

USAISEC

*US Army Information Systems Engineering Command
Fort Huachuca, AZ 85613-5300*

4

U.S. ARMY INSTITUTE FOR RESEARCH
IN MANAGEMENT INFORMATION,
COMMUNICATIONS, AND COMPUTER SCIENCES
(AIRMICS)

Message Handling in the Post-2000 Era:

Executive Summary

(ASQB-GC-90-013)

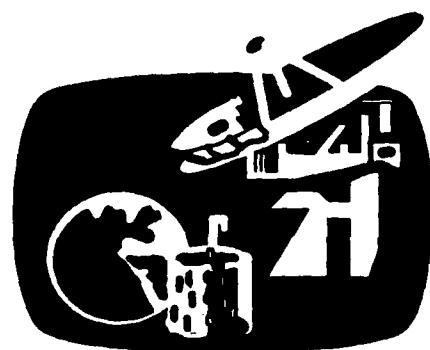
November, 1989

AD-A219 983

USAISEC
APR 03 1990
E
CD

Public release;
Distribution Unlimited

115 O'Keefe Bldg
Georgia Institute of Technology
Atlanta, GA 30332-0800



90 04 03 132

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

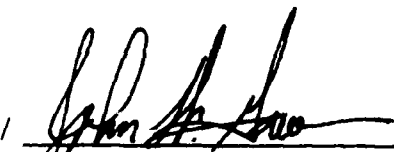
Form Approved
OMB No. 0704--188
Exp. Date: Jun 30, 1986

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b. RESTRICTIVE MARKINGS NATO													
2a. SECURITY CLASSIFICATION AUTHORITY N/A		3. DISTRIBUTION / AVAILABILITY OF REPORT Unclassified/Unlimited													
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE N/A															
4. PERFORMING ORGANIZATION REPORT NUMBER(S) N/A		5. MONITORING ORGANIZATION REPORT NUMBER(S) ASQB/GC-90-013													
6a. NAME OF PERFORMING ORGANIZATION Georgia Institute of Tech. Electrical Engineering	6b. OFFICE SYMBOL (if applicable) N/A	7a. NAME OF MONITORING ORGANIZATION AIRMICS													
6c. ADDRESS (City, State, and ZIP Code) Atlanta, GA 30332-0250		7b. ADDRESS (City, State, and Zip Code) 115 O'Keefe Bldg., Georgia Institute of Technology Atlanta, GA 30332-0800													
8a. NAME OF FUNDING/SPONSORING ORGANIZATION NATO/U.S. Army Signal Corp.	8b. OFFICE SYMBOL (if applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER													
8c. ADDRESS (City, State, and ZIP Code) U.S. Army Signal Center Fort Gordon, GA 30905-5090		10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. PROJECT NO. TASK NO. WORK UNIT ACCESSION NO. 612T83 DY10-03-01 08													
11. TITLE (Include Security Classification) Message Handling in the Post-2000 Era: (Executive Summary) (UNCLASSIFIED)															
12. PERSONAL AUTHOR(S) Browning, Douglas W., Wicker, Stephen B.															
13a. TYPE OF REPORT Final	13b. TIME COVERED FROM 2/15/89 TO 11/30/89	14. DATE OF REPORT (Year, Month, Day) 1989 November 17	15. PAGE COUNT 12												
16. SUPPLEMENTARY NOTATION															
17. COSATI CODES <table border="1"><thead><tr><th>FIELD</th><th>GROUP</th><th>SUB-GROUP</th></tr></thead><tbody><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></tbody></table>		FIELD	GROUP	SUB-GROUP										18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) Communications, Networks, Post-2000	
FIELD	GROUP	SUB-GROUP													
19. ABSTRACT (Continue on reverse if necessary and identify by block number) Communication architecture for message handling in the very far-term heavy tactical environment are considered. The projected limitations of technology, a taxonomy of possible architectures, and projected requirements are presented. Based on this information, the suitability of architectural options is analyzed, and an architecture is proposed for post-2000 mobile and nonmobile tactical communications. The implications for standards are discussed.															
20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED / UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS		21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED													
22a. NAME OF RESPONSIBLE INDIVIDUAL WINFRED Y. FONG		22b. TELEPHONE (Include Area Code) (404) 894-3136	22c. OFFICE SYMBOL ASOB/GC												

This work is done under contract DAKF11-86-D-0015 for the United States Army Institute for Research in Management Information, Communications, and Computer Sciences (AIRMICS), the RDTE organization of the United States Army Information Systems Engineering Command (USAISEC). This report is not to be construed as an official Army position, unless so designated by other authorized documents. The material included herein is approved for public release, distribution unlimited. Not protected by copyright laws.

Accession For	
NTIS GRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

THIS REPORT HAS BEEN REVIEWED AND IS APPROVED

s/ 
 John W. Gowens
 Division Chief
 CNSD

s/ 
 John R. Mitchell
 Director
 AIRMICS

Message Handling in the Post-2000 Era: Executive Summary

**Professor Douglas W. Browning
Professor Stephen B. Wicker**

Contract DAKF11-86-D-0015

Friday, November 17, 1989

1. Introduction

In the history of communication, there are three fundamental principles that stand out with amazing consistency:

- the most expensive component of a communication network is the media by which a signal is carried over a large distance
- communication network technology has been limited primarily by the ability to handle information at each switching point
- applications of larger, faster, and more efficient communication systems have always far surpassed the most far-sighted intentions of the developers.

In spite of the rapid advances expected in communication technology, there is no evidence that these principles will not continue to hold through the foreseeable future. The only exception is the limitation of the use of atmospheric propagation channels due to limited spectral availability as opposed to switching technologies.

The tactical communications environment in the post-2000 era will be drastically affected by two contemporary phenomena. The first is the rapidly evolving state of communication technology. The development of lightwave communications and the advancement of older technologies is greatly increasing the quantity and quality of voice and data communication available in the tactical theater. The second phenomenon is the ongoing evolution in weapons technology. Anti-radiation weapons are placing severe restrictions on radio emissions. In general the overall survivability strategy must be reevaluated to take into account the increased lethality of the tactical environment. This study was designed to take these and other factors into account and to propose an architecture for tactical message handling systems in the post-2000 era. The results of this study are outlined in the following executive summary.

2. Architectural Options

The first step in the study was the identification of options for the message handling system architecture. These options are broken up into the following five categories in rough accordance with the ISO protocol.

- **Media Options**
- **Cryptographic Options**
- **Communication Subnet Options**
- **Internetworking Options**
- **Higher Layer Options**

2.1 Media Options

The media options for tactical communication systems can be divided into two categories: atmospheric/free space channels and confined channels. The former consists of the following:

- **Over-the-Horizon HF and VHF (OTH)**
- **Line-of-Sight Radio and Optical (LOS)**
- **Sub-Orbital Platforms**
- **Low-Earth-Orbit Satellites**
- **Geosynchronous Satellites**

Each of the atmospheric/free space media has unique positive and negative attributes. As a whole, however, they share several characteristics that make them a good choice for some applications and a bad choice for others. For example, they do not require the deployment of a physical channel. This is clearly useful in mobile communication systems. Unfortunately the enemy has access to this channel as well and may thus employ interception (both passive and active) and jamming. Other negative attributes include limited bandwidth due to the frequency selective characteristics of transmitter hardware and the atmosphere itself. Finally survivability of the transmitter hardware is limited due to the existence of anti-radiation weapons.

Confined channels offer an alternative whose positive and negative attributes are virtually a mirror image of those provided by atmospheric/free space channels. Confined channels include

- **Copper Wire**
- **Waveguide**
- **Fiber Optical Cable**

Confined channels require that the physical channel be deployed prior to communication. In most mobile applications this is clearly impractical. There is also the additional problem of media destruction by enemy action and careless friendly armor. However, confined channels, particularly fiber optics, provide virtually unlimited bandwidth. They also require much lower transmitter power levels than their atmospheric/free space counterparts, reducing the weight of the transmitter. Confined channels also make it extremely difficult for the enemy to detect, intercept or jam communications. For example, passive or active coupling into a network can always be detected through time domain reflectometry (TDR). TDR not only detects intrusion but accurately pinpoints the location as well.

2.2 Cryptographic Options

The cryptographic options can be divided into private key systems and public key systems. Virtually all of the military cryptographic techniques used in the past can be characterized as private key systems. The basic operation of these systems is shown in Figure 1.

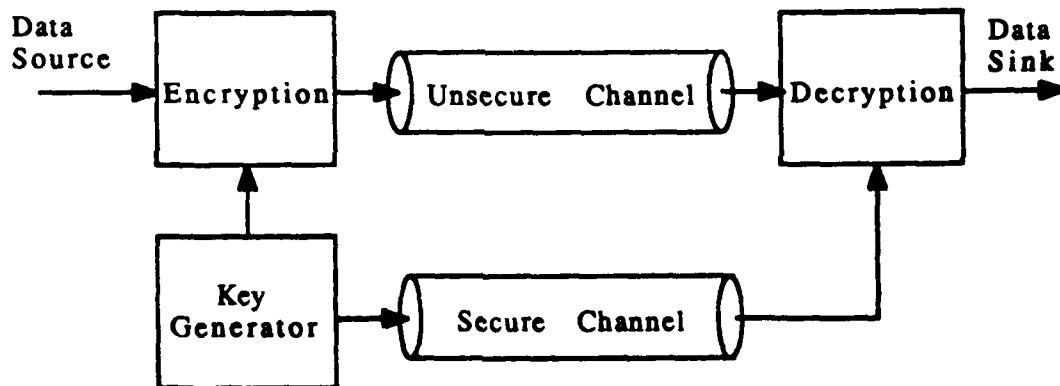


Figure One: Private Key Cryptosystem

Source and destination must first have agreed upon a cryptosystem. The source must then transmit a key to the destination so that the destination can properly set up his hardware for decryption. Since anyone with a copy of the key can decrypt the message, the key must be transmitted over a secure channel. This "secure channel" is generally in the form of a courier, and this entails a security risk.

Public key cryptography was first described in 1976 by Whitfield Diffie and Martin Hellman¹. It is based on the definition of a mathematical problem that is easily performed in one direction but virtually impossible in the other without the benefit of certain side information. Consider Figure Two. Two keys are created, one for encryption, the other for decryption. The encryption key can be made

¹W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Volume IT-22, Number 6, November 1976, pp. 644-654.

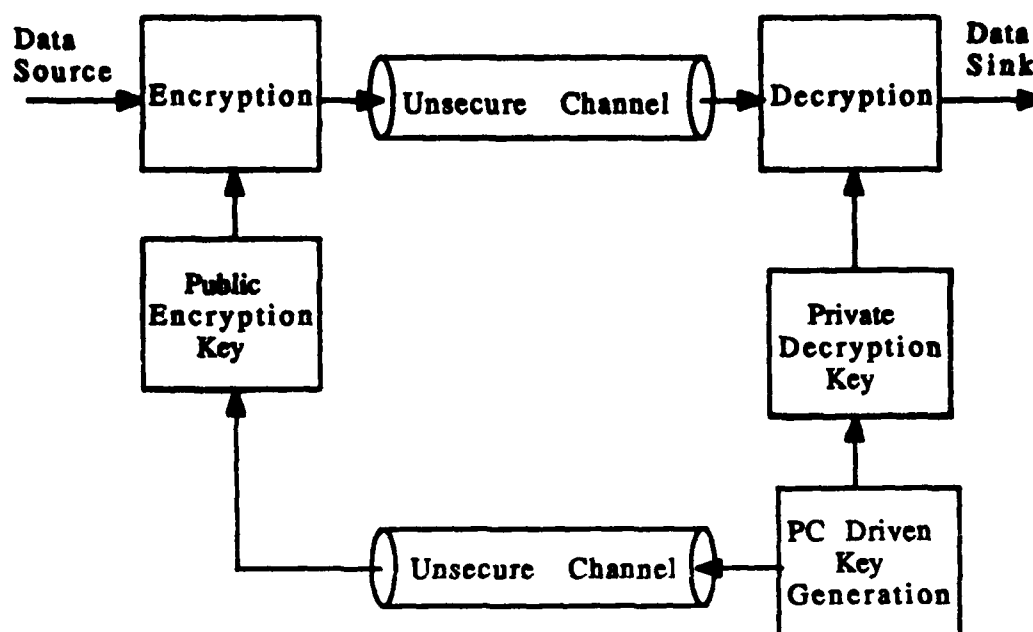


Figure Two: Public Key Cryptosystem

public, for it provides no help in the recovery of encrypted information. The decryption key is kept secret by the intended recipient, for there is no need for the encryptor or anyone else to be able to decipher messages to the recipient. The need for a secure channel has thus been eliminated.

Unfortunately the public key algorithms are much more computationally intensive and hence slower than the private key algorithms. For example, the best commercial private key systems can operate at 10 Kbps² while there exist commercial DES³ chips that can operate at T1.

The combined system shown in Figure Three is suggested as a possible solution. It maximizes speed through the use of private key cryptography for regular communications. The problem of key distribution is handled using public key cryptography, eliminating the need for secure channels while minimizing utilization of the slower public key hardware.

2.3 Communication Subnet Options

Communication subnet options can be classified as shown in Figure Four. The options are first divided into single-hop and multi-hop systems. In single-hop systems all transmissions are generally seen by all users. It is thus not necessary that routing decisions be made prior to or during transmission.

²RSA Data Security Inc., MILCOM 1989, Boston Massachusetts.

³DES, the Data Encryption Standard, is a private key system that is generally accepted as an encryption standard by the telecommunications and computing industry.

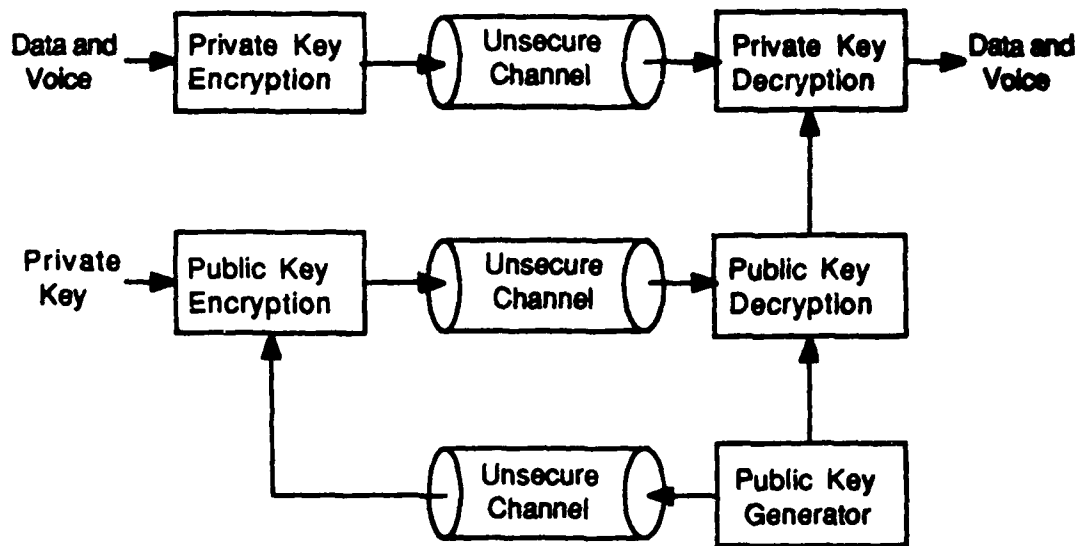


Figure Three: Combined Private/Public Key Cryptosystem

Furthermore packet queueing occurs only at the source and the destination. Examples of single-hop systems include buses, rings, and satellite relays.

Multi-hop systems call for both routing and flow control and are thus much more complex than single-hop systems. In general queueing may occur at each node in a packet's route through the network. The principal advantages of multi-hop systems are flexibility in deployment and increased survivability through increased connectivity.

Multi-hop systems may use either confined or broadcast channels. Those that use confined channels usually have a mesh architecture similar to conventional long-haul networks. Multi-hop systems using broadcast channels can be further subdivided according to whether these channels overlap or fall into distinct groups of users. The latter architecture includes Packet Radio Networks, the former includes interconnection of Local Area Networks by gateways.

2.4 Internetworking Options

The primary issues affecting internetworking are interconnectivity, compatibility, security, standards, and network performance. There are a large number of protocol options that deal with these issues, most of which are equally effective. The implementation of these protocols depends on the identification of simple effective solutions, agreement on standards, and the creation of translators for interfaces between differing standards.

2.5 Higher Layer Options

Higher layer options are application dependent. However a few generic concepts are expected to be included in all options. These include

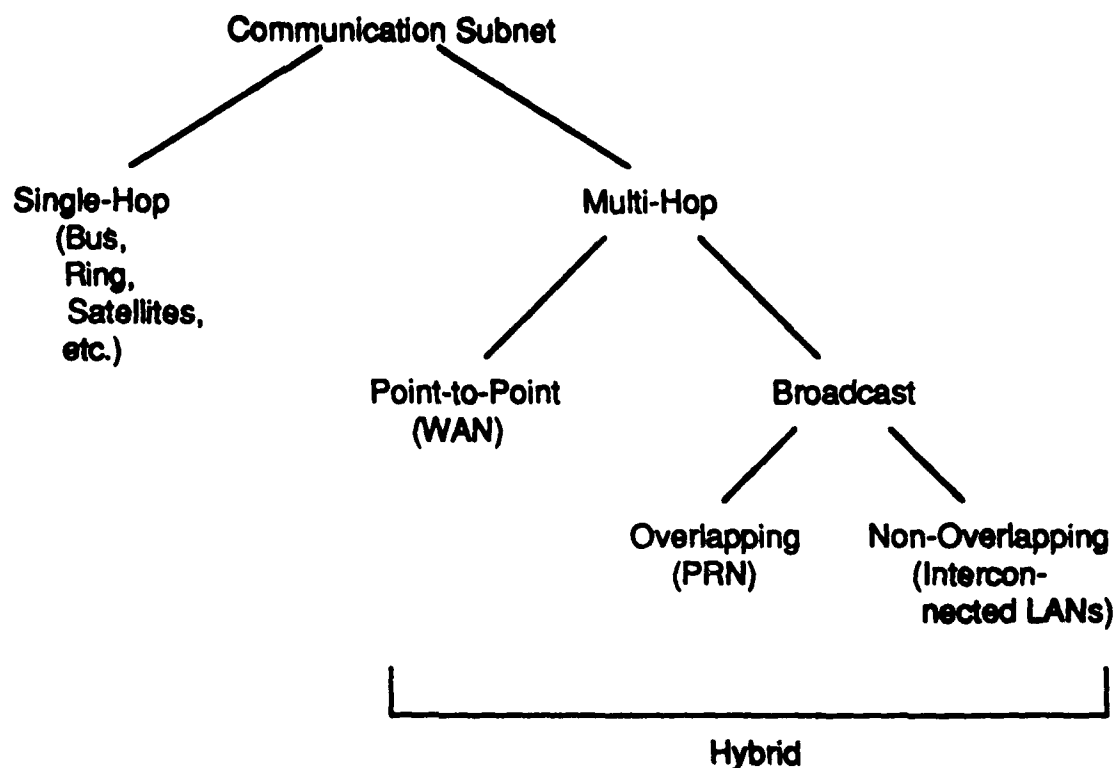


Figure Four: A Taxonomy of Subnet Options

- Distributed Databases
- Multi-Level Security
- Artificial Intelligence
- Distributed Process Control
- Pre-Processing of Data
- Software with Flexible Application

3. Suitability of Options for Non-Mobile Systems

Non-mobile systems can be divided into long-haul, base-level, and local area communication systems. Long-haul systems are characterized by their coverage of arbitrarily long geographical distances. In these systems the channel hardware dominates equipment costs and forces an emphasis on efficient channel utilization. Long-haul channels are generally not secure, and must rely heavily on data encryption. Survivability in these systems is achieved through highly connected topologies. The principle networking option for long-haul systems is a traditional mesh (arbitrary interconnection determined by the individual applications).

Base-level systems cover a more limited geographical area than long-haul systems. At the base-level switching devices join the communication links themselves as cost drivers. Despite the reduction in area coverage, base-level systems are still not secure. Data encryption must still be used extensively to ensure privacy. Survivability is once again provided through the use of highly connected topologies. The networking options are less clear than in the previous case. Individual point-to-point systems are inefficient and lack any significant degree of survivability. General mesh architectures (e.g. Wide Area Networks) may prove to be too expensive. Directional propagation LAN's lack survivability. The solution may lie with an optical fiber mesh in a constrained architecture. An emphasis should be placed on generic architectures with highly modular routing devices. Implementation of these types of networks will be heavily dependent on the development of effective photonic switches.

Local area communication systems should provide an inexpensive means of communication within an administrative unit. Due to the extremely limited geographic extent of the system, survivability is no longer a design factor. Since the local area systems will be the most numerous of all the systems, they should maximize the use of consumer off-the-shelf (COTS) hardware in their design. The physical and networking options for these systems are expected to focus on fiber optical channels and directional propagation topologies. Other methods may be used as dictated by commercial development.

4. Suitability of Options for Mobile Systems

Mobile communication within a tactical theater covers a wide range of distinct missions with differing characteristics. These missions include

- Connection to Non-Mobile Long-Haul Systems
- Medium Range Communication among Ground Units
- Local Area Communication among Ground Units
- Communication within a Mobile Command Post
- Communication to and from a Mobile Command Post
- Aircraft Communication

For near-range and medium-range connections to non-mobile long-haul systems, extensions of the medium range mobile system can be used in conjunction with a gateway. For long-haul connections several options exist, including satellites, commandeered public network channels, relay connections, and OTH radio. In all applications the choice will depend on distance, terrain, and friendliness of territory.

Two powerful options exist for medium range communication among ground units: packet radio networks and distributed cellular networks. Packet radio has the advantage of being self-configuring and relatively unstructured. A

distributed cellular system, however, offers much higher channel efficiency, conventional flow control, and a natural routing algorithm, three items sorely missed in packet radio systems. A third option lies in a combination of the two schemes. Distributed cellular networks can be designed with packet radio subchannels for maintaining network configuration.

Local area communication among mobile ground units poses a problem that is similar in many ways to the non-mobile case. The use of COTS hardware should be used as much as possible, but in a configuration that provides for easily replaced, modular components. If the ground units move relatively infrequently, then fiber optical cable can be used for interconnection. In most cases, however, LOS radio may be the only viable option.

Mobile command posts are envisioned to be a collection of vehicles deployed in a distributed fashion on the battlefield. The geographic distribution of the various elements of the command post is primarily intended for survivability. The transmitting element in particular should be placed well away from the remainder of the command post. Communication among the various units is anticipated to be at very high data rates. Media options include fiber optical cable (slow set-up, non-emissive) and line-of-sight radio (fast set-up, emissive).

In order to increase the operating lifetime of the mobile command post, the mobile communication network should be designed so that the command post looks like a standard node. Thus radio communication to and from the command post should be identical to that displayed by a lower-level mobile unit.

Communication to and from aircraft is currently envisioned to make use of the Air Force JTIDS program. This system provides reliable but low data rate communication with ground forces. Future options may include highly directional high bandwidth radio transmission to and from the aircraft.

Short-distance communication between aircraft should make use of high frequency LOS radio. If carrier frequencies are selected so as to lie in the oxygen or water resonant frequency bands, then detectability and jammability will be greatly reduced. Unfortunately transmitter power levels must be correspondingly higher.

5. Proposed Message Handling System Architecture

The message switching architecture for the Post-2000 tactical environment is driven by:

- projected user requirements
- projected limits of communication technology
- projected cost-effectiveness.

The recommended architecture includes the following components:

- Non-Mobile Local Area Networks
- Base-Level Networks
- Long-Haul Non-Mobile Network(s)
- Medium-Range Mobile Networks
- Connection between Medium-Range Mobile Networks and Long-Haul Networks
- Mobile Local Area Networks
- Mobile Command Post Internal Communications
- Connection between Mobile Command Posts and the Medium-Range Mobile Network
- Broadcast Connection with Aircraft
- Other Aircraft communication

The interconnection of these various segments is shown in Figure Five. The following paragraphs briefly summarize the authors' conclusions as to the future design, development, and implementation of each of these elements.

The use of non-mobile LAN's will be partially curtailed through the increased use of base-level networks. They will continue to be used, however, in cases where poor survivability is acceptable and as dictated by administrative concerns. Non-mobile LAN's will be constructed from COTS hardware or slightly modified (e.g. tempest) COTS hardware.

Base-level network links will be established using spatially separated interconnected fiber optical links. Secondary media will be used to increase survivability; LOS radio and optical links are suggested due to their complimentary performance characteristics (events that preclude the use of fiber optics might allow LOS transmissions and vice-versa). Nodes in the base-level networks will consist of modular photonic switches. Interfaces to long-haul networks, local users, and LAN's will be provided through appropriate gateways.

Long-haul non-mobile networks will be constructed using a fiber optical mesh capable of servicing all appropriate data types. The technology will parallel commercial systems except for the inclusion of higher connectivity for survivability. Secondary and possibly tertiary media will be used to further enhance survivability. OTH HF and LOS EHF satellite connections are suggested.

Medium-range mobile networks will be constructed from broadcast links. The networks will move data through a distributed cellular system while maintaining topology and configuration through the use of a packet radio subchannel. It is expected that the medium-range systems will incorporate variable transmitter power levels, spread-spectrum techniques, and distributed control algorithms.

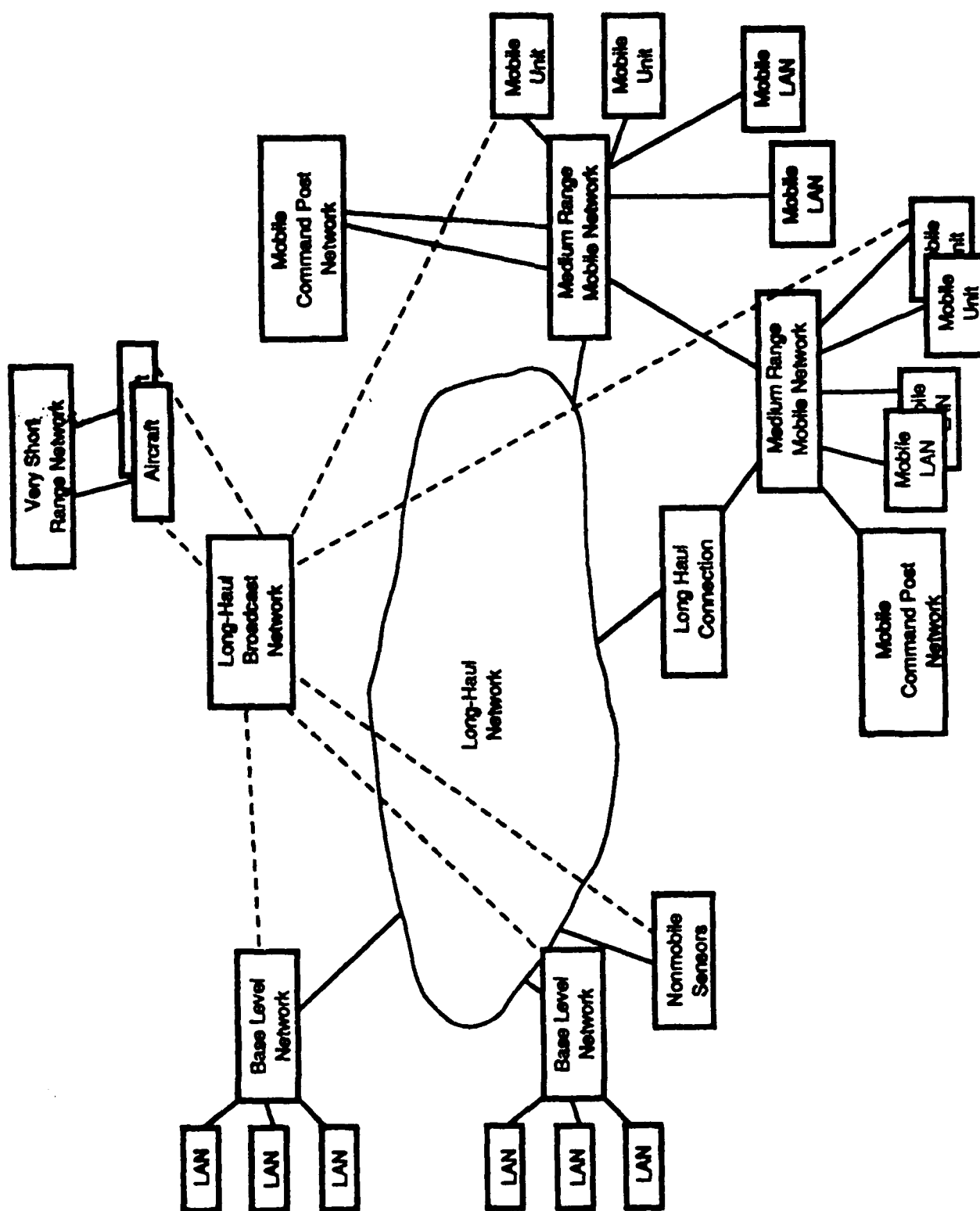


Figure Five: Recommended Architecture for Message Handling Systems in the Post-2000 Era

Near and medium range connections between medium-range mobile networks and non-mobile long-haul networks will be created through the extension of the mobile system and the addition of a gateway. Several architectures may be used, depending on the application. Satellites, commandeered public radio networks, relay connections, and OTH radio are suggested. Several issues remain to be resolved. For example, what is the role of the non-mobile system in providing connectivity within and among mobile networks?

Mobile LAN's may be selected from a variety of architectures, depending on the specific application. Low power radio (LOS in particular) and confined-channel systems (fiber optics in particular) are suggested. The low power broadcast systems offer survivability and flexibility, but suffer interference from nearby systems and are also jammable (though only through great effort on the part of the enemy). Confined channel systems offer poor survivability, but benefit from the fact that they cannot be intercepted or jammed. Clearly, however, the confined channel approach can only be used with units that move infrequently and do not wish to communicate while in motion. Interconnectivity issues and the survivability inherent in media switching may lead to the expensive requirement that all mobile units maintain both the radio and the confined channel systems. In all cases the use of COTS hardware is emphasized.

As noted earlier, connections to and from the mobile command posts should be such that they offer no clue as to the special function of the command post—the command post should appear to be a low-level node in the network.

Long-range communication with aircraft should maintain the JTIDS format, though the low bandwidth will remain a serious limiting factor. Transmissions from aircraft may incorporate phased array technology with adaptive nulling to reduce the effects of jamming and to reduce vulnerability to anti-radiation weapons. Communications between aircraft should make use of 60 GHz communication systems for exactly the same reasons.

6. Standards

Standards not only ensure multiple sources for specific technologies, but also serve to focus development efforts. The tactical message handling systems of the post-2000 era will require standards for the following:

- Non-mobile Local Area Networks
- Interfaces from non-mobile local area networks to base level networks
- Base-level networks
- Interfaces from base-level systems to long-haul non-mobile networks
- Long-haul non-mobile networks
- Interfaces among long-haul non-mobile networks
- Connection from long-haul non-mobile networks to medium range mobile networks

- **Medium range mobile networks**
- **Mobile Local Area Networks**
- **Interfaces from mobile Local Area Networks and mobile units to medium range mobile networks**
- **Mobile Command Post communications**
- **Aircraft positioning systems**
- **Communication to aircraft**
- **Communication from aircraft**
- **Inter-aircraft communications**

Commercial standards will be directly applicable in some of the above applications. The following are excellent candidates.

- **Non-mobile Local Area Networks**
- **Long-haul non-mobile networks**
- **Interfaces among long-haul non-mobile networks**

With modification, the following commercial standards can be used as well.

- **Interface from non-mobile Local Area Networks to base level networks**
- **Interface from base-level systems to long-haul non-mobile networks**
- **Mobile Local Area Networks**

Finally, it is unlikely that commercial standards will be available for the following applications. These standards must thus be defined by the armed forces in conjunction with the development of the appropriate technologies.

- **Base-level networks**
- **Connection from long-haul non-mobile networks to medium range mobile networks**
- **Medium Range Mobile Networks**
- **Interfaces from mobile Local Area Networks and mobile units to medium range mobile networks**
- **Mobile Command Post Communications**
- **Aircraft Positioning Systems**
- **Communication to aircraft**
- **Communication from aircraft**
- **Inter-Aircraft Communications**