TACTICAL INFORMATION EXCHANGE

Marlin G. Kroger
Consultant
Palos Verdes Estates, California 90274

ABSTRACT

This paper addresses the development of an architecture or framework to guide the design of future communications links and networks to support tactical military operations. In the next decade military forces are planned to be much more mobile and dispersed than they are today. Improved sensors and information processing capabilities will provide information needed to manage defense actions against numerically superior enemy forces, but the effective use of that information will require greatly improved communications capability. The resultant digital information traffic which consists of bursts of data between and among users and data sources must be accomodated efficiently, something that neither the present circuit-switches nor the current store-and-forward message transmission systems do well. Also, there is a requirement for much more interoperability between the systems of different services and nations.

Internetwork routing of data transmissions can provide more robust connectivity via alternate paths, to cope with jamming and physical attacks on specific transmission media or nodes. An approach to data network interconnection structure that has emerged over the past several years is the concept of a hierarchial set of protocol layers, each one building on the one below. In total, they constitute a reference model for “open systems interconnection.” The most common version of such a reference model is the International Organization for Standardization’s reference model of Open Systems Interconnection (ISO OSI) (1).

The ISO OSI model has been designed to serve the fixed plant, benign-environment commercial user. DoD has special needs for security, precedence, internetwork data transfer and user mobility that are not yet reflected in the ISO model. Because of these special needs candidate DoD models that are different from the ISO model have been proposed. However, an important consideration in the choice of or development of a DoD standard is that DoD Systems should be able to use commercial equipment and interface with commercial data networks. Also a consideration is that the reference model used for strategic and tactical communications should be a standard throughout DoD, although specific protocols could differ as necessary to support tactical vs. strategic needs. In total,

these requirements and considerations constitute a significant design challenge that must be addressed promptly if DoD is to have any influence on the finalization of the ISO OSI model to get it to accomodate DoD requirements as much as possible.

INTRODUCTION

Out-year plans of the U.S. military forces as described in sources like the Army's Air-Land Battle Concept briefing call for highly mobile defenses executing carefully orchestrated tactics. This paper presents an operational context in which future battles might be fought. It then outlines the associated requirements for the transfer of information between force elements in such battles and discusses the characteristics of an information exchange architecture or design framework needed to guide the development of related DoD communications systems.

OPERATIONAL CONTEXT

An offense strategy in land warfare is to probe the defender's strength with a multipronged initial attack and then to maneuver second-echelon attack elements so as to create overwhelming force ratios in selected areas to assure breakthrough. A typical array of attack forces at different points in time is illustrated in Figures 1 and 2. The Warsaw Pact countries currently enjoy nearly a 3:1 advantage in the number of armored force vehicles they can deploy against NATO in a short-warning war scenario. This means that NATO forces have about a battalion to defend against each Pact regiment. Studies of warfare through the years have developed a conventional military wisdom which says that defensive force can hold a position if the force ratio is not more than 3:1 against it. A 6:1 ratio virtually assures breakthrough in a period of about an hour. The deployments depicted in Figure 2 will produce a 15:1 adverse force ratio in the primary engagement area unless the defense takes timely actions.

The actions available to the defense are to commit its reserve units and/or to perform interdiction strikes to delay and incapacitate enemy units (Figure 3). At a minimum, the enemy units must be delayed and attrited such that when they arrive in the primary engagement area the force ratio becomes no worse than 3:1 for more than brief periods of time.

To dimension this scenario, if the enemy force-element arrows depicted in Figure 3 are regiments, the primary engagement area might be 10-15 km wide. The overall area depicted might be 50 km deep and less than that in width. The Warsaw Pact has sufficient forces to make seven or eight such eight-regiment breakthrough thrusts along the 700 kilometer width of Central Europe, and to have an equal or greater number of second

echelon army units backing up these attack forces, postured to exploit successful lower-echelon breakthroughs (Figure 4).

INTERDICTION TARGETING

As depicted in Figure 5, the enemy force movement is usually constrained by roads, towns, rivers and terrain features. Timely destruction of bridges can cause chokepoints to develop that constitute area-type targets for cluster munitions. Mining of roads can force maneuver units into the field, reducing their speed by a factor of two or more--as well as creating more chokepoints. Assembly areas, supply dumps and command centers constitute more area-type targets. Some of the targets such as chokepoints and assembly areas can be attacked to attrite the enemy directly and others such as roads, bridges and command centers can be attacked to slow him up and disorganize him, providing the delay needed to get defensive forces into position.

It should be noted that all of the interdiction targets discussed are ones which, with appropriate weapons, could be attacked on the basis of precise coordinate information, provided that the attack occurred within the target latency period. Target latencies for the types of targets discussed here range from a half hour for some of the chokepoints to a half a day or longer for some of the assembly areas and supply dumps. Being able to deliver weapons to a set of coordinates (as opposed to having to reacquire a target with sensors on the weapon delivery vehicle) is very important because of the dense enemy air defense environment that pertains to this scenario. Coordinate-based attacks allow stand-off weapon delivery or delivery from low altitudes which are safer modes.

INFORMATION TRANSFER NEEDS

The tactical communications, navigation and position fixing capability needed to adequately support fighting the type of battle described here is not in place today. The current FM radio nets, which are the backbone of ground force forward area communications, suffer from range limitations imposed in large part by the line-of-sight (LOS) characteristics of the radio frequencies employed. Tactical units all want all of the cover they can get from hills, gulleys and trees and they deploy their vehicles and antennas accordingly; and most roads are in valleys as opposed to on ridge lines. Especially in the hilly terrain in which U.S. forces in Germany are deployed, this means that few land force elements in tactical deployments are able to maintain dependable LOS communications at ranges of more than 5 or 10 kilometers between vehicles.

Today it is common to find tactical voice radio conversations being conducted at 0-3 dB signal-to-noise ratios. This provides about 50% word intelligibility which is judged poor but marginally acceptable by users. Zero dB signal to noise ratio corresponds to about a

10^{-1} bit error rate which would be totally unsatisfactory for digital transmission of coordinates or other numerical data. For that requirement, bit error rates of 10^{-6} are needed at a minimum. Enemy jamming considerations outweigh the gain that can be provided by affordable error detection and correction mechanisms.

One way to provide the much higher quality communications capability needed for mobile tactical forces would be to increase the use of relays to get over or around obstacles and to shorten path lengths. Relays can be emplaced on hilltops or installed in aircraft or spacecraft, although there are problems with each of these locations insofar as supporting a mobile tactical user is concerned. Individual radio users also can perform relay functions for each other, provided an appropriate system architecture is in place and suitable communications protocols are employed. The most effective use of relays requires a networking and internet architecture which is not yet in place.

The tactical information exchange problem transcends Service as well as national boundries. The Army need for more range and more jamming protection has just been discussed. The Air Force needs an improved information transfer capability to aid in all-weather and low-level weapon delivery, IFF and air defense. The Navy/Marine Corps has requirements similar to those of the other Services but has a unique air-surface requirement in addition. All Services recognize needs for communications security, including low-probability-of-intercept and the ability to avoid traffic analysis and other exploitation techniques as well as cryptographic penetrations.

ARCHITECTURE FRAMEWORK REQUIREMENTS

There will always be a mixed set of older and newer tactical information transfer systems in the field. Old systems will not be thrown away during new-system-phase-in periods and the diversity of users of information transfer systems ensures multiple networks of mixed vintage. Consideration of Allied systems confirms this view. A 1990’s system design concept that provides a framework for capability growth while maintaining system interfaces and interoperability features is needed to guide future design and development choices (2).

This framework must accomodate the rapid growth of ADP systems planned for the next 5-10 years. According to present DoD procurement plans, hundreds of ADP devices per Corps area will be in the field by 1990. Several thousand users will be involved in generating, analyzing or applying the information collected and/or managed by these systems. The users and systems requiring interconnection might be separated physically by as little as a meter or by as much as hundreds or thousands of kilometers. Allowable transmission delay times might be short, especially for sensor-weapon links. While many data messages will be short (a few hundred bits) and time perishable, peak traffic loads in

battle might be high, driven upward by sensor-weapon links and the tracking of air and ground targets. Thus, there is a requirement for efficient transmission of a large number of short messages.

The typical user accessing a computer data base would like a wide-bandwidth connection that could support rapid transmission and receipt of data. However, this same user only loads the communications link for short periods (normally tens of milliseconds), and there might be long pauses between uses. Such communications is characterized as “bursty”. This user not only needs a wide information bandwidth but also a low bit-error rate and survivable links. Thus, he needs an “expensive” channel he doesn’t plan to use much. Neither circuit switches nor conventional store-and-forward message switches meet this connection requirement well. Circuit switches can provide the needed bandwidth, but the time to make the connection would normally far exceed the time the circuit was used for any one transmission. Leaving the circuit up between transmissions would be unacceptably inefficient since it would dedicate resources needed by other users. Conventional store-and-forward message switches would be too slow.

ARCHITECTURE DESIGN CONSIDERATIONS

Four principal considerations drive the selection of an architecture for DoD information exchange:

– Aside from improvements in basic communication link design, the primary way to achieve survivability of connectivity is through increased internetting of individual communication systems to establish a “system of systems.” Survivability gains would result from the ability to relay messages automatically as well as the ability to use alternate communications media to achieve connectivity.

– Such an internetted system of systems can be accomplished more effectively on a digital rather than on an analog basis. Also, the bursty communications traffic requirements associated with ADP devices can be supported much more efficiently in a digital architecture.

– Voice communications will continue to be a prime requirement for tactical users whose hands and eyes are busy on other tasks and who must transmit and receive warnings, advice, etc. with minimal delays.

– The architecture must not obsolete current DoD investments in communications capability. Currently fielded equipment as well as that now in advanced engineering development or production must be usable as link and network building blocks.

ARCHITECTURE OPTIONS

An approach to network interconnection structure that has emerged over the past several years is the concept of a hierarchial set of protocol layers, each one building on the one below. In total, they constitute a reference model for "open systems interconnection." The most common version of such a reference model is the International Organization for Standardization's Reference Model of Open Systems Interconnection (ISO OSI) (1).

The ISO OSI model has seven layers:

(7) Application (the users interface to the interconnection process)

(6) Presentation (formatting and syntax translation)

(5) Session (organizing, synchronizing, controlling)

(4) Transport (network selection, management, flow control)

(3) Network (link selection, routing, error management)

(2) Data Link (media management, error detection)

(1) Physical (the media: wire, radio, etc.)

Standard protocols are envisioned to support each of the seven layers. Some of these exist, generally at the lower levels.

As illustrated in Figure 6, header information is added to the basic data block at each protocol layer, providing message handling instructions for succeeding layers. At the network layer level the data block and its headers constitute a "packet" which can then be routed through diverse links and media to its destination, having been multiplexed for transmission efficiency with other packets along the way. At the recipient's terminal, the process is reversed and the headers are stripped off in accord with the protocol instructions and the data block is delivered to the user in a form he understands.

Packet switching, per se, is a mature technology. It was conceived in the early 1960s and developed by the Defense Advanced Research Projects Agency (DARPA), and in parallel by the British, in the later 60s. During the 70s a number of commercial packet services became available, e.g., TELENET and TYMNET. Today, packet switching is incorporated in all the new "office automation" data transfer systems like Xerox's ETHERNET, ATV's ACS, IBM's SNA, etc. and commercial packet services are available internationally.

However, the concept of a standard, layered-protocol model to provide open systems interconnection is of more recent origin and the candidate models that exist are not yet well defined (3). Most of the efforts expended to date on developing a standard layered-protocol reference model have been driven by commercial interests. Thus, the focus has been on the fixed plant, benign environment of commercial users. DoD needs for security (including transmission and network control security), precedence, internetting and the support of mobile users have not been a concern for most of the participants in the model development process. In fact, some of the security issues are difficult to discuss in an unclassified forum.

Responding to a perceived need for a reference model more responsive to DoD requirements, DARPA has developed a candidate standard DoD protocol reference model which is designed around existing protocols as illustrated in Figure 7. The most significant difference between the DARPA and ISO models is the inclusion of an INTERNET layer by DARPA to provide individual packet “datagram” service when multiple networks are traversed.

There are sets of supporters for at least three approaches to the establishment of a standard reference model for DoD. Perhaps the largest of these sets is the one that says basically that the seven-layer reference model proposed by ISO is loosely enough defined that DoD can write its own specific definitions and use that model.

A smaller set of people is voicing concern that accepting the ISO nomenclature and writing DoD definitions is tantamount to encouraging anarchy. This group feels that DoD should negotiate an acceptable set of specific definitions and any necessary structural changes in the ISO model, to ensure compatibility between future DoD and commercial equipment and networks.

There is a third, and still smaller, set of people who feel that either of the above approaches is doomed to failure and that DoD should just go its own way and develop a model which meets DoD needs, paying attention to the use of commercial standard protocols where they are applicable.

There is probably still another set of people who think DoD should not worry about packet switching standards at all because they feel that improved circuit switches and conventional store-and-forward switches will be adequate.

CONCLUSIONS

1. Providing the robust interoperable communications capability needed for management of tactical forces in future warfare will require much more internetting of links, particularly data links.

2. The layered reference model for open systems interconnection is a good idea. When functional interfaces are specifically described at the model layer boundries, it will allow diverse systems to transfer packets in a transparent fashion.

3. The current broad acceptance of the ISO model is probably illusionary. The model will only work when it is specifically defined, but the reason it has so much acceptance is that, currently, it is not well defined and everyone can "see" what he wants/needs in it and make his own specific rules. Nevertheless, DoD should mount a coordinated effort to work with the ISO standards groups and press for layering and definitions suited to meeting perceived DoD needs. DoD will want to use both commercial equipment and networks for some of its needs, and the ISO model is at least a good start.

4. Neither of the present two standard DoD packet protocols, Internet Protocol (IP) and Transmission Control Protocol (TCP), corresponds to current ISO layering. There is some international acceptance of the concept of defining the ISO NETWORK layer as consisting of two sublayers, 3A and 3B. Layer 3B would be a "Global" layer supporting datagram service of the type implemented by IP. Layer 3A would be supported by CCITT X.25 or other network protocols. While this makes the ISO model effectively eight layers, it seems a good compromise if the new layers are properly defined. It is not yet as clear how the problem of mapping TCP into the ISO layers might be resolved (if it needs to be resolved).

5. A number of other protocols are becoming de facto DoD standards, e.g. Mail Transport Protocol (MTP), File Transport Protocol (FTP) and TELNET (terminal-to-host protocol). Many additional protocols remain to be written for a complete DoD information exchange system. These should be developed in accord with a standard DoD reference model, hopefully the ISO model as modified by international agreement.

6. The reference model for "tactical" and "strategic" protocols should be the same. However, specific protocols, for example at the Link level, may differ.

7. The Defense Communications Agency (DCA) has been designated as Executive Agent for DoD for computer communications protocols including host-to-host protocols such as TCP and IP. Thus, DCA has the responsibility for the layers of the reference model that are most in need of negotiation.

8. Much remains to be accomplished to get the tactical information exchange needs, as outlined in this paper, reflected in an international information exchange architecture.

ACKNOWLEDGEMENTS

The writer was technical director of a major study of future tactical information exchange (TIE) framework options(2)which was sponsored by the Services and DARPA during the past year. He is deeply indebted to the participants in that study for many thoughts, words and diagrams borrowed for use here. However, the TIE study participants should not be held accountable for this paper which presents personal viewpoints.

REFERENCES

1. American National Standards Institute Draft Proposal ISO/DP 97/SC16/537 Rev., “Data Processing - Open Systems Interconnection - Basic Reference Model” New York, NY March 31, 1981.

2. Tactical Information Exchange Working Group and Senior Review Group Final Report “Tactical Information Exchange (TIE) Framework Development (for the 1990s Time Frame)” RDA-TR-117100-001 Marina del Rey, CA October 1981.

3. Tanenbaum, Andrew S. “Network Protocols” Computing Surveys Vol. 13, No. 4, December 1981.

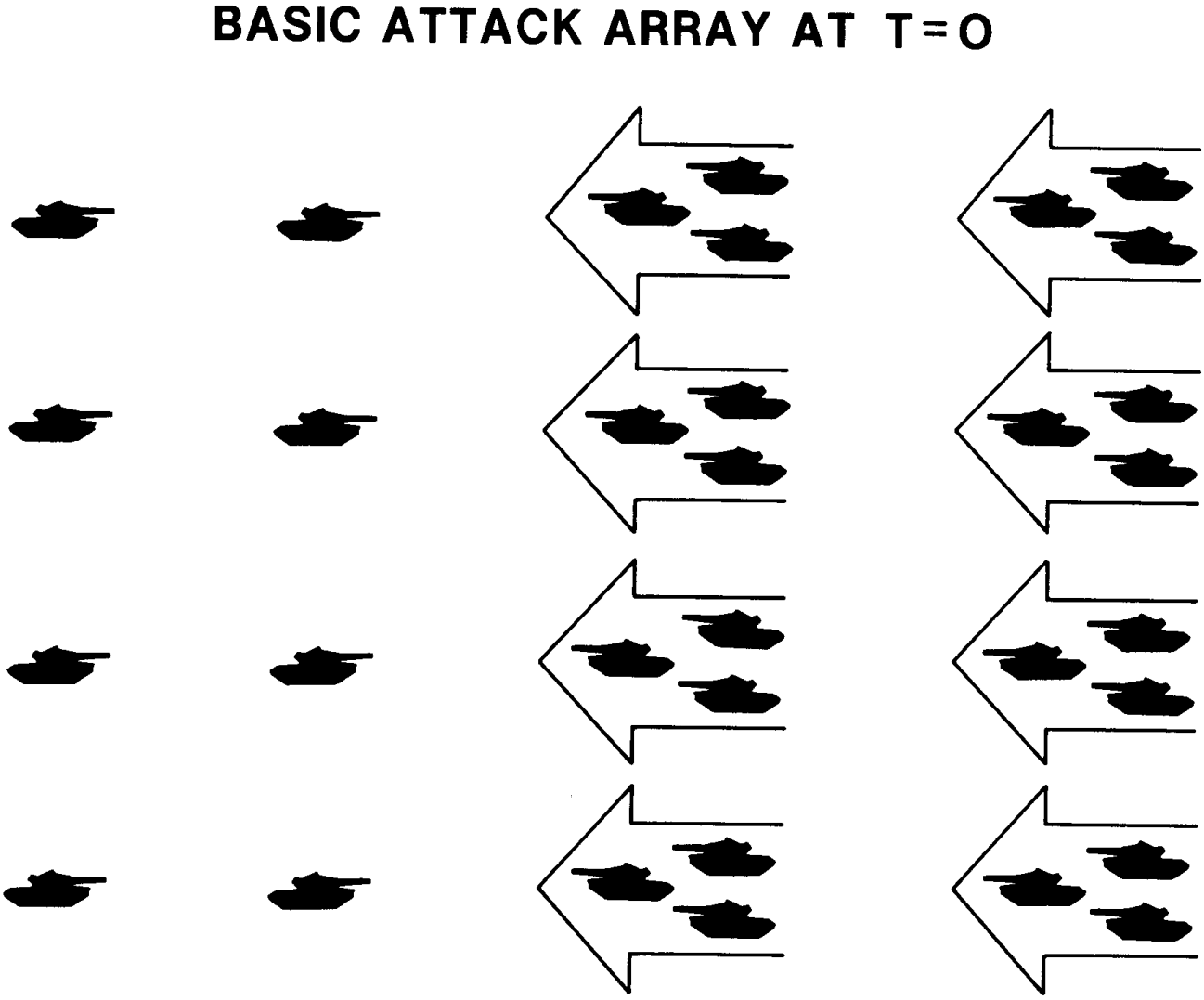


FIGURE 1

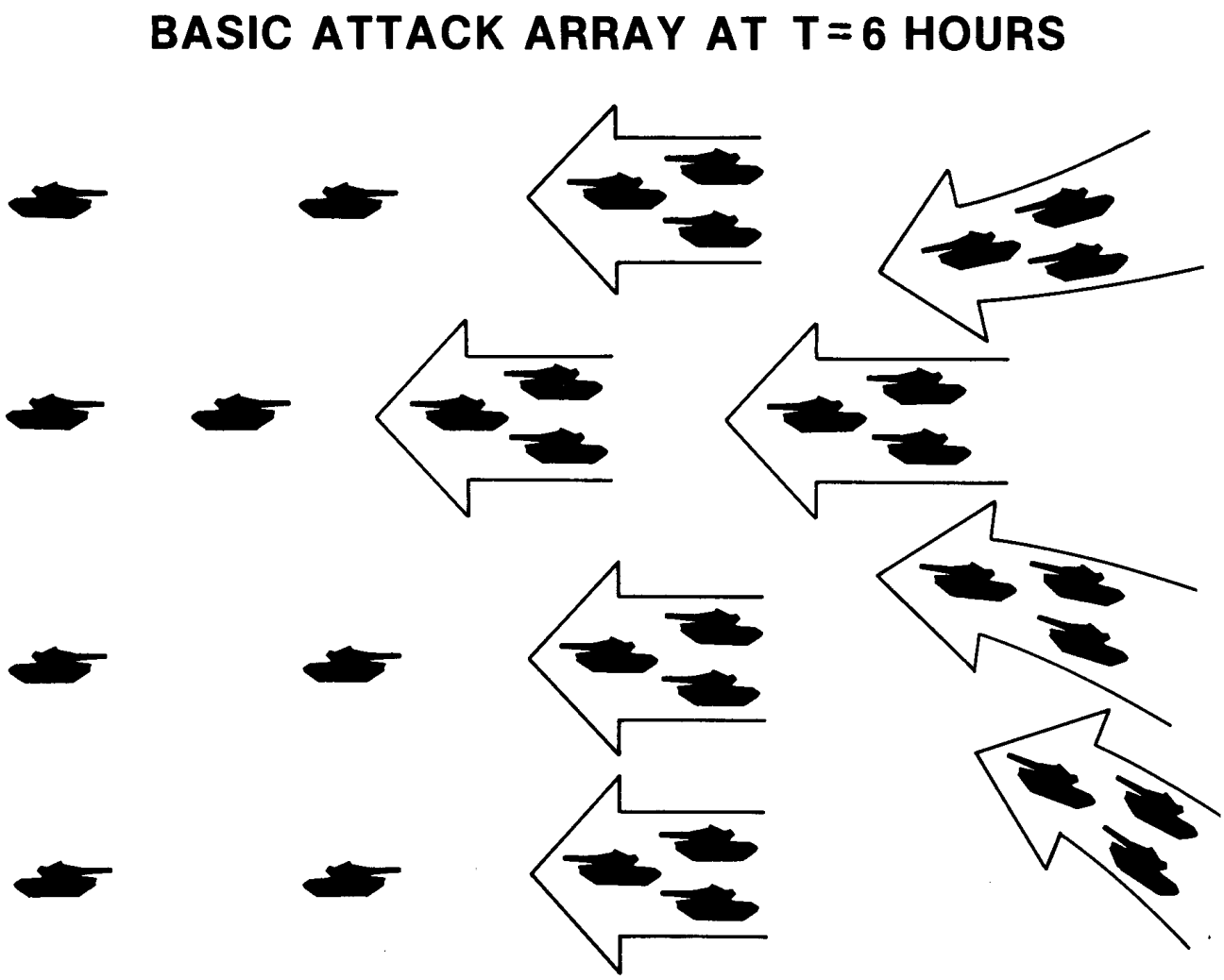


FIGURE 2

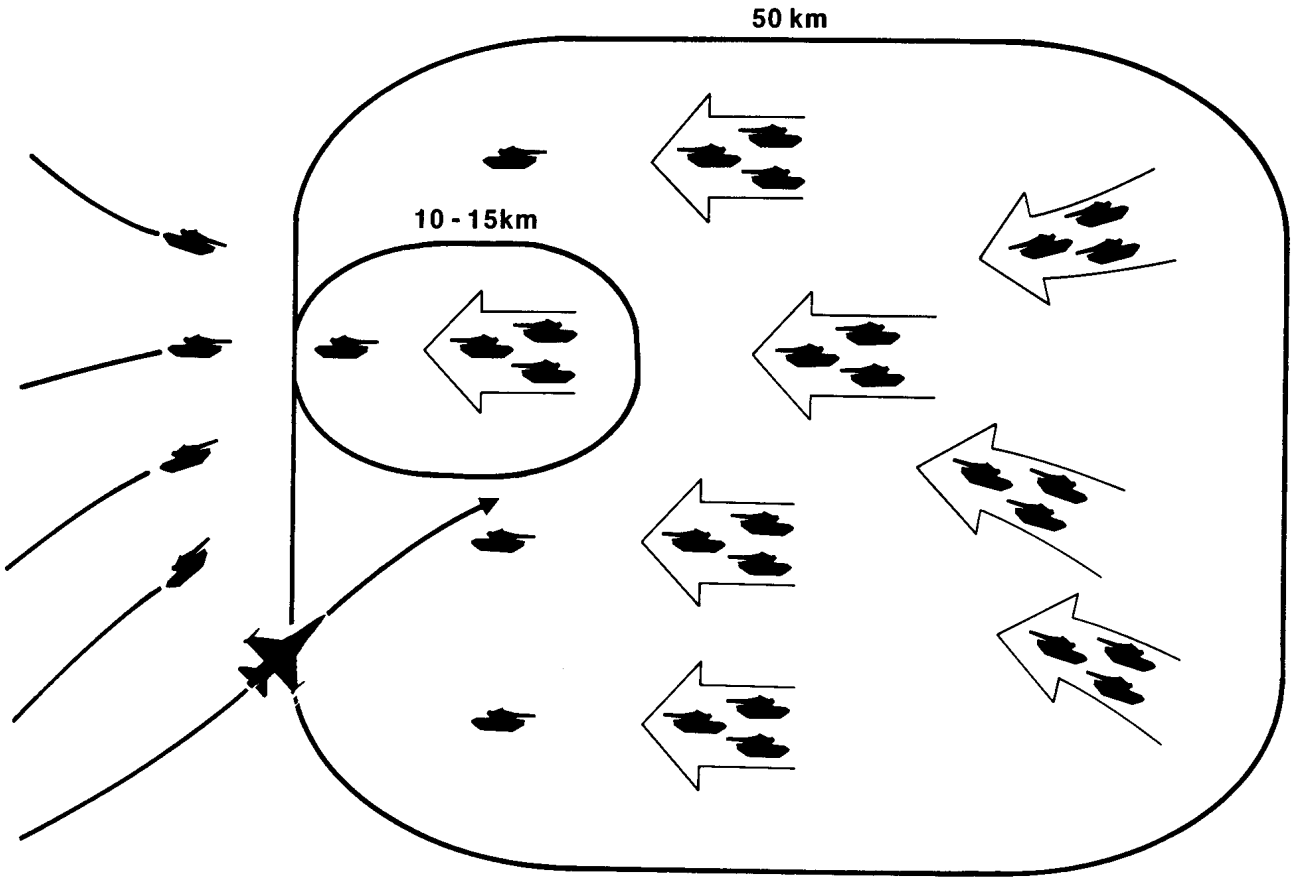


FIGURE 3

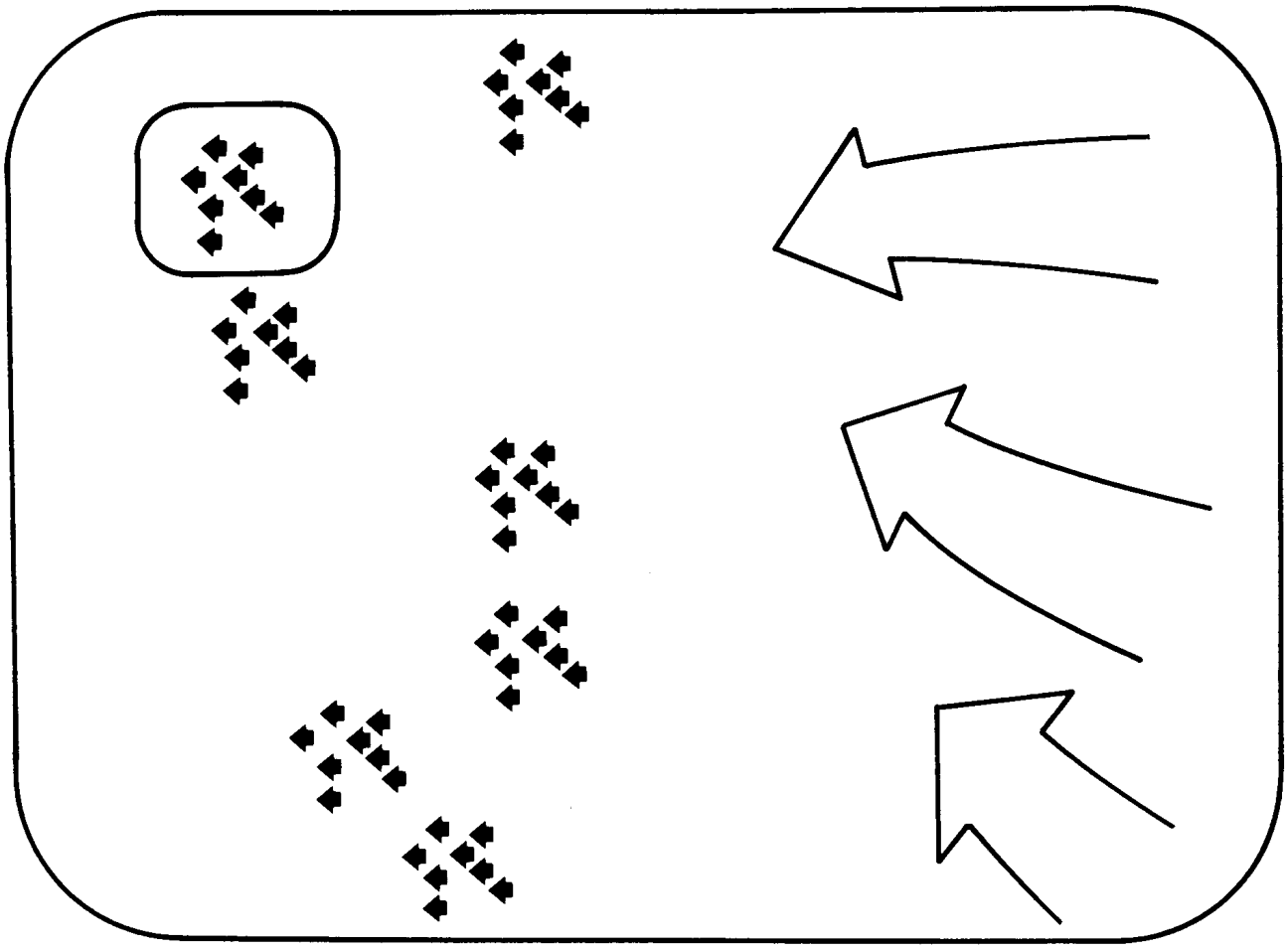


FIGURE 4

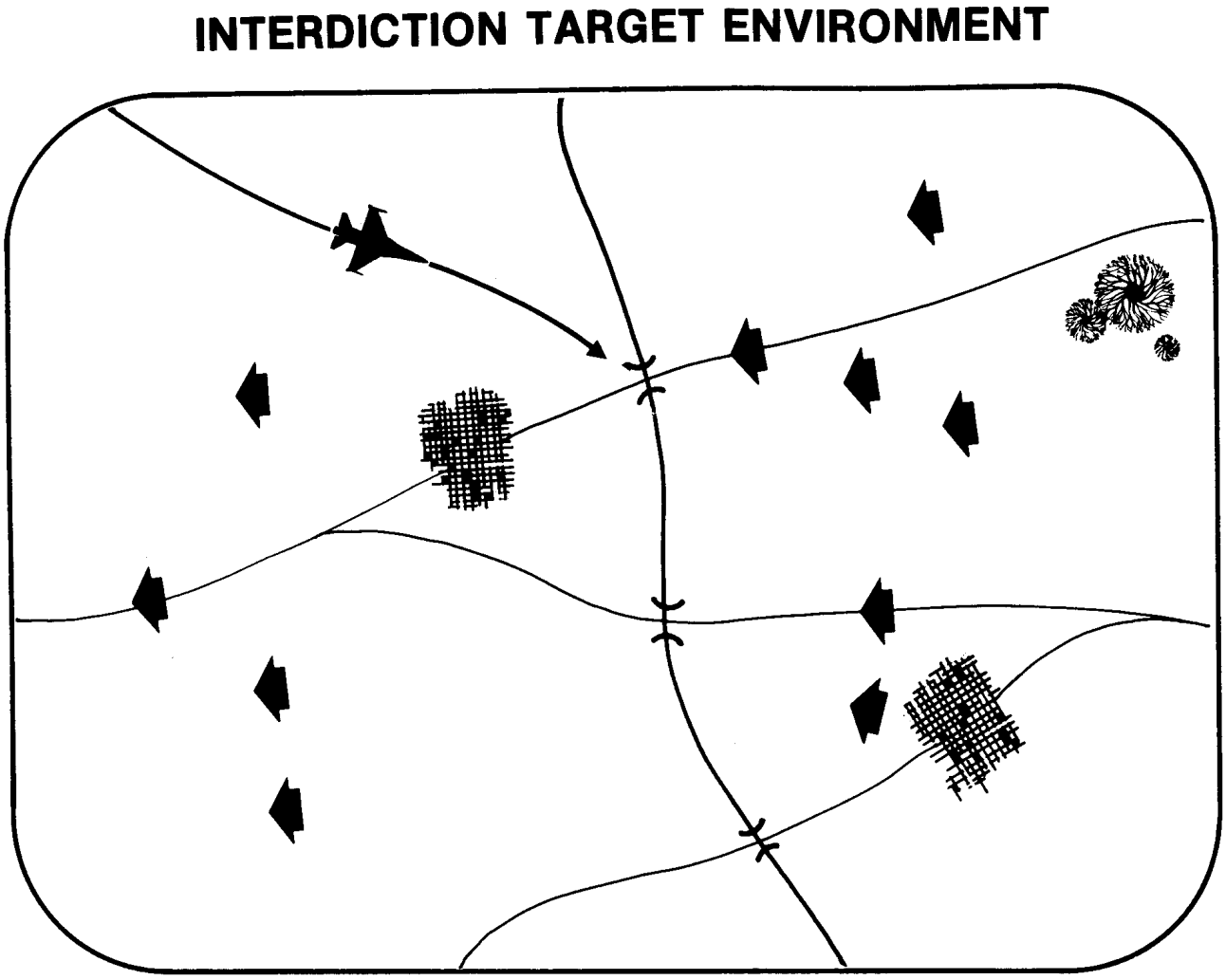


FIGURE 5

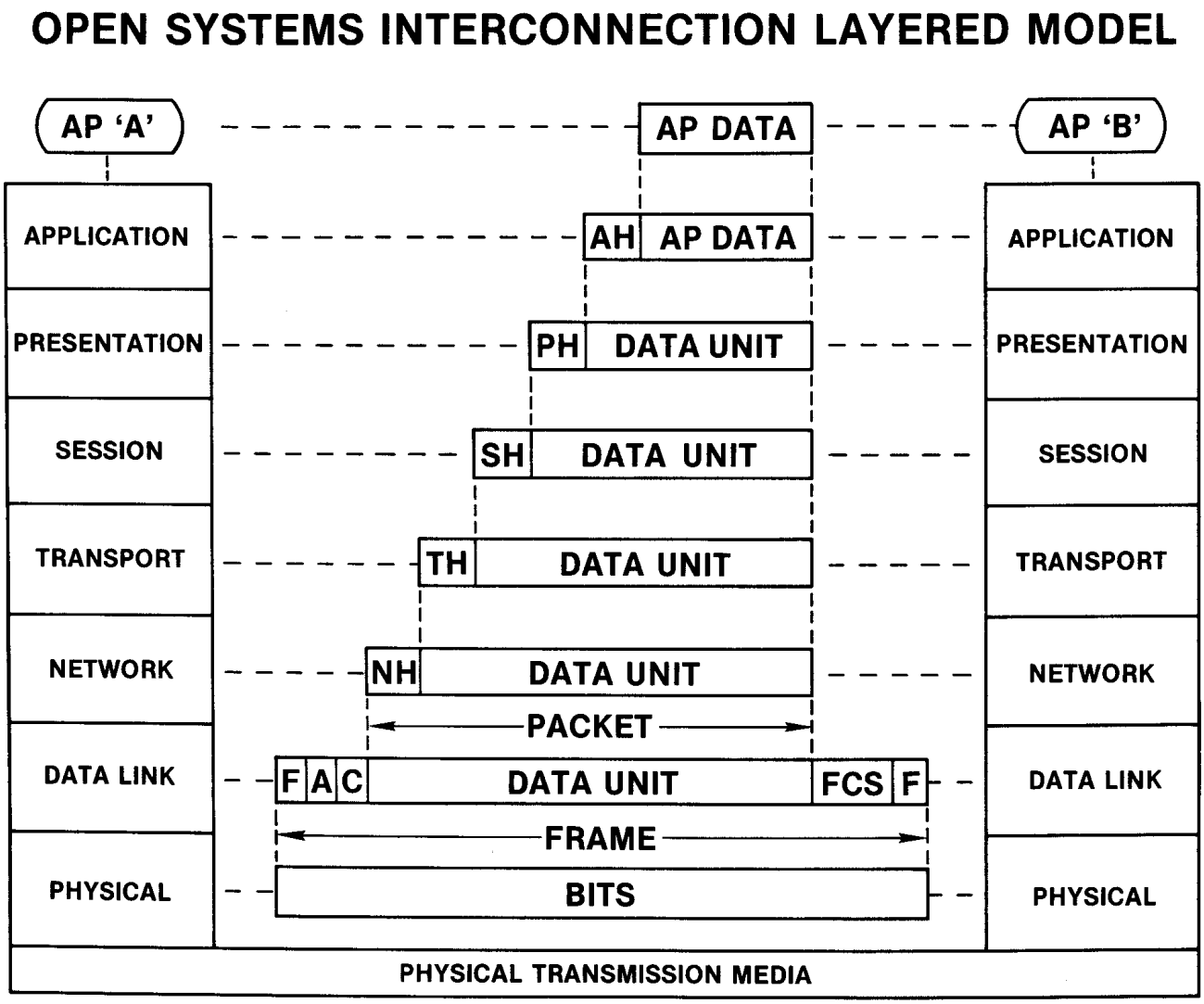
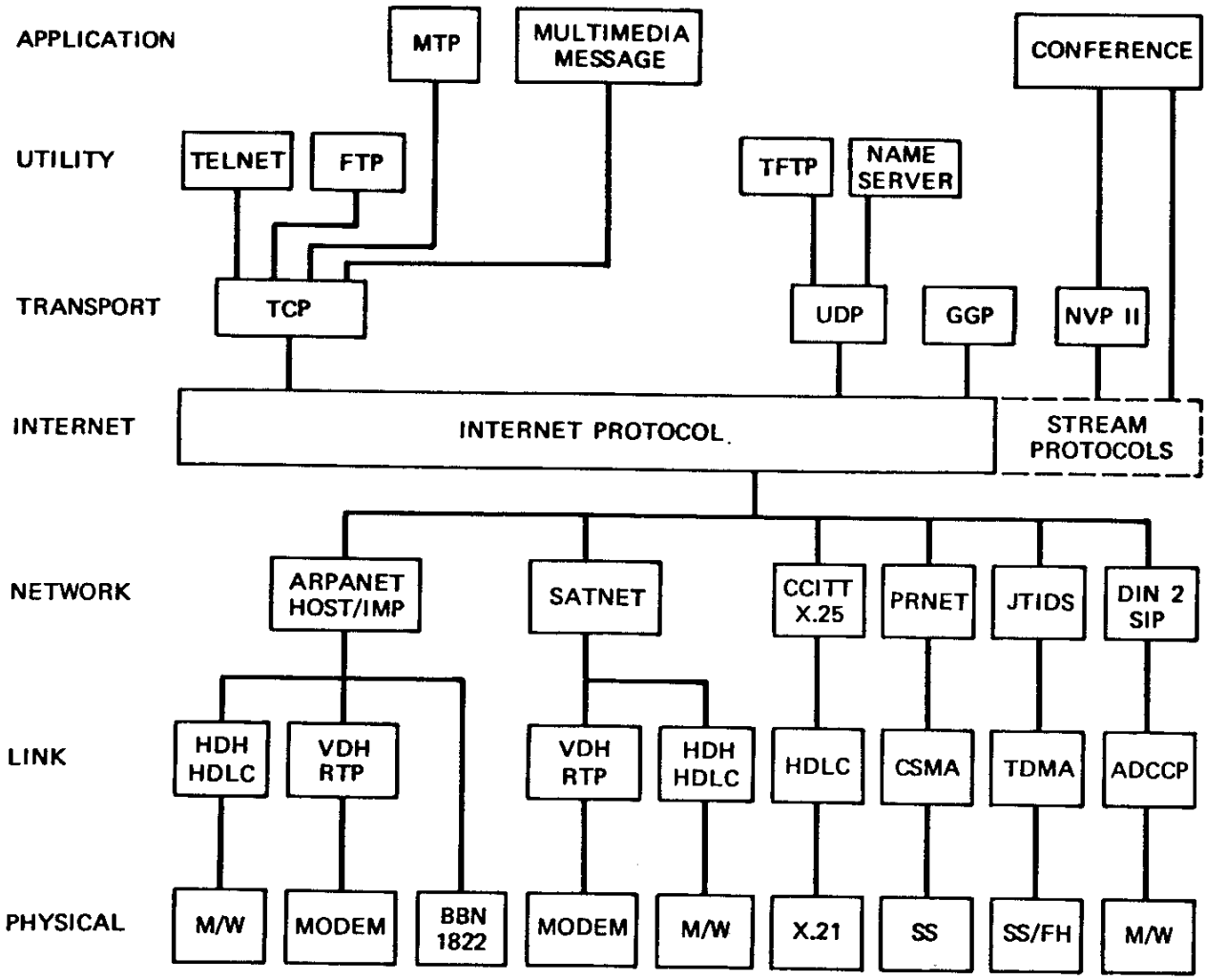

OPEN SYSTEMS INTERCONNECTION LAYERED MODEL
AP 'A'
AP DATA
AP 'B'
APPLICATION
AH
AP DATA
APPLICATION
PRESENTATION
PH
DATA UNIT
PRESENTATION
SESSION
SH
DATA UNIT
SESSION
TRANSPORT
TH
DATA UNIT
TRANSPORT
NETWORK
NH
DATA UNIT
NETWORK
PACKET
DATA LINK
F
A
C
DATA UNIT
FCS
F
DATA LINK
FRAME
PHYSICAL
BITS
PHYSICAL
PHYSICAL TRANSMISSION MEDIA

FIGURE 6



ADCCP	ADVANCED DATA COMMUNICATION CONTROL PROCEDURES
BBN 1822	SPEC FOR INTERFACE BETWEEN HOST AND ARPANET
CCITT	INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE
CSMA	CARRIER SENSE MULTIPLE ACCESS PROTOCOL
DIN 2 SIP	AUTODIN II SEGMENT INTERFACE PROTOCOL
FH	FREQUENCY HOP
FTP	FILE TRANSFER PROTOCOL
GGP	GATEWAY-TO-GATEWAY PROTOCOL
HDLC	HIGH-LEVEL DATA LINK CONTROL (PROCEDURE)
HDH	HDLC DISTANT HOST
IMP	INTERFACE MESSAGE PROCESSOR
JTIDS	JOINT TACTICAL INFORMATION DISTRIBUTION SYSTEM
MTP	MAIL-TRANSPORT PROTOCOL
M/W	MODEM/WIRE
NVP II	NETWORK VOICE PROTOCOL
PRNET	PACKET RADIO NETWORK
RTP	REAL TIME PROTOCOL
SATNET	(EXPERIMENTAL) SATELLITE NETWORK
SS	SPREAD SPECTRUM
TCP	TRANSMISSION CONTROL PROTOCOL
TDMA	(SYNCHRONOUS) TIME DIVISION MULTIPLE ACCESS
TELNET	TERMINAL/HOST TRANSPORT PROTOCOL
TFTP	TRIVIAL FILE TRANSPORT PROTOCOL
UDP	USER DATAGRAM PROTOCOL
VDH	VERY DISTANT HOST
X.25	CCITT VIRTUAL CIRCUIT PROTOCOL

Figure 7 Layered protocol structure for the DARPA reference model.