AD-A254 112 [REPORT DOCUMENT]ATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE Jun 92

3. REPORT TYPE AND DATES COVERED Final, Masters Thesis

4. TITLE AND SUBTITLE The Application of Artificial Intelligence to the management of the Army's Mobile Subscriber Equipment Communications ~~Network~~ Network

5. FUNDING NUMBERS

6. AUTHOR(S) CPT Charles E. Lane

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Colorado, Boulder
Boulder, Colorado

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT Public

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

See attached Page

14. SUBJECT TERMS Network Management, Mobile Subscriber Equipment, Artificial Intelligence

15. NUMBER OF PAGES 200

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclas	Unclas	Unclas	UL

DTIC THESIS ABSTRACT

The U.S. Army's tactical area communications system for the next 15-20 years will be the Mobile Subscriber Equipment (MSE) system. The Army expects MSE networks to carry the bulk of the voice and data communications between tactical command posts. The men and women who manage the MSE system need better network management tools than they currently have. Unfortunately, the Army faces an era of reduced budgets and cannot afford expensive solutions to its network management problems.

This thesis explores the potential to use Artificial Intelligence (AI) techniques in network management tools. It begins with descriptions of MSE and AI. The thesis analyzes the MSE network management problem and the potential for the development of AI-based tools. It concludes that commercial network management tools could not be directly applied to MSE but they do provide a framework to design MSE network management tools.

The thesis concludes with a recommendation for an objective network management architecture. This architecture incorporates solutions to the major network management problems. The Army could use this architecture to provide direction to its major vendors and a baseline to evaluate vendor proposals against.

The Application of Artificial Intelligence to the Management of the Army's Mobile Subscriber Equipment Communications System

by

Charles Edward Lane, Jr.

B.S. United States Military Academy, West Point, NY,

A thesis submitted to the Faculty of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

School of Business Administration

1992

This thesis for the Master of Science degree by

Charles Edward Lane, Jr.

has been approved for the

Department of

Information Systems

by

Kenneth A. Kozar

David A. Carlson

John S. Thompson

Date 6-25-92

Lane, Charles E. (M.S., Business Administration)

The Application of Artificial Intelligence to the Management of the Army's Mobile Subscriber Equipment (MSE) Communications System

Thesis directed by Professor Kenneth A. Kozar

The U.S. Army's tactical area communications system for the next 15-20 years will be the Mobile Subscriber Equipment (MSE) system. The Army expects MSE networks to carry the bulk of the voice and data communications between tactical command posts. The men and women who manage the MSE system need better network management tools than they currently have. Unfortunately, the Army faces an era of reduced budgets and cannot afford expensive solutions to its network management problems.

This thesis explores the potential to use Artificial Intelligence (AI) techniques in network management tools. It begins with descriptions of MSE and AI. The thesis analyzes the MSE network management problem and the potential for the development of AI-based tools. It concludes that commercial network management tools could not be directly applied to MSE but they do provide a framework to design MSE network management tools.

The thesis concludes with a recommendation for an objective network management architecture. This architecture incorporates solutions to the major network management problems. The Army could use this architecture to provide direction to its major vendors and a baseline to evaluate vendor proposals against.

CONTENTS

CHAPTER I

Thesis Introduction 1

Introduction 1

Problem Statement 4

Purpose of this Thesis 4

Methodology 5

Sources of Information 6

Prospective Audience 6

Thesis Organization 7

Disclaimers 8

CHAPTER II

The MSE Network Management Domain 9

Introduction 9

Improvements MSE Offers the Army 10

Technical Overview of the MSE System 13

The MSE Node Center 16

The Node Center Switch 17

The Node Management Facility 22

The Radio Access Unit and Mobile Subscriber Radio Terminal 24

The Small Extension Node 26

The Large Extension Node 30

The System Control Center 31

The Limitations of the SCC 36

Conclusion 37

CHAPTER III

Fundamental Concepts of Artificial Intelligence 38

Introduction 39

A Definition of Artificial Intelligence 39

The Turing Test 40

AI Programming vs Ordinary Procedural Computer Programming 41

Expert Systems 44

Advantages of Using Expert Systems 44

Characteristics of Human Experts 45

Types of Expert Systems 46

Components of Expert Systems 48

Knowledge Representation 51

Knowledge Representation Schemes 53

Dealing with Uncertainty 53

State Space Search 56

Forward vs Backward Reasoning 61

Neural Networks 62

Expert System Development 65

Criticisms of Artificial Intelligence 69

Conclusion 71

CHAPTER IV

An Analysis of MSE Network Management 72

Introduction 72

Commercial Integrated Network Management 73

Commercial Network Management System Architectures 77

Why Commercial and Military Network Management is so Different . . 83

MSE Network Management 86

MSE Network Planning 91

MSE Network Engineering 96

MSE Network Control 98

Deficiencies in the Present Network Management Process 101

MSE Node Center Management 102

Conclusion 106

CHAPTER V

The Potential for AI based Tools to Improve

MSE Network Management 108

Introduction 108

Research Methodology 109

Trends in Commercial Network Management Tools 111

Current Trends in MSE Network Management Tools 113

Commercial AI-Based Network Management Tools 116

Current Research in AI-based MSE Management Tools 120

Analysis of the Potential for AI Tools to Improve

MSE Network Management 127

MSE Network Planning and Engineering 127

What degree to automate MSE network planning? 128

MSE planning tool requirements 131

Plan evaluation 135

MSE Network Control 137

MSE network control tool requirements 138

MSE Node Center Management 145

Justifying the Development of AI-Based Tools 148

Obstacles to Developing AI-Based Tools for

MSE Network Management 149

Conclusion 152

CHAPTER VI

An Objective MSE Network Management Architecture 154

Introduction 154

Key Points of the Objective Network Management Architecture 155

Overview of the Proposed Architecture 156

Redesigning the SCC-2 158

Development of a Means to Gather Automatic Telemetry 165

Node Center Management System 167

Summary of the Proposed MSE Network Management Architectur . . . 170

Where is the AI? 171

Knowledge Acquisition 171

Issues with the Acceptance of AI-Based Tools 173

Conclusions 175

Recommendations for Further Research 176

BIBLIOGRAPHY 178

APPENDIX A 182

APPENDIX B 192

CHAPTER I

Thesis Introduction

Introduction

Every military operation depends on effective and reliable communications. Commanders control tank maneuver, spotters call in artillery, and sensors track enemy aircraft for air defense artillery missile batteries using modern digital telecommunications networks. Staff officers require reliable communications to plan the maneuver of combat units and the logistics to feed, fuel, and re-arm the units. No modern army can fight without an effective electronic telecommunications network.

Much of the Army's success in the Persian Gulf war of 1990-1991 was due to modern, reliable, and extensive communications networks. The Army used digital networks to help plan and coordinate battlefield operations, plan logistical support, and to coordinate with the other allied nations. The Army could not have achieved the total victory in the Persian Gulf without a reliable and secure communications system.

The officers and non-commissioned officers who manage the Army's tactical telecommunications networks have a difficult mission. Their signal units must always prepare to deploy, install, operate, and maintain communications networks anywhere in the world. The network managers must be able to quickly reconfigure the communications networks to support fast moving combat units. The networks must survive attacks and even continue to function while under attack. Today's networks also have many capabilities and user features that complicate the communications systems management.

The typical Army network manager is not an expert in telecommunications network management. The Signal Corps experiences a high turnover of network managers whose career paths require them to change jobs every three years. A typical network manager serves in a variety of staff and command positions during a military career. Few of these positions are in network management.

The network managers' mission is very important. The Army's communications worked well in the gulf war but the Army's future communications networks will be expected to do more. The Army plans to augment its current command and control process with the Army Tactical Command & Control System (ATCCS). The ATCCS will place a greater burden on the communications network managers.

The ATCCS is a distributed computer architecture that will coordinate combat unit maneuvers, assess the enemy disposition, plan artillery and airborne fire support, control the air defense system, and coordinate the logistical support. The ATCCS will depend on a network of three diverse communications systems. A data distribution system will relay medium data traffic between sensors and computers. A combat net radio network will provide voice communications at all command levels from the infantry squad to the division. The area common user telephone network provides voice and data links between brigade and higher level unit headquarters. This area common user system is called Mobile Subscriber

Equipment (MSE). This thesis will focus on the management of MSE networks.

The US Army Signal Corps, the Army's branch responsible for communications, is undergoing a downsizing similar to many businesses. Besides the Infantry, the Signal Corps has the largest number of soldiers in the Army. The Signal Corps of the future will have only half of the number of soldiers it has now but it will have even more missions than it has today.

These conditions help make the MSE network managers prime candidates for AI-based support tools. Their mission is difficult and critical and they work under harsh conditions. AI-based tools can help network managers plan, engineer, and control the MSE networks faster and better than they do now.

AI-based tools have the potential to help the Army better manage its tactical telecommunications networks. Expert systems, a subset of artificial intelligence, can apply knowledge gained from the experiences of network managers stationed around the world to network management. Expert systems can help insure a minimum level of technical competence to all signal units. AI systems have the potential to help managers plan the best telecommunications service with the most efficient use of resources. They could help network managers spot network problems and recommend solutions. Expert systems also can be imbedded in training aids to reduce the time it takes to train network managers.

Problem Statement

The current MSE network management system has problems. The MSE system has worked well so far in spite of its network management problems. The Army is currently looking for new tools to help solve its network management problems.[1]

The major problems with the current MSE network management system are:

- The current system relies exclusively on human-based information input.
- The Army's current strategy to improve network management may not provide the future network managers with the best tools to do their jobs.
- The Army is failing to take advantage of current AI developments in the commercial sector that could be adapted to MSE network management.
- The Army does not know which management processes need to be automated because it has not conducted a detailed analysis of how network managers operate.

The Army will need to address these problems if MSE is to support its future roles in the Army Tactical Command and Control System.

Purpose of this Thesis

The purpose of this thesis is to analyze how artificial intelligence can be applied to the management of MSE networks to improve network managers' performance. The thesis will analyze the current processes MSE network managers use to plan, engineer, and control MSE networks. It also will include an analysis of the current trends in the use of AI in commercial network management

---

[1]Jack Robertson, "Army Readies Range of Bids for Battlefield Com Equipment." Communications, October 7, 1991, p. 31.

systems to see how the Army can adapt AI techniques to network management.

An analysis of any new MSE network management system must include the reality of today's diminishing budget resources. The Army's future includes significant reductions in fiscal budgets and personnel. The Army will have little money to spend on network management improvements. Any proposed improvements to the management architecture will have to prove feasible and justifiable

Methodology

This thesis will propose a specific network management architecture that would take advantage of AI techniques to improve the network management process. The thesis will first have to introduce the MSE system and the processes that network managers use to manage the system. The reader will need a detailed description of the MSE system to understand MSE's capabilities and shortcomings. Otherwise, the discussion of the network management process will make little sense to the reader.

The thesis also will survey current trends in new MSE and commercial management tools. It will analyze why the planned improvements to MSE network management do not go far enough to solve the current problems.

Finally, the thesis will propose a network management architecture that would meet the Army's current and near term needs in MSE network management. The proposed network management architecture will include some sub-optimal solutions due to the realities of the Army's diminishing resources.

Sources of Information

This thesis will draw on current literature in applied artificial intelligence, tactical command and control, and telecommunications network management. It uses interviews of several project officers in the US Army and commercial organizations to determine the trends in MSE network management improvements. It also uses surveys and interviews with officers and Non-Commissioned Officers (NCOs) who have served as MSE network managers in peacetime and in war. Their experiences improve the analysis of MSE network management and help determine which aspects of MSE network management need improvement. They have used MSE in most possible situations. Their insights are invaluable in determining the aspects of MSE network management that work well and those that need improvement.

The thesis uses the author's personal experiences in the analysis of MSE network management. The author has extensive experiences with MSE which include spending four months in France studying the French Army's version of MSE, one year helping to develop the initial network management doctrine, and two years commanding an MSE equipped signal unit.

Prospective Audience

The thesis is written for several audiences who have differing levels of expertise with MSE, network management, and artificial intelligence. The primary audience is the thesis committee members who are knowledgeable in artificial intelligence and network management but not MSE. The thesis is also intended for other audiences who are knowledgeable in MSE and tactical network management but have little expertise with artificial intelligence. These other audiences include:

- Office of TRADOC Systems Manager (TSM) - MSE at Ft Gordon GA
- Office of Project Manager (PM) - MSE at Ft Monmouth, NJ
- GTE Government Systems Corp, Taughton, MA
- MITRE Corp, Eatontown, NJ
- Any other organization involved with the Army's MSE program

Thesis Organization

The thesis focuses on a specific problem domain, the Army's MSE telecommunications network, to determine how AI could best be used to improve network management. The diverse audience for the thesis requires that a significant portion of the thesis be devoted to the introduction of the MSE domain, the fundamentals of artificial intelligence, and basic concepts network management.

Chapter II details the network's architecture, capabilities, limitations, and management issues. It provides a level of knowledge about MSE and its problems needed for the network management analysis in chapters IV and V. Readers already familiar with MSE may wish to skim this chapter.

Chapter III discusses fundamentals of artificial intelligence and expert systems needed to analyze their potential use in MSE network management. It explains what artificial intelligence is and some of the techniques required to take advantage of it.

Chapter IV explains telecommunications network management and defines the unique problems faced by the Army's tactical telecommunications network managers.

Chapter V analyzes the potential for artificial intelligence based tools to aid network managers. It analyzes what obstacles today prevent the Army from developing AI-based network management tools.

Chapter VI concludes the thesis with a recommendation for an AI-based system development that could significantly aid the Signal Corps' network managers.

Disclaimers

The views and recommendations stated in this thesis are based on the author's personal research. They do not represent the policies of the US Army.

The use of the pronouns *he* or *his* do not represent a specific gender. The US Army Signal Corps consists of many outstanding male and female officers, non-commissioned officers, and soldiers.

CHAPTER II

The MSE Network Management Domain

Introduction

This chapter will introduce the basic terminology and concepts needed to understand the MSE network management domain. It will introduce the key equipment in the MSE system but not discuss the MSE equipment in detail. It also will discuss concepts network managers use in planning, engineering, and controlling MSE networks.

MSE is a secure digital area communications network used in the US Army's corps and division areas of operation. It replaces a mixture of outdated analog voice systems with a single digital voice and data system. MSE is a five billion dollar acquisition to modernize the Army's battlefield command and control systems.[1] GTE Government Systems Corporation of Needham, MA, is the prime contractor for the MSE system. Thompson CSF of France is the major subcontractor to GTE and is the sole source of some of the system's key components.

This chapter will divide the discussion of the key components of MSE into the following sections:

---

[1]Battlefield Automation: Army Tactical Command and Control System's Schedule and Cost, (United States General Accounting Office report number GAO/NSIAD-91-118BR, April 15, 1991), p. 19.

- Improvements MSE offers the Army
- Technical overview of the MSE system
- The MSE Node Center
    - The Node Center Switch (NCS)
    - The Node Management Facility (NMF)
- The Radio Access Unit (RAU) and the Mobile Subscriber Radio Terminal (MSRT)
- The Small Extension Node (SEN)
- The Large Extension Node (LEN)
- The System Control Center (SCC)
- The limitations of the SCC

Improvements MSE Offers the Army

MSE offers the Army several improvements over the previous generation communications systems. These include:

a. The extension of the area communications network closer to the lower level combat units. Previous communications systems extended only to the combat brigade level which is about ten kilometers from the forward units.

b. A completely digital system capable of transporting voice and data traffic throughout the entire area of operations. Every telephone and channel in the MSE network operates at 16 KB/s. Previous analog systems were poor carriers of digital traffic. The MSE network is also being upgraded to include an X.25 Packet Switched Network (PSN) in all the links. The packet switch network will provide data transport for new most data devices in the area of operations.

c. More and smaller signal nodes throughout the area of operation. Previous communications systems required large and heavily manned signal centers located close to the supported command posts. These large signal centers were lucrative targets for the enemy. The MSE system breaks up these signal centers into small and dispersed nodes. The typical corps area backbone network has evolved from four large signal nodes before MSE to twenty-two small node centers with MSE.

d. Same signal unit organizations in the division and corps operating areas. The older communications networks had different communications equipment in the rearward corps area and the forward division areas. MSE replaces both types of organizations. The Signal Corps now has same signal unit organizations in the division and corp operations areas. Corps level signal units once had to place terminating equipment teams in the division areas to extend communications to the divisions. The previous division and corps communications networks were separate networks that connected through gateways located in the division rear areas. With MSE, the division and corps networks are now a single network.

e. MSE extends the area communications network to key mobile users. Users in the previous networks entered the network only through wireline connections. MSE uses elementary cellular telephone technology to extend the network to mobile radio telephone users. Mobile users see few differences between the operation of wireline phones and mobile radio phones.

f. Army command posts have greater flexibility in selecting where to locate. The old communications networks required command posts to have radio *line of sight* to area communications nodes. MSE equipped signal units provide Small Extension Nodes (SENs) to command posts to link to the area backbone network. A SEN can displace its microwave radio terminal to a nearby hilltop and down link to the command posts with a Super High Frequency (SHF) radio link.

g. MSE is more secure than its predecessors. Every radio signal in the system is encrypted. MSE users have multiple levels of communications security available. Some users have telephones capable of providing encryption at the phone. The MSE switchboard operators are unable to listen in on these telephones. However, most wireline users in MSE have non-secure telephones. Calls on the non-secure phones are not encrypted between the telephone and the switchboard. Wireline users must locate within 1000 feet of the switch because of the length of wire each user has. There is little risk of anyone wiretapping non-secure telephones since the phones are close to the switches.

h. MSE provides network managers with easier customer management than previous systems. A customer's telephone number in the older communications networks was a function of the topology of the network and the customer's address on the switchboard. Network managers and switchboard operators had to manage customers down to the specific terminal addresses in the switchboards. With MSE, network managers merely pre-authorize users to enter the network. A customer only has to dial an entry code on the telephone to identify himself to the network. The network manager assigns a permanent telephone number to each customer which the customer keeps as he moves around the network.

i. MSE provides the network managers a few management tools. Each division signal battalion and corps signal brigade has a System Control Center (SCC) to help manage the network. The SCC can engineer radio links and monitor the network's status. It is also the prime focus of this thesis.

j. Finally, MSE provides greater flexibility in network configuration and location. All the major MSE communications system equipment are housed in standard army communications shelters mounted on M1037 Highly Mobile Multi-Wheeled Vehicles (HMMWVs). MSE equipment can be transported by Air Force cargo aircraft to almost any location worldwide. MSE nodes are usually linked by microwave radio systems. However, the MSE switching equipment is compatible with troposcatter and satellite radio equipment. Therefore MSE network managers can design MSE networks that use long haul transmission equipment to span continents and oceans.

Technical Overview of the MSE System

The MSE system can best be described as a layered system. It is an area common user system that spans most of the corps area of operation. A typical army corps has enough MSE equipment to provide communications coverage to 37,000 square kilometers of area. Signal units provide the area network and wire or mobile telephone entry points to the area network. The three primary layers of the MSE system are the backbone network, wireline access, and mobile subscriber access.

Network planners configure a backbone network by placing area signal nodes, called Node Centers (NCs), throughout the division and corps rear areas.

They plan line of sight microwave radio links between node centers to form a meshed network. Each node should have multiple links to adjacent nodes to provide multiple paths around the network. Multiple paths improve network survivability by providing alternate routing of calls. The distances between nodes are typically fifteen to twenty kilometers and vary due to terrain and mission requirements. Each node center consists of a digital switch, called a Node Center Switch (NCS), and Line of Sight (LOS) microwave radio links. The node center can establish twelve radio links to other node centers or extension nodes.

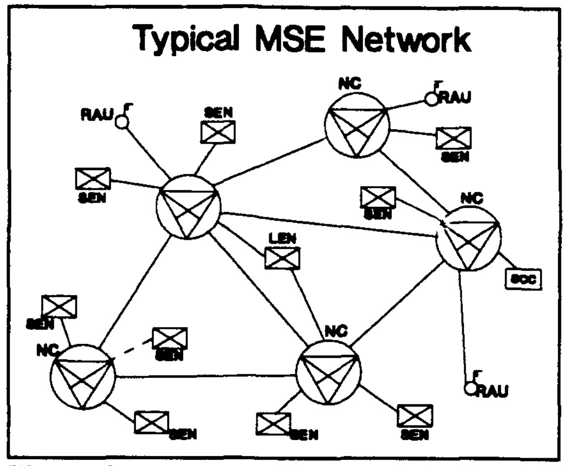

Figure 2-1

Most MSE customers are wireline users that access the network through extension nodes. The MSE system has two types of extension nodes. The first, Small Extension Nodes (SENs), are access points that the signal units place with unit command posts. SENs have a small digital switchboard capable of 26 or 41 users. These Small Extension Switches (SESs) link to the backbone network through microwave radio links to a nearby node center. The small extension switch also has a port to connect an IEEE 802.3 Ethernet Local Area Network (LAN) into the X.25 Packet Switched Network. The small extension switch's primary mission is to concentrate the 26 or 41 users to a 256 Kb/s (16 channel)

Digital Truck Group back to a node center. The SES also serves as a Private Branch Exchange (PBX) that can switch calls between local users.

MSE equipped signal units support heavy concentrations of wireline users with Large Extension Nodes (LENs). The switch at a LEN is a large digital switch closely related to the node center switch. The LEN performs the same mission as the small extension node switch, but on a larger scale. The Large Extension Node Switch (LENS) has a capacity of 176 wireline users. It also has a LAN port. The LEN connects to two nearby node centers with microwave radio systems. Because the large extension node switch is almost identical to the node center switch, it can be used as a smaller version of the node center switch. A LEN does not normally route backbone network calls between its two links, but it can be reconfigured to do so in an emergency.

Mobile users enter the MSE network through Radio Access Units (RAUs). A RAU can link up to eight mobile users to a node center switch simultaneously. Up to fifty mobile users can use a single RAU, but only eight can place calls at the same time. A RAU transmits a marker radio signal which the mobile user terminals use to keep contact with the network. A typical RAU has a range of fifteen kilometers. Network managers place RAUs to provide overlapping coverage of the area of operations with the RAUs. RAUs are located at both node centers and at remote sites. Remote RAUs link to nodes with microwave LOS radio systems while local RAUs connect to the node center switch directly with coaxial cable. The node center switch handles most of the mobile user telephone switching functions.

The MSE Node Center

The node center is the basic building block of the backbone network. The node centers interconnect to form a meshed grid across the corps rear area. Each link between node centers is set to 1024 KB/s, or 64 channels. Two of the channels are used for signalling and four are used for the X.25 packet network. The remaining 58 channels are for telephone switching. Nodes are designed to provide tandem switching. The multiple interconnections between nodes insure most calls have several potential paths.

The network uses a *"flood search"* technique for call routing that avoids a requirement for switch routing tables. When a customer dials a number, the NCS will check its customer database for the called party. If the called party is not a subscriber of the NCS, the switch will send a call request to every adjacent NCS. The call requests are passed along to every switch in the network until the called party is found or every NCS has been interrogated. Once the called party is found, the switches assign channels to form a path between the two parties. This dynamic call routing method allows the network to bypass failed nodes. There are no switchboard routing tables to manage.

Figure 2-2 shows the key equipment allocated to a typical node center. The node center switch uses three communications shelters. Two of the shelters are for the switching equipment and the third is a management shelter for the node center commander. Four Line of Sight (LOS) microwave radio terminals provide twelve potential microwave links to adjacent nodes or extension nodes. A node center also has a local Radio Access Unit (RAU) that connect directly to the switch.

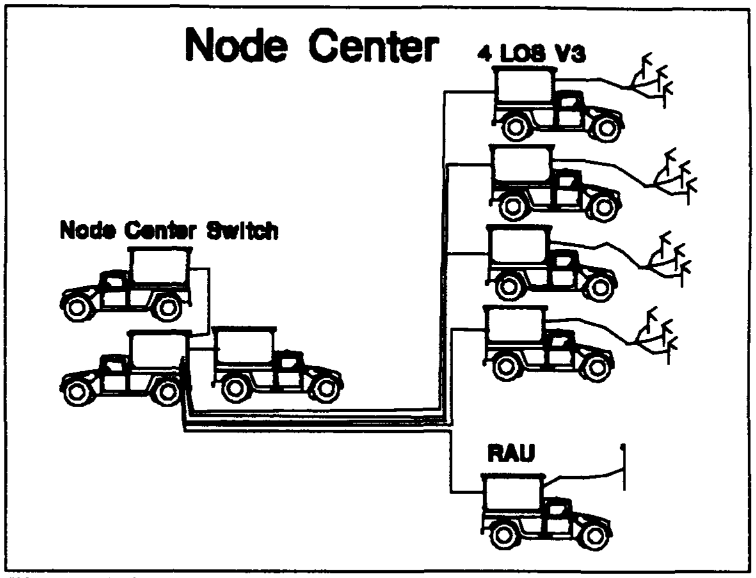

Figure 2-2

Each link from a node center is called a Digital Trunk Group (DTG). A DTG can be configured to one of several possible data rates. Links between node centers are usually at 1024 KB/s (64 channels). Links between node centers and large extension nodes are set to 512 KB/s (32 channels). Links to Small Extension Nodes (SENs) and remote Radio Access Units (RAUs) are set to 256 KB/s (16 channels). The DTGs can be reconfigured to smaller rates for special requirements such as satellite links.

The NCS multiplexes the three digital systems of the LOS terminal into a single Multiplexed Digital Trunk Group (MDTG) between the switch and the LOS terminal. This enables the node center to use only one coaxial cable or Super High Frequency (SHF) radio link between the switch and the LOS radio terminals.

The Node Center Switch

The Node Center Swtch (NCS) is a digital switch designed to route tandem calls and manage calls to attached extension nodes and radio access units. The NCS is normally configured to handle only 24 local wireline telephones. However, it can manage hundreds of customers served by extension nodes connected to the NCS.

The switch stores an affiliation status of each customer managed by the switch. A customer affiliates (or logs onto) to the network by dialing an entry code on the telephone. The customer must first be pre-authorized to enter the network before affiliating. A pre-authorized customer is considered pre-affiliated. A customer that has previously affiliated and since disconnected from the network is considered to be in an absent mode. The NCS maintains a customer database of pre-affiliated, affiliated, and absent customers' telephone numbers.

Network managers must instruct the switchboard operators to load special groups of MSE customer telephone numbers into the switches' customer databases. These groups, called Pre-Affiliation Lists (PALs), contain the subscriber data for hundreds of MSE customers. An MSE customer whose number is not loaded into any NCS cannot affiliate anywhere in the network. A customer whose number is loaded into multiple NCSs will also experience problems. One of the greatest management problems occurs when an NCS operator accidentally loads a PAL that was not supposed to be loaded by that NCS.

Each NCS maintains a database of the configuration of its hardware resources. The fifteen Digital Trunk Groups (DTGs) have a default configuration which is sufficient for most circumstances. However, the NCS operators must periodically reconfigure the NCS database to handie special circumstances. Figure 2-3 depicts the default database configuration. The default configuration has the fifteen DTGs allocated to five NCs, five SENs, one LEN, three RAUs, and an SCC.

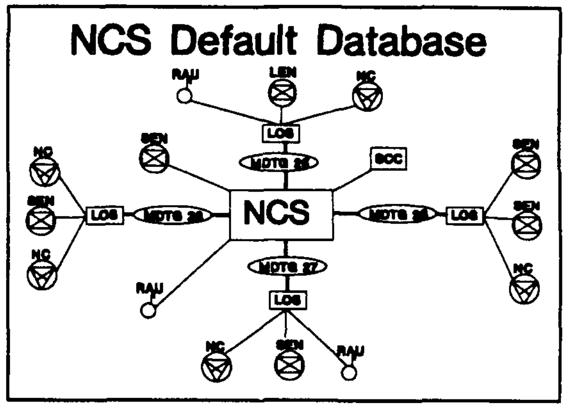

Figure 2-3

Database modification is a complicated and error prone process. Each DTG represents the allocation of several resources including Nine-Channel MUX/DeMUX (NCMD) cards, group modems, and Trunk Encryption Devices (TEDs). The default configuration fully employs all of the resources and the operator must reallocate resources to modify the database. Network managers must avoid forcing NCS operators to modify the NCS database. The task of modifying the database may be appropriate for an AI-based tool.

Each NCS controls the encryption of the DTGs and customer calls. A NCS has fourteen KG-93 Trunk Encryption Devices (TEDs). Each TED bulk encrypts a single DTG. Each DTG within an MDTG is bulk encrypted so there is no need to bulk encrypt the entire MDTG. The NCS operator must insure each TED has the correct encryption keys loaded. Network managers must insure that each NCS has the correct keys to load in the TEDs.

An encryption key in MSE is a software generated string of bits. Every encryption device in MSE uses the same kind of encryption key. It is possible, but not appropriate, to load the same key into every encryption device in the MSE network. Keys can be stored in a special device and manually transported to other locations. They also can be transferred electronically between nodes over the MSE system.

Each NCS has a TSEC/KG-94 Automatic Key Distribution Center (AKDC) that generates keys, transfers keys between nodes, and generates and downloads keys to the secure telephones. The AKDC also handles interfaces between secure and non-secure telephones. All mobile telephone users have a TSEC/KY-68 secure telephone that encrypts the customer's voice at the phone. The distant phone normally de-encrypts the voice. If the distant phone is not a KY-68, the AKDC in an NCS must de-encrypt the signal and send it plaintext to the non-secure phone. (This kind of call is considered secure because the clear signal is transmitted over bulk encrypted links or across physically secured wires).

The AKDC is a source of many network problems. An AKDC can store hundreds of encryption keys. The NCS operator must insure the correct keys are loaded into the correct memory addresses in the AKDC. Operators often load the keys into the wrong addresses. Although there is a small chance that any particular operator will load the keys incorrectly, there is a significant risk that one of the many NCS operators in the network will.

There are eleven different uses for encryption keys in MSE. Incorrect keys present different symptoms depending on which devices they are loaded into. MSE system experts can often spot and identify the exact encryption key problems because they recognize the symptoms and know which errors occur most often.

An NCS operator communicates with the switch's processor via a Video Display Unit (VDU). The VDU has a standard keyboard for input, a plasma screen for output, and a printer attached for permanent logs. The operator enters a command by requesting an interrupt and then typing a three letter mnemonic and any arguments to the command. For example, to request a list of the customers affiliated to the local RAU, the operator types DDL 12. The VDU displays the switch processor's output that is also printed on a line printer.

The processor output is in the form of raw data which often needs interpretation. For example,

TGM/DTG 23 13 TSB 12 5 TGC 6

means that the DTG 23 link to another NCS is working. In another example,

COMMAND 42 FAILED, KGX -9312 KG 8201 FAILED TO SYNCH WITH 24-35, D RCVR 4

means that a wrong encryption key was loaded into a customer's KY-68 (secure telephone). The phone failed to synchronize with the switch's AKDC when the customer attempted to place a call. The message also contains data that the network manager can use to isolate the location of the phone with the incorrect key.

The NCS operators and network managers often interpret the NCS processor output. The operators are trained to interpret the output and the managers learn from their experiences. Many important clues to network problems become hidden in piles of NCS processor printouts. The task of interpreting NCS processor output is another potential application for an expert system tool.

Another management function involves the duplication of the customer status information into adjacent node centers. The NCS operator instructs the switch's processor to send backup copies of the customer status information to an adjacent switch. The adjacent switch activates the subscriber data only if the first NCS fails or shuts down to move. This process, called duplication, is necessary to keep the customer authorization data in the network. If a switch operator fails to backup the customer data and his switch fails, hundreds of users can be left without service. It can take the network managers several hours to determine which customer numbers are lost and need to be reloaded.

The customer status duplication process is also complicated and error prone. The NCS operator must designate which adjacent NCS to send the duplicate customer data for each of the DTGs in the switch. A typical switch has more than ten DTGs with customer status data which must be duplicated.

The duplication scheme must be cleared and rebuilt periodically. Many times the NCS processor will show that it is correctly duplicated when in fact it is not. The design, implementation, and maintenance of a duplication scheme is yet another possible application for an expert system tool.

The Node Management Facility

The node center commander is responsible to input node status data into the System Control Center (SCC). The third shelter of the NCS cluster is called the Node Management Facility (NMF). It contains room for the node center commander and a workstation to send status data to the SCC. The node commander must manually input the status data into the workstation. The workstation then transmits the status data to the SCC's computer over the X.25 packet network.

Many signal units have bypassed the SCC input mechanism and implemented their own information systems. Some innovative MSE network managers have modified Zenith-184 laptop computers to send data over MSE phone circuits. The laptop computers were originally used to aid the node commander in data entry and transmission. Some units now use the laptop computer to send status information to other computers and bypass the SCC.

The MSE system does not provide a means to send NCS processor output in raw or processed form to a central network management center. The SCC network status information is all first input by a human. This insures that the SCC's data is a minimum of several minutes old. It also insures that much of the data hidden in NCS processor output is not put to good use. A system that gathers NCS processor data, interprets the data, and sends processes information to a network manager would improve the MSE network management.

GTE is fielding improved workstations for the Node Management Facilities (NMFs) to input status information to the SCC. The workstations perform the same functions that the MSE signal units did with laptop computers. The new node center manager workstations communicate with the SCC through the packet network instead of circuit switched lines.

GTE is also fielding an improved NCS workstation but the operator still has to interpret cryptic switchboard messages. The new workstation also uses Unix and X-Windows software. The NCS and NMF workstations do not have any AI-based software but there is capacity to add AI-based software later.

The Radio Access Unit and Mobile Subscriber Radio Terminal

The Mobile Subscriber Radio Terminal (MSRT) and Radio Access Unit (RAU) link the mobile users to the backbone network. The key component in the MSRT and the RAU is a unique radio called the RT-1539. The MSRT's RT-1539 radio links with one of the RT-1539 radios in the RAU to connect the user's phone to the node center switch. The RT-1539 is a VHF (30-88 Mhz) frequency modulating radio produced by Thompson CSF and is basically the same radio as the French Army's ER-222 radio.

The mobile user places MSRT calls much the same way a wireline user does. The user first affiliates the phone using the same entry code as with a wireline phone. To place a call on an affiliated phone, the user picks up the receiver and dials the number of the distant party. The RT-1539 will wait for the user to dial all the digits and then search for the marker signal of the RAU to which it is affiliated. Once it finds the signal, it initiates a dialog with a RT-1539 in the RAU. The radio in the RAU is connected through a Group Logic Unit (GLU) to a direct channel to a node center switch. The user's mobile telephone then has a link to the node center switch and the NCS then takes over the call.

Figure 2-4 depicts the typical configuration of a remote RAU. Network managers place remote RAUs wherever needed to cover gaps in coverage. The remote RAU links to a node center through a line of sight radio link. A remote RAU team consists of the RAU and LOS terminal crew. The team can install RAU and the LOS link to a node center in 15 to 20 minutes after arriving on site. The network managers usually locate remote RAU teams on high terrain away from any command posts. A RAU's electronic marker signal can make an electronically visible target.

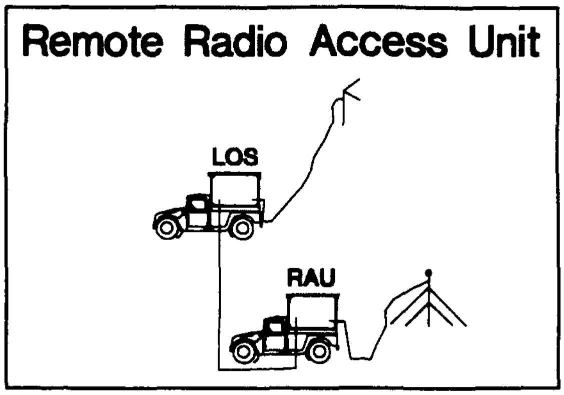

Figure 2-4

The RT-1539s in the MSRT and the RAU use the same frequency plan and encryption key. A frequency plan is the sequence of transmit and receive frequencies the RT-1539s in the MSRTs and RAUS use to communicate. The RAU and the MSRT must use the same pairs of frequencies in the frequency plan to communicate.

Network managers must control the frequency plans closely. The frequencies in these plans are in the same frequency range used by other military radios. The managers must insure the frequencies do not conflict with other communications devices. Users sometimes get incomplete or incorrect frequency plans and RAU operators sometimes load the wrong plans. Each problem creates symptoms that MSE experts can use to detect and solve a problem.

The RT-1539s use one encryption key and the telephones on the MSRTs are KY-68s that use two keys. The customers must load the three keys correctly for the MSRT to work properly. Users often load the wrong keys into their MSRTs. Sometimes MSRT users have the correct keys and the RAU or node center switch have the wrong keys. In either case, the managers often learn of the problem from frustrated customers.

Perhaps the most difficult problem with mobile user access that network managers deal with are RAU marker signals from RAUs. The MSRTs passively listen to the marker signals to maintain affiliation with the MSE network. As long as the MSRT can detect the marker signal from the RAU it is affiliated to, it will not attempt to affiliate to another RAU. A problem occurs when a node center switch fails and the RAU operator is unaware of the problem and fails to turn off the marker. Every mobile user affiliated to that RAU will not be able to place calls and the MSRTs will not attempt to find another RAU. A network management system should be able to detect this situation and tell the operator to turn off the marker.

The Small Extension Node

Most MSE wireline customers gain access to the backbone network through a Small Extension Node (SEN). The network managers assign at least one SEN team to each major command post. A typical corps with five divisions can have 168 SEN teams to support the major command posts. A SEN team consists of a LOS terminal team and a Small Extension Switch (SES) team.

The SEN has four primary missions. First, it provides access for up to 26 or 41 wireline users. It also has a port to connect an IEEE 802.3 LAN to the X.25 packet network. The SEN also has can connect two commercial central office lines to the MSE network. Finally, it can provide an interface to combat net radios. The commercial lines help Army units gain more communications capabilities by connecting commercial phone services into the tactical network. The Combat Net Radio Interface (CNRI) is a TSEC/KY-90 which can connect an MSE call to a tactical combat radio net. This enables MSE users to talk to lower echelon units not served by MSE but who have tactical combat net radios.

The small extension switch comes in two configurations. The only difference between the two versions is capacity of the switch. The higher capacity version can serve 41 users and the smaller capacity can serve 26.

Figure 2-5 depicts the major equipment of a SEN. The small extension switch can connect to the LOS microwave terminal by either a SHF radio link or coax cable. The SEN team can remote the LOS terminal away to a nearby hilltop and give the supported command post greater flexibility in site selection. The small extension

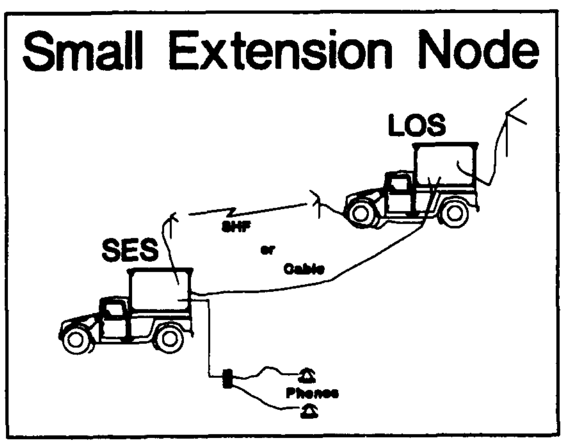

Figure 2-5

switch must be within 1000 feet of the users because the users only have 1000 feet of wire to connect their phones to the switch.

The LAN port provides significant new communications capabilities to command posts. Unit command posts will be able to link several computer systems together in a local area network to share data between staff sections. For example, the intelligence staff section can send target data directly to the artillery staff section. These LANs can communicate with all other LANs in the MSE network through the X.25 packet network. The artillery staff officer can transmit target data through the network to the artillery unit closest to the target. The artillery unit's computers will be able to send ammunition requests to the logistics support unit's computers. The interconnections of the computers around the battlefield will significantly improve the Army's command and control capabilities.

MSE network managers have fewer planning criteria with small extension nodes than they do with node centers. However, the managers do have several management concerns with SENs. Customer management is the first priority with the SENs. The customers' telephone numbers must be pre-affiliated in one of the node center switches before the customers can affiliate. There is no backup if the node center fails or has to move because SENs have only one link to a node center. Network managers often pre-plan backup radio links for the small extension nodes. They also have to set priorities of which command posts in the network are most important when problems occur or resources become scarce.

Network managers also control the combat net radio and the commercial network interfaces. They must plan the locations, phone numbers, frequencies, call signs, and encryption keys for these interfaces. There are only enough KY-90s to place one in every fourth SEN. Therefore, the network planners have to place the KY-90s with the SENs that can serve the most combat net radio users. The network managers also must provide the customers a means of determining the phone number of the closest KY-90 to any CNR user.

The network managers also control the commercial office interfaces. Non-secure commercial networks interfaces to secure tactical networks create security risks. The managers also have to coordinate the commercial interfaces with the commercial vendors in advance. Controlling the costs of the commercial network use is difficult because any MSE user can call through a commercial office interface to place a toll call on the commercial network

MSE units have discovered a significant problem for network managers. The node center switch processor can be slowed drastically if the customers at a SEN do not put their phones into the subscriber absent mode before the SEN shuts down for a move. In this situation, the NCS which serves the SEN will continue to attempt calls to customers at the SEN though the SEN is no longer connected. The NCS eventually loses calls and may have to be shut down and restart to clear the problem.[2] Any network management tool developed for MSE should be able to prevent this problem.

---

[2]III Corps MSE Tactical Standing Operating Procedures, (Department of the Army, Headquarters, III Corps, Ft Hood, TX, June 1, 1990), p. 3-8.

The Large Extension Node

The Large Extension Node (LEN) provides wireline access to large concentrations of users. It also has the same LAN, commercial network, and combat net radio interface capabilities as the small extension node. Because the Large Extension Node Switch (LENS) is similar to the node center switch, it has many of the same features and management considerations as the node center switch.

Figure 2-6 shows the major equipment assigned to a large extension node. The LENS uses three shelters including a node management facility. It can have two 512 KB/s microwave links to nearby node centers. The switch connects to the LOS terminal with two SHF radio links or coaxial cables.

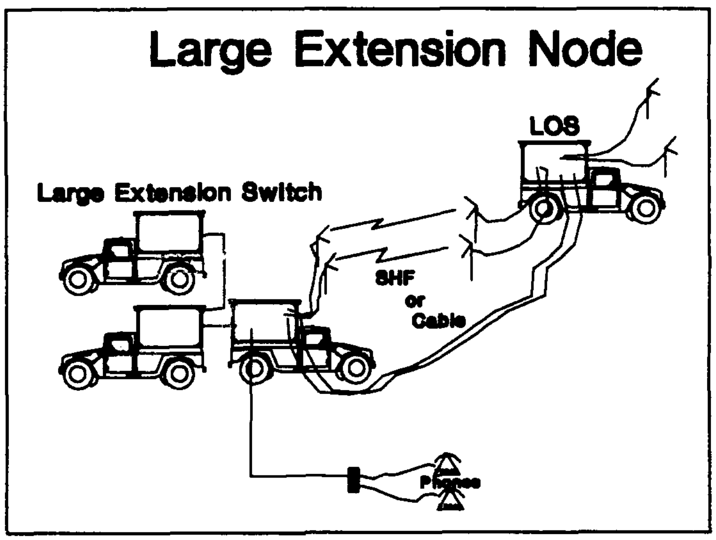

Figure 2-6

Although the LENS is similar to the node center switch, it has several key differences. First, the LENS does not have an MDTG like that of the node center switch. Both links from the LEN have separate cables or SHF radio systems. The Digital Trunk Groups (DTGs) in the LENS are configured differently from the node center switch. The DTGs in the node center switch are configured to link to other nodes or extension nodes and those in the LEN are configured to support customers. The LENS only has three Trunk Encryption Devices (TEDs) instead of the fourteen in a NCS.

LENS operators can configure the database to link to extension nodes or to increase the links to the node centers to a data rate of 1024 KB/s instead of the normal 512 LB/s. This involves configuration database modifications similar to those discussed earlier about the node center switch. This is also a potential task for an AI-based tool.

MSE Network managers treat the LEN much the same as a node center. The LEN has the same AKDC, encryption keys, SCC network status input, and customer management capabilities as the node center. The LENS operators must also perform the same duplication procedures to backup customers' status data as the NCS. The LENS can also be configured to switch tandem calls like a node center switch. Network managers often reconfigure the LENS default database to perform more NCS functions because there are rarely enough MSE customers in one location to tax all of the LENS' resources.

The System Control Center

The MSE network managers use the System Control Center (SCC) as their primary tool for planning, engineering, and controlling MSE networks. The SCC is a computer-based network management tool derived from a similar tool used by the French Army.[3] It was supposed to be the one tool MSE network managers would need to control the network but has not lived up to expectations.

The SCC can perform the following management functions:[4]

- Personnel management
- Network status display
- LOS link engineering
- RAU/MSRT frequency management
- Encryption key management
- Equipment management
- Prepare and issue orders
- LOS frequency management
- Customer management
- X.25 Packet network mgt

The most used functions are LOS link engineering and frequency management. The SCC uses a digitized terrain database developed by the defense mapping agency for the LOS path loss calculations. Network managers use this data to determine the best locations to place node centers, radio access units, and relay stations.

The SCC also maintains a database of LOS radio frequencies. It has a program to assign frequencies based on the location of the terminals, azimuth of the radio systems, the terrain, and the authorized frequencies. The program reuses frequencies as often as possible to gain better use of the frequency spectrum and to confuse enemy direction finding equipment.

The LOS path profiling and frequency allocation functions have mixed reviews. A survey done by the author reveals that some units only trust the SCC to do these two functions. However, some units based in Germany experience

---

[3]Don Rickerson and Robert D. Rood, "Mobile Subscriber Equipment Leaps New Network Bounds," SIGNAL, November 1991, p. 21.

[4]System Control Center Requirements Document Number 01 (SCCR-2-01), (GTE Government Systems Corporation, January 3, 1991), p. 51.

significant frequency interference and use other Army software to assign frequencies. To be fair, Europe is a highly congested environment for radio frequencies.

The SCC workstations can display a network status graph in a graphics window. The display uses the locations, link status, and current state information from a network database to portray a network status map. The network status database information is provided by the node center commanders who input the data through the terminal in their node management facilities.

The SCC database suffers from a dependency on human input. The SCC computer receives data input messages from the node commanders and updates the database automatically. There is no automated telemetry from the node centers to the SCC. The dependency on human input causes errors and network managers to lose time in detecting and correcting faults.

The SCC uses modern computational equipment, has high capacity, and can expand for future enhancements.[5] It is housed in three communications shelters. One shelter holds the computers and file servers and the other two house workstations connected through a local area network. Each workstation uses a 25 MHz Motorola 68030 CPU, has 16 MB of random access memory, and uses a fifteen inch 1,024 x 1,248 bit color display. The file server has two 170 MB disk drives. The workstations use the UNI-GRAPH/X operating system based on the AT&T UNIX 5.2 operating system. The system database uses the INGRESS

---

[5]Rickerson and Rood, p. 23.

relational database software and many of the applications programs are written in the C programming language. Unfortunately, much of the system software adapted from the French SCC was written in a proprietary French language called Langue Temps Real (LTR). All of the software belongs to GTE or its sub-contractors.

The network managers need a high capacity network management tool because of the number of network elements that they manage. A five division corps can have the following MSE teams:

MSE TEAMS	Number
Node Centers	42
Small Extension Nodes	224
Large Extension Nodes	9
Radio Access Units	98
Combat Net Radio Interfaces	44

Each of these teams move periodically to support a rapidly changing area of operations. This forces the network managers to reconfigure the network. There are Signal officers at each command post who coordinate Signal support but command posts often move with no warning to the MSE network managers.

The 3rd Signal Brigade of the III US Army Corps, stationed at Ft Hood, TX, developed a laptop computer based network to overcome some of the SCC's deficiencies. Each 3rd Signal Brigade node manager has a Zenith-184 laptop computer that connects to a data port in the Node Management Facility (NMF). The software, developed by the III Corps MSE planning cell, formats the data input messages to the SCC. The laptop computer insures that the messages are formatted correctly.[6]

The 3rd Signal Brigade units have taken the laptop computer network beyond its original mission of entering data to the SCC. The laptop computer can send messages to other node centers and laptop computers at the SCC. These units have improved the program to include most of the management data they need to control the network and the signal units that provide the MSE teams. The SCC personnel and equipment management software proved inadequate for the 3rd Signal Brigade.

The 3rd Signal Brigade used the laptop computer network as much as the SCC to manage its MSE network in operations Desert Shield and Desert Storm. They used the laptop computers to send all status reports to other laptop computers at the SCC. The network managers used the laptop computers to send operational orders requests for information to the node centers. They used the SCC primarily to engineer LOS links and assign LOS and MSRT/RAU radio frequencies.[7]

The MSE network managers have the SCC as their primary network

[6]Laptop Computer User's Guide for MSE, (Department of the Army, 3D Signal Brigade, Ft Hood, TX, June 21, 1990), p. 1.

[7]Interview with CPT David Brazier who served as an MSE network manager with the 3rd Signal Brigade during Operation Desert Storm.

management tool. The laptop computer network is used by most MSE units but the US Army Signal Center does not sanction or support it. The laptop computer network is only an interim solution and has little opportunity for growth. The laptop computers use the Intel 8086 CPU and have only a 20 MB hard drive. These computers are not capable of running complex network management software applications or AI-based tools.

GTE Government Systems Corporation is currently delivering to the Army an updated SCC called the SCC-2. The older SCC uses outdated eight bit processors that are not powerful enough to manage the large and complex MSE networks. The SCC-2 uses thirty-two bit processor based workstations linked together on a Local Area Network (LAN). The workstation software is based on Unix and X-Windows. The SCC-2 maintains distributed databases in each of the SCCs located in the division and corps signal units.

The SCC-II improves on the performance of the original SCC but not on its functions. The software runs on faster processors but remains dependent on input from the node center managers. There are no tools to monitor network status information and predict faults. The original SCC and the SCC-2 both force network managers to operate in reactive rather than proactive modes.

The Limitations of the SCC

The SCC provides limited network management tools. Its planning capabilities are limited because the SCC only provides network managers elementary tools. There are no AI-based planning tools to help the managers plan optimal networks.

The SCC can predict the success of LOS links, allocate radio frequencies, and print operational orders for each MSE team.

The network engineering capabilities of the SCC are adequate. The SCC uses the Longley-Rice algorithm to predict the success of LOS microwave radio systems. The frequency allocation software has proven to be good but it can assign LOS frequencies that interfere with other MSE frequencies. Network engineering is the SCC's most successful function.

The SCC is not adequate for network control. It relies on human input for network status information. The SCC's tools are reactionary based. Network managers who rely solely on the SCC have old information and learn about most faults only after they occur. It has no tools to monitor the network status and automatically alert the managers to possible faults. There are not expert tools to help network managers troubleshoot faults.

Conclusion

This chapter has introduced the major components of the MSE system. It discussed the functions, capabilities, and shortcomings of each component. It also discussed planning factors MSE network managers use to manage the MSE system. Chapters IV and V will expand on this discussion in describing the network management process and how AI-based tools can improve network management.

Chapter 3 will introduce the fundamental concepts of artificial intelligence needed to evaluate the potential of AI to improve MSE network management.

CHAPTER III

Fundamental Concepts of Artificial Intelligence

This chapter will explore the basic concepts of AI needed to analyze the potential benefits of AI tools for network management. It also introduces the terminology used to describe most AI systems. The reader should be familiar with the concepts discussed in this chapter because AI-based tools are significant investments. AI-based tools can provide a high payoff in improved network management or prove to be an expensive waste of effort.

Artificial intelligence is a broad field of study. It would require much more than this thesis to describe auequately every concept of AI. This chapter divides the discussion of AI into the following sections:

- A definition of AI
  - The Turing Test
- AI programming vs ordinary procedural programming
- Expert Systems
  - Advantages of using expert systems
  - Characteristics of an expert system
  - Types of expert systems
  - Components of expert systems
- Knowledge representation
- Dealing with uncertainty
- State-space search
- Forward vs backwards reasoning
- Neural networks
- AI/Expert system development
- Criticisms of artificial intelligence

Introduction

The field of Artificial Intelligence (AI) holds great promise to produce smart machines that can perform complex tasks. The field is also filled with controversy and unfulfilled expectations. Modern research into AI began in the late 1940s when digital computers were advanced enough to provide adequate platforms for intelligent programs. Soon after that, AI promoters and writers began describing intelligent computers that could think faster and better than humans. Science fiction novelists described computers that would take over the world unless stopped.

Unfortunately, the field of AI has yet to produce a machine or program that could outperform a human child in the simplest of tasks. This chapter will show that some researchers and philosophers believe that it is simply not possible to create a machine capable of intelligence.

A Definition of Artificial Intelligence

There is no single definition of artificial intelligence on which all researchers agree. As recently as 1983 there were 140 documented definitions of artificial intelligence.[1] Steven L. Tanimoto defines AI as

"A field of study that encompasses computational techniques for performing tasks that apparently require intelligence when performed by humans." [2]

---

[1]Eric C. Ericson, Lisa Ericson, and Daniel Minoli, ed. Expert System Applications in Integrated Network Management (Norwood, MA: Artech House, Inc., 1989), p. 5.

[2]Steven L. Tanimoto, The Elements of Artificial Intelligence (New York: Computer Science Press, 1990), p. 6.

Another definition is that AI is a branch of computer science concerned with the automation of intelligent behavior.[3] Most definitions of AI seem to come down to:

(1) Smart computers
(2) Computer models of human intelligence
(3) Machines that simulate human intelligent behavior.[4]

Perhaps one reason there is no consensus on the definition of AI is there is no consensus on the definition of intelligence. Most people can recognize intelligence when they see something exhibit it but cannot explain what makes something intelligent. Philosophers and cognitive scientists have debated what comprises intelligence for centuries. For the purpose of this thesis, the Turing Test conditions of intelligence and artificial intelligence are sufficient.

The Turing Test

The Turing Test, proposed by Alan Turing in 1964, attempts to determine whether or not a computer is intelligent. Turing hypothesized that a person attempting to determine intelligence in a computer would be biased by the fact it was a

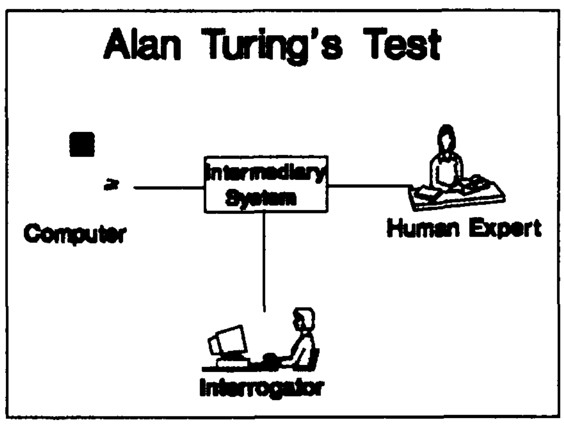

Figure 3-1

[3]George F. Luger and William A. Stubblefield, Artificial Intelligence and the Design of Expert Systems, (Redwood City, CA: The Benjamin/Cummings Publishing Company, 1989), p. 1.

[4]Ericson, Ericson, and Minoli, p. 5.

computer. Turing's test attempts to remove that bias when determining the intelligence of a machine.

Figure 3-1 depicts the Turing Test which involves a human interrogator, another human who is an expert in some field, the computer being tested, and an intermediary system to isolate the interrogator from the computer and human expert. The intermediary system can be any medium which the interrogator uses to ask questions of both the human expert and the computer. Its purpose is to prevent the interrogator from knowing beforehand which of the two parties is the human expert or the computer. The interrogator presents questions to the human expert and the computer through the intermediary.

The computer passes the test if the interrogator cannot determine which is the computer and which is the human expert. Turing's hypothesis was that if a computer exhibited human behaviors associated with intelligence, that was good enough.[5]

AI Programming vs Ordinary Procedural Computer Programming

It is important to distinguish between AI programming and ordinary procedural programming. All computer code is eventually decomposed to binary numbers that instruct the computer to perform tasks. Almost any task performed by an AI-based program can be written using an ordinary procedurally-based programming language. Given this, there must be advantages to using artificial intelligence techniques over simple procedural programming.

---

[5]Tanimoto, p. 9.

Two key features that distinguish AI from ordinary procedural programming are the use of heuristics and the method of the execution control.[6] These features allow greater flexibility in problem solving.

Procedural programs are simply coded instructions that tell the computer what tasks to perform. Human experts rarely reason in terms of procedures or algorithms when solving problems. They usually think in terms of *"rules of thumb,"* or heuristics. Experts can recognize when a particular lead may be the best to explore to solve a problem. They also can see when a lead should be left alone because it likely would lead to a *"dead end."* Procedurally-based programs usually explore every option or lead to solve a problem.

Human experts solve problems by applying knowledge in a *"data driven"* manner. They try to match known conditions with rules of thumb to gain more knowledge about the problems. A procedural program on the other hand acts as a human novice and has to follow a set procedure to troubleshoot a problem.

Consider the following example. A signal unit is unable to install a microwave radio link between two hilltops. It is known that a similar radio link was established some time ago between the same two hilltops using similar radios. One can infer from this information that the reason the radio link will not work is probably not due to terrain blocking the radio path. Knowing that the problem is not terrain, one can narrow the search for a problem cause to equipment, radio

---

[6]Anna Hart, Knowledge Acquisition for Expert Systems, (New York: McGraw Hill, 1986), p. 20.

frequencies, human error, or a combination of these.

A procedural program could be coded to solve this problem as could an AI-based program. However, an AI-based program can easily add another possible cause to its knowledge base. Consider in the previous example that another possible cause to the problem could be enemy jamming. An AI program can add the fact by putting another rule in its set of rules about microwave radio links. A procedural program would require significant recoding and possible recompiling to add this knowledge.

AI programs can make decisions under conditions in which standard procedural programs would many times fail. These conditions include:

(1) Incomplete or contradictory data about the problem
(2) Low confidence placed in some of the data
(3) So much data available that it would have to be analyzed before making a decision
(4) The problem cannot be described easily by an analytical model.
(5) The problem could be so complex that an exhaustive method to determine the solution would take too long
(6) The problem could be ill-defined.[7]

There are several reasons to explore the development of AI techniques to aid in some network management functions. AI programs are data driven rather than procedurally driven. They use heuristic searches rather than algorithms to solve problems. These properties enable the programs to behave more like human experts than procedural programs. AI programs can be also updated with new knowledge easier than standard procedurally-based programs.

---

[7]Ericson, Ericson, and Minoli, p. 7.

Expert Systems

Expert systems are a special subset of the AI field which not only exhibit human behavior, but also human subject matter expertise. One definition of expert systems is

> *"A program which has a wide base of knowledge in a restricted subject domain, and uses complex inferential reasoning to perform tasks which would normally require a human expert."* [8]

General artificial intelligence systems are not restricted to modeling human expertise.

Expert systems are limited by the current state of the technology to expertise in limited subject areas. A system designed to troubleshoot mobile radio telephone problems would be of no use in predicting which stocks should do well in the stock market. In the same light, a world class orthopedic surgeon would probably not be able to pick good stocks either.

Expert systems represent the real world with symbols in their memory. They do not manipulate knowledge but rather representations of the knowledge. It does not matter to the expert system what it is modeling as long as it can manipulate the symbols. Expert systems model human behavior and expertise from an external perspective only.

Advantages of Using Expert Systems

There are significant advantages to the use of automated expertise for network management aids. These include availability, consistency, and

---

[8]Hart, p. 19.

comprehensiveness.[9] These advantages may justify the expense of developing automated network management systems.

An automated system is always available. Expert systems can be replicated and used simultaneously by Army units around the world. Human network management experts take a long time to train. A typical Army network manager rotates to a different job after two to three years. In most domains, it takes humans at least five years to gain enough experience to become an expert.

Expert systems offer consistency in their performance. All humans have good and bad days while an automated expert does not get tired. Automated systems can monitor mundane data for hours without getting bored or sleepy. A system correctly designed will give the same and hopefully correct answers all of the time.

Expert systems can be comprehensive in their knowledge in their limited domains. The Army's worldwide mission is too large for any one person to be the leading expert in MSE network management. The knowledge of every units' experiences can be captured and added to an automated knowledge base. Acquiring this knowledge would be a challenging project with a high potential payoff. Expert systems can be designed to capture more knowledge over time which the Army could periodically consolidate to update all expert knowledge bases.

---

[9]Ibid, p. 20.

Characteristics of Human Experts

Experts are valuable resources. They have greater knowledge about a domain than a layman. They have knowledge not contained in operating manuals and know where the operating manuals are wrong or do not apply. They have accumulated experiences over time that were never anticipated by the designers of the equipment or the authors of the operating manuals. They can generalize their knowledge to form a guess on the solution of a new problem. Experts have a proven record of good performance.

Experts are effective and efficient. They become experts by being successful most of the time. They can solve problems much faster and accurately than novices because they can recognize patterns from previous experiences.

Experts usually know their limitations. They can recognize when they cannot find the solution to a problem. Most experts will admit when they are not absolutely certain of their recommendations. They also can describe what makes them unsure of their recommendations. The knowledge of their limitations helps them learn more about their domain each time they fail.

Experts are called on to provide information, solve problems, and explain their reasoning. An expert can review a plan, spot weaknesses, and recommend alternatives. Experts are called on to troubleshoot problems and recommend solutions. Experts earn legitimacy for their recommendations by explaining how they come to their conclusions and by how certain they are of their conclusions. Experts also train other people to become experts as they perform these tasks.

Types of Expert Systems

There are many different types of Expert systems. Those of interest to the network management domain are discussed below.

Network design and equipment configuration systems can design near optimal communications networks which provide the greatest coverage while using the least amount of resources.[10] Most attempts to apply AI techniques to tactical network management to date have dealt with network design.

There have been two significant tactical network design projects. The COMmunications Planning ASSistant (COMPASS), a prototype built by the US Army Signal Center, used AI techniques to aid a planner in designing a network and producing an OPerations ORDer (OPORD) for signal units based on the final network design.[11] The MITRE corporation developed another network design prototype tool called the BIGFOOT. It was able to help the user design a network and test several different solutions.[12] Both prototypes were developed as demonstrations and then abandoned.

Monitoring and interpretation systems can examine network status data to determine meaning and then present the data in meaningful ways to humans. The

---

[10]Robert N. Cronk, Paul H. Callahan, "Rule-Based Expert Systems for Network Management and Operations: An Introduction," in Eric C. Ericson, Lisa Ericson, and Daniel Minoli (eds.), Expert Systems Applications in Integrated Network Management, (Norwood, MA: Artech House, Inc., 1989), p. 94.

[11]"COMPASS - Communications Planning Assistant," Artificial Intelligence Project Summaries, US Army Artificial Intelligence Center, May 23, 1990.

[12]MITRE Corp literature from the 1989 Signal Symposium, Ft Gordon, GA.

data may be fragmentary, voluminous, or contain errors. These systems may present the analyzed data in the form of graphics or simple alarms when certain conditions are met. Interpretation systems review "snapshots" of the network such as traffic metering reports or switchboard printouts. Monitoring systems conduct the interpretation process continuously.

Control systems use the results from an interpretation system to recommend changes to the network. An example could be a system that spots traffic loads near capacity in a particular link and recommends a parallel link to reduce traffic on the link. Some control systems may actually issue orders to subordinate nodes to perform the actions.

Diagnostic systems can troubleshoot problems and recommend solutions. They have significant potential in aiding network management at all levels from the network operations down to the individual node. These tools can use expertise not available in operator manuals to troubleshoot equipment malfunctions, subscriber problems, and network problems.

Components of Expert Systems

Expert systems emulate the behavior of human experts but do not copy the structure of the human mind. Their external behavior may be all that resembles human intelligence. A typical expert system is made up of four main components. Three of these components: user interface, working memory, and an inference engine are common to most expert systems. The fourth component, a knowledge base, is unique to each expert system. Figure 3-2 depicts the relationships between these four components.

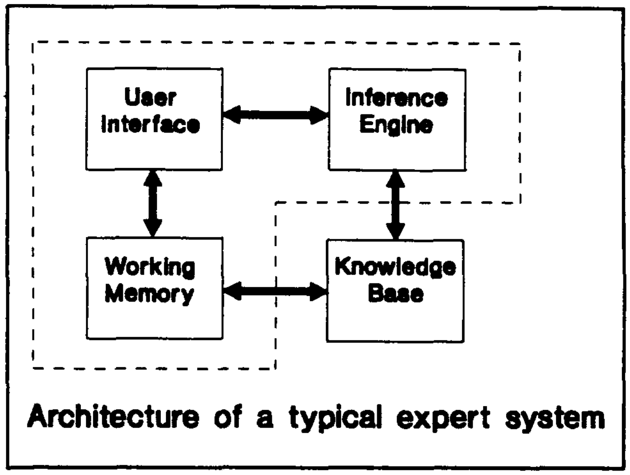

Figure 3-2

The knowledge base is the heart of the expert system. It contains the information about the problem domain. Most expert systems represent knowledge in the knowledge bases in the form of *if... then* ... rules. An example rule may look like:

If (similar radio system has been established recently)
Then (rule out terrain as the likely cause).

The *if* portion is called the rule's antecedent while the *then* portion is called the consequent. Not all knowledge bases store knowledge in the form of if ... then ... rules. Other knowledge representation schemes are discussed later.

The working memory is a *"scratch pad"* which the program stores information about the current problem. The inference engine compares the contents of the working memory to the rules in the knowledge base to infer more knowledge. The working memory is usually computer Random Access Memory (RAM). Many applications require considerable amounts of memory. Most PC based expert systems require between 5 and 20 megabytes of RAM.[13]

The inference engine drives the knowledge search and inferring. A typical

[13]Ericson, Ericson, and Minoli, p. 13.

inference engine in a rule-based expert system will look at each rule in the knowledge base and compare the antecedent to the working memory. Whenever an antecedent is satisfied (eg. the *if* statement is true), a *match* occurs. Whenever the inference engine finds a match, it *fires* (executes) the consequent statements of the rule. The rule consequent can alter current knowledge or add more knowledge to the working memory. The new information may enable the antecedent conditions of other rules to test true. The inference engine searches the knowledge base and working memory again to check for more rules to fire.

The inference engine is responsible for resolving conflicts in the rule testing. When the inference engine tests each rule consequent, it may find more than one rule eligible to fire. Whenever the inference engine finds multiple matches on rule consequent, it must decide which rule or rules to fire. The inference engine usually defines a utility value for each rule in the knowledge base which it uses to resolve the conflict. There may also be special rules, called *meta-rules*, which could be used to solve the conflict. Meta-rules can be described as *"knowledge about the knowledge."*

The user interface protects the user from the intricacies of the expert systems. The user asks questions and enters data to the expert system through the user interface. The user interface may also obtain information from sources other than the human operator. A systems designer also can use the user interface to add more knowledge to the knowledge base.

The separation of the knowledge base from the rest of the expert system enables knowledge engineers to concentrate on the acquisition of knowledge rather than the internal workings of the expert system. It allows the engineer to represent the knowledge in the form of the if ... then ... rules. It also enables the addition of more knowledge without major recoding. The user interface, working memory, and inference engine together are called an expert system shell.[14]

Knowledge Representation

Two key issues in expert system development are how knowledge is to be stored in the knowledge base and working memory, and how the inference engine is to search the stored knowledge to solve a problem. Expert systems designers assume it is possible to represent the real world in a computer's memory in the form of symbols, and manipulate these symbols to find the solution to a given problem. The issue for expert systems is how best to represent the world as symbols.

Most problems that AI systems are designed to solve do not lend themselves to traditional forms of knowledge representation. AI problem solving is concerned with qualitative rather than quantitative representations of knowledge. AI techniques are designed for reasoning rather than calculation. In order to support qualitative reasoning, the knowledge representations must:[15]

A. Handle qualitative knowledge.

Qualitative knowledge implies relationships rather than quantities.

---

[14]Luger and Stubblefield, p. 295.

[15]Ibid., p. 30.

B. Allow new knowledge to be inferred from a basic set of facts.

The earlier microwave radio system example showed how new knowledge about a problem can be inferred from old knowledge. The knowledge that a similar system had been installed before allowed the expert to rule out terrain blocking as a likely cause of the radio problem.

C. Allow representation of general principles as well as specific situations.

The variables defined by the program must be able to refer to a variety of type entities. They must be able to change dynamically. Traditional computer languages such as FORTRAN do not allow variables to represent more than one type of entity. For example, once a variable is declared as an integer, it cannot be used to represent a string. This allows the program to store *cause not likely terrain blocking* as well as *cause = malfunction.*

D. Capture complex semantic meaning.

Meaning about an entity cannot always be represented by a listing of its attributes. For example, a microwave radio link has frequencies, azimuths, and distances for quantitative attributes. Semantic information about an MSE radio link is that it is a kind of digital link between two network nodes This in turn implies more quantitative information about data rates and which node supplies timing to the link.

E. Allow for meta-level reasoning.

Experts know information about their knowledge. For example, the source of the knowledge may not be reliable, or unsure of the knowledge. The knowledge may not be reliable enough to use to make an inference without first being verified. Expert systems must be able to make use of meta-knowledge to be intelligent.

Knowledge Representation Schemes

There are several knowledge representation schemes used in the AI field. Each scheme has particular strengths and weaknesses for different type problems. These representations schemes are semantic networks, frames, production rules, objects, and predicate logic. Appendix A discusses the types of knowledge representation schemes best suited for the types of knowledge-based systems discussed in this thesis.

Dealing with Uncertainty

Experts cannot be always absolutely certain of their conclusions. Sometimes they have to use unreliable or unconfirmed information to solve a problem. There are several methods expert systems can use to deal with uncertainty. One of these methods is called certainty theory.

Certainty theory is an algebraic approach to expressing confidence. The theory assumes that the knowledge content of rules is more important than the algebra of confidences that holds the system together.[16] The confidence measures assigned to an input or a conclusion correspond to informal evaluations that human experts attach to them. This is similar to the qualifications experts attach to their conclusions such as *probably true* or *highly unlikely*.

---

[16]Luger and Stubblefield, p. 311.

The algebra of certainty is not complicated. The measure of confidence in a hypothesis is called a Certainty Factor (CF). A CF is a real number between -1 and +1. A CF of 1 shows complete confidence in the hypothesis while a CF of -1 indicates complete disbelief in the hypothesis. A CF of 0 indicates the expert has no evidence to either prove or disprove the hypothesis. For example, an expert may state the rule:

> IF *another LOS system has recently worked between the same locations*
> THEN *the problem is not terrain blocking (CF .95)* .

The expert may have reduced the confidence from 1 to .95 because there are some circumstances that terrain may be the cause of the problem (perhaps an obstacle such as a water tower was recently constructed between the two sites).

The certainty factor can also apply to the input. In the previous example, the network manager consulting the system believes there may have been a recent LOS system between these two locations but is not positive of the fact. This should decrease the certainty of the rule's conclusion. For example, the network manager believes a system likely had worked between these two locations recently. The expert system could assign a CF of .6 to the antecedent. This would reduce the CF of the rule's conclusion to .9.

The algebraic formulas for certainty theory are not presented in this thesis. However, one should not confuse certainty theory with probability theory that looks the same as certainty theory but is not.

There are some criticisms to certainty theory. One criticism is that certainty theory is too ad hoc. Although it is defined by formal algebra, there is no rigorous definition to the certainty factors. One expert may assign a CF of .9 to the qualification probably true while another expert may assign a lower certainty factor to the same qualification.

Another problem with certainty theory is that it can prevent an expert system from reaching a conclusion. For instance, the cause of a problem may be identified but the CF attached to it is not high enough to stop the search. More rules may be fired which could unintentionally reduce the CF of the conclusion more. The expert system could fail to reach a conclusion even though a human expert would have.

Other approaches to the uncertainty problem are the *fuzzy set theory* and *nonmonotonic reasoning*. Fuzzy set theory deals with the problem of vagueness in spoken languages. It deals with vagueness by assigning degrees of membership to the possible meanings in a manner similar to confidence factors.

To illustrate this concept, consider the following question. What temperature is the transition point from cool to cold? For the sake of simplicity, assume that the transition between cool and cold occurs between 50 and 45 degrees fahrenheit. An expert system could use multiple answers to the question and attach a degree of membership to each. The answer could be: 50(.05), 49(.1), 48(.2), 47(.25), 46(.5), and 45(.8). The numbers in the parentheses are the degree of membership of each temperature to the answer to the example question.

Fuzzy set theory gives the expert system designer a means of handling vagueness. Unfortunately, it also increases the computational load on the expert system. It can dilute its inferences and prevent an expert system from reaching a conclusion in a manner like certainty theory could.

Nonmonotonic reasoning is a means of reviewing previous conclusions once new or better information is found. A system that uses nonmonotonic reasoning would make the best assumptions given the available information and continue the inferring process. If information that contradicts the assumption becomes available, the system changes the assumption and reviews every conclusion that depended on the assumption. Nonmonotonic reasoning emulates the human reasoning process but can create large computational burdens on the expert system if basic assumptions prove false.

State Space Search

Many computer programs must search along constrained paths through intricate networks of knowledge, states, or conditions to find important information or to reach a goal.[17] An analogy can be the example of a treasure hunter searching for a treasure hidden deep in a vast cave network. The explorer would be limited in the search by the geometry of the caves. The network of caves may be so intricate that it would not be possible to exhaustively search for the treasure in every tunnel. The treasure hunter would need some formal search method to find the treasure in a reasonable time. The treasure hunter searches for the goal of the treasure using a formal search technique. AI programs search foı answers to a problem in the same manner.

---

[17]Tanimoto, p. 163.

AI programs deal with four aspects of search. The first, state space, is the set of all possible states for a problem. A chess game has thousands of possible states, or configurations, of its game board. AI programs have move generators that enable them it to calculate a new state given the present state. The third aspect of search which programs need is a method to control the exploration of the search space.

The fourth aspect is search heuristics. These make the search shorter by selecting the likely best paths first. AI problems are often too large to exhaustively search every possible state to find the goal. In the example of cave, the treasure hunter cannot explore every inch of the cave network to find the treasure. Likewise, AI programs may not have the time nor the processor power to exhaustively search the entire search space.

The two most common search methods are breadth first and depth first strategies. Both are exhaustive search strategies that traverse the search space in different ways. Both methods have advantages and disadvantages based on the problem being explored. Most other search methods are variations on these.

Each of these search methods view the search space as a tree. Each node on the tree is a possible state. The tree's root is the initial or start state. The root has a branch to each state for each possible next state. Each of the successor states have branches to other possible successor states. Each level of the tree represents a generation of states.

A depth first search traverses the tree by going down before going across.

Figure 3-3 shows that at each node, the program would generate a possible next state and compare that state to the program's goal. If the state does not match the goal, the program would cycle through another generate and compare process. If the program reaches a dead end of the tree where it cannot generate another state, it backs up to the last state with another possible successor, and begins to explore that path.

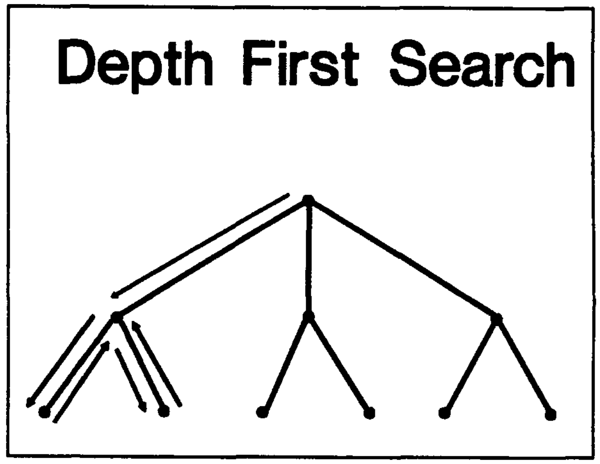

Figure 3-3

The depth first search method would be guaranteed to find the goal if it existed, but it may not find the shortest path to the goal. However, the method is susceptible to combinatorial explosion if any of the branches of the tree is infinitely deep with next generation possible states. The program would need to overcome this possibility by limiting the depth of the search before backing up to attempt new paths.

The breadth first search is a more conservative approach than the depth first method. Figure 3-4 shows that the program generates all possible successor states and compares each of the successor states to the goal. If the goal is not found, the program takes each of the successor states and performs the same cycle to each until the goal is found or there are no other possible states. A good program can save time when using this method by recognizing a repetition of a previous state and not attempting to explore that state any further.

The breadth first search will find the shortest path to the goal, though it may take longer than a depth first search. A breadth first search may take forever if a given state can have an infinite number of successor states. As a depth first search could go infinitely deep into the tree, the breadth first search could go infinitely across the tree. Depth first searches are well suited for solution spaces that are deep and narrow. Breadth first searches excel in the opposite type of solution space.

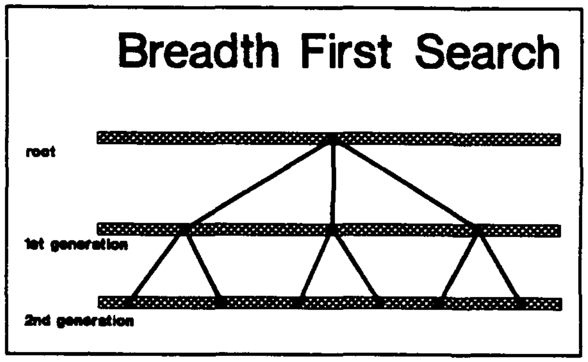

Figure 3-4

Depth first and Breadth first are *dumb* exhaustive search techniques. Many problems would cause the computer to *"bog down"* in a combinatorial explosion of the search space. The treasure hunter in the cave would likely guide the search in the cave for the hidden treasure by applying rules to increase the chances of finding the treasure early.

Inference engines can apply search heuristics to guide the search process. The heuristics range from simple functions to complex models. A detailed explanation of search heuristics is beyond the scope of this thesis, but three methods are discussed below.

The Best First Search (BFS) method uses a function to determine which next generation node, or state, to explore. The function can be simple such as which node has the least cost or is the shortest distance from the current node. The Best First Search method's efficiency at reducing the search time is based on the efficiency of the function.

All of the search heuristics involve keeping a list of states that have been previously explored. Whenever a state is calculated which matches a state previously explored, that state is not explored. This prevents the computer from wasting time exploring dead end paths more than once.

A similar method called Uniform Cost is a modification of the breadth first search. It orders the next generation set of nodes in a least cost order. It then explores each node in that order. The uniform cost method can be the same as the Best First search, depending on what the Best First's Search function is.

A more complex search heuristic called A* (pronounced A-STAR) uses a function to estimate the distance from each present state to the goal. Nodes are explored in priority based upon the shortest estimated distances from each state to the goal. The A* search can be complex and its efficiency is based on the quality of the function that estimates the distances to the goal.

The term *planning* in the AI realm refers to a problem solving activity with the goal to produce a set of procedures to accomplish a task. The resulting set of procedures is called a *plan*. Planning involves searching a space of configurations to find a path that corresponds to the desired sequence of operations. The search space for a large problem can be reduced by breaking the problem into smaller problems and planning each sub-problem hierarchically.

An example of a planning problem in the MSE problem domain is modifying the configuration data base of a node center switch. A node center data base refers to the configuration of the resources of a node center switch. A switch operator may be called on to modify the data base to reconfigure a digital trunk group from a 256 Kb/s data rate to a 512 Kb/s rate. The problem has many solutions, few of which could be considered good. A planning algorithm would consider the current state of the data base and search the space of all possible data base configurations to determine how best to modify the switch's data base.

Forward vs Backward Reasoning

AI programs are designed to discover a path through a search space between an initial state and a goal. The search can go either forward from the initial state to a goal or backward from a goal to find the path to the initial state. The choice of which direction to take is based on several factors. These factors include the topology of the search space tree, the number of possible initial states vs the number of possible goals, and the need to justify each step in the reasoning process.

Backwards reasoning, or goal directed search, starts by picking a goal and looking for the facts to prove the goal. If the program finds a fact that disproves the goal, the program rules out the goal and tries another. In a production rule system, the inference engine would scan the consequents of the rules to find rules that can prove the goal. The inference engine then tests those rules to see which ones could fire. If none could fire, it then begins the same process to find enough facts to fire a rule that may help prove the goal.

Goal directed search is good to use in several circumstances. One is when the number of initial states is larger than the number of possible goals. Goal directed searches are good if the program needs to explain each step it used to solve the problem.

Forward reasoning, or data driven search, starts by looking at the known data and applying the rules to derive more information. A production system would fire every rule in which the antecedent tested true. It would then test every other rule to see if knowledge derived from the firing of the rules enabled more antecedents to test true. The process would continue until a goal state was found or no more rules could be fired.

Data driven search is best used under the opposite best circumstances for goal driven search. It is good to use when the number of initial states is less than the number of possible goal states. The explanation of each step in the reasoning process is harder with data driven search. Data driven search may not be proper when the program must explain itself through the search process.

Neural Networks

Neural networks are another branch of the artificial intelligence field that go beyond simply emulating human behavior. Neural networks model the actual structure of the human neurological system. These networks can be used for may that can prove the goal. The inference engine then tests those rules to see which ones could fire. If none could fire, it then begins the same process to find enough facts to fire a rule that may help prove the goal.

Goal directed search is good to use in several circumstances. One is when the number of initial states is larger than the number of possible goals. Goal directed searches are good if the program needs to explain each step it used to solve the problem.

Forward reasoning, or data driven search, starts by looking at the known data and applying the rules to derive more information. A production system would fire every rule in which the antecedent tested true. It would then test every other rule to see if knowledge derived from the firing of the rules enabled more antecedents to test true. The process would continue until a goal state was found or no more rules could be fired.

Data driven search is best used under the opposite best circumstances for goal driven search. It is good to use when the number of initial states is less than the number of possible goal states. The explanation of each step in the reasoning process is harder with data driven search. Data driven search may not be proper when the program must explain itself through the search process.

Neural Networks

Neural networks are another branch of the artificial intelligence field that go beyond simply emulating human behavior. Neural networks model the actual structure of the human neurological system. These networks can be used for may problems that involve pattern recognition.

Biological and artificial neural networks base their architectures on two primary elements: processing elements and interconnections. A processing element, or neuron, takes one or more inputs and produces a single output. Interconnections are the links between external stimuli and the processing elements. The interconnections determine the structure of the network. Knowledge is represented by the network's structure.[18]

Figure 3-5 depicts a single neuron. A neuron takes one or more inputs (interconnections) and converts them to a single output. The output will be zero unless the sum of the inputs is greater than some pre-determined threshold level. Each input signal is weighted to represent the levels of importance to each input signal. When the sum of the inputs exceeds the threshold level, the processing element applies a transfer function to the input signal to determine the output signal.

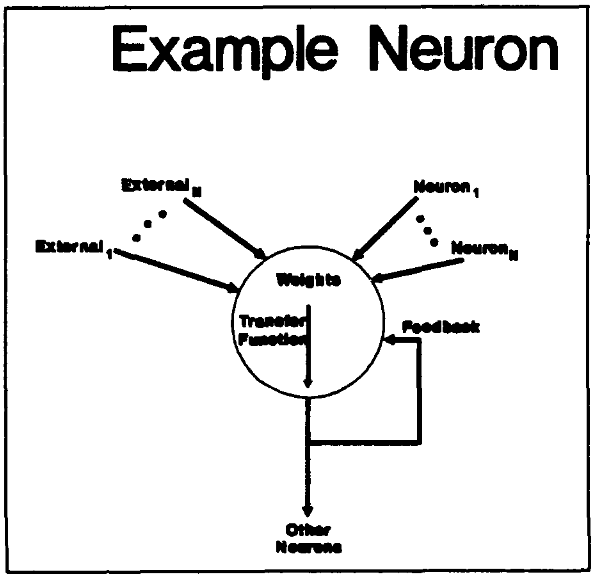

Figure 3-5

[18]Maureen Caudill, "Neural Networks Primer: Part 1," AI Expert, December 1987, p. 47.

The output signal can connect to other neurons as inputs or to itself as a feedback input.

Neural networks do not apply rules to known information to derive knowledge. They instead derive knowledge from experience. Thus, neural networks learn by doing. Neural network learning, or training, can be supervised or unsupervised. Neural networks adapt new knowledge by adjusting the input weights in individual neurons.

In supervised learning, the network has interconnections from an external input that tells the network what the state of the network should be after the network is stimulated in some way. The network has a mechanism to adjust the weights of each input in every neuron. In unsupervised learning, the network does not have an external input to tell it what the state of the network should be.

Neural networks have specialized applications. Researchers have successfully applied neural networks to pattern recognition, speech synthesis, vision problems, and telecommunications network management. Neural networks excel at recognizing a pattern and responding appropriately.

Neural networks are not good for computational intensive problems. They do not calculate a result based on an input. A neural network could be developed and trained to determine the approximate path loss of a microwave radio system. However, it would be much easier to write a function to calculate the estimated path loss. The calculation function would execute much faster and be more accurate. It also would not require many repetitions to train it develop an approximate answer.

Expert System Development

Expert systems must be managed like any other Information System (IS). They do have special management considerations in addition to that expected in other information systems. These considerations are discussed below.

The role of the systems analyst is slightly different with expert system development. In conventional IS development, the analyst works with the firm's management to determine the systems' requirements and with the users to determine how the users get the job done before the new IS system. With expert systems, the analyst does this and acts as a knowledge engineer to acquire the knowledge of one or more Subject Matter Experts (SMEs). The knowledge engineer may also acquire knowledge from resource materials such as user manuals or product specifications.

The Systems Development Life Cycle (SDLC) for expert systems follows the traditional waterfall SDLC used in most conventional information systems development. The conventional SDLC is a methodical management model for developing information systems. The steps to the SDLC include:

Planning - To identify what projects the organization will pursue.

Requirements Analysis - To determine the scope and success factors of individual projects. It includes feasibility studies to determine the costs and benefits of individual projects. The result of this effort is a requirements specification.

Systems Design - To design the interfaces, data storage, and processes which the information system will need to meet the requirements specification. The design at this stage is a logical design that is not machine specific.

Implementation - To produce, test, and deploy the information system based on the systems design. This often requires changing the logical design to meet specific machine and software compatibility requirements. It also includes training the users on the system.

Maintenance - To insure the information system is measured to identify problems areas that need improving.

The Department of Defense software development standard 2167A is based on the waterfall SDLC. These standards have come under heavy criticism for being inflexible and a barrier to innovation.[19]

Systems analysts often use prototypes or storyboarding to improve user and management involvement with the systems development. Prototypes are functional models of the information systems. They give the users a first look at what the information system will look like and do. Users often clarify their requirements and think of new ones once they see a prototype.

Storyboarding is a prototyping technique that shows the user how the interface works without developing a full functional prototype. A storyboard

---

[19]Stephen J. Andriole, Information System Design Principles for the 90's: Getting it Right!, (Washington: AFCEA International Press, 1989), pp. 29-42.

shows the user interactive screens of system functions. The storyboard is driven by a simple program or prototyping tool. Storyboards are easy to develop and are good tools to verify system requirements.[20]

There are several important management considerations specific to expert systems development. These are presented below in relation to the SDLC.

Problem identification is critical to successful expert systems development. Problems that expert systems are good for must be specific in nature. There must be experts available who are willing to cooperate with a knowledge engineer. The problems should be of the type which can be solved with available information. Expert system developers have to identify every possible problem situation that the system would have to diagnose. Expert systems are also not good at overcoming unexpected problems by generalizing information from previous but dissimilar experiences.

Knowledge acquisition is the process of extracting the information from an expert. The knowledge engineer must be able to extract the knowledge and to present it to the subject matter expert for verification. This is a very difficult process because the knowledge engineer usually knows little about the problem domain and many subject matter experts have considerable egos. Many times the SMEs do not believe their knowledge can be put into a machine or they believe they will be replaced by a machine.

---

[20]Stephen J. Andriole, "Storyboard Prototyping: A New Approach to User Requirements Analysis," IT for Command and Control, (New York: IEEE Press, 1991) p. 82.

There is no set format for the knowledge acquisition process. However, the knowledge engineer likely attempts to find out the following from the SME:[21]

- What data are important? In what order and form?
- What are the interrelationships between data items?
- How important and how accurate are the data items?
- What data might be missing?
- What assumptions does the expert make?
- What constraints does he have?
- What sort of inferences does he make?
- How does he form concepts and hypotheses?
- How do these relate to each other?
- How does the expert move form one state of belief to another?
- Which evidence suggests particular goals or concepts?
- What are the causal relationships?
- Are there any logical constraints on the system?
- Which problems are easy, common, hard, or interesting?

The design phase presents some crucial decisions for the expert system development team. They must choose the best knowledge representation schemes and inference strategies. The best mix of representation and inference strategy depends on the domain and the type of knowledge. The wrong mix of these will result in unworkable systems.

In the implementation phase, the expert system development team must develop and test the expert system thoughtfully. The team must choose the best development tools. It will have to make changes to the design based on the hardware and software. The team will need to work with the subject matter experts to verify the performance as much as with the users to verify the requirements.

[21]Hart, p. 34.

A problem with all information systems, and especially with expert systems, is the acceptance of the system by the users. Expert systems are designed to do more than automate simple tasks. They are designed to offer advice to the users. The users must trust the expert system if it is to be effective.

The maintenance phase presents some special considerations to the project team. The expert system will need to improve over time. Most expert systems, including any MSE network tool, exist in multiple copies. A well designed system can learn from failures and improve itself over time. There must be a method to bring lessons learned back to a central location so they can be incorporated in software updates for everyone.

Criticisms of Artificial Intelligence

The field of AI has its share of criticism, much of which is earned. The field has great potential and greater expectations. The Department of Defense is the largest contributor to applied research in AI. There are some who argue the money could be better spent elsewhere.

The first major criticism of AI is that it has not lived up to the expectations of most people. It has been oversold in the past and has not delivered much for the near billions of dollars of research funds invested in it. These large investments have produced some impressive AI-based systems for specialized applications. Unfortunately, the research has yet to produce a *"killer application"* that would make AI systems attractive to more users.[22]

Expert systems have been criticized as being *"novice systems"* rather than expert systems. In most expert systems built to date, the computers can perform better than a beginner and even exhibit some useful competence, but cannot rival the experts whose rules are used by the expert systems.[23]

The problem with expert systems goes beyond the issue of capturing the knowledge of experts. There is evidence that human experts use intuition and images rather than logical rules to solve problems. The skills of experts become so much a part of them that they need be no more aware of them than they are of their own bodies. Airplane pilots report that as novices they felt they were flying their planes, but as experienced pilots they simply experience flying itself.[24]

Evidence shows that humans use images and not descriptions to understand and respond to situations. Humans can look at a photograph and instantly identify objects, their depth from the camera, and emotions on human faces. Computers can convert photographs to a bit images and manipulate the images but are still unable to deduce much information from them. Neural networks hold promise for

---

[22]Stephen J. Andriole "Artificial Intelligence and National Defense: An Agenda and a Prognosis," in Stephen J. Andriole (ed.), High Technology Initiatives in C^3I, (Washington:AFCEA International Press, 1986), p. 200.

[23]Hubert Dreyfus and Stuart Dreyfus, "Why Computers May Never Think Like People," Technology Review, January 1986, p. 54.

[24]Ibid, p. 46.

improved pattern recognition but they will not likely soon solve the problem.[25]

Conclusion

The field of artificial intelligence offers great promises for information systems and management tools that capture human expertise to do specific tasks. Although AI-based tools can be expensive to develop, they can provide a high payoff in improved performance. They can help organizations like the Army overcome a shortage of trained personnel. They can also help organizations share lessons learned by one group with the rest of the organization. Chapter V will show that AI-based network management tools can perform many important tasks for commercial and military communications networks.

Chapter IV will discuss the basic concepts of commercial and MSE network management.

---

[25]Hubert Dreyfus and Stuart Dreyfus, "Why Expert Systems Do Not Exhibit Expertise," IEEE Expert, Summer 1986, p. 88.

CHAPTER IV

An Analysis of MSE Network Management

Introduction

MSE network management is a specialized field with its own set of concepts and buzzwords. The purpose of this chapter is to describe and analyze the current MSE network management processes. As part of this discussion, this chapter will also discuss the essential elements of commercial and military network management. The reader needs the information in this chapter to analyze the potential for AI tools to improve MSE network management presented in the next chapter.

This chapter begins with an introduction to commercial network management. It discusses the evolution of commercial network management from single vendor systems to modern integrated multi-vendor environments. It also introduces network management standards and communications protocols.

The chapter outlines the current Army doctrine for how MSE network and node center managers plan, engineer, and control networks with the currently available set of tools. Chapter II introduced many of the planning factors MSE network managers use in managing the system. This chapter describes how they use these planning factors in the management process. It also explains why none of the commercially available tools can be adapted to manage MSE networks.

This chapter divides the discussion into the following sections:

- Commercial Integrated Network Management
- Commercial Network Management System Architectures
- Why Commercial & Military Network Management is so Different
- The MSE Network Management Process
    - Network Planning
    - Network Engineering
    - Network Control
    - Deficiencies in the Present Network Management Process
- The MSE Node Center Management Process

Commercial Integrated Network Management

Many non-telecommunications businesses today operate private voice and data communications networks. These businesses acquired private networks because information technology has become such a strategic resource for them. They also have discovered that managing telecommunications networks is demanding and resource intensive.

There are three primary factors behind the move to private network management. They are technology, the divesture of American Telephone and Telegraph (AT&T), and the importance of telecommunications in the information age. These factors have forced many businesses to take on the task of network management though they are not in the telecommunications industry.

The pace of technology change is getting faster. New communications techniques, services, and equipment appear each day. The field changes so quickly that no one person can be a subject matter expert on all of the latest technologies.

Telecommunications has become vital to many businesses. Airlines, stock brokers, and financial institutions would shut down if their networks failed. The American Airlines SABRE reservations system is worth more than some small airlines. Financial institutions conduct millions of dollars worth of transactions every minute. These industries cannot afford to depend on outside vendors to provide the telecommunications services so vital to their businesses.

The divestiture of AT&T in 1984 is perhaps the single greatest factor in the growth of private networks. AT&T and its competitors began to offer private T-carrier systems. Several vendors soon offered the multiplexers and customer premise equipment once provided only by AT&T. Business began to obtain network equipment from different vendors. The advantage for businesses was to have more options and better prices for telecommunications. The disadvantage was that their networks contained equipment supplied by different vendors.

Early network management consisted of monitoring transmission links and the computers, modems, and multiplexers in the network. Vendors usually provided a monitoring system for their own equipment. Telecommunications departments soon had different management systems for each type of equipment in their networks.

Modern commercial network management consists of tools and processes to optimize large, complex, and diverse telecommunications networks. A typical network management center has a number of monitors each showing the status of a portion of the network controlled by a separate management tool or system. Network managers are now getting tools to help coordinate these different management systems under one umbrella system.

Commercial network managers expect several functions from network management systems. These include:

- Control of network assets from a single location
- Network status displays in graphical form
- Identification of faults
- Anticipation of faults
- Equipment alarm interpretation
- Network performance measurement
- Billing and accounting functions
- A single database of network information
- Network configuration planning.[1]

There are seven commonly accepted requirements for commercial network management systems. Modern network management systems support each of these seven requirements. Each of these requirements apply in varying degrees to MSE network management. These requirements are:

(1) User Interface. This is the most important element in any information system. The user interface should present information in the most clear and concise form possible. Network management systems typically use a high resolution graphics display with a windowing interface. Most modern user interfaces use object-oriented graphics-based input and output screens and a pointing device.

(2) Application extension. A network management system should be able to take on new applications as networks grow and become more diverse.

(3) Data repository. Every network management system must have some form of a database to maintain current network status and historical data for trend

[1]Holly J. Karr, "Network Management: Current Trends and Future Directions," (Masters Thesis, University of Colorado, Boulder: 1987), pp. 27-35.

analyses. The data repository should be flexible and easily accessed.

(4). Element management translation. Integrated management systems should translate the management information from vendor specific systems to some common representation. This gives network managers a single view of the network and enhances manipulation of specific network devices.

(5) Communications protocols. This requirement is similar to the element management translation requirement. The management systems should communicate with network elements and other management systems using a common protocol. The two major protocols are the Simple Network Management Protocol (SNMP) and the Common Management Information Protocol (CMIP). The MSE Packet Switched Network (PSN) uses the SNMP protocol.

(6) Performance. Performance is a requirement of any information system. A network management system should provide timely information and be responsive to the user.

(7) Costs. Network management systems must be cost effective. Current commercial network management products are expensive. They can cost hundreds of thousands of dollars.

Current network management systems support these requirements at different levels of acceptability. New products meet these requirements better as technology improves, standards become widespread, and customers demand it. The MSE network management system addresses each of these requirements except element management translation.

A trend in commercial network management is to provide customers a single point of contact, called a help desk, for their network problems. Help desks are usually staffed by Information Systems (IS) department members knowledgeable in the topology and workings of the network. The help desk has access to the latest network status information. It also serves to inititate actions by the problem management system.

Many firms co-locate their help desks with their network management center. A customer with a problem can call the help desk line to report the problem and possibly resolve it while on the phone. The help desk operators usually have a network management terminal that can show the network's overall status or the status of an individual node. The operator always starts a *trouble ticket* which helps keep track of the problem until resolution and becomes an entry in a historical problem file. Some MSE units are experimenting with help desks and trouble tickets.

Commercial Network Management System Architectures

Most commercial and military network management systems fall into one of four types of management architectures. These architectures are:

a. Universal Interface (figure 4-1)
b. Manager of Managers (figure 4-2)
c. Network of Managers (figure 4-3)
d. Platform[2] (figure 4-4)

[2]James Herman, "Enterprise Management Vendors Shoot it Out: Will End-users Get Caught in the Crossfire?" Data Communications, November, 1990, pp. 234-243.

These architectures represent an evolution of the approaches to network management in the multivendor environment. Chapter V will show that the Army plans to evolve to a Manager of Managers (MOM) network management architecture.

The universal interface approach depends on each vendor following the same communications protocol. A centralized manager controls every managed device directly. This is the approach many SNMP management systems follow. A single SNMP workstation communicates directly with bridges and routers. This approach has the advantage of simplicity. However, many vendors continue to use proprietary communications protocols in their equipment. This approach limits the size of the networks that a single manager can control.

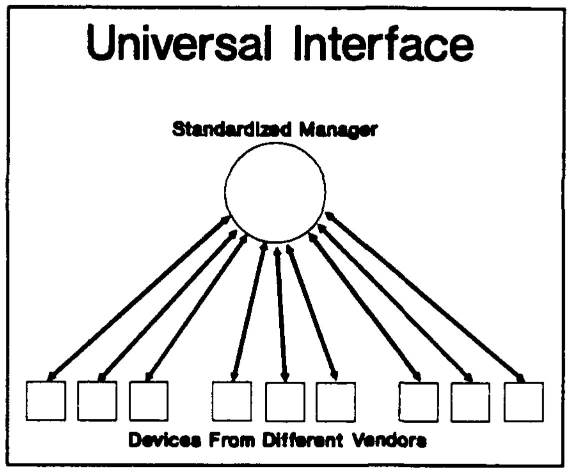

Figure 4-1

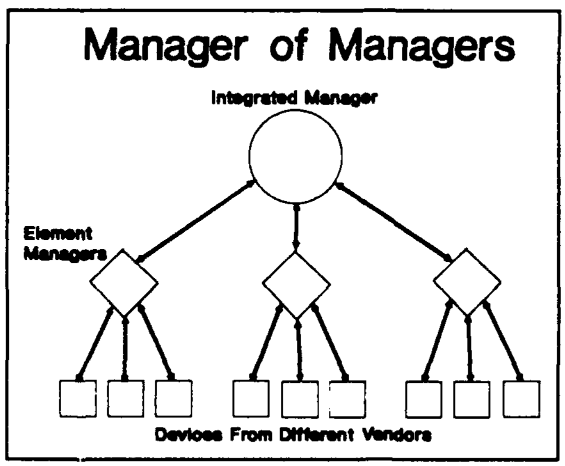

Figure 4-2

The manager of managers architecture distributes the management load to subordinate managers. This hierarchical approach allows vendor specific management systems to work in an overall management system. This architecture is similar to the Army's MSE management architecture.

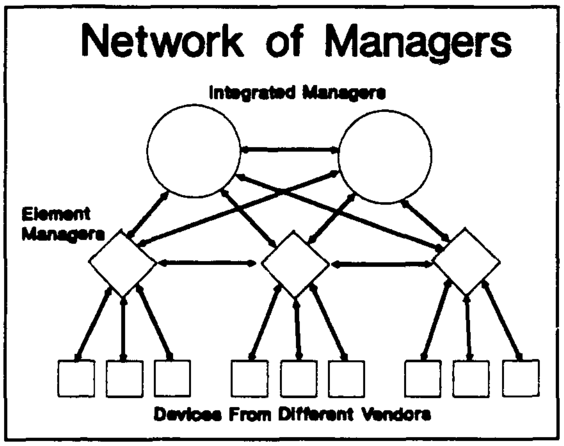

Figure 4-3

The subordinate managers, called element managers, control the devices in their own domain. The element managers are vendor specific management systems that control devices provided by that vendor. For example, if a vendor provides the Private Branch Exchanges (PBXs) in the network, that vendor likely offers a management system for the PBXs. That PBX management system becomes an element manager in the overall management system. It may use a proprietary communications protocol with the PBXs and a common protocol with the manager of managers. In some cases, the integrated manager can communicate with multiple element managers using different protocols.

There are several advantages to the manager of managers approach. Network managers can develop an integrated management system faster by taking advantage of existing element managers. The approach also protects vendors who insist on maintaining proprietary protocols. It also distributes the management load. A disadvantage of this architecture is that network managers will likely have to bypass the network management system and use the element managers to troubleshoot managed devices. This approach encourages the continued proliferation of proprietary management protocols.

The MSE management architecture is similar to the manager of managers approach. The element managers are the node centers. Each node center controls the switching and transmission equipment located at the node center. Node centers also control the extension nodes which connect to the node centers. Each node center reports to the System Control Center which is responsible for their portion of the network. The MSE management architecture differs from the commercial approach slightly because it depends on human input at each level while the commercial approach is mostly automated.

A network of managers architecture allows for distributed network management at the highest level. This enables businesses to manage their networks from several locations with each manager having the same view of the network. This method improves on the advantages of the hierarchical approach but has the same disadvantages.

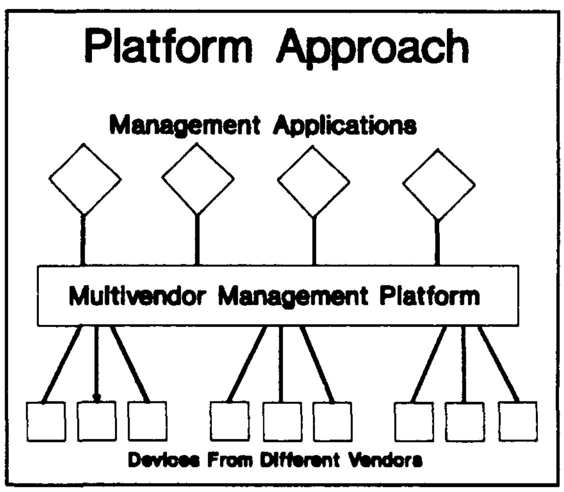

Figure 4-4

The best approach to network management with available technology is the platform architecture. In this approach, a standard platform handles the system level mechanics of reading, writing, displaying, and storing management data. The platform provides *software hooks* for vendors to attach their applications. Vendors can concentrate their efforts to value added services and leave the basic system functions to the platform. This approach is similar to the Microsoft Windows ® environment for personal computers. Windows handles common system level functions and provides software hooks for vendors to write applications programs. The platform approach to both network management and personal computers has encouraged standardization.

There are five major vendors that offer integrated network management systems. There are many vendors offering systems that manage their specific products.

Table 4-1 summarizes the integrated network management products offered by these vendors. The purpose of Table 4-1 is to show some of the characteristics of the available systems. The table uses terminology not explained in this thesis but is common to the information systems and telecommunications fields.

Table 4-1

Current Integrated Network Management Products[3]

VENDOR	IBM	AT&T	HP	Digital Equip Corp	SUN
Product	SystemView NetView	UNMA ACCU-MASTER	Openview	EMA	SunNet
Focus	Networks & Systems	Networks (Public & Private)	TCP & OSI Networks	Dist. systems	Work-groups
Protocols	Proprietary SNA	Early version of CMIP	SMIP, SNMP	CMIP, SNMP	SNMP
Open/Closed Architecture	Extendable, published specs	Closed	Open API specs	Open APIs	Open APIs
Architecture	Mainframes with workstations	Single mini w/ workstation	Dist Servers, X Windows	Dist VMS Nodes	Dist agent & Servers
Operating Systems	MVS, VM, VSE, OS/2	System V Unix, MV, MVS	HP, Unix, DOS	VMS, MVS, VSE	SunOS
User Interfaces	3270, S/390, Presentation Mgr	OpenLook on Sun workstation	X.11, OSF, Motif	DEC WIndows	Open Look, X.11
Database	DB2, Info/Man	Informix	None	Object Oriented	None
Hardware Platforms	S/370, AS/400, PS2	3B mini, Sun workstation	HP 9000, X Terminals	VAX WSs	Sun WS
Automation Features	Tables, scripts	Scripts, Expert System	None	None	None

[3]Herman, p. 233.

Why Commercial and Military Network Management is so Different

Military network management is quite different from commercial network management. Military networks have different objectives and characteristics than business networks. Also, the communications equipment that makes up the components of the military networks is much different. Finally, the managers of the military and commercial networks are different.

Military networks have different objectives than business networks because they operate in different environments. American national strategy is based on projection of military power to anywhere in the world. The Signal Corps must be able to deploy networks in force packages with combat and combat support units. They also must expect to connect to US Air Force and Navy networks, Allied networks, and a host nation's telecommunications infrastructure.[4]

The objectives of military networks are continuity, security, versatility, and simplicity. To achieve continuity, the networks must be survivable, reliable, and redundant. Security involves physical and information security, dispersion of important assets and a means of deceiving the enemy. Network managers must plan for flexibility, interoperabilty, and autonomy of the networks to achieve versatility. Simplicity involves making sophisticated networks simple to operate, use, and connect to other networks.

Although businesses and the military use telecommunications to gain

---

[4]"Signal 2000: White Paper on Signal Support for AirLand Operations in the 21st Century," (Department of the Army, US Army Signal Center, Ft Gordon, GA, October 9, 1991), p. 4.

competitive advantage, businesses have different goals for their networks. Businesses share the goals of continuity, security, versatility, and simplicity but also must balance these goals with costs. Although military networks must be cost effective, their primary objective is to provide communications under the worst of circumstances. Businesses have the luxury of backing up their networks with multiple long distance providers when considering the costs of providing continuity. Businesses cannot justify high costs for ruggedized networks when less expensive options are available. The business environment is highly competitive but it is not lethal.

Military networks are more fluid, temporary, and deployable than most commercial networks. Business network managers reconfigure their networks as new requirements come up. Military network managers reconfigure their networks constantly as customers move to new locations. Military networks usually remain active only for the duration of a military operation while commercial networks remain active continuously for years. Military networks deploy with their customers anywhere in the world. Military network managers often have only days to plan and engineer their networks.

Military and commercial networks have different equipment with different levels of complexity and automation. Commercial networks often use state of the art components while military communications equipment is rugged and simple. Soldiers can troubleshoot most of the newer communications equipment by pushing a built-in test button and exchanging circuit cards The military usually purchases its communications network equipment from a single contractor while businesses often purchase equipment from multiple vendors.

Business and military networks operate at different data rates. Most American commercial data rates are based on multiples or fractions of the AT&T T-1 (1.544 MB/s) standard. Military networks are based on data rates in multiples of 16 KB/s.

Perhaps the most significant differences between commercial and military network management is in the people who manage the networks. Most commercial network managers have years of experience. They often come from their firms' information technology departments. Commercial network managers are usually professionals who have made careers out of network management.

Army network managers are Signal Corps officers and Non-Commissioned Officers (NCOs) who only have the job for two to three years. Military officers and NCOs hold many different jobs in their careers and can hurt their careers by remaining in one job for longer than three years. They learn to manage networks in short (2-3 week) courses or as a small portion of their basic and advanced training courses at Ft Gordon, GA. Military network managers are no less professional than their civilian counterparts but usually have less experience in network management.

The problem of experience is often more severe in National Guard and Army Reserve signal units. These units do not have the opportunity to train as often as active duty units. National Guard and Reserve network managers usually remain in their positions longer than active duty network managers. However, MSE is too new for them to have gained enough MSE experience to become experts.

The differences between commercial and military network management make it difficult to adapt a commercial network management application to MSE network management. Military networks are more dynamic, less sophisticated, and more temporary from commercial networks. Military network management systems must operate in more hostile environments than commercial systems. Although military networks are different than commercial networks, they can benefit as much from AI-based network management tools.

MSE Network Management

US Army doctrine divides all Army telecommunications network management into three functions:[5]

- Planning
- Engineering
- Controlling

Every network management related task falls into one of these three functions. Theses three functions relate to each of the five commercially accepted functions of configuration, fault, performance, security, and asset management.

Army Field Manual (FM) 11-38, MSE System Management and Control, sets the general guidelines for how network managers manage MSE networks.

---

[5]Signal Support in the AirLand Battle, (Department of the Army Field Manual 24-1, October 1990), p. 4-7.

The remainder of this chapter describes MSE network management based on FM 11-38 but described in non-military terms. The description of MSE network management is in a form that supports a future analysis of MSE network management as an initial step for developing AI-based network management tools.

MSE network planning is the process of determining in advance what services MSE signal units will provide to customers and how the signal units will provide those services. The network managers usually plan the initial network before deploying the signal units. The managers plan the:

- Initial network topology
- Locations of the node centers
- Most likely network reconfigurations
- Contingency plans for emergency situations
- Gateways to other networks
- Logistical sustainment of the MSE teams.

The managers develop the plan based on the maneuver commander's intentions. They also update or rework the plans as they need to reconfigure the network to support changing situations.

Network engineering is the process of providing the technical details of the plans. It is the detailed empirical portion of network planning. Planning and engineering are overlapping functions. The engineering process determines:

- Azimuths of each LOS radio link.
- Frequencies for all LOS and SHF radio links.
- Predicted free space radio fading of all LOS radio links
- Details of the encryption key plan
- MSRT frequency plans

The network managers engineer the MSE system as part of the pre-deployment planning and as they reconfigure the network in the field.

Network control is the process of monitoring the network for compliance with standards and making changes to the network when needed. The extension node teams report their status information to the node centers. Node center managers collate this information and report their node center status to the System Control Center (SCC). The network managers analyze all of the network status information to determine if the plan is working and to make changes as needed.

Once the network is working, the network managers monitor the network for problems. They also watch the tactical situation to determine when to reconfigure the network. The network managers re-deploy the network at the end of an operation in a logical sequence to provide communications to the key customers as long as possible.

MSE network managers manage the MSE network in four phases:

- Phase I: The pre-deployment planning
- Phase II: The initial move to the area of operations and the establishment of the backbone network
- Phase III: The establishment of the extension nodes and gateways
- Phase IV: The ongoing operations of the network as the mission evolves.

Figures 4-5 and 4-6 depict the current MSE management process. The boxes represent the external elements that interact with the management system. The network managers communicate with the signal

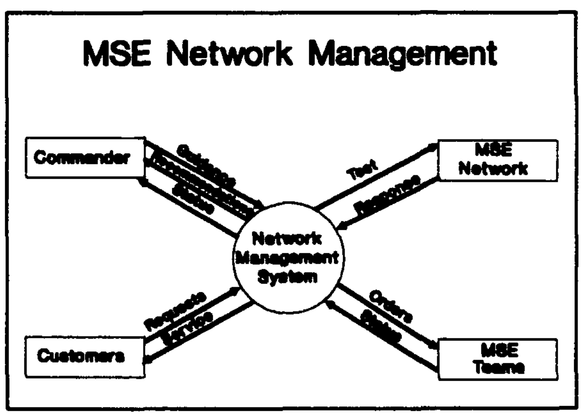

Figure 4-5

commander, customers, MSE teams, and the MSE network. The arrows represent the data sent to and from the network management system.

The signal commander provides guidance to the network managers in the form of mission statements, special orders, the maneuver commander's intentions, and the tactical situation. The network managers use this information to develop a recommendation for the commander. If the commander approves the plan, the managers implement it in the form of orders to the node centers.

The customers send requests for communications service to the network managers. There is a signal officer in each supported unit who coordinates the support requests with the network managers. The unit signal officers inform the network managers of their planned unit command posts locations and special communications requirements. The output from the network management system to the customers is MSE telecommunications services.

MSE teams provide the network managers the status of their equipment and personnel. The Small Extension Node (SEN) and Radio Access Unit (RAU) teams relay this information through the node centers. The network managers communicate orders to the node center managers to open and close links, move to new locations, and to report specific information. The managers use this information to keep from over-committing MSE teams short of equipment or personnel. The managers also use the status information to determine the state of the network and to identify faults.

The network managers test the MSE network to verify the status information they get from the node centers. They can test the network by dialing up switchboard operators and Group Logic Units (GLUs) located in each Radio Access Unit (RAU).[6] Network managers also call Mobile Subscriber Radio Terminals (MSRTs) at known locations to check the RAU coverage. The managers infer knowledge about the state of the network from the responses they get from testing the network.

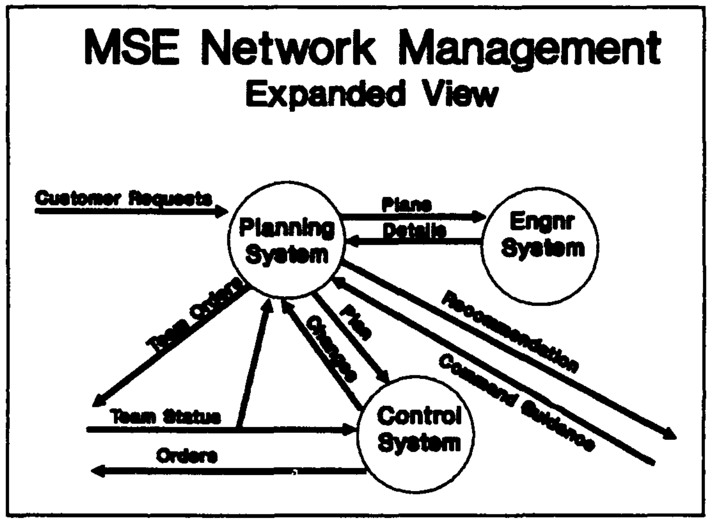

Figure 4-6

Figure 4-6 shows the interaction of the three sub-systems of the MSE network management system. Each subsystem represents one of the network management functions and is a combination of the network managers and their management tools that perform a certain class of tasks. The subsystems are separated only to show the different tasks performed by the same managers using the same tools.

The planning system uses the commander's guidance, customer requests, and team status to develop a recommendation for a network plan. Once the

[6]Soldiers have discovered that an affiliated Group Logic Unit (GLU) will respond with a low pitch sound when dialed up on a voice circuit. This test has been nicknamed *"burping the Rau."*

commander approves the plan, the engineering system fills in the details such as frequency assignments. The planning system completes an operations order and team packets for every MSE team. An operations order describes all details about how the network will be installed and operated. Team packets contain the specific instructions for each team. MSE teams and customers use the operations order to determine their specific roles in the communications network.

The control system uses the commander's guidance, the plan, and the MSE team status information to monitor the network. The control system takes remedial actions when the network is not progressing according to the plan. It also provides a status of the network to the commander.

MSE Network Planning

The network planners do their planning as far in advance as possible. They try to plan and engineer the network and prepare the orders before the MSE teams leave their motor pools or assembly areas. Figure 4-7 shows the major processes in MSE network planning.

All Army planners consider each factor in the acronym METT-T during the planning process. METT-T stands for Mission, Equipment, Troops, Terrain and weather, and Time available to plan. The equipment and troops information affect what the signal units' capabilities are and what special planning factors they have. Terrain affects the network topology and placement of the Radio Access Units (RAUs). Weather affects the time to move the MSE teams and install the network. Time available affects the detail and quality of the plan. AI-based tools can have

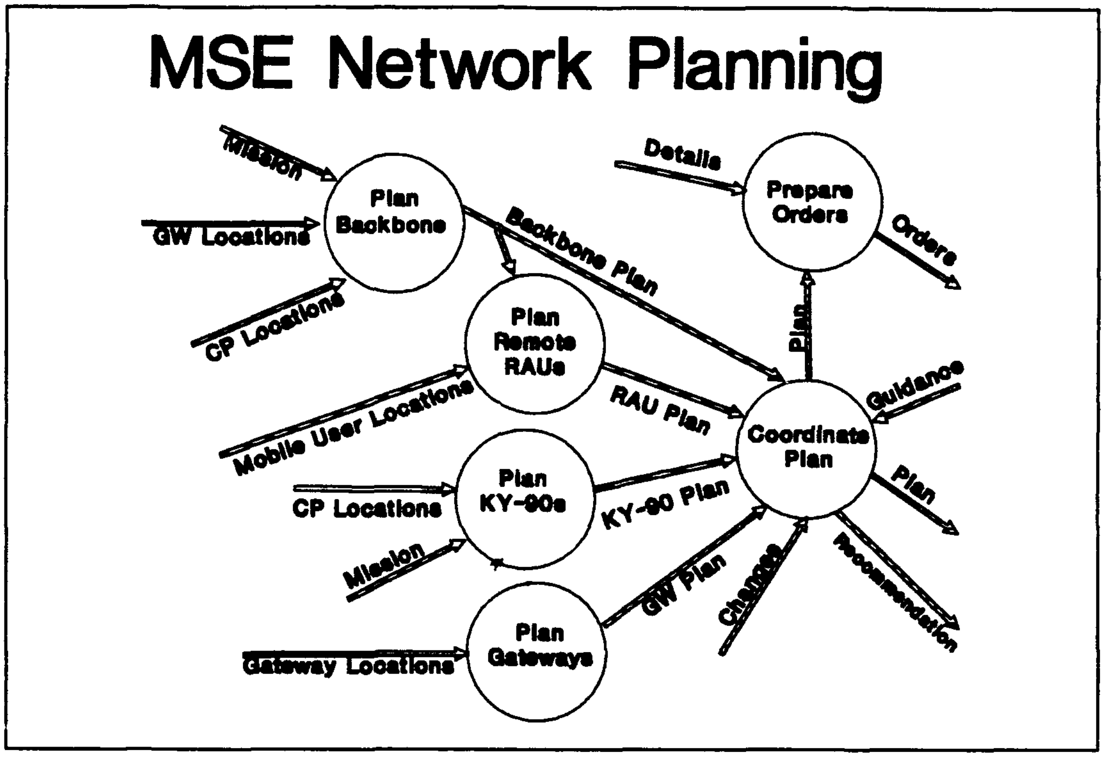

Figure 4-7

the greatest impact in the planning process on the time it takes to plan.

The network managers begin the planning process with an analysis of the mission and the commander's guidance. Typical missions vary from large corps size combat operations to small brigade size training exercises. The managers determine how many MSE teams will be needed to participate to meet the mission requirements. They also analyze the maneuver commander's intentions to determine the likely reconfigurations of the network. The commander's guidance usually states the priorities for MSE service to the customers.

The network managers coordinate with the unit signal officers to determine the initial locations for every command post. This information dictates the initial locations for small and large extension nodes. The managers also find out the initial operating areas and main re-supply routes used by the mobile users. They use this information to determine where RAU coverage will be critical.

Once the managers determine the locations of the SENs and LENs, they plan a backbone network that provides line of sight connectivity to the extension nodes and redundancy for call routing. The managers have to plan for the backbone network to connect to other networks such as theater level communications, adjacent MSE networks, or host country facilities.

The managers plan the backbone network using special heuristics. They first analyze locations for node centers that were used in the past. If they cannot design a backbone network that uses previously used sites, the managers search for other potential node center sites. The network managers use topographical maps and the SCC's high point database to look for potential node center locations.

The network managers analyze each potential site to see if a node center can deploy the site and install LOS links to other sites. They check the terrain profiles using the SCC computer to see if the backbone links and links to extension nodes will work. The task of computing line of sight paths between sites falls under the engineering subsystem. The network or node center managers often conduct a physical site reconnaissance if possible to insure that the signal unit has permission to use the site and that there are no obstacles to heavy vehicles. (Note: In peacetime, units must get the landowner's permission to use a site. In both peacetime and in war, the units must obtain authorization from the higher unit headquarters to use a site to insure other units or weapon systems are not affected).

Once the managers complete the backbone plan, they plan where to place remote RAUs. There are often gaps in RAU coverage because of the distances between node centers, terrain, node centers without operational local RAUs, and because node centers do not locate near combat units. The network managers use topographical maps and RAU range templates to predict where there will be gaps in coverage. They also use the command post locations and the road network patterns to predict high concentrations of MSRTs. The network managers insure that most MSRT users will be covered by a RAU and that no more than fifty MSRTs will be served by one RAU.

The network managers analyze the customers' command post locations and the mission to determine where to place the KY-90 Combat Net Radio Interfaces (CNRIs). There are only enough KY-90s to put one in every fourth SEN. They have to be placed at the critical locations which can vary with each mission. The signal commander usually sets the priorities for the KY-90 plan in the commander's guidance. The managers plan which SENs and LENs will have a KY-90 and what telephone numbers to assign each KY-90. The managers also coordinate with the units to insure the MSE teams will have the correct CNR frequencies and call signs.

The gateway plan sets the methods and priorities MSE teams use to install gateways. Gateways are places in the MSE network that link to other networks. A gateway may be to a nearby but separate MSE network. There also may be an

Echelons Above Corps (EAC) network which the MSE network must connect to at specific locations. The gateways are usually to other digital networks but can be to analog networks. The managers have to coordinate the equipment settings such as data rates, timing, routing tables, or area codes between the MSE teams and the other networks.

The network managers can plan most of the gateways as LOS radio links. However, other types of gateways are not as easy to plan. Gateways to an allied army's network require a NATO Analog Interface (NAI) to convert the MSE digital signals to NATO standard analog signals. The planners can locate these gateways at node centers or at remote locations. The remote NAI teams connect to a node center through an LOS microwave radio link.

The network managers coordinate the different plans to complete a recommendation to the commander. They also consider changes to the plan due to team status changes or network faults. The managers present their recommendations to the signal commander only after they insure there are no conflicts between the plans and that the plans will support the customers' needs.

Once the commander approves the plan, the network managers go through the engineering process to fill in the details. After they have the details, they prepare the operations order and team packets to present to the commander, MSE teams, and the customers. The operations order is the final product of the initial planning process.

MSE Network Engineering

Network managers conduct network engineering concurrently with network planning. The engineering process fills in the details of the plan. It includes calculating LOS path losses, assigning frequencies and antennal polarization to LOS systems, and assigning frequencies to MSRT frequency plans. The SCC's engineering tools are adequate for most of the engineering tasks.

Figure 4-8 depicts the engineering processes. The input to the process is the network plan. The plan may be incomplete or not yet approved. The process outputs the details back to the planning process. The engineering process communicates only with the planning process.

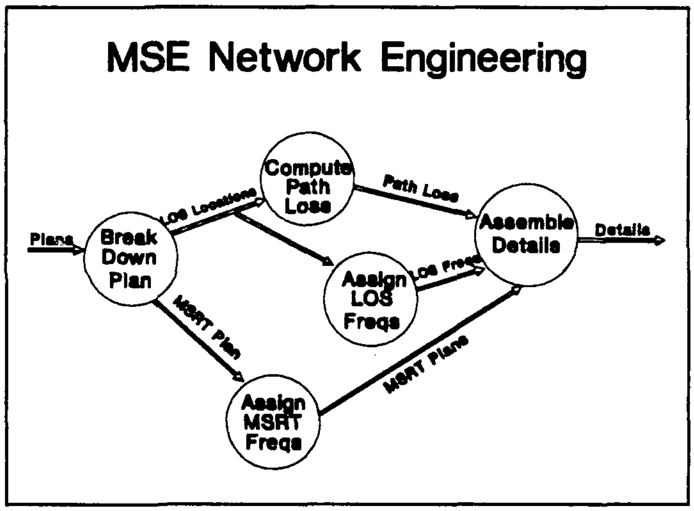

Figure 4-8

The path loss computation process predicts the success of the LOS microwave radio link based on a digitized map maintained in the SCC. The path loss is a function of the distance between the terminals and the frequency band of the system. The algorithm that predicts the path loss assumes that each LOS terminal uses a fifteen meter tall antenna. The SCC uses the digitized map to calculate a terrain profile of the earth between the two terminals. The digitized map shows if the terrain has thick vegetation that can affect the LOS path loss. If the SCC does not have a digitized map of the area, it predicts a path loss by assuming the LOS systems are on flat terrain.

The SCC predicts the success of the system but does not prevent the network manager from planning a link not likely to work. The manager can override the program and force the SCC to assign frequencies and order the teams to install the system. The SCC has a high success rate for predicting LOS paths that will not work Its predictions of successful paths are not as accurate because there are many factors other than terrain that can cause an LOS system not to work.

The network manager allocates the frequencies manually or assigns a block of frequencies to the node managers. The node managers then choose their own SHF frequencies from this block of frequencies. The SCC allocates frequencies to only the LOS microwave radio systems. It does not allocate frequencies for SHF systems. This usually does not present a problem because the SHF radios operate on low power, their radio beams are highly directional, and the systems extend for only short distances.

The SCC assigns LOS frequencies from a pool of authorized frequencies. The network managers obtain the authorized MSE frequencies from other signal agencies such as the Army Frequency Control (AFC), the Federal Communications Commission (FCC), or host nation authorities.

The SCC generates MSRT frequency plans randomly from a pool of authorized radio frequencies. The RT-1539 operates with two frequency ranges which are separated by 20 Mhz. These frequencies fall in the VHF 30 - 88 Mhz range. Each RT-1539 channel uses one frequency in the low band and another in the high. Whether a frequency is the transmit or receive frequency depends on if the RT-1539 is working as an MSRT or a radio in the RAU. The network managers use the SCC to download the plans to a RAU. Once the plans are in a RAU, they can be downloaded electronically to MSRTs and distributed to customers through the unit signal officers.

The final process in network engineering is to assemble the details. These details include network engineering not covered by the other major processes. This includes the encryption key assignments and the time periods that each frequency plan and encryption key assignments will be in effect. It also includes the designations of which teams act as masters and slaves. The engineering process output goes back to the planning process to complete the operations orders.

MSE Network Control

The network control process begins as the MSE teams assemble in their motor pools and continues until the signal commander shuts down the network and sends the teams back to their motor pools. The network managers monitor the status of the network continually to insure the network meets standards, customers maintain communications, and the commander is informed of the network's status.

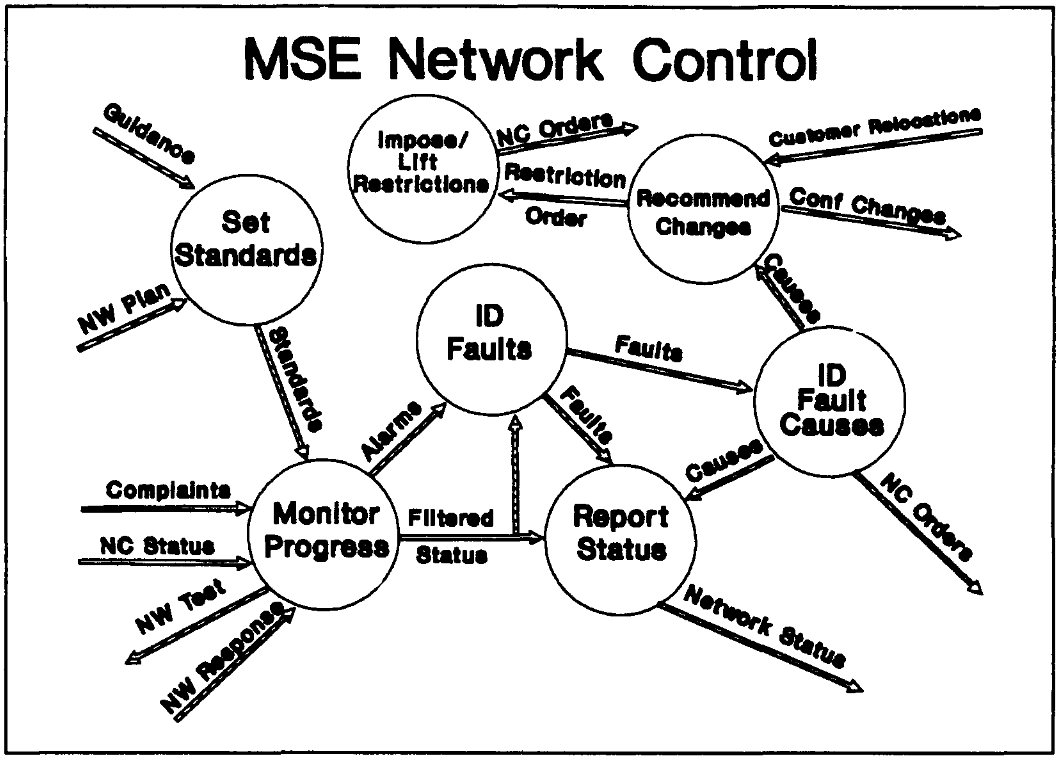

Figure 4-9

The managers analyze inputs from the commander, the MSE teams, customers, and the network to determine if there is a problem or if they need to prevent one. The managers report the state of the network to the signal commander. They send orders to MSE node centers to perform corrective actions or report new information. They also determine changes to the network that should take place and forward these changes to the planning process for new orders.

The network managers set the standards for the network from the commander's guidance and the plan. The standards include the times for MSE teams to open or close LOS radio links. The standards also include quality of service and the conditions that trigger a restriction of services to some customers.

The purpose of the rest of the control process is to insure the network meets the standards.

The managers monitor the progress of the network by analyzing the status information from the node centers and by testing the network. They filter the status data and report the network status to the commander. The managers also initiate internal alerts when the information shows a possible fault.

The network managers also analyze the filtered status information to look for potential faults. For example, if they detect a pattern of MSRT encryption key mismatches, the managers attempt to trace the problem to specific customers or MSE teams. The network managers report a problem to the commander when they detect a fault. They then begin to troubleshoot the fault.

The purpose of the troubleshooting process is to identify the sources or causes of the faults. The managers decide whether to fix the fault or to make a network configuration change to prevent the conditions that caused the fault. They usually direct MSE teams to take specific actions to help troubleshoot the faults.

The managers use the planning, engineering, and controlling processes collectively to manage the MSE network. These processes are overlapping and are performed in real time. The planning process takes place prior to deploying the network but begins again when the control process identifies a needed change. The monitoring process continues as the changes are planned and engineered. The processes may also be done by the same network manager.

Deficiencies in the Present Network Management Process

The current network management process works, but the available tools are inadequate. The network managers do not have modern tools to help aid the planning process other than the SCC's terrain profiling system. There are no tools to suggest good node center and remote RAU locations or to calculate RAU coverage gaps.

Some units have responded by developing non-standard tools to solve their problems. One unit obtained a terrain analysis program called Terrabase to calculate terrain line of sights.[7] Several network managers responding to a survey stated that their units adopted the laptop computer program developed by the 3rd Signal Brigade.

The proliferation of non-standard automation tools in any organization, especially Army Signal units, can lead to more network management problems. The Signal Center does not support these non-standard tools. These tools lead to problems with standardization of network management across the Army and the training of network managers at the Signal Center.

The network managers do not have any tools that monitor and analyze the network status information to spot potential problems. There is no automated telemecry from the node centers on the status of the node center switches, the extension nodes, or the RAUs. There are no tools to help troubleshoot problems or recommend network configuration changes.

---

[7]Interview with a former MSE network manager.

The current system has the potential for expansion. For example, several survey respondents stated that they wished that there was remote access to the NCS printouts from the SCC. One network manager reported that a GTE field engineer used the TELNET program on an SCC workstation to log-on to a NCS workstation and examine printouts. This feature cannot be verified but the packet network documentation states that the packet network supports TELNET.[8]

MSE Node Center Management

MSE node center management is a subset of network management but is significant enough to deserve a separate discussion. The node center is a complex and vital part of the network. The typical node center commander is a twenty-four year old lieutenant with less than two years experience in the Army. He or she usually works with several experienced non-commissioned officers. The lieutenant manages the teams at the node center, four small extension nodes, and a remote RAU. The node center commander must manage these assets and accurately report their status to the network managers at the SCC. Node center management consists of the planning, engineering and controlling processes.

Figure 4-10 shows the inputs and outputs of the node center management system. The top level view of the node center management system looks much like the network management system. The node center commander communicates with the signal commander, MSE network managers, customers, logistics support

[8] MSE Packet Network X.25 Interface Description Appendix SR-43, (GTE Government Systems Corporation, January 5, 1991), p. 7.

teams, and the MSE teams. The node center commander must get maintenance, fuel, food, and personnel support from signal support elements. Network managers seldom deal directly with the support elements as part of the network management process.

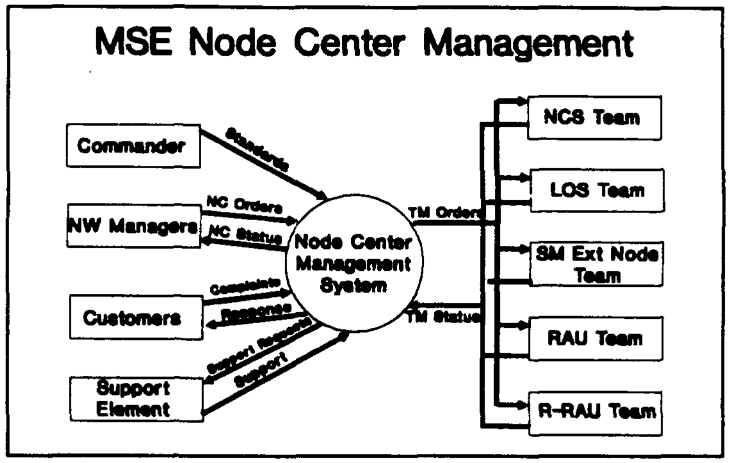

Figure 4-10

Figure 4-11 shows the planning and engineering functions of node center management. Node commanders plan the site layouts of their node centers and engineer the configuration of the NCS configuration database. They receive guidance from the signal commander and specific orders from the network managers. The node center commanders produce their plans based on these inputs. They also send orders to

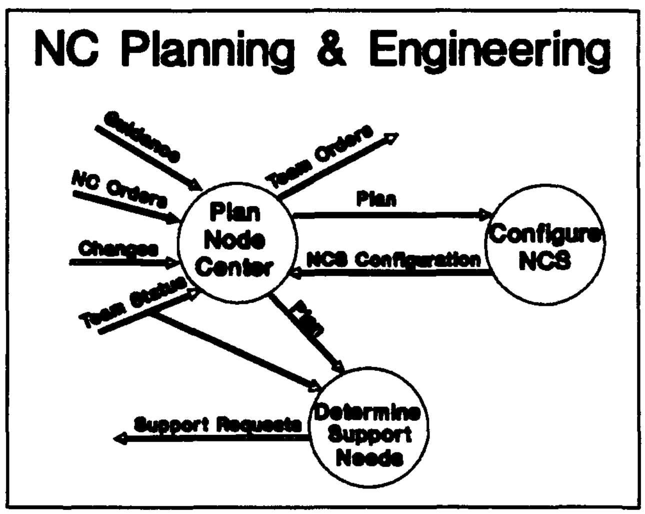

Figure 4-11

the MSE teams under their control.

A node commander engineers the plan by determining how best to configure the NCS database to support the mix of internode, extension node, and RAU links. The commander might modify the standard configuration because of extraordinary commitments or because of the mix of terrain at the site and the directions of each link.

The primary cause of NCS database changes is network reconfigurations after the node center is operational. Network managers change the network topology as unit command posts move to new locations. The node center commander must plan the assignments of the digital trunk groups to the LOS radio terminals so no two radio antennas point in directions that cause their radio beams to cross.[9] He may have to change the NCS configuration to prevent crossing LOS radio systems.

Consider the following example of a situation that would force a database modification: A node center has a link to a Large Extension Node (LEN) due north of the node center. The node center commander assigns MDTG 25 to an LOS terminal on the north side of the site because that MDTG is set up for a LEN link. The network managers later order the LEN to move to a location due south of the site and reestablish the link to the node center. The node center commander will not be able to use the same DTG without turning the LOS antenna due south

[9]Don Rickerson, "MSE Node Center Site Reconnaissance," Army Communicator, Summer/Fall 1990, pp. 22-25.

and shooting over the node center site and other LOS systems. The lieutenant would then have two options:

- Reconfigure the NCS database to install a LEN link on another MDTG
- Break down one or more systems and reconfigure the LOS terminals.

The node center control processes mirrors most of the network control processes. However, the tasks steps of these processes are different at the node center level. The node center commander watches the progress of the node center and the other MSE teams under the control of the node center. The lieutenant must forward the status information to the SCC to keep the network managers informed. He also must identify and troubleshoot problems as they occur. The lieutenant cannot impose communications restrictions on MSE services without directions from the network managers. The node center manager also does not set the communications standards for the node center.

The node center control process is entirely manual (figure 4-12). The lieutenant depends on the NCS switch operator or the extension nodes to tell him if there is a problem. The node center commander is often near the NCS and can hear alarms or the operator talking to other

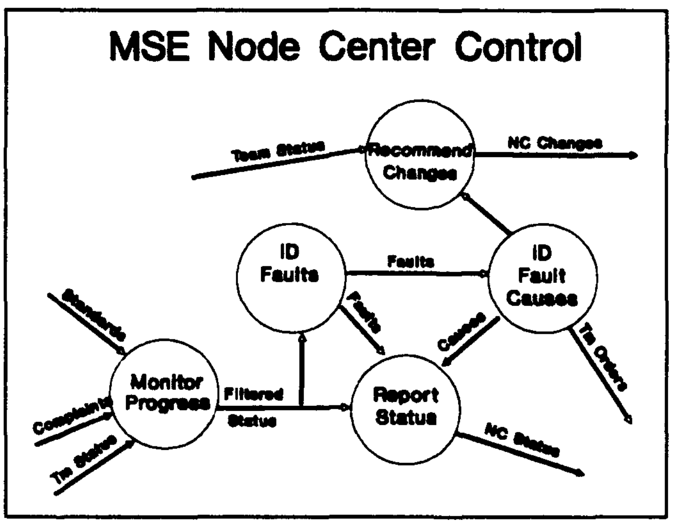

Figure 4-12

teams. The NC commander has to input the status information into a workstation or laptop computer to send the information to the SCC. There is no means to capture status information automatically from the node center equipment or the extension nodes and let the node center commander analyze or forward the information to the SCC.

The NC commander does not have an expert consulting tool to help troubleshoot problems. He uses his non-commissioned officers, technical manuals, personal notes, and standard operating procedures to troubleshoot problems. Typical problems that node center commanders troubleshoot are:

- LOS radio systems that will not come in
- Encryption key mis-matches
- MSRT customer problems
- Customer telephone problems
- RAU frequency plan errors
- Lost subscriber pre-affiliations

The lack of automated information gathering slows the reporting, fault identification, and fault troubleshooting processes. Much of the data that can warn of impending faults or help isolate fault causes is lost in NCS printouts. The node center commander is often overloaded with identifying faults and reporting them to the SCC. Inexperienced managers become frustrated and can affect the effectiveness of much of the network.

Conclusion

The discussion of the MSE network management processes in this chapter has shown that:

- Commercial network managers share a need with military managers for improved network management tools
- None of the commercial network management tools are suited to MSE network management
- The MSE network management process is complex
- MSE network and node center managers need better management tools

Both commercial and military networks have similar goals but different circumstances. Military networks have to operate in hostile environments and commercial network managers must be highly cost efficient. Both military and commercial networks are complex and need network management tools. However, military networks are unique enough to require different kinds of network management tools.

MSE network managers have some management tools but need better ones. The System Control Center (SCC) needs improvement. The node center managers have no automated management tools to help them do their job. The lack of tools slows the network managers who have no sophisticated tools to help manage the overall network. Chapter V will discuss the features network managers need in improved management tools. It will also discuss ways artificial intelligence can be applied to the network management domain in general and the MSE management problem in particular.

CHAPTER V

The Potential for AI based Tools to Improve MSE Network Management

Introduction

This chapter will explore the potential of AI-based tools to help MSE network managers do their jobs better and faster. Chapter IV described the MSE network management process and the deficiencies with the tools now available to the managers. It also showed that commercial telecommunications network managers face similar management problems and there are tools available to help them manage their networks. Unfortunately, those tools cannot be directly applied to the problem of MSE network management.

This chapter will show that newer commercial network management tools are making use of AI techniques. These commercial tools cannot be directly adapted to the MSE domain, but the AI techniques they employ can be applied to MSE tools.

Finally, this chapter analyses how AI techniques can be specifically applied to the MSE network planning, engineering, and controlling processes. The Army recognizes there is great potential for applying AI techniques to network management. The US Army sponsors a great deal of AI research but it has not done much research into how specific AI tools can be applied to managing MSE networks. This chapter explores some of the projects that contractors have developed to demonstrate the potential of MSE network planning tools. The chapter concludes with an analysis of the obstacles to adapting AI techniques to new or improved network management tools.

The discussion in this chapter is divided into the following sections:

- Research Methodology
- Trends in Commercial Network Management Tools
- Trends in MSE Network Management Tools
- Commercial AI-Based Network Management Tools
- Current Research in AI-based MSE Management Tools
    - Communications Planning Assistant (COMPASS)
    - MSE Network Planning Tools (NPT)
    - Enhanced Switch Troubleshooting (EST)
- Analysis of the Potential for AI Tools to Improve MSE Network Management
    - Network Planning and Engineering
    - Network Control
    - Node Center Management
- Justifying the Development of AI-Based Tools
- Obstacles to Developing AI-Based Tools for MSE Network Management
- Conclusion

Research Methodology

The recommendations and conclusions in this chapter are based on three sources:

- Surveys sent to MSE network managers stationed in the United States and Europe
- Interviews with current and former MSE network managers
- The author's personal experience with MSE network management.

The surveys were mailed to each MSE signal unit and distributed to the MSE network managers conference held at Ft Gordon, GA, 30 March - 3 April 1992. Forty percent of the surveys were returned. The responses included the Corps Signal Brigade and at least one Division Signal Battalion from each MSE equipped corps.

The survey questions were designed to identify problems with the current network management system and to get network managers' ideas on how to improve the system. Each respondent was assured anonymity in accordance with the rules of the University of Colorado. Appendix B is a copy of the survey.

The interviews were of qualified group of MSE network management experts. The group included five former and two current network managers. The five former network managers are Army graduate students at the University of Colorado. The two current network managers serve in a Corps Signal Brigade and were interviewed via electronic mail (E-Mail). Each of the five Army graduate students served in an MSE unit during their most recent assignments. Four served in MSE units as part of operations Desert Shield and Desert Storm of the Persian Gulf War of 1990-1991. They served at both the Corps Signal Brigade and Division Signal Battalion levels. Each interviewee has served eight to twelve years in the US Army.

The purpose of the interviews was to determine how they managed MSE networks and what information they needed to manage the networks. Each interviewee was asked how their units employed and managed the MSE system. Each described the problems they encountered with the management system and how they overcame the problems.

The survey respondents and interviewees were largely unaware of how AI tools could help manage networks. Several made suggestions of the type of AI tools they would want to take over time consuming tasks. Their comments proved invaluable in verifying the analysis of MSE network management and identifying the deficiencies of the current management system.

The conclusions reached in this chapter are the author's. They are based on the analysis presented in this chapter. The conclusions include the requirements or capabilities a new generation of network management tools should have. The chapter concludes with a recommendation of what the Army should do to improve its network management situation.

Trends in Commercial Network Management Tools

Commercial network management has been the subject of considerable research and development. The most promising developments are in:

- graphical displays and user interfaces
- rule-based expert systems and neural networks
- object-oriented analysis, design, and programming.[1]

Each of these developments has the potential to improve MSE management as well as commercial network management.

The developments in graphical displays and user interfaces take advantage of the adage that *"a picture is worth a thousand words."* Humans can process more information graphically than with numbers and text. Graphical displays enable managers to scan and check a network status quickly. Well designed Graphical User Interfaces (GUIs) tend can be more intuitive than text-based interfaces. Improved displays and interfaces can reduce the amount of training

[1]Raymond H. Swanson, "Emerging Technologies for Network Management," Business Communications Review, Vol. 21, No. 8, August 1991, pp. 53-58.

needed to use management tools.

The Unix operating system with X-Windows is becoming a de facto standard for network management software development in the commercial sector. The Unix operating system first gained widespread popularity through university research programs and is now popular in commercial research. X-Windows is a graphical interface developed by the Massachusetts Institute of Technology (MIT) and released as public domain software. Many of the new commercial and military network management tools are being developed with this software.

Much of the GUI-based software uses X-Windows for basic windowing functions. Two popular GUI toolkits that use X-Windows library functions are Motif and Open Look. One of these two competing toolkits will likely become a standard for most GUI development.[2] Unix, X-Windows, and the MOTIF or Open Look toolkits promise to shorten software development time for network management tools.

A goal of the graphical displays and user interfaces is to relieve the managers from routine monitoring tasks. Graphical displays can highlight detected or predicted network faults. They also can use a visual or audio indicator to alert managers to look at the display when faults occur. Network managers will be able to concentrate more on strategic network issues and less on network monitoring.

The object-oriented paradigm is also improving network management software. The object paradigm is the combination of object-oriented analysis,

---

[2]Ibid, p. 55.

design, and programming. Two major promises of the object paradigm are that analysts can design software that resembles the real world and that they can save development time by reusing program code. Analysts will be able to design program code objects that represent the attributes and behaviors of network elements. They will be able to re-use the objects in multiple applications. The concentration of program code into reusable objects also promises to aid software maintenance by isolating the effects of software changes to only the objects being modified.

Object-oriented techniques are found in the new network management standards. The CMIP protocol discussed in the previous chapter is a product of object-oriented analysis. Each network element is defined as an object that communicates with pre-defined messages and exhibits pre-defined behaviors. Vendors design their own network element agents as they want as long as the agents exhibit the external behaviors designed for CMIP.

Research in neural networks and Rule-Based Expert Systems (RBES) is based on a recognition that current management systems are reactive rather than proactive. Monitoring systems notify network managers of faults only after they occur. This forces managers to correct faults rather than prevent them. Network managers should have tools to warn them of impending faults and suggest ways to prevent the faults or to mitigate their effects on the network.

Current Trends in MSE Network Management Tools

There are two trends in MSE network management architecture. The first is the improvement of the platforms on which the network management tools run but not the network management processes. The second trend is the concentration of the management functions of different networks into a central facility. These trends can be seen the Army's requirements documents, future communications doctrines, and the products being offered by vendors.

The Army plans to concentrate most of the management functions of three diverse tactical communications networks into one management system. This system will be called Integrated System Control (ISYSCON). The ISYSCON will be a tool to plan MSE, Combat Net Radio (CNR) , and Army Distributed Data System (ADDS) networks. Most of the MSE network planning and engineering functions will be done with the ISYSCON and the network control functions will remain with the SCC.[3] The Army plans to begin fielding ISYSCON to signal units beginning in 1995. The Army has not yet awarded the contract for ISYSCON but the two main contenders are GTE Government Systems Corporation and UNISYS.

The ISYSCON's functional architecture will be a mix of a universal interface and a network of managers. The ISYSCON will directly manage CNR networks and indirectly manage MSE and ADDS networks. The ADDS networks

[3]Memorandum, Department of the Army, Headquarters US Army Training & Doctrine Command, Subject: Required Operational Capability (ROC) for the ISYSCON, dated 26 November 1990, not paged.

will have a network manager similar to the SCC.[4] There will be several ISYSCONs within an Army corps. Each division signal battalion in a corps will have an ISYSCON and the corps signal brigade also will have one. Each of the ISYSCONs in an MSE network will maintain a distributed database and communicate through the MSE Packet Switched Network (PSN).

ISYSCON will not have any AI-based tools initially but the Army plans to incorporate AI-based tools into future upgrades. The plans call for AI tools that will help in network analysis and redesign.[5] The ISYSCON development plan is to encourage vendors to develop AI tools and offer them to the Army.

The Army's current procurement strategy is to buy off-the-shelf tools. It does not define specific management tools but allows different vendors to propose their tools and to choose the best. Although the Army calls for the incorporation of AI tools into the ISYSCON, it has not defined any explicit objectives in the requirements documents.[6]

The current trend with new MSE management tools is to provide tools that perform the same functions on better platforms. Another trend is to concentrate network planning at the ISYSCON and use the SCC primarily for network control. The ISYSCON requirements document shows that the Army plans to put some AI-

---

[4]The ADDS networks have not yet been fielded and the funding for them may also be in jeopardy.

[5]ISYSCON Required Operational Capability, not paged.

[6]Telephone interview with CPT Kholeman, Director of Combat Developments, US Army Signal Center, Ft Gordon, GA, January 16, 1992.

based tools into the ISYSCON, but has not specified what those tools should be or do.

Commercial AI-Based Network Management Tools

The following commercial network management tools demonstrate techniques that may be applicable to the MSE network management problem:

- NYNEX ALLINK
- GTE COMPASS
- KNOBS/TCP

This list is not a complete list of all commercial AI-based network management tools. Each of these tools uses AI techniques to perform tasks that relate to some MSE network management tasks. The ALLINK is the newest of these tools and is the only one developed as a commercial product for sale. It is also an integrated network management system while the others are only network management tools. ALLINK costs about $200,000 depending on options and is in use in several companies today. The others were developed as demonstration projects.

The NYNEX ALLINK is a manager of managers system that processes status information from subordinate element managers to present an overall picture of the network to the managers. It routes all inbound status information through a rule-based expert system to help spot or predict problem areas. ALLINK also maintains a management information base (a database) and provides a sophisticated user interface. The management information base is available though the user interface and the rule-based expert system. The operator stations, management information base, rule base, and communications gateways al! reside on a Local Area Network (LAN).

The rule-based expert system provides two advantages for the ALLINK. First, it makes tailoring the system to individual customers easy. The system uses rules that apply to the customer's specific networks. The rule base is an open system that allows the customer access to the rules. The second advantage of the rule-based system is that it makes maintenance of the system easier. The customer can add more rules as the network evolves.

The rule-based approach creates a performance trade-off. Any application written with a rule-based system also can be coded in a procedural language to run faster. A rule-based system requires a high performance processor to run at an attractive speed. However, a rule-based system is easier to maintain than a procedural code system. British Telecom's Concert management system, a competitor to ALLINK, initially used a rule-based expert system. However, British Telecom replaced the expert system with procedural code to make it run faster.[7]

ALLINK has several other features that would be desirable in an MSE network management tool. These features include:

· Filtering of unwanted messages from lower level managers to prevent

---

[7]David M. Rappaport, "Carrier Approaches to Integrated Network Management," Business Communications Review, Vol. 21, No. 6, June 1991, p. 34.

inundating network managers
- Collapsing of multiple related event messages or alarms into a single alarm
- Prioritization of alarms into five levels of severity
- Icon representation of network objects on the graphics display
- Text display of all relevant data on an object when the user clicks the mouse on the object
- Context sensitive help screens to aid the operators
- Archival of all messages, events, and alarms for later analysis
- On line capability to modify the rule base.

COMPASS (Central Office Maintenance Printout Analysis and Suggestion System) is an expert system that analyzes the output from the GTE No. 2 EAX analog central office switchboard to detect faults and suggest maintenance actions. The GTE COMPASS was developed in 1985 as a research project. GTE wanted to learn if AI techniques could be developed and used effectively. This was a task actually performed by experts who periodically reviewed switchboard printouts to look for faults.

COMPASS is an off-line tool that stores switchboard maintenance printouts and analyzes them in a batch mode. It sorts the messages into groups of messages likely to be related to the same faults. COMPASS analyzes the groups of messages to determine if faults exists and their causes. It then prioritizes the faults and suggests maintenance actions to repair them. It also recommends preventive maintenance actions to head off predicted faults.

COMPASS uses a frame-based knowledge representation scheme and a forward chaining search algorithm. It creates a frame for each possible fault. The forward chaining inference engine examines the messages and attempts to create a frame for each suspected fault. COMPASS examines the frames after all the rules have been applied to determine which frames are complete enough to represent actual faults.[8]

KNOBS/TCP (Knowledge-based Network Observer/TCP) is an expert system tool that monitors and diagnoses problems in TCP/IP networks. It analyzes data gathered by various internet monitoring programs. The KNOBS/TCP project relates to MSE network management because the MSE Packet Switch Network (PSN) is a TCP/IP-based network. KNOBS stands for Knowledge-based Network Observer.

KNOBS/TCP uses an object-oriented knowledge representation scheme and a blackboard architecture. A blackboard architecture is a system of several knowledge systems that share data about a problem. TCP/IP network problems are usually combinations of multiple problems. The KNOBS/TCP knowledge sources infer information about specific domains and contribute to a common database known as a blackboard. A central scheduler assigns time to each knowledge source based on an overall strategy.

KNOBS/TCP works as an advisor to help experts diagnose problems faster. It can also help tutor novices in diagnosing system faults. The system does not attempt to take over the control of a TCP/IP network from human operators but acts as an expert fault diagnostic tool.[9]

---

[8]Jay Liebowitz, Expert System Applications in Telecommunications, (New York: John Wiley & Sons, 1988), pp. 18-23.

[9]Bruce L. Hitson, "Knowledge-Based Monitoring and Control: An Approach to Understanding the Behavior of TCP/IP Network Protocols," in Eric C. Ericson,

These network management tools each show techniques or features that should be considered for an MSE network management system. The NYNEX ALLINK features a rule-based system that is open to the customers to modify or update. The GTE COMPASS tool shows that it is possible to design an AI tool to analyze switchboard printouts. The KNOBS/TCP tool shows there already exist AI-based management tools for TCP/IP networks, that a management tool can help network managers diagnose problems faster, and a management tool can help tutor novice network managers.

Current Research in AI-based MSE Management Tools

There has been some research into AI tools to help manage MSE networks. Most of this research has been done by vendors hoping to sell the Army their products. One project was developed by the US Army Signal Center to explore the potential to use AI in MSE network planing. The major AI-based network management projects to date are:

- COMPASS (Communications Planning Assistant)
- Network Planning Tool (Mitre Corporation)
- Enhanced Switch Troubleshooting (GTE Government Systems Corporation)

· Communications Planning Assistant (COMPASS)

The COMPASS project was a demonstration of the potential for AI to enhance communications planning. It was developed by a special project officer within the Directorate of Combat Developments at the US Army Signal Center, Ft

---

Lisa Ericson, and Daniel Minoli (eds.), Expert System Applications in Integrated Network Management, (Norwood, MA: Artech House, Inc., 1989), pp. 170-181.

Gordon, GA, during 1986-87. The Army's COMPASS project is not related to the GTE COMPASS project. The Army's COMPASS program ran on a Symbolics 3600 workstation and was written in a language called Common Lisp. The Signal Center abandoned the project when the project officer left the Army in 1988. There is no program code and little documentation left on the project.[10]

COMPASS was designed to help an MSE network manager plan a network and produce an operations order. It used a color graphical terrain display based on a digitized map of the area of operations. It represented MSE network teams with icons. The aim of the COMPASS software was to develop a network topology plan and to produce a printed operations order based on the plan.

The user planned a backbone network by placing extension node icons at the map locations where customers planned to locate their command posts. The user then placed node center icons where he believed the node centers could maintain line of sight with other node centers and extension nodes. The computer would automatically compute line of sight terrain profiles to each adjacent node center, extension node, and RAU. The computer would represent each good line of sight link with a solid line between sites. The computer would recalculate line of sight links each time the user moved the icon with a mouse.

The computer would create and print an operations order shell based on the network design once the user was satisfied with the layout of the network. The

[10]Telephone conversation with Mr. Dave Duke, Directorate of Combat Developments, US Signal Center, 16 January 1992.

program used a database of the MSE teams and their status to assign missions to specific teams.

The operations order shell provided by COMPASS was a starting point for a complete operations plan for an exercise. It contained the technical details of the MSE plan. A signal operations order also includes details of logistics support and the commander's intentions. However, it is much easier to develop an operations order if the technical portion can be automated.

The COMPASS project was never expanded to include all of the MSE engineering processes. It did interactively calculate terrain line of sight profiles but did none of the other engineering functions such as frequency assignments.

One can debate whether or not the COMPASS project was an example of artificial intelligence. It used an object-oriented knowledge representation scheme but did not search a state space to solve a problem. A true AI program might have suggested a distribution of node centers and radio access units based on the locations of the extension nodes. It might also help the user develop a plan and then evaluate the plan using an expert knowledge base.

COMPASS was only a demonstration of the potential of an AI system but it offered more capabilities than any of the tools available to network managers now. It is unfortunate that there is nothing left to salvage of the COMPASS project that could be used as a start point for another tool.

· MSE Network Planning Tool (NPT)

The MSE Network Planning Tool (NPT) is a an AI-based tool to help network managers plan the initial topology for an MSE network. It will provide several of the features of the earlier COMPASS project. The NPT is being developed by MITRE Corporation under a contract from the US Army Communications-Electronics Command (CECOM).[11] The NPT will link electronically to the SCC to help the network managers prepare the orders and initialize the SCC with the initial network topology.

The Network Planning tool will help the user to develop a network plan. A plan consists of the layout of the node centers, LENs, SENs, and RAUs. The program provides a terrain display as the background for the user to place network elements with either a pointing device or by text input. The initial user input to the program consists of the customers' and extension node expected locations. The user also designates areas of high MSRT densities with a mouse.

The NPT and the user interactively plan the network topology. The program can suggest a node center location in an area the user defines with a mouse. The suggested location is the optimal location to link to other MSE elements. The user can drag team icons to refine locations. It automatically suggests links to adjacent node centers and extension nodes. The NPT also suggests RAU locations based on the MSRT densities defined by the user.

The NPT will work with another planning tool called the MSE FURIES to engineer a completed plan. FURIES (Frequency Utilization Resource Integration

[11]Telephone interview and subsequent correspondence with Mr. Kevin Kelly, Mitre Corporation, February 11, 1992.

Engineering System) is a program that inputs a network plan in the form of a database file from the NPT. FURIES will compute terrain line of sight profiles, assign frequencies to the LOS systems and Radio Access Units, and conduct an electronic warfare threat analysis of the plan. It outputs the engineering plan back to the NPT in database files. Figure 5-1 depicts the relationships and information flow between these tools. The Army hopes to enable the FURIES to initiate SCC projects to update the SCC database and print the team orders based on the completed plan.

Although the network planning tool will provide the network managers a better planning tool, it does have some shortcomings. NPT will not evaluate a plan and suggest potential problems. (FURIES will conduct an electric warfare threat analysis based on frequencies used and enemy capabilities). NPT will not use actual equipment or team status data from an SCC's database to prevent network managers from over-committing teams, although NPT may gain this capability as development continues. The NPT will not help the network managers complete some of the details of the plan like assigning Pre-Affiliation Lists to node centers or allocating KY-90s to SENs. The NPT however shows the Army remains committed to improving MSE network managers tools.

· Enhanced Switch Troubleshooting (EST)

GTE Government Systems Corporation is developing the Enhanced Switch Troubleshooting (EST) as an improvement to the workstation in the node center switch. EST is in the development stage and GTE cannot release much information on the project. The Army has shown interest in EST but has not made any commitments.[12]

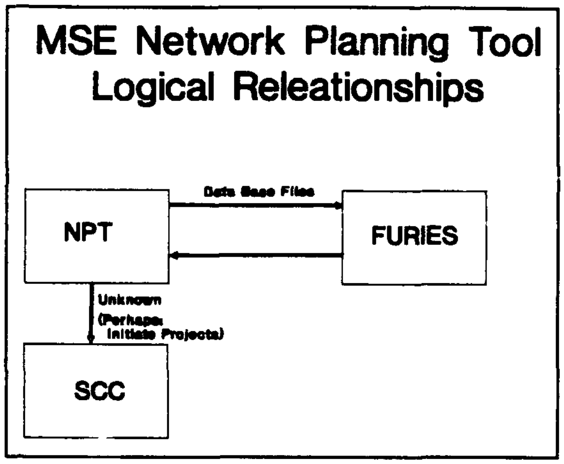

Figure 5-1

The literature available from GTE states that the EST will use expert system techniques to help the NCS operator identify and troubleshoot faults. It monitors all of the switchboard messages to identify and prioritize faults. Then, the EST will guide the operator through the steps to troubleshoot faults. The system will use expertise acquired from Army node center switch experts and GTE engineers. It will also use an on-line technical manual based on the current paper-based manuals.

EST will also have other desirable features that are likely to be based on conventional or object-oriented program code. The first feature is the translation of the switch messages to graphic displays. The advantages of graphic displays were discussed earlier. The second feature is the extensive use of Graphical User Interfaces (GUIs) for operator input. Figure 5-2 shows what GTE expects EST's screen to look like. The third conventional feature of EST will be the ability to

---

[12]Telephone conversation with Mr. John Hoaglund, US Army Communications-Electronics Command (CECOM), 5 February, 1992.

archive all the switchboard messages.

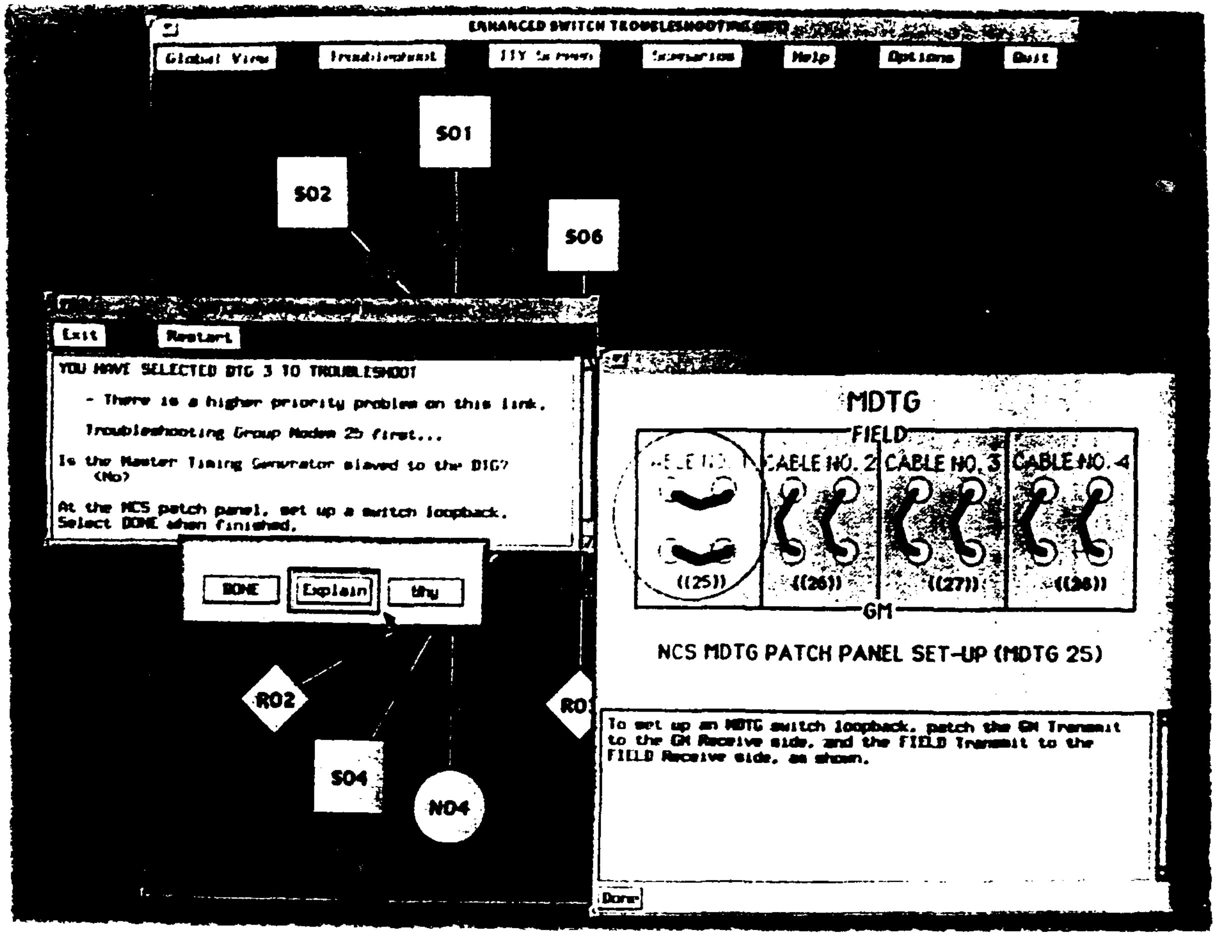

Figure 5-2

There are two important features that EST either does not have or cannot be determined to have from the available information. The most important missing feature is the automatic telemetry of status data from the EST to the SCC or another central network management tool. Another important missing feature is the capability to update the expert system's rule base with new or improved knowledge. These two features are important for effective network control.

The EST project represents a serious effort by GTE to improve the NCS operator's ability to manage the node center switch. GTE is taking advantage of improved AI and object-oriented technology to make an effective tool. EST shows that GTE is willing to explore the use of AI in network management tools. GTE will likely use similar technology to improve the SCC.

Analysis of the Potential for AI Tools to ImproveMSE Network Management

This thesis has introduced the MSE network management process and the special problems that network managers have in managing networks. It also introduced the basic concepts needed to understand artificial intelligence and telecommunications network management. This section will analyze the realistic potential for AI-based tools to enhance network management.

The reader should keep in mind that the major consideration in evaluating the potential to improve MSE network management is cost. The US Army is in an era of tight resource constraints. The budgets for all of the military services are expected to be cut significantly in the near future as the country scales back its military forces. The reduction of budgetary resources makes the development of expensive management tools unlikely. However, it also highlights the need for improved tools because network managers will have to best use the available resources.

MSE Network Planning and Engineering

Artificial intelligence-based tools can significantly improve MSE network planning and engineering. Network planning and engineering is a computation intensive process. Network managers could use AI-based tools to plan MSE networks faster and with fewer people.

Planning the backbone network and the remote RAUs are the most time consuming tasks in network planning. The backbone network plan depends on the maneuver commander's intentions, the locations of the customers' command posts, and the concentrations of Mobile Subscriber Radio Terminals (MSRTs). It forms the base for the entire network plan. The remote RAU plan depends on the backbone plan, the MSRT customer's locations, and where the gaps in local RAU coverage form. The KY-90 and gateway planning processes are minor compared to the backbone and remote RAU planning.

What degree to automate MSE network planning?

It would not be realistic to expect to fully automate the network planning process. There are too many planning factors that network managers would have to input to an automated planning system. The best plan for a particular operation is often the product of the signal commander's ingenuity and can be significantly different from any previously developed plan. The signal commander chooses the best plan but relies on expert advice from his staff to suggest alternatives or to point out potential problems. It may be technically feasible to design an algorithm to automatically develop a plan but it would not be worth the effort.

Each mission puts unique requirements on the network planning process.

These requirements demand creative answers. The 3RD Armored Division's MSE network in the Persian Gulf War of 1991 is a good example of this point. The 3RD Armored Division's mission involved high speed advances over great distances. The division signal battalion's MSE managers decided to use a topology never tried before. The MSE network managers planned a network that stretched along a single axis. It supported only 200 MSRT users and four command posts while the division was moving. The plan provided for alternate routing around failed node centers by using an LOS relay station located at each node center. The plan was risky because the loss of one entire node center team would break the network. The signal battalion was able to keep the RAU coverage up with the division's advances as it moved 150 kilometers into southern Iraq in just a few hours. The network managers reconfigured the network to a more standard meshed network once the division slowed down.[13] An automated planning tool would not likely have designed such an innovative solution to that complex problem.

An automated planning tool would not be practical because there are too many scenarios that network managers have to plan for. Each scenario calls for planning factors which would have to be put into the computer. These planning factors include off limits areas, areas likely to be in the way of friendly forces in the near term, or special communications requirements for customers not normally

[13]Bryan S. Goda, "Communications on a Mobile Battlefield in the 100 Hours War," Army Communicator, Spring 1991, pp. 42-47.

served by the MSE network. In the time it would take the network managers to input all the information unique to the operation, they could design a network with the tools they have available now.

Perhaps the best reason there would be little payoff for a highly automated network planning system is because of the confusion factor in warfare. No plan will work without changes once the battle begins. There are too many circumstances to go wrong with a plan. A node center commander can get lost or move to the wrong location. There might be enemy units where network managers planned to put some node centers. Customers might not put their command posts where they said they would. The maneuver commander might see a threat or opportunity that causes a fundamental change in the overall mission. Military history shows that the best military commanders are not those who develop elaborate plans but those who make simple plans that can be easily understood and modified.

While there would be little payoff in fully automating network planning, there can be a tremendous payoff in enhancing the network manager's capacity to plan a network quickly. Last minute changes to network plans that require the managers to reconfigure the network topology are often the most troublesome for the network managers.

AI-based planning tools can do for network managers what personal computer spreadsheets did for financial analysts. Network planners could evaluate different options or do *"what if"* analyses of minor topology changes. Planning tools can give the network managers the capability to put more analysis into their recommendations. Signal commanders could have the network managers explore more options.

MSE planning tool requirements

Any MSE network planning tool should be able to:

- Share data with the SCC's database
- Initiate SCC projects
- Modify and re-engineer plans
- Use graphical user interfaces to:
  - Suggest NC locations
  - Depict RAU coverage
- Generate an operations order shell
- Help prepare alternate plans based on alternate scenarios
- Evaluate plans based on expert knowledge

Most of these features are best developed with procedural code. However, the evaluation of plans should be developed using AI techniques.

A planning tool should be able to share data with the SCC's database to save network managers from entering network data multiple times. One signal brigade currently inputs customer locations five times into the following tools:

- A Digital VAX program to calculate terrain line of sight (better than the SCC)
- Harvard Graphics to depict network topology
- Quatro Pro to create a connectivity matrix between NCs and extension nodes
- Multimate to write the operations order
- The SCC to initialize the SCC to the initial network configuration[14]

Entering data multiple times increases the probability of errors and forces network managers to spend time doing elementary tasks instead of network analysis.

A planning tool would have to use a special database in addition to the

---

[14]Interview with a network manager who responded to a survey.

SCC's database. The SCC database does not contain all of the data fields that a planning tool would need. It can maintain only one current and one planned location for each MSE team. It does not store the configuration of node center switch databases nor the locations of MSRT users. A planning tool would need to maintain this information and share the data with the SCC and any other management tools.

A planning tool should initiate SCC projects. A project is the term used to describe the SCC software processes involved in preparing for an event such as the moving of a node center of opening an LOS radio link. An open link project causes the SCC to calculate a terrain profile, assign radio frequencies, and prepare order messages for the MSE teams involved. A planning tool that starts these processes within the SCC can save network managers considerable time and decrease the chance of errors.

Any planning tool must be able to modify and re-engineer plans. This would give the network managers the opportunity to explore multiple options and to make last minute changes in the plans. This process should be able to initiate the appropriate projects in the SCC to reconfigure the initial network topology and prepare the MSE team orders for last minute changes.

The reader should note that planning tools cannot prevent all of the confusion caused by last minute changes. No tool can guarantee that all MSE teams get word of last minute changes. There will be copies of outdated orders floating around. There are some things that only humans can do.

New network planning tools should take advantage of Graphical User Interfaces (GUIs). Most computer users are aware of GUIs and like them. GUIs are intuitive and easy to learn. GUIs can take advantage of the map reading skills every soldier learns in basic training. Army network managers can easily interpret topographic depictions of network topology and RAU coverage.

A network planning tool should be able to suggest possible node center locations. These suggested locations would have to be start points in the manager's search for node center locations. A planning tool can store a digitized map but would not be able to determine site accessibility or permission of the land owner. The SCC's database maintains information on sites based on previous reconnaissance records but cannot suggest sites not in its database.

A planning tool should suggest a site based on the line of sight radio connectivity requirements and terrain. The manager would move the icon around the area close to the suggested location or have the tool search for locations in a defined area. The manager would look for sites that could be reached from roads and the Army could obtain permission to use. The NPT will have this capability. The program should recompute terrain profiles automatically as the COMPASS program could. The capability to determine good node center locations quickly can save network planners hours of terrain analysis for each operation.

Any network planning tool should provide the network managers with an operations order shell with the technical details of the plan filled in. A military operations order follows a standard format. The network managers should be able to complete the operations order with the non-technical details of the situation, commander's intentions, logistical support, and other coordinating instructions. The network managers should have the option of completing the operations order with the planning tool or to transfer the operations order shell to a word processor.

Planning tools should be able to depict RAU coverage. A popular method of depicting RAU coverage is to place an icon at the location of the RAU and to show lines radiating out from that icon. The lines would mark each five degree radial (72 lines in 360 degrees) and would stop at the edge of the coverage area or would be broken at places where terrain blocks the RAU coverage. Network managers could see the projected coverage gaps. They would have to determine if the coverage gaps need to be filled by moving the RAU or by placing another RAU to fill the gaps.

A desirable feature for a planning system would be the capability to obtain the locations of the customers' command posts and MSRT locations automatically. This capability is technically possible but may not be reasonable. The Maneuver Control System (MCS) has this information and uses the MSE Packet Switch Network (PSN) to communicate. A planning tool could obtain the information from the MCS through the packet network.

Unfortunately, the capability to obtain customer locations automatically may be more expensive than its payoff. The initial network planning is done before moving to the field. The MSE network would not be in place to support the MCS system until the customers move to the area of operations. This capability may be worth exploring as part of the network control process.

Each of these features should be developed with conventional object oriented-programming techniques. None of these features require cognitive skills. All these tasks are computational intensive and would run faster with conventional program code.

Plan evaluation

The task of evaluating a plan is a good candidate for an expert tool. A plan cannot be completely correct or incorrect. It is the optimal mix of a series of cost and performance trade-offs that depend on the METT-T planning factors. Every network plan is evaluated by humans. The network planners develop one or more plans and recommend one to the signal commander who evaluates the plan to make a final decision of which plan to carry out.

A network planning tool should use a backward chaining or reasoning process and an expert rule base to evaluate network plans. A human expert that evaluates a network plan uses a backwards chaining process to determine if several goals are satisfied. The goals an expert tries to satisfy when evaluating a plan are:

- Key customers are identified and served by the network
- No MSE teams are over-committed
- All Pre-Affiliation Lists (PALs) required are assigned to NCSs
- All encryption key responsibilities are assigned to appropriate teams
- All required network gateways are served
- Commercial phone lines are assigned to correct extension nodes
- The KY-90s are assigned to appropriate extension nodes
- Ring codes for Orderwire Control Units (OCUs) do not conflict

Each of these goals should by satisfied for every network plan. Some goals that should be satisfied but are often left unsatisfied in good plans are:

- Every extension node is within terrain line of sight to an alternate node center in case its primary node center fails
- All standard customers are served by the network
- Alternate routes are available to prevent the network from fragmenting if a single node center fails
- All extension node links do not require an SHF downlink to reach a node center

A human expert uses backward reasoning to evaluate a network plan for several reasons. The number of goals is small in comparison to the number of possible network configurations (or solutions). The evaluation process seeks to determine if the plan is good, not to suggest a better plan. The human expert also has to explain his reasoning in the evaluation.

These factors make backwards reasoning desirable. Human experts are usually unaware that they use a backwards reasoning process when they evaluate a network plan. They just do it.

A planning tool should use a backward reasoning process for the same reasons human experts do. The tool should be able to evaluate the plan and make the same conclusions a human expert would. It should also be able to explain the reasons for its conclusions. Network managers need to know the reasoning for the conclusions so they can correct the network plan or adjust for the risks involved with the plan. They may have good reasons to ignore the tool's advice. The network managers should see the expert evaluator as a trusted specialist looking at their plan.

An evaluation tool should use an expert rule base to evaluate plans. The network managers should have access to the rules so the Signal Center could update the evaluation tool. There is no way to develop an evaluation tool free of errors or omissions. Signal units will discover additional rules, incorrect rules, or situations where some rules do not apply. Network managers will trust the planning tool's evaluation of plans only when they trust the tool's rule base.

Although this discussion of network planning has concentrated on the initial network topology, these features apply to network reconfigurations. The network control process identifies requirements to reconfigure the network. A planning tool should be able to plan changes to the network based on the current state of the network. This means that the planning aid should use the same database that a network control tool uses.

MSE Network Control

MSE network managers can benefit immensely from AI-based network control tools. They have a critical mission to keep the network operational. Network managers often work with incomplete or incorrect information. They work in real time and have little time to decide. AI-based tools can insure that novice managers have expert help or training immediately available.

This section will analyze the features and characteristics an AI-based MSE network control tool would require. The analysis follows the network control processes of setting standards, monitoring progress, identifying faults, identifying fault causes, making recommendations, and imposing or lifting network restrictions. Each of these processes are now performed manually and most require cognitive skills to execute.

The network control process relates to the node center control process much more than the network planning process. The planning process uses node center status information only to insure the network managers do not over-commit MSE teams. The network control process works interactively with the node center control processes. Node center managers periodically report their status to the network managers. They also execute special instructions from the network managers to reconfigure the network or to help troubleshoot network faults. The network control process cannot work unless the node center managers do their mission. AI-based tools can reduce some of the dependency on the node center managers to keep the network managers informed.

MSE network control is a complex process that monitors the network to insure it meets the standards. The commander sets the standards for events to take place, the quality of service, and a priority of essential customers. The commander depends on the network managers to insure the network meets the standards.

MSE network control tool requirements

A MSE network control tool should be able to:

- Extract system events from the plan
- Test the network to verify or determine information
- Infer network topology from known information
- Initiate alarms to alert the managers
- Prioritize network faults
- Diagnose network problems
- Initiate trouble tickets
- Report the network status

· Recommend changes to the network.

· *Extract system events from the plan*

The first feature a network control tool should have is the capability to extract system event times from the plan. The SCC extracts system event times from the projects. A control tool should maintain a set of additional network standards in its knowledge base such as the number of allowable subscribers per RAU or the number of times an LOS radio system may take radio noise bursts in one minute before suspecting a fault. Most of the network standards not specified in a network plan remain constant. Network managers modify these standards only for special reasons.

· *Test the network to verify or determine information*

Network monitoring is the process of analyzing network status information to determine if the network is meeting the performance standards. The current SCC monitors node center status updates to determine if system events are taking place on time. The SCC will highlight a planned link or network element on the network display if its planned activation time has passed without an activation report. It will also highlight a link if the SCC receives a report of traffic overloading on the link. Remember that each of these reports depend on human input.

Network monitoring is both passive and active. The SCC does passive monitoring by maintaining a network status based on the node center messages.

The network managers do active network monitoring by testing the network manually. They dial up node center managers or SEN operators to test network connectivity. The managers cannot verify individual link status information unless they can call a node center switch operator that they know can only be reached by one path. They can also test to see if a Group Logic Unit (GLU) in a RAU is affiliated by dialing it up and listening for the special *"burp"* tone.

· *Infer network topology from known information*

The network managers use these tests to infer information about the network's status. They often verify the report of a SEN activation by calling the SEN operator. They try to determine if a MSRT user has the correct encryption keys by attempting to call that user's MSRT. They also test some of a node center switch's encryption keys be calling a KY-68 secure telephone affiliated at the switch.

An expert control tool should be able to make active measurements automatically. It could make more measurements at more intervals than a human. The control tool could do these tests in a background mode and obtain more information if the tool could dial up data devices instead of humans. Data devices can answer calls automatically and also can perform data transmission tests to verify system performance.

The control tool would need to use a rule base to infer which devices it should attempt to call. It should infer conclusions based on the success or failure of the calls. The tool would need to determine the current topology of the network from known status information. It would then call the devices that would be able to verify or deny the network status information. The tool would need the rule base to determine what action to take when it discovers a difference between the network status information and the actual network status.

A network control tool can infer a significant amount of information by monitoring the traffic on the packet network. The SCC-2 sends a test packet message to every packet switch in the network once every minute. The control tool can infer the system connectivity to every node center and extension node just by listening to the packet traffic between the SCC and the packet switches.

The SCC-2 uses the information from these tests to maintain a network display. This network diagram is current and based on the automatic telemetry from the test packets. The packet switch network display resides only on one of the SCC workstations. Unfortunately, it does not share this information between the packet switch network workstation and the other workstations in the SCC. The PSN's display will not even resemble the physical topology of the network unless a manager inputs the NC and extension node locations into the workstation even though the locations are in the SCC's database.

· *Initiate alarms to alert the managers*

A network control tool should be able to set alarms for detected or predicted faults. The alarms would alert the network managers of the problem and trigger a fault identification process. The tool would need a means of informing the network managers of the alarm and communicating the exact nature of the alarm.

The network control tool would need to be able to correlate alarms. Often a single fault will trigger multiple alarms. The network managers need to know only the fault that caused the alarm and not the fact that the fault has set off several other alarms.

An example of a fault that might trigger multiple alarms is the failure of a node center link to a Radio Access Unit (RAU). The node center may report the link out and other node centers might report failed calls to customers served by the failed RAU. The network managers may receive reports of customer complaints if the RAU operator fails to turn off the RAU's marker. A network control tool should be able to correlate these different alarms to all be related to the original fault of the failed link.

· *Prioritize network faults*

A network control tool should be able to prioritize faults. Network faults have different levels of urgency. A failed node center switch is a more serious fault than a failed RAU unless the two faults are caused by the same problem. The priority of faults depends on the effects of the faults and on the mission.

· *Diagnose network problems*

An important feature for a network management tool is the capability to diagnose network problems. Fault diagnosis is a cognitive task now performed by the network managers. The tool should be able to suspect a fault by recognizing a pattern of reports. It should test the network to verify or disprove its suspicions and draw conclusions of the nature and cause of the alarms. The tools should be able to advise the network managers of the consequences of the faults and the measures to correct them.

An example of a fault that a network control tool might diagnose is a lost customer telephone number. This type of problem would likely be reported by a node center manager handling a customer complaint. The customer is unable to affiliate his telephone but can dial a "0" to talk to an operator. The node center switch operator would be unable to verify the customer's number is pre-affiliated anywhere in the network. The network control tool would need to identify if the customer' s number is in a Pre-Affiliation List (PAL) and if that PAL was assigned to a NCS to be loaded. If the PAL was assigned to a node center switch, the tool would need to test other numbers from that PAL to determine if all of the numbers were lost. Finally, the tool would have to recommend one of several actions to correct the problem. The tool could make the situation worse if it recommended the wrong action to correct the problem.

· *Initiate Trouble Tickets*

MSE network managers need a help desk tool that can also initiate trouble tickets. The tool should have access to the network status information and any diagnostic expert tools. The tool should be staffed by a network manager familiar with the network plan. It should provide an automated trouble ticket entry form.

The trouble ticket system helps track problems. An automated system can show the status of all unresolved problems. It would also provide a historical database for network managers and management tools to use to identify systemic problems. The trouble ticket database can also serve to document needed changes to management tool rules bases.

· *Report the network status*

Any network management tool should be able to report and explain the network's status. The best method is a graphical network display. A graphic display can show a general network status but the operator should be able to interrogate the tool to obtain detailed information. The tools should be able to show the alarm on the network display and the operator should be able to open a window and have the system explain how it discovered the fault.

· *Recommend changes to the network*

Perhaps the most important feature for a network control tool would be the capability to recommend changes to the network. These recommendations are often the result of a fault diagnosis and involve minor network modifications. Recommendations might be actions to correct a fault or mitigate its effects. For example, the recommendation may be as simple as loading another PAL or as serious as shutting down the entire network and reloading all customer numbers.

A desirable feature for a network management tool would be the capability to test its recommendations. The tool could conduct a network simulation to identify effects of a recommended change. The tool also could input the state of the network with the modifications to the evaluation program in the planning tool. Network managers would be better equipped to convince the signal commander of the recommendations if their recommendations were tested by a network management tool.

This discussion has dealt with the features that network planning, engineering, and controlling tools should have. The discussion of the needed features was partitioned by the network management functions and does not imply that these features should be put into separate tools. The best tool would be one that works as part of the system control center to take advantage of the available information and to enhance its capabilities.

MSE Node Center Management

There are several potential applications for AI-based management tools in the node center switch, small extension node switch, radio access unit, and the node management facility. This section will explore the potential features for each of these tools.

The node center switch is the best source of network information within the MSE network. Most information needed to determine the status of the MSE network can be retrieved from node center switches. The problem with the current generation equipment is that none of this available information is sent automatically to the network managers as telemetry.

GTE Government Systems Corporation's research into the Enhanced Switch Troubleshooter (EST) is a step in the right direction. It would improve the node center switch operator's ability to detect and troubleshoot problems. It will translate NCS output into English sentences and use expert knowledge to suggest troubleshooting techniques to the operators. Unfortunately, EST will not provide telemetry to the network managers.

The ideal tool for the node center switch operator should include all the functions of the EST. It also should be able to immediately notify a network control tool of the following events:

- Failed call due to encryption key problem
- Failed call because the called party was not found
- Failed search for a customer telephone number from the NCS operator

These events show possible network level problems. Although encryption key problems are often due to incorrect procedures by node center switch operators, they can also be caused by incorrect encryption keys given to customers. Missing customer numbers point to either node center errors or network level problems. This information could provide a centralized network management tool the information it needs to spot specific network level problems.

A node center switch tool should also forward periodically the following status information to a network control tool:

- Bit Error Rate status of each link to other node centers and extension nodes
- Telephone numbers of the customers affiliated to each RAU
- Telephone numbers of the customers affiliated to each SEN
- Non-standard database configurations
- Traffic metering reports (number of calls in/out of switch)
- Designations for any gateways at the NCS or attached extension nodes

A network control can use this information to verify the status and look for problems with each node center. For example, the network managers would need to consider taking some action if more than 35 customers are affiliated to a RAU.

If a RAU near the one in this example had no customers affiliated to it, the network managers might suspect problems with the second RAU or its NCS.

Node center switch tools should not tell a network control tool of every event. That would cause too much network management traffic on the MSE network and inundate the network control tool with too much data. These tools should be able to filter all NCS messages and infer the need to inform the network control of a possible problem. For example, an LOS radio system may begin to fade in and out. This would cause the NCS to print a number of status messages. The NCS tool should decide to notify the network control tool of the problem. The problem may have begun when a new LOS system began transmitting. The NCS should inform the network tool of the problem and its start time, but not of every change in the state of a network element. Only the network tool would have enough information to diagnose the problem as radio interference. The tool should also notify the NC manager whenever it reports an event to a centralized manager.

A node center switch tool would need to be able to generate a plan to modify the NCS database contingent on new missions. This task requires cognitive skills to select the best digital trunk groups to modify. The process to do the actual modification is tedious and error prone. The tool should be able to issue the commands to do the switch modifications automatically.

A good node center switch tool would reduce the traffic between the node center manager and the network managers. However, the node center manager would still need an AI-based management tool and troubleshoot customer complaints and node level problems. An AI-based tool also can help plan the assignments of LOS links to specific NCS digital trunk groups. The combination of an improved EST and workstation for the node center manager can reduce the administrative burden on the node center manager. The best node center managers are those that are free to move around the node center site to insure all is well.

A management tool for the RAU should do the following:

- Forward periodically to the NCS the status of the marker signal, which frequency plan is in use, and the number of radios operational
- Turn off the marker signal if the link to the NCS fails
- Turn on the marker signal on command from the network managers or NC manager
- Change the frequency plan on command from the network managers or NC manager

These features do not require any cognitive skills and are not likely choices for AI-based tools. However, a RAU management tool would help the node center and network manager tools by providing timely information.

The features needed by a SEN management tool include:

- Capability to initiate a search for a customer's phone number pre-affiliation
- Capability to prevent the SEN operator from breaking the link to the node center before all the customers dis-affiliate their phones
- Provide status of the KY-90
- Information on the use of an SHF relay
- Provide status of commercial lines

These features, like the RAU's, are not good candidates for AI-based tools but are useful for providing information to AI-based tools at the node center and SCC.

Justifying the Development of AI-Based Tools

The decision to develop AI-based tools cannot be taken lightly. The development of AI tools involves significant costs and risks. However, the payoff can be high.

AI tools can be justified when the following conditions exists:

- Cognitive skills are required to solve a problem
- Human experts are available to transfer knowledge
- The task is difficult enough to justify the expense
- There potential payoff is high
- Human expertise is limited or being lost
- The risk is reasonable

The MSE network management domain unquestionably meets several of these conditions. Network management is a cognitive problem. There is expertise in MSE management throughout the Army but it is limited because the network managers move to new jobs.

The question of justifying AI tools for MSE depends on the costs and the risks. AI tools are traditionally expensive. The Army would have to prove it would use the AI tools effectively to justify their expense. The experiences of commercial network management systems shows that AI tools can have high payoffs at reasonable costs.

Obstacles to Developing AI-Based Tools for MSE Network Management

There is a justified need to develop AI-based tools for MSE network management. Unfortunately, there are several barriers other than cost to developing these tools. The major problems are GTE proprietary hardware and software and the traditional problems of knowledge acquisition and data capture.

The MSE system was a Non-Development Item (NDI) acquisition. This means that the Army purchased an existing product from GTE instead of researching and developing MSE in house and contracting GTE to build it. All of the hardware and software documentation belongs to GTE. GTE has not released the software and hardware interfaces to the Army or the public.

The Army's options to overcome these obstacles are to:

- Buy new network management tools from GTE
- Develop separate tools that take advantage of the circuit switched and packet switched networks to communicate.
- Buy the documentation from GTE and release the interfaces to other vendors to propose network management tools

Buying AI-based network management tools from GTE may be the best option. The enhanced switch troubleshooter shows that GTE is interested in developing better network management tools. However, GTE is developing these tools piecemeal because the Army has not stated what it believes its needs in network management tools are.

The danger in the Army's current procurement strategy is that GTE does not have an objective management architecture to build towards. The Army does not have a target architecture to evaluate a GTE proposal against. It is also in GTE's financial interest to introduce better management tools in a piecemeal fashion to keep the Army's business longer.

The Army should do the following if it is to rely on GTE to produce AI-based network management tools, it must:

- Define an ideal management architecture
- Insist on an open architecture that enables the Army or other vendors to add features in the future
- Insist on an open rule base for any expert systems that can be updated

with additional rules to improve the tools

An Army ideal management architecture would provide a standard for GTE or another vendor to compare their products against. It would also require the Signal Center to analyze the network management process and define an objective network management architecture. It would also encourage GTE to propose a comprehensive management architecture rather than a piecemeal one.

An open architecture would allow the Army to add features in the future without waiting for GTE. It would encourage other vendors to compete with GTE for network management products. It is likely that GTE would resist this option for these reasons.

An important feature of any AI-based system would be an open knowledge base. Neither the Army nor GTE could develop an adequate knowledge base until the tools have been in use for extensive testing and operations. The knowledge base will have to be updated to fix bugs and incorporate lessons learned. The Signal Center must be able to update the knowledge base without depending on an outside contractor.

The option to build separate tools instead of improving the management tools being fielded would be awkward. The Army does not need more devices to maintain. More devices would create additional training and logistics problems for the signal units that would receive them. It is likely that the units would not want more network management tools if they were packaged in separate boxes.

The option of buying the documentation to the SCC and NCS software may be good if the price is not too high. The Army could open competition for future management tools to other vendors. Unfortunately, GTE would likely demand a high price for their software rights.

Knowledge acquisition will be a difficult task. The Signal Center will need to identify a group of network management experts to provide the initial knowledge base. The Signal Center could expect the common AI problems of getting the knowledge from the experts and reconciling conflicting rules.

Fortunately, the Army's AI school is at the same military installation as the Signal Center. The AI school has a three week expert system course the Signal Center could use to train the network management experts in the fundamentals of AI. The AI school also has a Knowledge Engineering (KE) group of experts that could help develop rule bases. The task of knowledge acquisition is difficult but the Signal Center has the necessary resources.

The problem of data capture relates directly to management tools in the RAU, SEN, NCS, and the node management facilities. A network management system without a means of automatic telemetry would offer little improvement over today's management tools. AI-based tools need a lot of data to make good recommendations. The Army at a minimum must acquire tools for the network managers, node center managers, and the node center operators.

Conclusion

The discussion in this chapter has shown there is significant potential for the development of AI-based tools to help MSE network managers do their jobs faster and better. Commercial network managers are now getting AI-based tools that help them better manager complex networks. Military network managers share the need for improved tools. Several AI projects show that the Army and vendors are interested in developing AI-based tools.

This chapter analyzed the features that would be needed in an AI-based network management architecture. It also showed that it would not help much to develop only a portion of this architecture. Any management tool will require automatic telemetry from the MSE network elements.

Chapter VI will expand on the required features of the MSE management architecture. It will propose a plan the Signal Center could use to develop an AI-based network management architecture that would improve MSE network management.

CHAPTER VI

An Objective MSE Network Management Architecture

Introduction

This thesis has analyzed the potential for AI-based tools to improve MSE network management. It revealed that the technology can support the development of new network management tools to help network managers do their jobs better and faster. Commercial network managers have proven that AI-based tools can free managers of much of the mundane workload to let them to concentrate on strategic network issues.

This thesis has also shown that MSE network managers need better tools than they have now. The MSE networks will become even more critical as they transport more data. Many of the MSE units have developed non-standard tools to help solve their network management problems. The Army's current procurement strategy will not provide future MSE network managers the best possible tools. The Army can improve its procurement strategy by defining an objective network management architecture to provide direction but not requirements to vendors.

The purpose of this chapter is to define one possible MSE objective network management architecture. This architecture is based on the analysis of MSE network management in the previous chapters, the analysis of AI-based tools in the commercial sector, and the available computer platforms for the near future. It also addresses the MSE network management problems highlighted in the previous chapters.

Key Points of the Objective Network Management Architecture

The key features of the recommended network management architecture are:

- A redesign the SCC-2
- The development of a means to gather automatic telemetry from the MSE teams
- Development of node center management tools

The redesign of the SCC-2 is based on the need to provide better network management tools and the fact that the SCC-2 will be the network management platform for the near future. The computer workstations in the SCC-2 are adequate or can be upgraded to support AI-based tools. The Army will not likely agree to field a completely new version of the SCC soon because of budget cuts and the investment in the SCC-2.

Chapter IV discussed the requirement for automated telemetry in detail. The current management system suffers from a total dependence on human input. Automated telemetry can provide network managers and their tools with greater and more timely information.

This thesis has also detailed the need for improved node center level management tools. The node center managers have the burden of controlling their teams and providing the network managers the status of the MSE teams. The node center managers are typically young and bright, but inexperienced. They have no expert tools to help them manage their MSE teams. GTE is poised to field dramatically improved node center management tools through software upgrades to their new node center workstations.

Overview of the Proposed Architecture

The Army's planned overall tactical communications network management architecture is based on the manager of managers architecture described in chapter IV. Figure 6-1 shows that the ISYSCON will manage all of tactical communications networks.

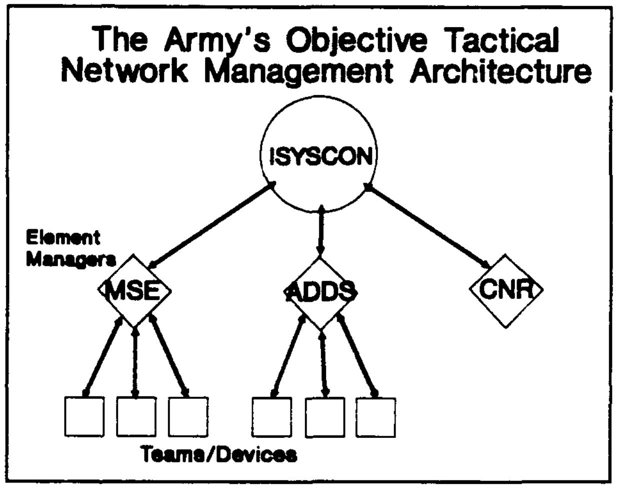

Figure 6-1

Each of the three types of networks (MSE, Army Distributed Data System, and Combat Net Radio) will have a subordinate management system. Commercial network management architectures refer to subordinate management systems as element managers. In the overall scope, the MSE network management system will be an element manager.

This thesis will not address the relationships between the element managers and the ISYSCON. The Army has not clearly defined these relationships which are beyond the scope of this thesis. As stated in chapter V, the Army desires to employ AI techniques in the ISYSCON at a future date.

The proposed objective MSE network management architecture also uses a variation of the network of managers architecture. Each SCC will manage a portion of the MSE network. The element managers will be the node center managers and each node center will manage the MSE teams assigned to it.

The proposed architecture is slightly different from the network of managers architecture discussed in chapter IV. In a pure network of managers architecture, the network managers would each manage each of the element managers. Figure 6-2 depicts the proposed MSE network management architecture. It will have the network managers control only the element managers (node centers) assigned to it. This maintains unity of command which is a basic tenet of military operations. A pure network of managers architecture would also call for the element managers to coordinate among themselves. The node center managers would not automatically coordinate the management among themselves in the proposed MSE architecture.

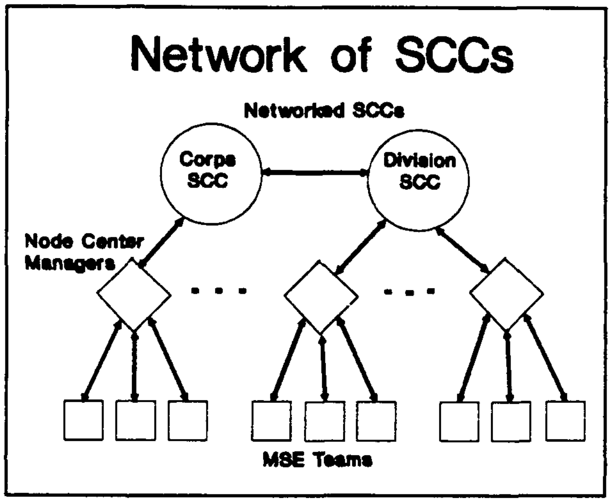

Figure 6-2

Each MSE team would have a means to send automatic telemetry to the node center managers. Many commercial network products such as Private Branch Exchange (PBX) switches or multiplexers use agents to communicate with network managers. An agent can be resident software in network elements that recognize and respond to management communications (SNMP or CMIP). It could also be an attached hardware device to do the same function. This chapter will discuss the details of the MSE team agents later. However, there is no need to incorporate AI based software into the MSE network element agents.

Each node center management system would be responsible to manage the assigned MSE teams and send telemetry to the SCCs. The node center management systems would provide the capabilities described in chapter V. These capabilities include expert systems to plan node center switch configuration databases and diagnose system faults.

The MSE network management system would be the improved SCC-2. The improvements to the SCC-2 would include adding a knowledge base server to monitor all management traffic to spot potential problems and to diagnose network faults. It also would incorporate the Network Planning Tool being developed by MITRE corporation. The SCC-2's software would also be upgraded to improve its control functions and add a help desk capability.

Redesigning the SCC-2

The NYNEX ALLINK provides a good model for an improved SCC-2. The ALLINK is an integrated network management system. It offers operator workstations, a management information base, rule server, and a communications gateway built on a Local Area Network (LAN).

The current version of the SCC-2 is built around a LAN (figure 6-3). Each workstation has access to the packet and circuit switched networks.

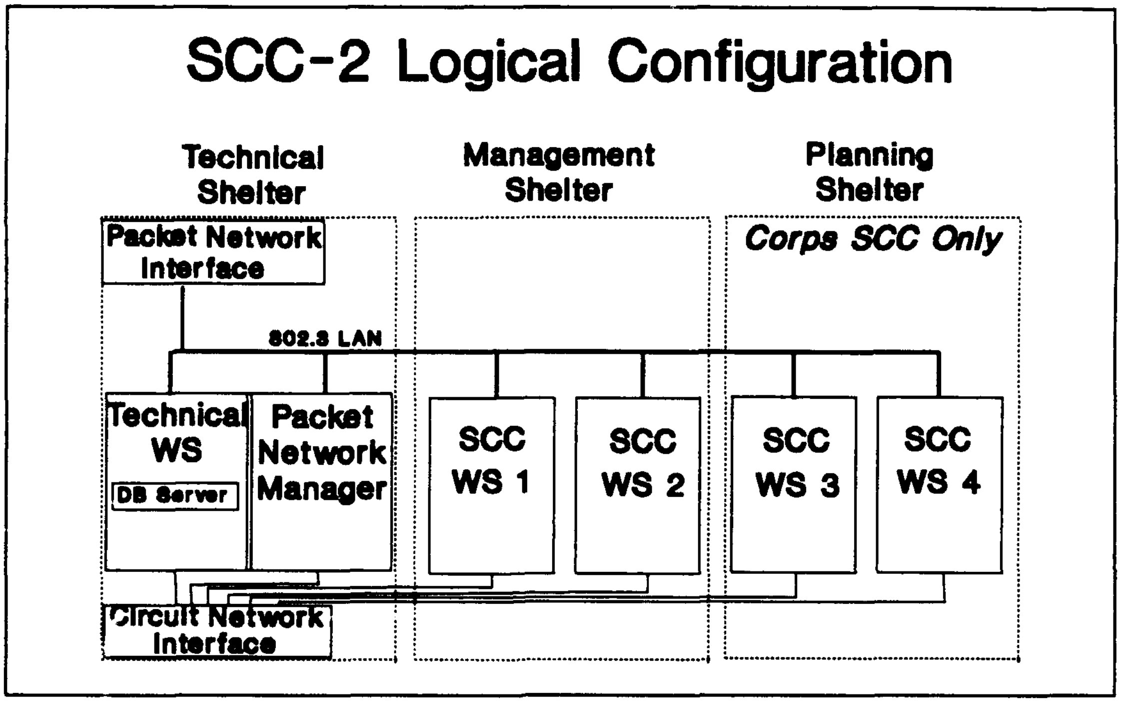

Figure 6-3

The proposed SCC-2 redesign calls for improving the workstations already on the LAN.

The major changes to the SCC-2 would be:

- Addition of a knowledge base server
- Upgrade of the SCC database to a management information base
- Incorporation of the NPT into the SCC
- Development of a network control tool
- Addition of a help desk function

Figure 6-4 depicts the proposed hardware modifications to the SCC-2. The major changes include replacing one of the workstations with the NPT, and using one of the remaining workstations as a help desk. The technical workstation would also act as a knowledge base server in addition to a database server.

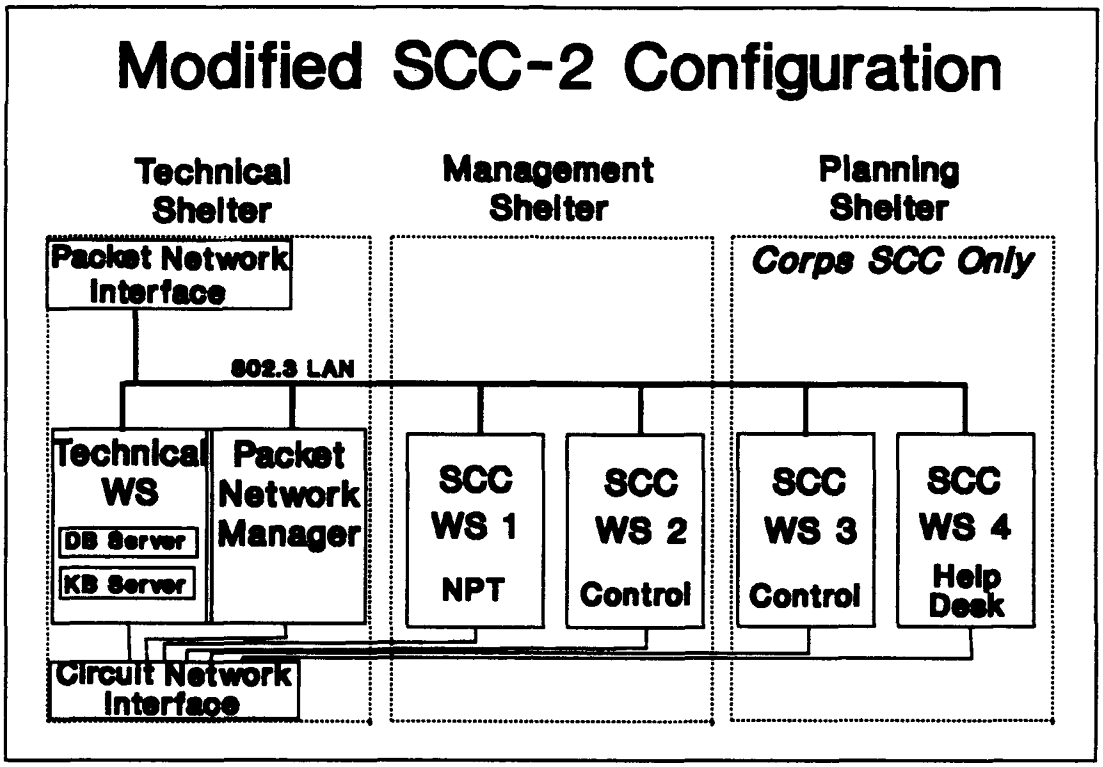

Figure 6-4

· *Addition of a knowledge base server*

The knowledge base server would screen every incoming message to look for potential problems. It should use a commercial object-oriented expert system shell and a rule base developed jointly by the vendor and the Army. One possible commercial expert system shell is Level5 Object, an expert system shell developed and sold by a company called Information Builders. Most commercial expert system shells offer quality graphics-based user interfaces, good documentation, and extensive support.

The knowledge base server should reside on the SCC technical workstation. The technical workstation already serves as a database server for the other workstations. This would make the interception of all message traffic by the knowledge server easy.

The knowledge base server also can run separate diagnostic sessions when started by a network manager. The expert system can use the database information and ask questions of the network manager to diagnose problems. It should also trigger processes to test the MSE system whenever possible.

· *Upgrade of the SCC database to a management information base*

The SCC database should be expanded to a complete network management information base. The network information base should include complete status information on every network team. The information would be sent automatically from the network agents every one to five minutes and changes updated in the information base. Each of these updates also would go through the knowledge base server.

· *Incorporation of the NPT into the SCC*

The Network Planning Tool (NPT) should be incorporated into the SCC. This would require replacing one of the workstations with a more powerful processor and larger screen. The NPT would require a larger processor because of the computation intensive planning and evaluation program. A larger screen would display map and network data for a large portion of the operations area.

The NPT would need to be changed under this proposal because the current NPT is being developed on a different platform than the SCC workstations. It should work on a modified SCC workstation that could run both NPT and the other SCC software. The NPT should also use the SCC's topographic, MSE team, and frequency data from the network information base rather than a separate database. It also should be able to initiate SCC projects once the commander approves the plan.

· *Development of a control tool*

The SCC should have an improved network control tool. The control tool would do the same control functions as the current SCC and more. The major functions of the tool would be those listed in chapter V and below:

- Extract system events from the plan
- Test the network to verify or determine information
- Infer network topology from known information
- Initiate alarms to alert the managers
- Prioritize network faults
- Diagnose network problems
- Initiate a trouble ticket
- Report the network status
- Recommend changes to the network.

The AI functions of the control tool would be handled by the technical workstation. The control tool's primary mission would be to monitor and test the network and to diagnose faults.

The control tool should be integrated with the packet network controller to give the manager an accurate picture of the network. The packet controller receives near real-time data on the backbone network and the links to the small and large extension nodes. The control tool should rely on other telemetry to determine the status of the radio access unit links. This should be an easy upgrade because the packet controller is on the LAN with the other workstations.

The control tool should extract system events from the plan. The NPT should be able to forward an approved plan to a control workstation that would start the SCC projects to carry out the plan. The NPT workstation should be able to run both the NPT and the control software so it could initiate the SCC projects based on the plan. However, it would often be helpful to use the NPT to conduct further planning and use another workstation to carry out the plan. The SCC should give the network managers the option to do both.

The control tool should use visual and graphical alarms to alert network managers of potential or actual faults. The visual alarms should be highly visible icons in one corner of the screen. The tool should sound an audible alarm, such as a beep, whenever the status of the alarms change. These alarms should appear on every workstation running the control software. Key alarms should appear on every workstation.

The control tool should have an enhanced network reporting mechanism. It should display or print-out the network topology, numbers of users, numbers of calls, and numbers of packets sent from each packet switch. This data should be displayed in graphic form or in easy to read tables.

The control tool should use the knowledge base to prioritize network faults. Whenever the technical workstation receives an alarm or the knowledge base detects an error, it should set an alarm on every control workstation. The control tool would maintain an alarm window with a priority list of alarms. The knowledge base should consolidate multiple related alarms into one alarm.

The control tool should be able to open a window on any network team to let the network manager inspect its status. The control tool would only display network data maintained in the SCC database since it would take too long for the control workstation to interrogate each network team's agent. This feature requires that the agents update the SCC at least every one to five minutes.

Each window in the control tool should use icons and colors to show status information. For example, a window displaying a Node Center Switch (NCS) configuration database would shade the Digital Trunk Groups (DTG) not in use. It could display in red any DTG in use but experiencing a problem. Each icon should display a menu whenever a node manager clicks the pointing device on it. The use of windows and icons help make traversing the network information base easy for the network manager. Figure 6-5 shows how the control tool's screen might look.

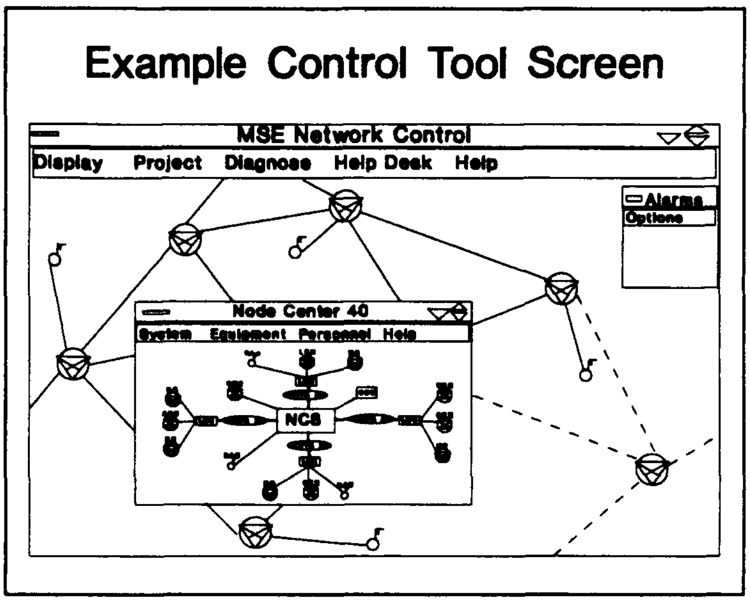

Figure 6-5

The control tool should help the network manager diagnose problems and generate trouble tickets. The problem diagnosis function would be an expert system consultation running on the technical workstation and displaying in a window on the control workstation. The expert system would obtain information from the network information base, by interrogating network agents, or by asking questions of the network manager. The expert system would likely use an object or frame-based knowledge representation scheme to diagnose faults.

· *Addition of a help desk function*

The control tool should have a help desk function designed to report and diagnose customer telephone problems. Most customer telephone problems relate to Pre-Affiliation Lists (PALs), frequency plans, encryption keys, and node center database backups. The help desk operator should be able to pinpoint the cause of a subscribers problem from the workstation. The help desk function should give the operator access to all of the network information base. It should also provide an expert diagnosis system to troubleshoot customer problems. The help desk should be able to initiate a project to instruct a node center to load a PAL.

These improvements to the SCC would give network managers the best possible tools for the foreseeable future. The network managers would be able to look at an accurate status of each MSE team quickly. The AI-based planning and control tools would help the managers to plan more options and maintain better control of the network while using the expertise gained from all of the MSE units. However, these improved tools require accurate and frequent automatic telemetry from each MSE team.

Development of a Means to Gather Automatic Telemetry

The proposed network management architecture would use agents in the

Small Extension Nodes (SEN) and the Radio Access Units (RAU) to gather data and funnel it to the Node Centers (NC). The agents would use both the packet switched network and dial-up circuits to transmit data to the node center.

The agent in the SEN would be a laptop computer whose main purpose would be to transmit the following data to the NC:

- Status of the KY-90
- Use of an SHF relay
- Status of commercial lines

This data would have to be entered into the laptop computer by hand because there is no current means to capture the data automatically. The laptop computer could also initiate requests for a customer search, act as a message terminal, and run an expert consultant program to diagnose problems. The computer would be in the Small Extension Switch (SES) and it would connect to the packet switch network port which is also in the switch.

The RAU agent should be the Group Logic Unit (GLU) located inside the RAU shelter. The current SCC can dial up the GLU and download frequency plans to it. The GLU could be modified to capture and transmit the following data to the NC:

- Status of the marker signal
- Which frequency plan is in use
- The number of RT-1539 radios that are operational and in use.

This data can be captured by the circuitry in the GLU. The RAU agent would likely be another circuit card inserted into the GLU. It would have to use a dial-up line to send its information to the NCS because the packet network does not extend to the RAU.

The RAU agent should execute the following commands automatically or on order of the NC or the SCC:

· Turn off the marker signal if the link to the NCS fails
· Turn on the marker signal
· Change the frequency plan

These functions can each be done within the circuitry of the GLU. The GLU already communicates with the SCC to download frequency plans. To add these features to the GLU would only require adding mor: .de to the firmware in the GLU.[1]

The NCS agent and the node center management system should be included into the NCS workstation software. Although the NCS would send telemetry to the NC management system, both the NCS agent and the NC management system would be part of the same software and reside on the same computer.

Node Center Management System

The latest upgrades to the node center switch provide a good platform to run a node center management system. The NCS and the Node Management Facility (NMF) workstations are both part of the node center switch. The workstation in the NMF is a subordinate terminal to the NCS processor The workstation software was written in Unix and X-Windows and can be revised to add more capabilities. Both workstations have access to the packet and the circuit

[1]Phone conversation with Mr Robert Rood, GTE Government Systems Corporation, 24 April 1992.

switched networks.

The node center management would serve two primary functions: providing telemetry to the SCC and helping the NCS operator and node center manager do their jobs better and faster. The system would receive, process, and relay the telemetry from the assigned small extension nodes and radio access units. It would also improve the NCS operator's user interface to the switch and provide AI-based tools to help identify and diagnose equipment and network problems.

The node center management system should act as a filter for the SCC. It would screen the telemetry from the SENs and RAUs and forward periodic updates to the SCC. The NCS should update the SCC only when something changes at a SEN or RAU, a significant event occurs, or at set intervals. This would reduce the management traffic on the packet network and reduce the workload on the SCC's database and knowledge base servers.

The NCS should forward to the SCC the status of itself periodically. The status information should include:

- Bit Error Rate status of each link to other node centers and extension nodes
- Telephone numbers of the customers affiliated to each RAU
- Telephone numbers of the customers affiliated to each SEN
- Non-standard database configurations
- Traffic metering reports (number of calls in/out of switch)
- Duplication Status
    - Time of setup
    - Details of which Digital Trunk Groups (DTGs) are duplicated in each adjacent NCS.
- Records of which encryption keys have been transferred to other switches
- Designations for any gateways at the NCS or attached extension nodes.

In addition, the NCS should sent a notification to the SCC each time the following events occur:

- Failed call due to distant end could not be located
- A KY-68 failed to synchronizes with the encryption equipment in the NCS
- A failed search when the NCS operator initiated a search for a customer's directory number
- DTG experiencing bursts of errors.

These events can be meaningless or a sign of potential problems. This information can help the knowledge base server at the SCC spot systemic problems in the network.

The NCS should have a database and knowledge-base server. The database server should maintain a historical log of all events in the NCS and the subordinate SENs and RAUs. The knowledge base server should screen all message traffic to look for potential problems. It would also serve as a diagnostic expert system available to the NCS operator and the node manager. The knowledge base server would of course access the database server.

The node center management system should provide the NCS operator and node manager with graphics based user interfaces. The operator should be able to click a pointing device on an icon and access a menu of options. The current system requires the operator to type three letter commands to the switch. A graphical user interface would help the operator work faster and interpret overall status information at a glance.

The NCS operator would have access to expert help to identify and diagnose problems. The knowledge base server would scan every NCS processor message and the incoming telemetry to spot potential problems. It also would provide on-line expert consultation to diagnose problems.

The GTE Enhanced Switch Troubleshooting (EST) tool described in chapter V would form a good start to this feature. The EST would need to be expanded to the NMF workstation to provide the same information and features to the NC manager. The EST's knowledge base would also need to be open to allow the Army to update it with more rules. The current information on the EST indicates that it will have a limited knowledge base and will be intended solely for the NCS operator.

Summary of the Proposed MSE Network Management Architecture

This proposed network management architecture would solve the most important deficiencies in the current system. These shortcomings include the lack of automatic telemetry and the ability to control network assets from the SCC. It would provide better tools to the network managers and help provide better service and help to the customers.

The purpose of this proposed architecture is only to provide a baseline to evaluate new management tools against. It is based on the analysis presented in this thesis, but it is not necessarily the optimal solution to the MSE network management problems. The Army does not currently have an objective MSE network management defined and this proposal seeks to fill that gap.

The US Army Signal Center should study the proposal and consider adopting it as the official objective architecture. This thesis has shown that the Army needs to develop a management architecture that gives vendors direction in their efforts and provides a baseline to evaluate proposals. The Signal Center can form a project team to study the MSE network management problem and propose a solution. This thesis would provide a good starting point for their work.

Where is the AI?

The proposed architecture makes modest use of the available AI technology to provide network managers with intelligent tools. Most network management tasks can best be developed using conventional computer program code that uses fewer resources and runs faster. Conventional programming tools are also cheaper than those for AI and should be used when appropriate.

The use of AI in MSE network management tools should be limited to the tasks which are best suited for AI. The best tasks for AI-based tools are those that would require human knowledge or behavior. They include the development and evaluation of network plans which require a mixture of computation intensive and cognitive tasks. AI also would be good for the analysis of telemetry and switchboard output because these tasks take expertise and are monotonous. AI would be best for diagnostic tools because the knowledge would be represented in the form of rules that can be easily updated. and most problems deal with uncertain or missing information.

Knowledge Acquisition

Knowledge acquisition for AI-based has traditionally been difficult. It is often hard to find human experts or experts that can agree with one another. Experts are often eccentrics who have difficulty communicating with others that are not competent in the experts' field.

The Army cannot expect to buy AI-based tools *"off the shelf"* with the proper knowledge bases already loaded. The MSE network management problem is unique to the Army and most MSE network management experts are in the Army and not working for commercial vendors. The Army will have to work with potential vendors to develop the knowledge bases.

The Army does have several advantages that can make knowledge acquisition easier. First, the MSE network managers are soldiers who all have common skills and experiences with the potential knowledge engineers. Army network managers are trained to cooperate and communicate with other staff members. The Signal Center has a local AI training facility that it can use to train former network managers as knowledge engineers. Finally, the network management problem can be well defined to narrow the scope of the knowledge needed.

The US Army Signal Center would need to develop four knowledge bases for an MSE network management system. These rule bases are for:

- The evaluation of a network planning tool developed plan
- The analysis of telemetry
- The analysis of node center switch processor output
- Diagnosis of equipment and network problems.

The Army would require a way to keep the knowledge bases current. It must require vendors to open the knowledge bases of any AI-based tools. The Signal Center should assume the responsibility to consolidate lessons learned by signal units and maintain the knowledge bases. The Army's hierarchical command structure and technology both make the distribution of rule base update easy.

Issues with the Acceptance of AI-Based Tools

There are several issues which must be addressed when considering developing AI tools for MSE network management. Any effort to improve network management will be wasted if the managers who the tools are designed for reject the tools. These issues must be addressed during each phase of the system development life cycle. These issues are:

1. The experts who provide the knowledge must be convinced of the project's value. They must believe that there is a need for the project and that their knowledge can be captured and used by the AI tools to improve the management of MSE networks.

The experts must also be convinced the project is not a threat to them. They must not feel they will be replaced by computers. They may fear that they would give the knowledge engineers correct knowledge that the AI tools would apply incorrectly to give bad advice. The MSE experts must believe that any failures of the AI tools would not be blamed on their input to the knowledge bases.

2. The Signal leaders must be convinced that the project is not a threat. Humans are skeptical of about the ability of computers to do complex tasks. Military officers have long been reluctant to rely on machines because machines fail at the worst times. They must be convinced that a failure at the

worst possible time would not be catastrophic.[2] They must be convinced that the human network managers will not rely on the computers so much that they could not manage the network manually if the computers failed.

The Army operates by assigning responsibility to humans. The network managers must know that they are responsible for their plans and that they cannot put the blame for a poor plan on bad advice from a network management tool. Likewise, the managers must trust the tools' advice.

3. The technology must be appropriate for the tasks and the users must believe the technology is appropriate. The tools must be able to handle complex network information. The users must be convinced that the tools are capable of handling the network information. The users will remember the system's failures longer than its successes.

The users must see improvement over time in the tools' performance. Military officers and NCOs understand that new people and machines make mistakes. They admire soldiers who learn from their mistakes and improve their performance over time. They would admire network management tools that learn from failures and improve. The users must know there is an improvement process and that they are a part of that process.

4. The project must have the support and attention from the highest levels. A network management tool would require the support of the Commanding

---

[2]Stephen B. Sloane, "The Use of Artificial Intelligence by the United States Navy. Case Study of a Failure," AI Magazine, Spring 1991, pp. 80-92.

General (CG) of the US Army Signal Center to succeed. The Signal Center's CG is the highest ranking officer that oversees signal projects and personnel.

The support from the CG must last the full life cycle of the project. Most military projects last longer than the terms of the generals who sponsor them. For example, the COMPASS project had the support of the Vice Chief of the Army who ordered it to be fielded to a unit at Ft Hood, TX in 1988.[3] The project ran into problems and the Vice Chief of the Army changed. However, the project's primary action officer left the Army and the project was abandoned.

5. The tools must be advertised as advisors only. Human experts know when to ignore certain rules in critical situations. They may not know which rules to ignore until the situation dictates some action. The users must not be afraid to ignore the tools' advice or try a different approach to get the job done.

An AI-based system is not guaranteed success if each of these issues are addressed. However, failure is almost certain if these issues are ignored. The most important element in any information system's development is the human.

Conclusions

This thesis has shown that the Army should take advantage of current AI and conventional technologies to improve the MSE network management tools. The available software development tools, current research into management tools, and the MSE packet switch network combine to make AI-based network

---

[3]"COMPASS - Communications Planning Assistant," Artificial Intelligence Project Summaries, US Army Artificial Intelligence Center, May 23, 1990.

management tools a reasonable investment.

The current situation of diminishing resources and increasing missions for MSE make the need for better management tools acute. The Army will have less money to train network managers at the Signal School. Network managers will have less experience as large scale military exercises are reduced. The pressure to provide stable communications networks will be even greater as remaining field exercises become more important. The Army will be expecting better productivity from its network managers and it should provide them the tools to be productive.

Recommendations for Further Research

This thesis has documented the initial research needed to develop an improved network management program. It has highlighted the problem and proposed a solution. More research is needed to prove the findings of this thesis and to build on the recommended network management architecture. The Army should assign the Communications-Electronics Command (CECOM) and the Signal Center to research the following:

- How network managers plan, engineer, and control MSE networks
- What objective network management architecture should the Army pursue
- How to integrate the Network Planning Tool (NPT) and the Enhanced Switch Troubleshooting (EST) into an overall management system
- How to transfer research to other military network.

The Army should continue the research into the MSE network management process. This thesis presented an analysis of the current process in chapter IV. It discussed tools to help network managers become more productive but it did not research ways to improve the process itself. The Army's research should include an analysis of other processes to manage networks.

This chapter presented a network architecture to solve the Army's network problem. The Army should continue the research to prove or dispute its potential to improve network management. The Army Signal Center can assign personnel and resources to study the problem. The architecture discussed in this chapter is only a proposal.

The Army should research ways to integrate the research it is conducting now into an overall management system. The NPT and the EST are promising but they do not work together. The current SCC manages the circuit and packet switched network, but the two are not integrated. The Army will not be able to capitalize on the synergy of all of its tools if it does not integrate them.

Finally, the Army should study how to apply the research on MSE network management to other military networks. The TRI-TAC system is a higher echelon communications network closely related to MSE that has similar network management problems. The US Air Force and the US Marine Corps both have tactical networks similar to MSE. The same can also be said for other North Atlantic Treaty Organization (NATO) armies. This thesis should just be considered a start for a long string of projects to make military telecommunications network management more effective and efficient.

BIBLIOGRAPHY

Andriole, Stephen J., ed. Artificial Intelligence and National Defense (Washington, D.C.: AFCEA International Press, 1986).

Andriole, Stephen J., and Halpin, Stanly M., ed. Information Technology for Command and Control: Methods and Tools for Systems Development and Evaluation (New York: IEEE Press, 1991).

Andriole, Stephen J. and Heilmeier, George H., High Technology Initiatives in C^3I, (Washington, D.C.: AFCEA International Press, 1986).

Brachman, Ronald J., " 'I Lied about the Trees' Or, Defaults and Definitions in Knowledge Representation," AI Magazine, Fall 1985, pp. 79-91.

Caudill, Maureen, "Neural Networks Primer: Part 1," AI Expert, December, 1987, pp. 47-61.

Coad, Peter, and Yourdon, Edward. Object-Oriented Analysis, 2nd ed., (Englewood Cliffs, NJ: Yourdon Press, 1991).

Douglas, Theodore Douglas., Tactical Automated Network Management Systems, University of Colorado - Boulder, 1989.

Dreyfus, Hubert and Dreyfus, Stuart, "Why Computers May Never Think Like People," Technology Review, January 1986, p. 54.

Dreyfus, Hubert and Dreyfus, Stuart, "Why Expert Systems Do Not Exhibit Expertise," IEEE Expert, Summer 1986, p. 88.

Erickson, Eric C., Erickson, Lisa Traeger, and Minoli, Daniel, Expert Systems Applications in Integrated Network Management, (Massachusetts: Artech House, Inc. 1989).

Goda, Bryon S., "Communications on a Mobile Battlefield in the 100 Hours War," Army Communicator, Spring 1991, pp. 42-47.

Hart, Anna Knowledge Acquisition for Expert Systems, (New York: McGraw Hill, 1986).

Hays, Jan A., Integrated Network Management Tools and Solutions for Battlefield Communications Systems - An Analysis, University of Colorado - Boulder, 1990.

Hendler, James A. Expert Systems: The User Interface, (Norwood, NJ: Ablex Publishing Corp, 1988).

Herman, James, "Enterprise Management Vendors Shoot It Out: Will End-Users Get Caught In The Crossfire?" Data Communications, November 1990, pp. 234-243.

Karr, Holly J., Network Management: Current Trends and Future Directions, University of Colorado - Boulder, 1987.

Levine, Robert I., and Drang, Diane E., A Comprehensive Guide to AI and Expert Systems Using Turbo Pascal, (New York: McGraw Hill, 1988).

Liebowitz, Jay. Expert System Applications in Telecommunications, (New York: John Wiley & Sons, 1988).

Luger, George F., and Stubblefield, William A., Artificial Intelligence and the Design of Expert Systems, (California: The Benjamin/Cummings Publishing Co., Inc. 1989).

Lusher, Elaine P., "AI and Communications Network Design," AI Expert, August, 1990, pp. 40-47.

Parkin, Edward James., The Application of Expert Systems to Telecommunications Network Management, University of Colorado - Boulder, 1989.

Pinson, Lewis J., and Wiener, Richard S. An Introduction to Object-Oriented Programming and SmallTalk, (Massachusetts: Addison-Wesley Publishing Co., Inc. 1988).

Rappaport, David M., "Carrier Approaches to Integrated Network Management," Business Communications Review, Vol. 21, No. 6, June 1991, pp. 30-39.

Rheingold, Howard, Virtual Reality, (New York: Summit Books, 1991).

Richer, Mark, AI Tools and Techniques, (Norwood, NJ: Ablex Publishing Corp, 1989).

Rickerson, Don, "MSE Node Center Site Reconnaissance," Army Communicator, Summer/Fall, 1990, pp. 22-25.

Robertson, Jack, "Voicing Concern on Army Communications," Electronic News, Vol. 37. No. 1882, October 14, 1991.

Scarbalis, David A., An Analysis of Army Battlefield Automation Systems, University of Colorado - Boulder, 1989.

Sloane, Stephen B., "The Use of Artificial Intelligence by the United States Navy: Case Study of a Failure," AI Magazine, Vol. 12, No. 1, Spring 1991, pp. 80-92.

Swanson, Raymond H., "Emerging Technologies for Network Management," Business Communications Review, Vol. 21. No. 8. August 1991, pp. 53-58.

Tanimoto, Steven L., The Elements of Artificial Intelligence, (New York: Computer Science Press, 1990).

Wenger, Etienne, Artificial Intelligence and Tutoring Systems, (Los Altos, CA: Morgan Kaufmann Publishers, Inc, 1987).

Artificial Intelligence Handbook (Vol 1: Principles, Vol 2: Applications), (Research Triangle Park, NC: Instrument Society of America, 1989).

GOVERNMENT DOCUMENTS

AirLand Operations: A Concept for the Evolution of AirLand Battle for the Strategic Army of the 1990s and Beyond, Department of the Army, US Army Training and Doctrine Command, Ft Monroe, VA, August 1, 1991.

Artificial Intelligence Project Summaries, US Army Artificial Intelligence Center, May 23, 1990.

BATTLEFIELD AUTOMATION: Army Tactical Command and Control System's Schedule and Cost, US General Accounting Office, Report Number GAO/NSIAD-91-118BR, April 1991.

MSE System Control Center (SCC) Requirements Document, GTE Tactical Systems Division, GTE Government Systems Corporation, January, 1991.

MSE Packet Switched Network Requirements Document, GTE Tactical Systems Division, GTE Government Systems Corporation, January, 1991.

III Corps MSE Tactical Standing Operating Procedures, Headquarters III Corps and Ft Hood, Ft Hood, TX, June, 1990.

FM 11-30 MSE Communications in the Corps/Division, Headquarters, Department of the Army, Washington, D.C., June, 1990.

FM 11-38 MSE System Management and Control, Department of the Army, Washington, D.C., April, 1991.

FM 24-1 Signal Support in the AirLand Battle, Headquarters, Department of the Army, Washington, D.C., October, 1990.

GOVERNMENT STUDIES

"An Analysis of Battlefield Communications," Headquarters, Department of the Army, Washington, D.C., 1989.

"Battlefield Information Systems in 2015 Study," National Security Industrial Association Command, Control, Communications and Intelligence Committee, Washington, D.C., Sept. 1989.

"Branch Operational Concept: Objective Signal Support System (Post 2000)," (Department of the Army, US Army Signal Center, Ft Gordon, GA, October 11, 1991).

"Signal 2000: White Paper on Signal Support for AirLand Operations in the 21st Century," (Department of the Army, US Army Signal Center, Ft Gordon, GA, October 9, 1991).

"US Army Signal Center Lessons Learned (Unclassified)," (Department of the Army, US Army Signal Center, Ft Gordon, GA, November 13, 1991).

APPENDIX A

Knowledge Representation Schemes

This appendix expands on the discussion in Chapter III on knowledge representation schemes. It discusses semantic networks, frames, production rules, objects, and predicate logic. The purpose of this appendix is to provide background information on the most common knowledge representation schemes used by AI-based tools. Readers already familiar with AI may wish to quickly skim this appendix.

Semantic Networks

Semantic networks were originally designed by Collins and Quillian to model human information storage and management. They hypothesized that humans store knowledge hierarchically and that knowledge is kept at the highest abstract level possible in the hierarchy.

Semantic networks represent knowledge as a set of nodes and arcs connecting the nodes. A node can represent an object, place, condition, or event. The arcs represent relationships between the nodes. These relationships include "is-a," "a-kind-of," "a-part-of," or "has-part." Figure A-1 shows that a MSE Network "is-a" communications system. A Node Center "has-a" Management Shelter and a Node Center Switch. A Communications Node is "a-part-of" a MSE Network.

Semantic networks represent an inheritance hierarchy. Lower level nodes can inherit properties from higher level nodes. Properties can be canceled out when inheritance is not appropriate. The Node Center Switch is "a-part-of" a node center and is "a-part-of" a MSE Network. This inheritance allows lower levels of the hierarchy to assume attributes from higher levels without explicit declarations.

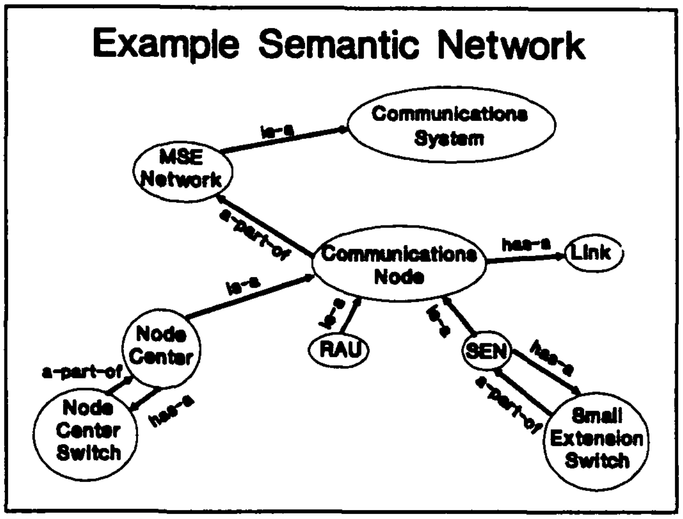

Figure A-1

Semantic networks have an advantage of being intuitive. They can make a useful mechanism for storing knowledge in an AI system. However, there are other knowledge representation schemes such as frames and objects which build on the inheritance feature and may be better suited for knowledge representation.

Frames

Researcher Marvin Minsky developed the concept of Frames to describe how humans organize knowledge about common concepts and situations.[1] Minsky hypothesized that people do not construct new knowledge structures from scratch when they encounter a new situation. Instead, humans take a similar experience

[1]David Rutberg, "Fundamentals of Problem Solving," in A. Eli Nisenfeld and James R. Davis (eds.), Artificial Intelligence Handbook, (Research Triangle Park, NC: Instrument Society of America, Vol. 1., 1989), p. 13.

and add or change aspects of the previous experience to make it fit the new situation. The reuse of similar knowledge structures reduces the amount of memory required to store new information. Minsky called these knowledge structures frames.

Frames can be viewed as complex semantic nets. Frame diagrams show the relationships between nodes as semantic nets do. However, frames can take on a great deal of internal structure. Each node, called a frame, represents some entity type such as a communications node. The frame is made of a collection of named slots. Each slot can be an attribute about the entity, such as color, or a link to another frame. Frames can also have facets which store information about the slots.

Figure A-2 shows an example of frames. Each frame has a name and a link to a higher level frame. Each frame has slots which can store default information about an entity. Frames also inherit slots from parent frames. Slots can also have code attached which is set to execute whenever the

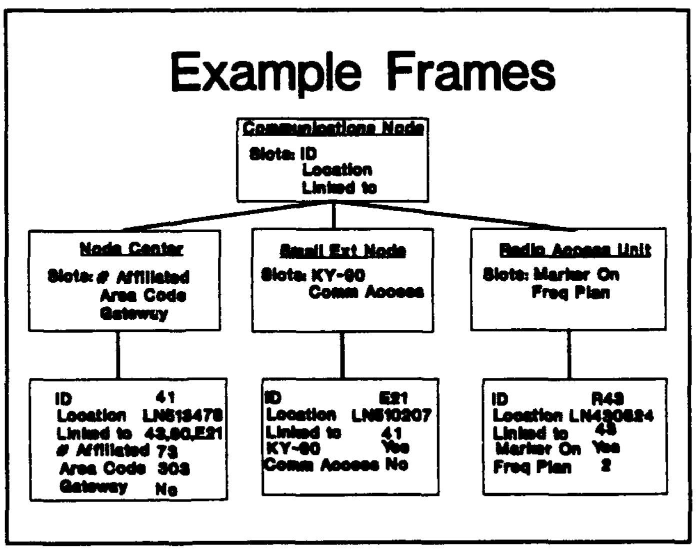

Figure A-2

value of the slot changes. This property enables the use of demons which are side effects of changes. Frames can be used to describe dynamic situations. The effects of change in complex models can be represented by attaching code to slots.

Expert systems can use multiple copies of the same type frame to store similar information. For example, an MSE network has many like nodes. An expert system can develop a frame to describe a MSE node center. The developer can make a copy of the frame for each node center and tailor each frame to the particular attributes of the nodes. Each node would have the same base of attributes and behaviors and additional information unique to the node.

The process of taking a default frame and filling the particular information about the entity is c. ed instinciation. In the previous example, the system instinciates a frame for each node in the network.

Frames have significant advantages as knowledge representation structures. They are intuitively appealing because they model entities in ways similar to how humans do. Frame structures can handle default values and generic behaviors. Their inheritance feature can save memory space and coding effort.

Frames can also have significant disadvantages. The inheritance feature can cause unintended attributes of entities to be represented.[2] Most fram.-based systems do not provide a means for distinguishing between the essential and non-essential properties of an entity. A system could theoretically instinciate a frame

[2]Ronald J. Brachman, " 'I Lied about the Trees' Or, Defaults and Definitions in Knowledge Representation," AI Magazine, Fall 1985, p. 80.

about a microwave radio link that does not have radio frequencies assigned. The overall effect is to make universal truths impossible to model.

Production Rules

Production rules are a simple and common means of expressing knowledge. Human experts' heuristics can many times be represented as a set of production rules. Production rules consists of an antecedent and a consequent. As previously stated, the antecedent is the IF part of an IF ... THEN ... sequence. Whenever the antecedent tests true, the inference engine fires the rule's consequent. The action of firing rule consequents can infer enough knowledge to cause other rule antecedents to become true.

Production rules are popular because of their simplicity and readability. An expert system designer can easily verify the rules with the human expert. Unfortunately, production rules alone are not complex enough to model most problems.

Objects

Objects and Object Oriented Programming (OOP) represent both a knowledge representation structure and a method for solving problems. The knowledge representation is in the form of data structures called objects. The problem solving is in the interaction between the objects.

An object is a distinct package of code that represents a physical object or an abstract idea. Objects are self contained and cannot be accessed from the outside. They communicate with other objects by sending messages. The only way for an object to access another data in another object is for the first object to send a message to the second.

Objects have private data, shared data, global shared data and behavior. Private data is data used internally by the object and other objects cannot access the data except by requesting the data with a message. Shared data is available to a group of objects. Each object can have code which references or alters shared data. Global shared data is data available to all objects in the system. Behavior is the actions an object can perform such as responding with data or calculating some value.

Like objects are grouped together into classes. Each member object of a class has the same shared data and behaviors.[3] Each member also has the same set of private data whose values can be unique to each object. This relationship is often called classes and instances. It can also be called classes and objects. The class is the group of the like objects. Each object (or instance) has the same properties of every object in the class plus the private data unique to the object. For example, one can define a node center class with the attributes and behaviors common to all node centers. Each object (or instance) in the node center class contains the private data such as location and configuration unique to each node center.

There are four specific properties to object oriented programming. A

---

[3]Peter Coad and Edward Yourdon, Object-Oriented Analysis, 2nd ed., (Englewood Cliffs, NJ: Yourdon Press, 1991), p. 73.

computer language must exhibit each of these four behaviors to be considered a true OOP language. These properties are abstraction, encapsulation, inheritance, and polymorphism.[4]

Abstraction refers to a concise representation of a more complicated idea or physical object. The designer determines what attributes and behaviors of an object need to be represented to solve a problem. For example, to solve network management problems, it is not necessary to model every aspect about a node center. The weights of the communications shelters are usually not relevant to planning MSE networks.

Encapsulation refers to the hiding of the internal representations and behaviors of objects. This allows several designers to work on developing specific objects. Each designer builds the objects individually without worrying about how specific code will affect other objects. The only coordination between designers is to insure a correct protocol of messages between the objects. Encapsulation also enables updates to individual objects to not affect the behaviors of other objects as long as the messages share a common protocol.

Inheritance in OOP is similar to inheritance in frames. Objects can be designed on a hierarchy like frames. The objects inherit the data and behaviors of the objects above. Inheritance reduces the amount of program code needed to model similar objects.

---

[4]Lewis J. Pinson and Richard S. Wiener, An Introduction to Object-Oriented Programming and Smalltalk, (Reading, MA: Addison-Wesley Publishing Company, 1988), p. 1.

To illustrate inheritance, consider a class hierarchy similar in structure to the example frames in figure A-2. If the communications node class defined location and linked to as private data, the node center, small extension node, and radio access unit classes would each have the same private data automatically. Each of these classes would then be able to define additional private data as needed.

Polymorphism refers to ability to assign multiple meanings to messages. The meaning of a particular message is determined by the code in the object that receives the message. Each object can define an individual meaning to the message unique to that object. A common example of this concept is the "+" operator. In most cases, a "+" refers to addition but in some cases it can mean "concatenate string." The meaning for the "+" message would be defined in the objects the message was sent.

Objects and Object Oriented Programming are powerful tools. They are related to frames and share the problem of non-sensible inheritance with frames. Objects offer an intuitive way to model MSE networks and their behaviors. They also allow the problem domain to be divided among multiple designers. OOP is a conventional programming paradigm that can be adapted to the AI field. Chapter four explores some OOP tools.

Predicate Logic

Predicate logic is another type of knowledge representation and reasoning based on formal syntactic manipulation of logic formulas using pre-defined rules of inference.[5] A predicate logic program manipulates the knowledge based on syntactic but not semantic meaning. This form of knowledge representation and reasoning is good for some simple tasks in well defined domains but not for complex tasks.

Knowledge in predicate logic is represented as symbols that denote relationships between objects. The program searches defined relationships to assert new ones. A description of the predicate logic symbols is beyond the scope of this thesis. For simplicity, the facts and rules in the following example are expressed in English.

Consider the following example of a predicate logic inference. Given that Node Center (NC) 41 is west of the battalion command post and the battalion command post is west of NC 42. A predicate logic program can infer that NC 41 is west of NC 42. If given more facts about the node centers and the command post, a predicate logic program would continue to apply rules of logic to make more inferences.

This knowledge representation scheme has limited use. It requires a well structured domain and many parts of the MSE domain are well structured. A problem with predicate logic programs is that they apply rules until there are no more to apply. This can lead to combinatorial explosion. Another problem is that all facts are treated equally. A predicate logic program cannot focus its attention on a subset of the facts.

---

[5]Rutberg, p. 24.

Conclusion

This appendix has discussed some of the common knowledge representation schemes used in AI-based software today. These knowledge representation schemes represent powerful ways to describe the real world situations in computer memory. Each scheme is suited for specific types of applications while no scheme is suited for all possible types of applications. AI-based tools often use a mix of these knowledge representation schemes or even other schemes not discussed in this thesis. However, any potential AI-based MSE network management tool will likely use a mix of these schemes to represent network status and events.

APPENDIX B

MSE NETWORK MANAGER SURVEY QUESTIONS

8 March 1992

MEMORANDUM FOR: MSE Network Managers

SUBJECT: MSE Network Management Survey

1. I request your input on several MSE network management related questions.

2. I need your ideas as part of my masters thesis work at the University of Colorado, Boulder. The subject of the thesis is the application of artificial intelligence techniques to MSE network management.

3. I know that your time is valuable. The enclosed survey should only take a few minutes of your time.

4. Per University of Colorado regulations:

a. You are not required to participate in the survey. However, a complete set of responses would make my research more valuable. You may choose to omit any question on the survey.

b. You are not required to identify yourself on the survey. If you identify yourself, your name will not be released to anyone else. I will only use your name to contact you for more information.

c. There are no risks to you for completing the survey. There are no direct benefits to you for completing the survey. Do not include any classified information on the survey.

d. I am a graduate student. My advisor is Dr Ken Kozar, Graduate School of Business, Campus Box 419, U of Colorado, Boulder, CO 80309-0419. Phone: 303/492-8347.

5. Thank you for your help.

Charles E. Lane
CPT, SC

MSE Network Management Questionnaire

1. Which of the following message formats do you actually use to get network information from Node Centers to the SCC?

____ Open/Close Links
____ RAU plan changes
____ Other (Please specify):
____ COMSEC information
____ Open/Close/Move Teams

2. Do you often use free text messages to get network information from Node Centers because you need information not available in any of the other type messages? If so, what information do you send in these messages? (Note: If you use voice or laptop computers instead of TTY to get this information, your response would still be helpful). Please consider what reports you require from Node Centers.

3. If you could make five improvements to the network management hardware and/or software, what would they be?

1. ______________________________

2. ______________________________

3. ______________________________

4. ______________________________

5. ______________________________

4. What are the most time consuming tasks (SCC or manual) you do related to MSE network management? Please break your answer down into:

Planning

Engineering

Controlling

5. What specific MSE network problems do you diagnose and/or troubleshoot the most often? Please consider each phase of the network deployment.

6. In your opinion, do you believe that Node Center OIC/NCOICs have the tools they need to effectively manage the network at their level? If not, what else do you believe they need to do their job better?

7. **Optional:** If I need more information, can I contact you? If so, please list your name, address, and duty phone.

Name:
Address:

Duty phone:

E-Mail:

8. Imagine that you have been tasked to design an effective network management architecture to replace the SCC. You have the authority to put a *"black box "* in the NCS, SEN, LEN, and the RAU. Theses devices could automatically send status information to your centralized network management system.

What information would you want to automatically obtain from each of these devices to help your MSE management tool effectively plan, engineer, and control networks. Please **add** to the lists data items you can think of and **delete** those you don't think are needed.

Information from Each NCS/LEN to the Network Manger **Additional Info**

- Current configuration of NCS data base
- Breakout of link status by DTG/TGC for each active link
- Directory numbers affiliated by DTG
- Directory numbers pre-affiliated
- Duplication Status
  - Time of setup
  - Breakdown of backup to adjacent NCSs
- Bulk transfer logs

Status of Gateway/Commercial office (DGC command)

- Automatic notification for every instance of:
  - Called Directory Number not found
  - KY-68 failed to synch with LKG
  - Failed search for a directory number (DSS command)
  - Link taking hits every __ seconds

SEN Status Information to the Network Manager

- Directory numbers affiliated by terminal address
- Status of KY-90
- Status of commercial lines
- SHF relay in use (Y/N)

RAU status Information to the Network Manager

- GLU affiliated (Y/N)
- Marker on (Y/N)
- Frequency plan in effect
- KY-68 affiliated and able to place calls (Y/N)

Other MSE teams

The Application of Artificial Intelligence to MSE Network Management

Thesis Defense

CPT Charles Lane, US Army

25 June 1992

Thesis Defense Agenda

- Why this topic
- Current situation
- What was researched
- Who will benefit from this research
- Research methods
- How analysis was developed
- Conclusions
- Limitations of the research
- Recommendations for further research
- General questions

Why This Topic

- Desire to contribute to Army research
- Personal experience in Army MSE networks
- Courses and interests in AI and network mgt
- Recognition of current shortcomings

Current Situation

MSE Network Management

- MSE the primary tactical commo system
- Management is difficult
- Managers have limited experience
- Cumbersome management tools
- Piecemeal improvements in management tools
- NDI acquisition strategy

What Was Researched

- Is using Artificial Intelligence based network management tools a good option?
- What could the Army expect to see in AI based network management tools?
- Would "off the shelf" tools be appropriate?
- What should the Army do now to improve network management?

Who Benefits From This Research

- US Army Signal Center
  - TRADOC Systems Manager (TSM) - MSE
  - Directorate of Combat Developments
  - Signal Leadership Department (SLD)
- US Army Communications-Electronics Command
  - Project Manager (PM) - MSE
  - MITRE Corporation
- GTE Government Systems Corporation

Research Methods

- Literature search
  - Academic journals and trade magazines
  - Vendor brochures and manuals
  - Military journals and manuals
- Interviews
  - Telephone and E-mail
  - Personal
- Surveys
  - MSE equipped signal units
  - MSE network managers conference (April)

Analysis Development

- Literature search to find what was available in the commercial sector
- Research and analysis of how MSE networks are managed
- Analysis of if commercial tools would work for a tactical military network
- Research of what tools have been developed for MSE
- Analysis of what AI-based tools should do for MSE
- Proposal for an MSE network management architecture

Conclusions Reached

- Army should conduct a formal analysis of how it manages MSE networks
  - identify what tasks should be automated
  - identify where using AI would be appropriate
- Solve problem of no automatic telemetry
- Develop a possible management architecture
- USA Signal Center
  - define network management architecture
  - system to develop knowledge base
  - system maintenance procedures
- USA Communications-Electronics Command
  - develop network management tools

Limitations of the Research

- No documented analysis of MSE network management
  - Expanded scope of thesis to more areas
- Lack of travel
  - Observation
  - Interviews
  - Visits to research facilities
- No prototypes of AI based tools

Recommendations
for Further Research

- Analysis of how MSE network management processes could be improved
- Analysis of MSE AI-based tool development
- How Army can capture MSE expert knowledge
- How AI can improve network management training

Summary

- Worthwhile area of research
- My research is only a beginning
- Army should consider conducting more formal research
- US Army has the best tactical commo system in the world
- American taxpayers deserve to have it managed the best way possible