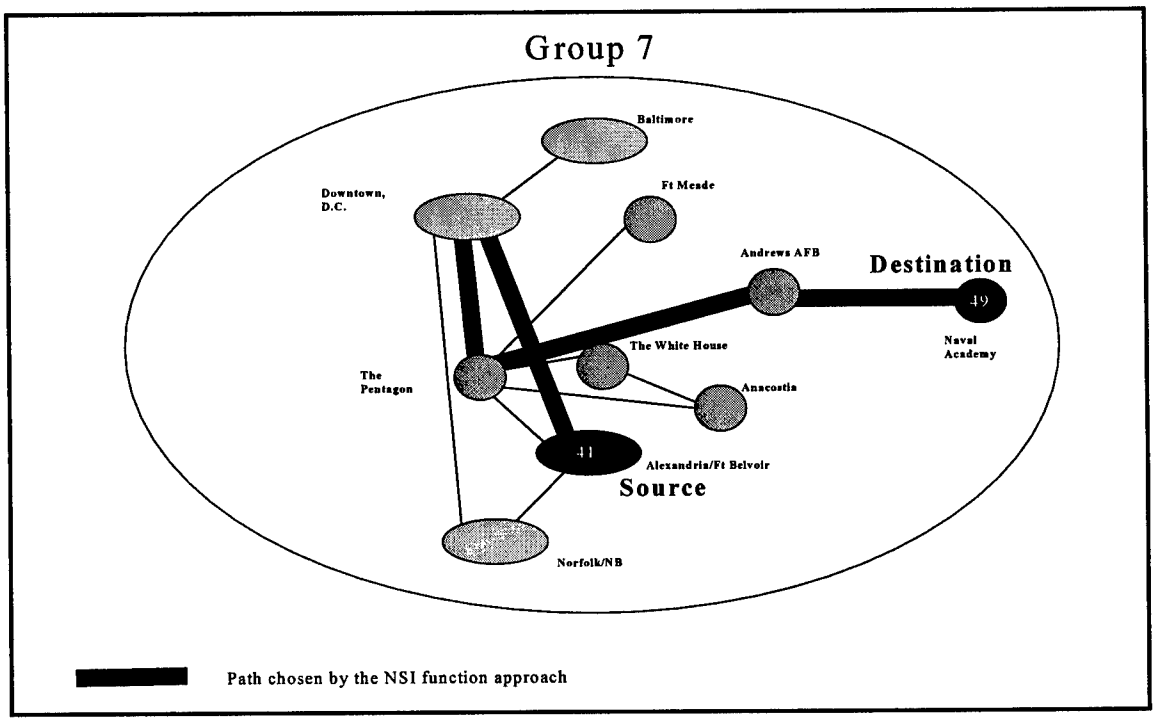



Figure 44. Path selection for the call made between Alexandria and the Naval Academy under the NSI function approach.

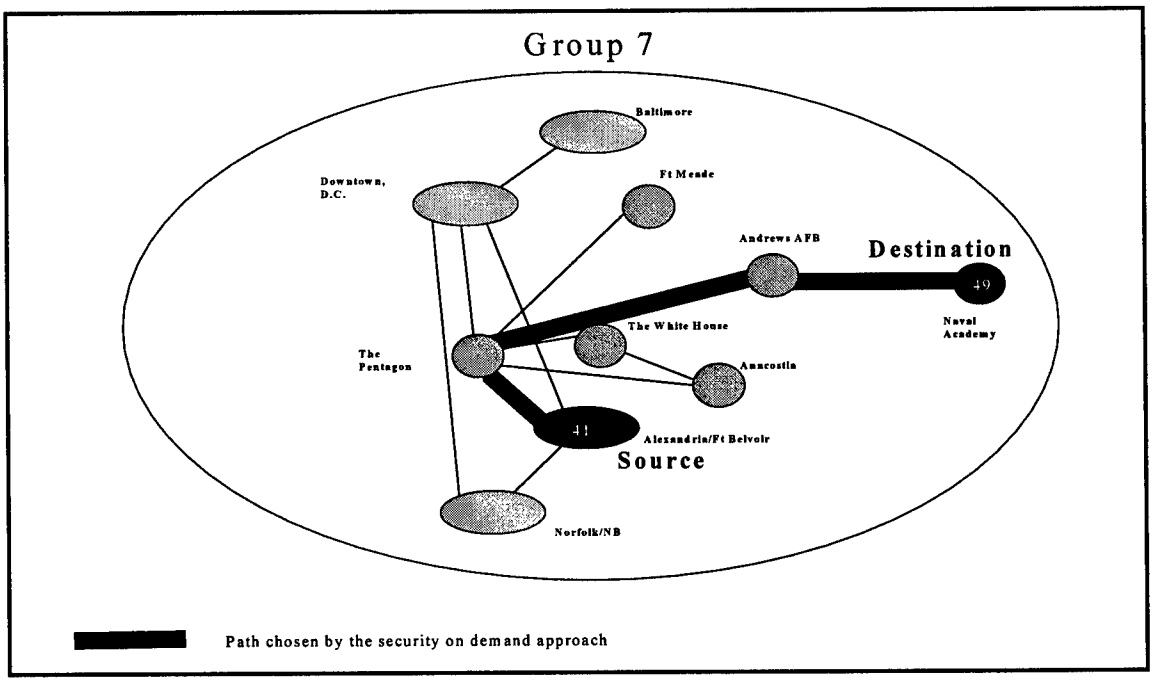



Figure 45. Path selection for the call made between Alexandria and the Naval Academy under the security on demand approach.

The success of all 4 calls under the security on demand approach and failure of two of the same 4 calls under the NSI approach illustrate the disadvantage of "spreading" calls across possible paths in a highly stressed network.

### Analysis of the Behavior of a "Mixed Use" ATM Network

A unique characteristic resulting from security on demand is realized through the combination of resources of isolated networks. The military, which could be the first to benefit from combining its networks, could connect its Top Secret, Secret, Confidential and Unclassified networks as well as connecting these networks to the public ATM backbones. Any unclassified traffic which previously was routed over a secure network

could be routed onto commercial nodes, relieving congestion on secure nodes. Secure traffic would be routed across military links and nodes as before. The combined network could also offer, in the future, civilian users the ability to send data over secure paths.

The ability to connect these previously isolated networks is a significant paradigm shift which can result in lower costs. If the call success rates and call setup times of the mixed use network are in the same range as in the isolated, military network, the military would benefit from such a combination of networks. The results, shown in figure 46, of a series of behavioral studies using the NSI model on the 3 representative military, commercial and mixed use networks show the differences in the average call success rates at each node for calls originating at that node, as well as the overall call success rates for all nodes and calls. Examining the results for the 50 and 40 node networks plotted in figure 46 show not only that such a combination of networks would not be detrimental to call success rates, it would improve them.

The overall call success rate of the 50 node, mixed use network is 40% or 8.6 higher than the 31.4% overall call success rate of the 40 node military network. The total number of successful calls for the mixed use, 50 node network is 2101, slightly higher than the 32 node commercial network's 1145 successful calls and 40 node military network's 950 successful calls or combined total of 2095 successful calls. The increase in the call success rates across the majority of nodes, as well as for the network overall, is due to the richer topology of the 50 node network which introduced multiple paths between nodes.

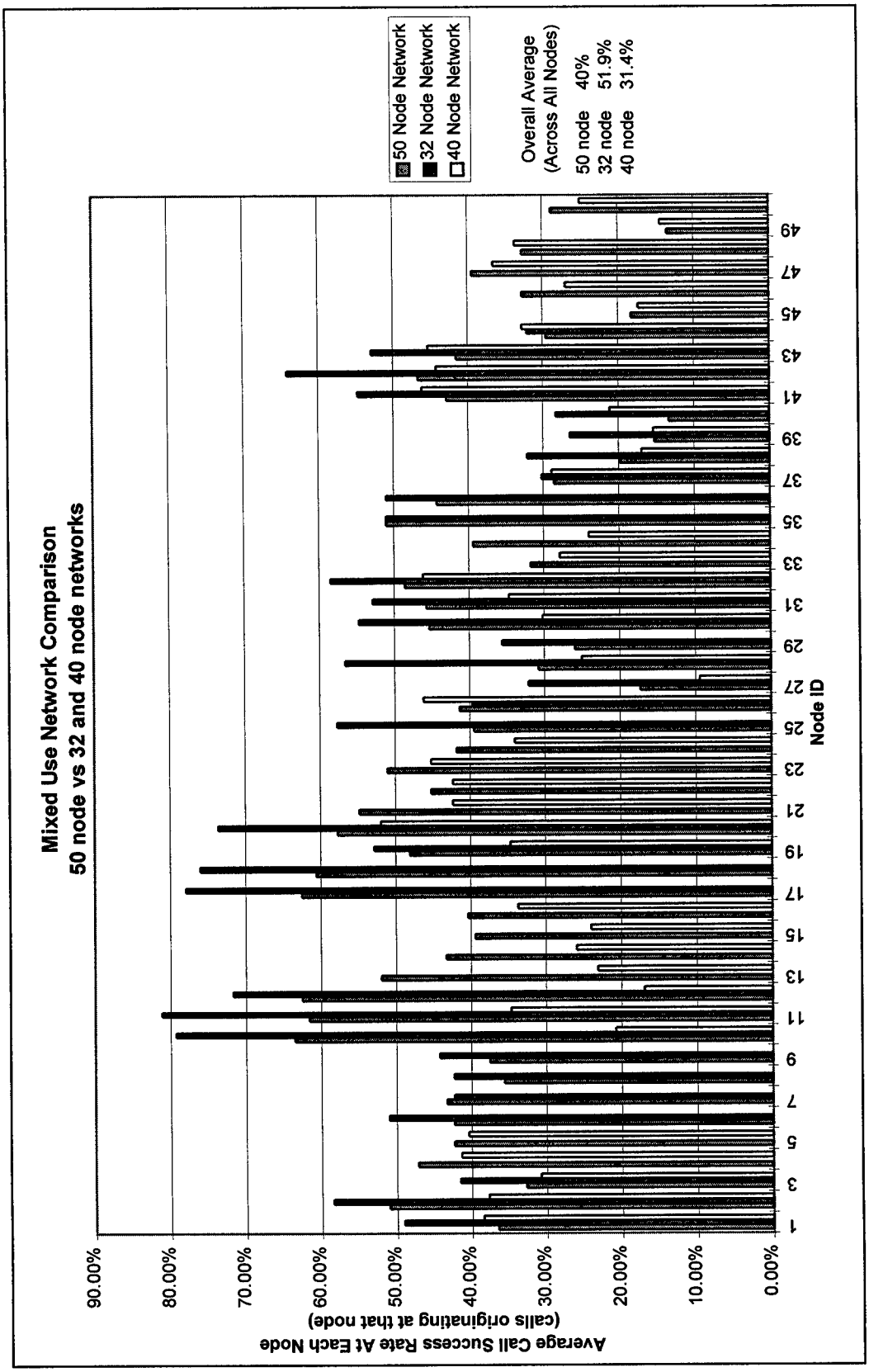



Figure 46. Comparison of the call success rates between the 50 node, "mixed use", 32 node, commercial and 40 node, military networks.

Every group of military nodes in the 50 node network, except group 7, show an improvement in the call success rate. Group 7 shows a slight decrease as a result of a lack of additional links being added when the commercial and military networks are combined into a 50 node network. The slight lowering of the call success rate at each node in group 7 is due to the increased call volume at the joint nodes 41, 42, 43 and 44 due to the insertion of the commercial traffic at these nodes which now compete for bandwidth on links between nodes 42 and 47 and nodes 47 and 41. The additional commercial traffic at the joint nodes within the group causes other calls from the solely military nodes to fail since node 47 is a critical node in the paths to all of the sole military nodes within group 7. Overall, the average call success rate increases for military nodes in a mixed use network when compared to the results from a solely military network.

One potential disadvantage of combining commercial and military networks is the drop in the call success rates of the commercial network nodes when compared to the 50 node, mixed use network's nodes. The rich topology of the commercial network is an asset under high traffic loads produced by this study, but when the high traffic loads of the solely military and joint nodes are combined with the solely commercial and joint nodes and compete for the limited bandwidth the call success rate drops. The overall call success rate of the 50 node, mixed use network of 40% was 11.9 lower than that of the 32 node, commercial network.

One potential advantage to civilian network users in combining military and civilian networks into a mixed use network would be the ability to request security assets for the protection of critical information.

A comparison of the average call setup time at each node for the mixed use, commercial and military networks is shown in figure 47 and an examination of the results shows an increase in the average call setup times at each node in the "mixed use" 50 node network. The increase in the call setup times is due to the increased number of calls being generated at the joint nodes in the network. These natural choke points in the network become aggravated when the military and commercial networks are combined due to the increased traffic loads. The increase of calls at choke points in the network causes a non-linear increase in the average call setup time at these nodes which, in turn, raises the overall average call setup time of the mixed use network. The average call setup time of 6736.1 timesteps for the mixed use network is 2867.8 times stamps longer than the commercial network and 2436.9 timesteps longer than the military network.

For example, at the choke point, group 4 which includes nodes 26, 27, 28 and 29, the call setup times are greater in the 50 node network compared to the 40 node network due to the additional link from group 3. The large increase on nodes 26, 27, 28, 29 and to a smaller extent nodes 37, 38, 39 and 40 is caused by a combination of two factors: (1) network topology, these nodes are part of choke point groups for intergroup calls (2) the success of more intergroup calls due to a richer network topology. Intergroup calls in

the 40 node, military network which were previously unsuccessful have an alternate path to group 4 in the 50 node, mixed use network.

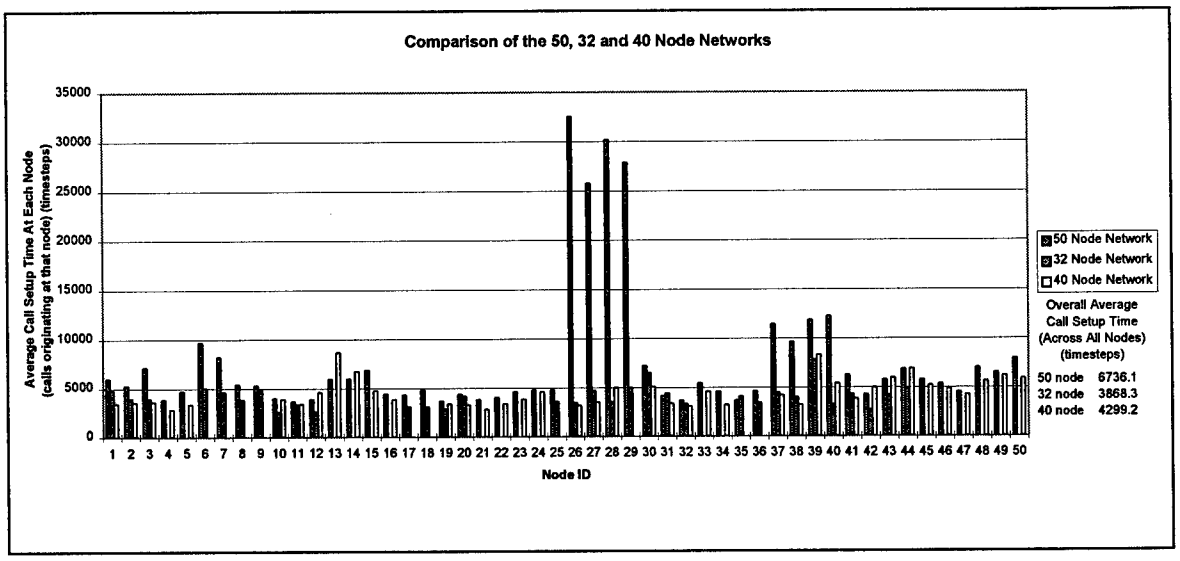



Figure 47. Comparison of the average call setup times by node between the 50 node, "mixed use", 32 node, commercial and the 40 node, military networks.

An analysis of an actual call between Seattle and Rocky Flats illustrates what is taking place on a larger scale through the network. The link between group 3 and group 4 which is present in the 50 node network does not exist in the military network. This additional link provides an alternative path which considerably reduces the number of hops for some intergroup calls. Analysis of the data for an actual call from Seattle in group 3, to Rocky Flats in group 4 using the military network, shows it followed a path, shown in figure 48, through San Francisco and San Jose in group 2 and fails in group 1 at Los Angeles due to lack of bandwidth.

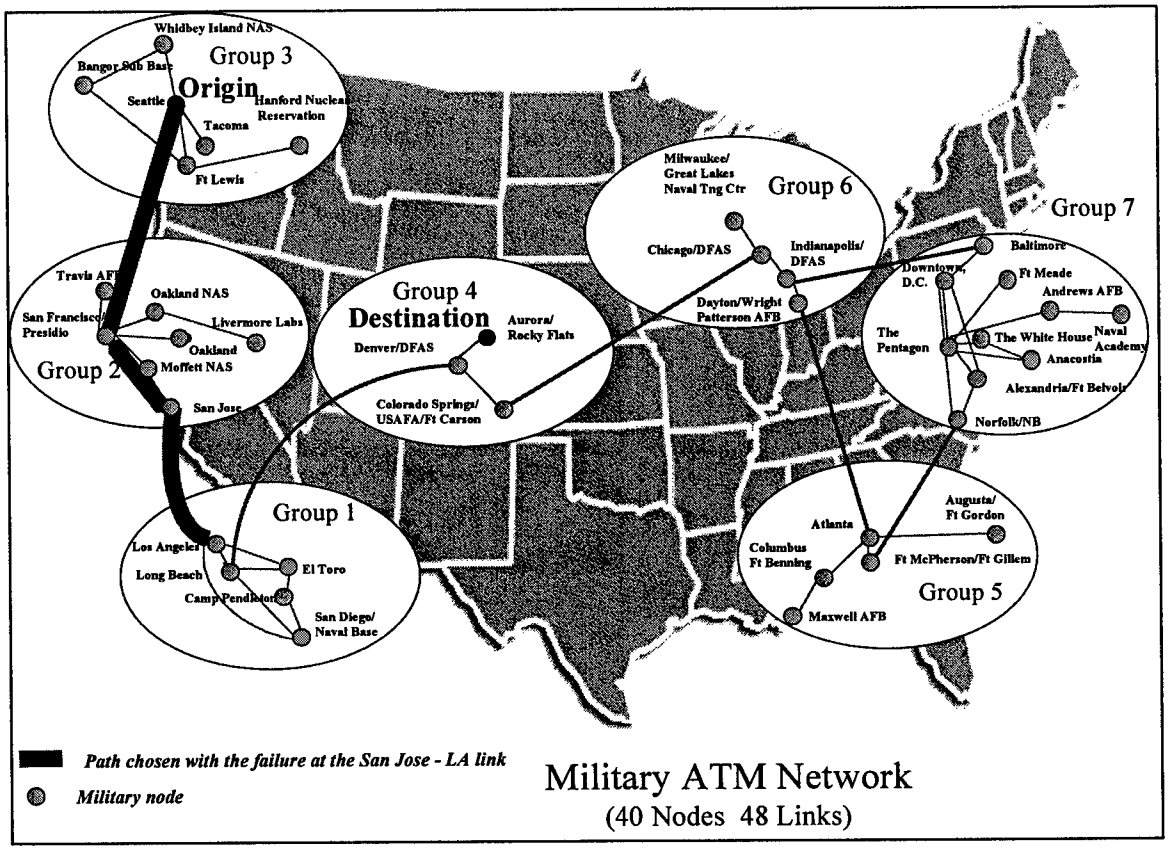



Figure 48. Route selection between Seattle and Rocky Flats.

If the call were successful, the number of hops to the final destination would have been six and followed a path through LA, Long Beach, Denver and finally, Rocky Flats.

Analysis of the data for the same call in the 50 node, mixed use network simulation showed the call is successful and followed a path, shown in figure 49, from Seattle through Redmond, Boulder and Denver to Rocky Flats for a total of 4 hops.

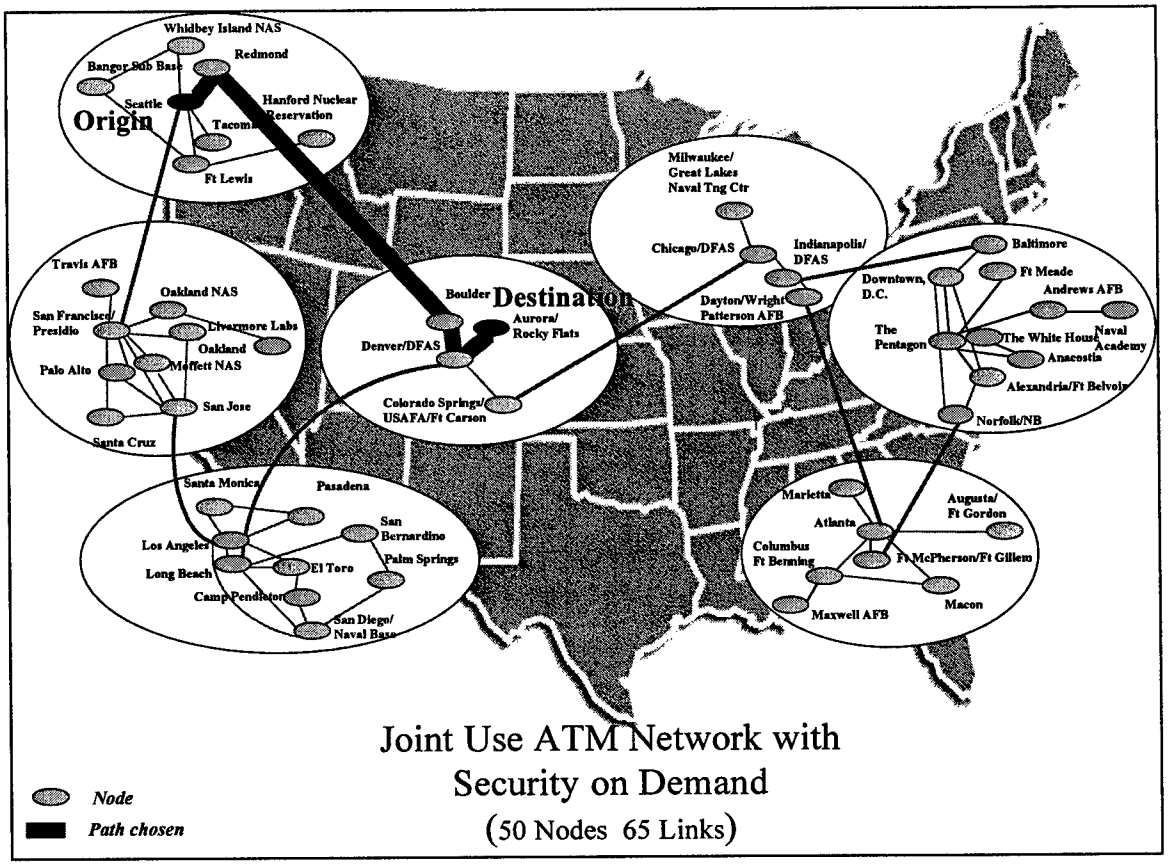



Figure 49. Route selected between Seattle and Rocky Flats.

The longer average call setup time is also due to a higher hop count for the routes chosen for the call setup message, in the 40 node network where the hop count is high and corresponding hop success rate low compared to the 32 node network where the hop count is low and success rate is high. The 32 node network has a total node hop count of 6044, 3485 successful calls and a success rate of 58% compared to the 40 node network which has a hop count of 10443, 4329 successful calls and a success rate of 41% and the 50 node network which has a hop count of 15585, 7948 successful calls and a success rate of 51%.

In summary, there appears to be an averaging of the two 32 and 40 node network's performance when they are combined into one, 50 node network. While the 40 node network has a larger total number of nodes used in routing and a low call success rate, the 32 node network has a lower total number of nodes used in the routes and a higher call success rate resulting in a lower average call setup time for the overall network, as well as across each node. The benefit of integrating the security on demand system into the operation of an ATM network is that it enables users from any group to use the network and maintain their security requirements. In the case of the military network, there is the additional benefit of improved call success rate across the majority of nodes under the same input traffic loads. This ability to combine previously isolated, secure networks with the public ATM infrastructure is significant due to the performance gains in call success rates. A more efficient use of the security resources is achieved by allowing the calls which do not require security to be routed on links which do not have security resources thereby freeing up the links with security resources for processing of calls which require security.

### Understanding the Limits of the Performance Impact of Security on Demand: Fast Dissemination of the State of the Network (Near PGOD)

An additional series of behavior studies are conducted which increases the flooding rate in order to gauge the effect on performance. Information is propagated by every node to every other node in the network through flooding. When flooding, which is first discussed in Chapter 4's section on the NSI and restated here, each node

propagates its knowledge of network topology information to its immediate nodes and so on. At each flooding interval, this action takes place until ultimately, all nodes within the network are aware of every other node and their topology information. Although all connected nodes will eventually receive new information on other nodes in the network, the exact times at which the nodes receive the information will differ. This time interval between the receipt of information at a node and the propagation from the original node is referred to as data latency. It causes uncertainty and is one potential cause of a call setup message to fail. Of course, the further away a node is located from the original node, the later it will receive the node's topology information which causes a loss of accuracy in the sense of timeliness.

Flooding can also overload a network if it occurs too frequently. In a network which has no physical propagation delay on network links and call processing takes zero time, flooding of network topology information would take zero time, eliminating data latency and allowing the choice of a call setup message route to be based on the most current network information. Lee describes using these ideas to determine the absolute performance of a network and calls the technique the Perfect Global Optimization Device (PGOD) (1996). While PGOD is a technique used to determine the absolute performance of a network, the author chooses a more pragmatic approach of reducing the data latency effects on a network's performance. While eliminating the physical propagation delay and switch processing times is not possible in an actual network, increasing the frequency of the flooding of network topology information is possible. Improving the timeliness of

topology data at the nodes will theoretically improve performance by improving the timeliness of the data used to determine the route for the call setup message and increasing the chances of a successful call setup if a path satisfying the user requirements exists. The author refers to this pragmatic approach as near PGOD or N-PGOD. A set of simulations with flood rates of every 5000 and 25,000 timesteps show the effects of reducing data latency. The same nine node network used in the stability study and shown in chapter 6's figure 17, is chosen for the N-PGOD study to mitigate the increase in the simulation execution time resulting from the increased flooding. Analysis of the results show a 5% improvement in the overall call success rate across all 9 nodes equivalent to a total of 55 additional successful calls. The average call success rates across each node are shown in figure 50.

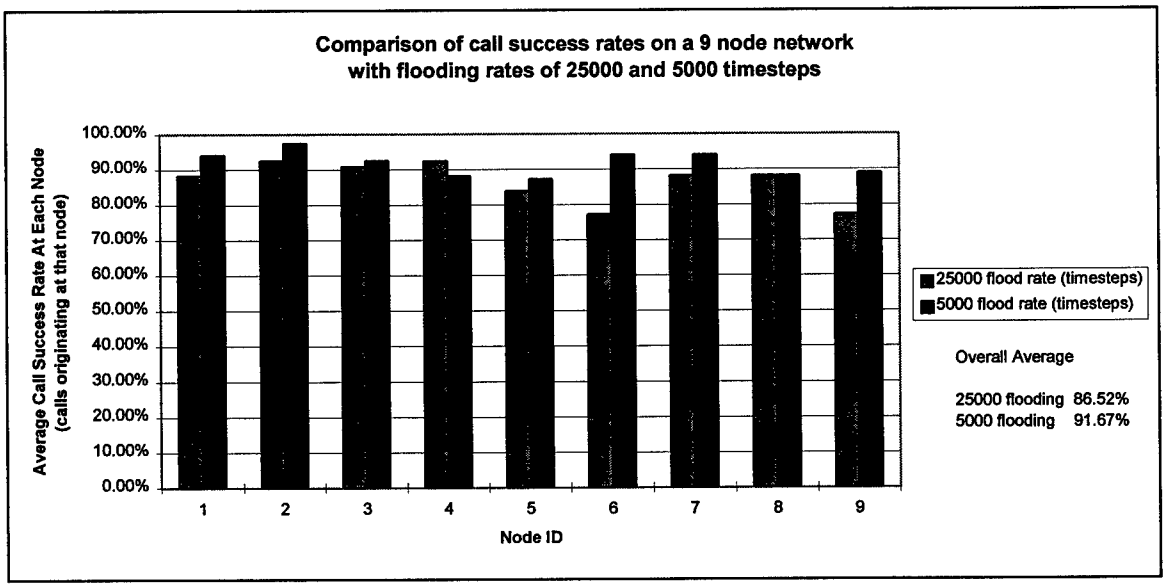



Figure 50. Comparison of the average call success rates at each node between studies using a flood rate of 25000 and 5000 timesteps.

The overall average call setup time, shown in figure 51, increased slightly using more frequent flooding to an average of 3466.38 timesteps per call from an average of 3252.86 per call when flooding occurs every 25000 timesteps. The increase in call setup time is due to the higher average number of hops per call. Using an approach where topology information is flooded every 5000 timesteps, the overall average number of hops per call is 1.86 while the average for flooding every 25000 timesteps is 1.71 hops. The higher average translates into a higher call setup time per call. Since a higher hop rate means a greater number of nodes, on average, are required to process a call. The average call setup time across each node is shown in figure 51.

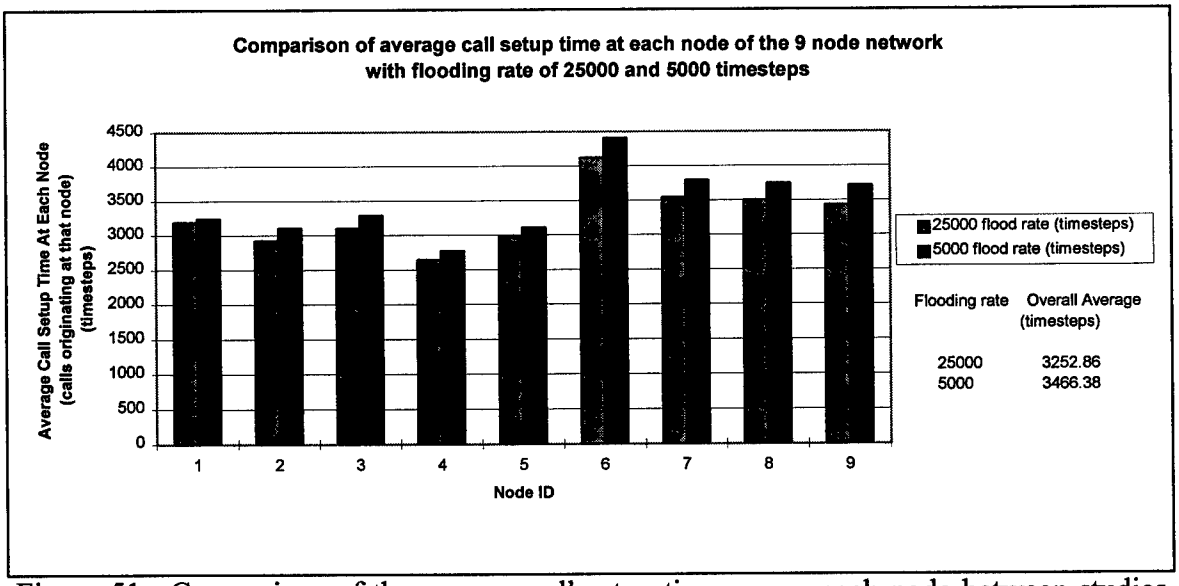



Figure 51. Comparison of the average call setup time across each node between studies using a flood rate of 25000 and 5000 timesteps.

The results show that even in the highly stressed, 9 node network, it is possible to improve the average call success rates by providing more up to date information on network topology used in the call setup process. The drawback is a increase in the average call setup time per call.

These results show what the analysis of the results of the baseline, security on demand and NSI models also show and that is while refinements to the call setup process can improve one measure of the performance of a network, they can also cause a decrease in other measures of performance. The benefit of flooding topology information more frequently in hopes of achieving perfect call success rates is accomplished at the cost of an increase in signaling bandwidth and a higher call setup time.

# CHAPTER 8

# CONCLUSIONS

The scientific validation of the integration of the user level security on demand system into the operation of an ATM network is significant as it makes possible a paradigm shift in the way security is integrated into a network, enabling distributed security resource allocation. For the first time, integration of previously isolated networks into one, mixed use network is possible through a security on demand system available at the user level. Military users would realize increased call success rates resulting from a richer network topology, as well as an increase in the number of possible paths for traffic not requiring security. Civilian users would benefit from the addition of security resources and the ability to request those resources for transmission of their sensitive data.

The analysis of the data from the modeling and implementation in an ATM network simulator of the three different approaches reveals the following. A security on demand system can be integrated into the operation of an ATM network resulting in little degradation in performance as measured by call success rate and average call setup time at each node and over all nodes. Topology influences the performance comparison of the approaches: baseline, security on demand and NSI function. A rich topology with multiple paths between a source and destination favors the security on demand approach. A goal of reducing average and overall call setup time also favors the security on demand

approach in highly stressed networks with constant traffic. A goal of "spreading" the successful calls across many links favors the NSI function approach.

The results of the series of behavioral studies show the military could benefit by a switch to the security on demand system by combining its isolated classified networks with the public, civilian infrastructure, creating a "mixed use" network, resulting in improved performance and optimal use of security resources.

The user level, security on demand system changes the security paradigm from a static, compliance based view to a dynamic risk management approach. Instead of the security resources being locked in at a certain level for all users, at all times, the security on demand system enables security resources to be requested at the user level allowing optimal resource allocation. The security framework used by the security on demand system provides a structured methodology which is comprehensive, dynamically updated and uniform for all networks.

A lack of a comprehensive network security framework with user level designation of required security prevents the connection of classified, military networks to the public infrastructure which degrades performance and does not make optimal use of security resources. Current and planned high speed networks such as the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII) mandate a comprehensive view of all aspects of network security, a method for satisfying a request for some or all of the user requested security elements and an implementation which has minimal performance impact while making optimal use of all security

resources. The user level, security on demand system modeled and scientifically validated, satisfies these requirements.

The security on demand system performance can be improved to accommodate the different user group service priorities through the use of an NSI function. The NSI function reflects one or more network topology factors. The use of an NSI function does not always guarantee improved performance, but does modify the routing of calls which under certain conditions is desirable. In highly stressed networks, simple routing functions based on the shortest number of hops are observed to produce better performance.

Another method to improve call success rates is to flood topology information more frequently. However, excessive flooding may cripple the network bandwidth and overload the node. Therefore, a careful analysis of the network behavior including the frequency of call setup requests, average session duration, density of nodes and links, and the percentage of resource utilization, is important to manage flooding. Increased flooding does improve call success rates and average call setup time, but at the cost of increasing signaling bandwidth.

This dissertation presents the integration of the fundamental framework for network security into the operation of an ATM network to produce a security on demand system available down to the user level. The unique set of principles, inherent in the framework, enable the realization of the dynamic risk assessment approach across the different types of networks and for any type of user -- civilian, military, or government.

The security on demand system enables mixed use, ATM networks which fulfill each class of user's security requirements drawing from the network security framework developed by the author. In combination with the fundamental unique characteristics of ATM networks namely, the call setup process, the framework also offers "security on demand" down to the user level which is a new paradigm in network security. The proposed approach to the user level, security on demand system views security as a distributed network resource and allocates it to each user call based upon demand and dictated by the need making it consistent with the basic characteristics of and fundamentally the most logical approach to security in ATM networks.

## Future Work

### Menu of NSI Functions

One method of further refining the performance of the security on demand system would be to offer a menu of NSI functions tailored to the specific user groups and their preference priorities. The result would be a more focused predictor of a successful route for a particular class of users. The user would have the choice of specifying which function would be used to calculate a proposed route for the call setup message depending on the user's priorities.

### Integration of the User Level Security on Demand Approach into an ATM Switch

The next logical step in the development of the user level, security on demand system is to integrate the code developed for the ATM simulator into an actual ATM switch. The author has been in discussions with various ATM switch manufacturers who have expressed an interest in the security on demand system, which could lead to a joint project for the implementation of the security on demand system in a commercial ATM switch.

### Use of ATM Simulator to Design and Study the Behavior of the DII and NII

Another logical extension of this research would be to use the ATM network simulator with the security on demand to design and study the behavior of the worldwide Defense Information Infrastructure (DII) and National Information Infrastructure (NII) ATM networks. Such networks are being formed by the DoD and federal government and these efforts would greatly benefit from a behavioral study drawing from planned locations of ATM switches and the addition of a user level security on demand system. The author has been requested to brief the Army Science Board on the research described in this dissertation which may further this goal.

# REFERENCES


ATM Forum Technical Committee. 1996. *Private Network-Network Interface Specification Version 1.0 (PNNI 1.0)*, Internet version af-pnni-0055.000, available on-line: www.atmforum.com/atmforum/specs/approved.html (March).

Abrams, M. D., and M. V. Joyce. 1995. Trusted system concepts. *Computers and Security* 14, no. 1:45-56.

*The American Heritage Desk Dictionary*. 1981. Boston: Houghton Mifflin.

AT&T. 1998. *AT&T WorldNet Managed Internet Service Internet site*: www.att.com/worldnet/wmis/misb.html (April).

Backhouse, J., and G. Dhillon. 1995. Managing computer crime: A research outlook. *Computers and Security* 14, no. 7:645-651.

Baggett, C. C. 1996. Keynote address from National Security Agency at the Network Rating Model, first public workshop (March 20-22), Williamsburg, VA.

Billington, R., and E. Khan. 1992. A security based approach to composite power system reliability evaluation. *IEEE Transactions on Power Systems* 7, no. 1 (February):65-71.

Chaffee, C. D. 1988. *The Rewiring of America The Fiber Optics Revolution*. New York: Academic Press.

Chambers, T. 1995. Case study: A managerial perspective on an Internet security incident. *Computer Security Journal* XI, no. 1:17-23.

Chuang, S-C. 1995. A flexible and secure multicast architecture for ATM networks. *IEEE Globecom '95* (November 14-16) Singapore:701-707.

Cohen, G. N. 1995. ATM payload encryption and security-on-demand. In *Proceedings of SPIE—the International Society for Optical Engineering*:2615 (Oct) 292-299.

Computer Sciences Corporation. 1994. UCA and DIAS information security analysis. EPRI Technical Report TR-103773. Palo Alto, CA.:Electric Power Research Institute (Aug).

Conover, J. 1997. ATM backbone switches: how strong is your backbone? We scrutinize 5 switches. *Network Computing* 8, no. 21 (November 15):78-89.

Cylink. 1996. Cylink and GTE announce first successful demonstration of secure video teleconferencing! Infoguard 100 proves commercial viability of secure ATM networks. *Business Wire*. Internet; accessed on PointCast 21 June 1996.

Deng, R. H., L. Gong, and A. A. Lazar. 1995. Securing data transfer in Asynchronous Transfer Mode networks. *IEEE Globecom '95* (Nov 14-16) Singapore:1198-1202.

Department of Defense. 1985. *Department of Defense trusted computer system evaluation criteria*, 5200.28-STD. Washington, DC:GPO.

Department of Defense. 1987. *Trusted network interpretation of the trusted computer system evaluation criteria*, NCSC-TG 005. National Computer Security Center, Ft. George Mead, Maryland, ISBN 306-A-19, (July 31):GPO.

Department of Defense. 1990. *Trusted network interpretation environments guideline*, NCSC-TG 011 version-1. National Computer Security Center, Ft. George Mead, Maryland, ISBN S-235, 465, (August 1):GPO.

Dijkstra, E.W. 1959. A Note on Two Problems in Connection with Graphs. *Numerische Mathematik* 1:269-271.

Dorsen, N. and S. Gillers eds. 1973. *Government Secrecy in America: None of Your Business*. New York: Viking Press.

Edfors, P. Speech on 21 March 1996. Network Rating Model conference, Williamsburg, VA.

Ferguson, P. and G. Huston. 1998. *Quality of Service.* New York: Wiley.

Fernandez, I. B., and W.V. Subbarao. 1994. Encryption based security for ISDN Communication: Technique and Application. *IEEE SOUTHEASTCON '94*:70-73.

Fitzpatrick, S. K., and P.J. Hargaden. 1994. Multimedia communications in a tactical environment. In *Proceedings of the IEEE MILCOM* 1:242-246.

Geer, D. E. 1995. Electronic commerce, banking and you. *Computer Security Journal* XI, no. 2:55-62.

Guidoux, L. 1995. Intelligent solutions for data communications networks. *Telecommunications* 29, no. 6 (June 6):25-29.

Helman, P., and G. Liepins. 1993. Statistical foundations of audit trail analysis for the detection of computer misuse. *IEEE Transactions on Software Engineering* 19, no. 9 (September):886-901.

Hill, S., and M. Smith. 1995. Risk management and corporate security. *Computers and Security* 14, no. 3:199-204.

Hitchings, J. 1995. Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers and Security* 14, no. 5:377-383.

Horton, F. and D. Marchand, eds. 1982. *Information Management in Public Administration.* Arlington, VA: Information Resources Press.

Hosmer, H. H. 1995. Security is fuzzy! Applying fuzzy logic to the multipolicy paradigm. *Computer Security Journal* XI, no. 2:35-45.

Janson, P., and R. Molva. 1991. Security in open networks and distributed systems. *Computer Networks and ISDN Systems* 22:323-346.

Klein, S. A., and J.N. Menendez. 1993. Information security considerations in open systems architecture. *IEEE Transactions on Power Systems* 8, no. 1 (February):224-229.

Kumar, S., and E. H. Spafford. 1994. An application of pattern matching model in intrusion detection. Technical report 94-013, Department of Computer Sciences, Purdue University (March).

Lee, T., and S. Ghosh. 1994. A distributed approach to real-time payment-processing in a partially-connected network of banks: modeling and simulation. *Simulation - The Journal of the Society for Computer Simulation* 62, no. 3 (March):180-201.

Lee, T. 1996. On the concept of "Stability" in asynchronous, distributed, decision-making systems. Ph.D. diss., Brown University.

Lin, P., and L. Lin. 1996. Security in enterprise networking: A quick tour. *IEEE Communications Magazine* (January):56-61.

Lunt, T. F., and R. Jagannathan. 1988. A prototype real-time intrusion-detection expert system. In *Proceedings of the 1988 IEEE Computer Society Symposium on Security and Privacy* (Apr 18-21):59-66.

Lunt, T. F. 1993. A survey of intrusion detection techniques. *Computers and Security* 12, no. 4:405-418.

Madron, T. W. 1992. *Network security in the '90s - Issues and solutions for managers.* New York: John Wiley and Sons.

Mitchell, B. and T. Donyo. 1994. Utilization of the U.S. Telephone Network. Rand Corporation Study in cooperation with the European-American Center for Policy Analysis(HE8815.M58).

National Security Agency. 1996. Network Rating Model (NRM): Strawman, 20-22 March 1996.

Nessett, D. M. 1989. Layering central authentication on existing distributed system terminal services. In *Proceedings of the IEEE 1989 Computer Society Symposium on Security and Privacy* held in Oakland, CA. 1-3 May1989:290-299.

Oliver, C. 1995. Privacy, anonymity, and accountability. *Computers and Security* 14:489-490.

Peyravian, M., and T. D. Tarman. 1997. Asynchronous Transfer Mode security. *IEEE Network* 11, no. 3 (May/June):34-40.

Power, R. 1995. CSI special report on information warfare. *Computer Security Journal* XI, no. 2:63-73.

Pecas Lopes, J. A., F. P. Maciel Barbosa, J. P. Marques de Sa, and J. M. G. Sa da Costa. 1987. A new approach for transient security assessment and enhancement by pattern recognition. In *Proceedings of the Second European Workshop on Fault Diagnostics, Reliability, and Related Knowledge Based Approaches* (April 6-8) Pergamon Press:189-215.

*Report by the President's commission on critical infrastructure protection, critical foundations.* 1997. By R. Marsh, chairman. Washington, D. C. (October):GPO.

Sato, K., S. Ohta, and I. Tokizawa. 1990. Broad-Band ATM Network Architecture Based on Virtual Paths. *IEEE Transactions on Communications* 38, no. 8 (August): 1212-1222.

Schumacher, H. J., and S. Ghosh. 1997a. A fundamental framework for network security. Feature presentation and In *Proceedings of the 9th Annual Canadian Information Technology Security Symposium* held in Ottawa, Canada 12-16 May 1997:45-63.

Schumacher, H. J., and S. Ghosh. 1997b. A fundamental framework for network security. *Journal of Network and Computer Applications* 20, no. 3 (July): 305-322.

Schumacher, H. J., and S. Ghosh. 1998a. An integrated approach to security on demand in ATM networks. *Information Systems Security* 6, no. 4 (winter):10-21.

Schumacher, H. J., and S. Ghosh. 1998b. A fundamental framework for network security towards enabling security on demand in an ATM network. *Computers and Security* 17, no. 6:527-542.

Schumacher, H. J., and S. Ghosh. 1999. Top Secret Traffic and the Public ATM Network Infrastructure. *Information Systems Security* 7, no. 4:27-45.

Schwartau, W. 1996. *Information warfare*. New York: Thunder's Mouth Press.

Simonds, F. 1996. *Network security: Data and voice communications*. New York: McGraw-Hill.

Soh, B. C., and T. S. Dillon. 1995. Setting optimal intrusion-detection thresholds. *Computers and Security* 14, no. 7:621-631.

Spanos, G. A., and T. B. Maples. 1996. Security for real time MPEG compressed video in distributed multimedia applications. *IEEE 15th Annual International Phoenix Conference on Computers and Communications* held in Scottsdale, AZ 27-29 March 1996:72-78.

Stevenson, D., N. Hillery, and G. Byrd. 1995. Secure communications in ATM networks. *Communications of the ACM* 38, no. 2 (February):45-52.

Tenenbaum, J. M., C. Medich, A. M. Schiffman, and W. T. Wong. 1995. CommerceNet: Spontaneous electronic commerce on the Internet. In *Proceedings of the IEEE Computer Society International Conference '95 (COMPCON 95):*38-43.

Vaccaro, R. S., and G. E. Liepins. 1989. Detection of ANOMALOUS computer session activity. In *Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy* (May 1-3):280-289.

*Webster's Third New International Dictionary of the English Language*. 1993. Springfield, MA: G. & C. Merriam.

Weerasooriya, S., M.A. El-Sharkawi, M. Damborg, and R.J. Marks II. 1992. Towards static-security assessment of a large-scale power system using neural networks. In *IEE Proceedings, Part C, Generation, Transmission, and Distribution,* 139, no. 1 (January):64-70.

White, G., E. Fisch, and U. Pooch. 1997. Government-based security standards. *Information Systems Security* (Fall):9-19.

Wilcox, C. A. 1996. ATDNet research at the National Security Agency. *IEEE Network* (July/August):42-47.

Winkler, I. 1997. *Corporate espionage*. Rocklin, CA: Prima Publishing.

Wolfe, H. B. 1995. Computer security: For fun and profit. *Computers and Security* 14, no. 2:113-115.