NEW PROTOCOLS FOR TACTICAL DATA

by

Clifford Warner and C. M. Keune

Naval Ocean Systems Center
San Diego, California 92152

ABSTRACT

Tactical networks handle data types which are very different
from those handled by conventional networks such as the
ARPANET. The characteristics of tactical data call for the
development of new reliable connectionless host-to-host pro-
tocols. This paper discusses the data likely to be handled by a
tactical network, their characteristics, and the design of new
protocols suitable for use with that data.

INTRODUCTION

Tactical networks differ from conventional networks such
as the ARPANET in several aspects. Some of these differ-
ences will affect the design of their protocols. Of particular
interest in this paper is the types of data handled in a tactical
network, and the impact that they have on the design of the
ISO Model Transport Layer Protocols [1].

TACTICAL DATA TYPES

Three types of data are expected to be transmitted in tacti-
cal data networks. These are track reports, broadcast com-
mand and control messages, and directed command and
control messages.

Track Report Messages

Track report messages are sent to all network platforms and
are members of a class of transmissions which are called non-
directed messages since they are not directed toward any par-
ticular node but are expected to disseminate the same
information to all nodes. Track reports contain information
on track position, velocity, etc., and will likely be updated on
a regular basis at fixed intervals.

Broadcast Command and Control Messages

Broadcast command and control messages are the second
member of the class of nondirected messages. These messages
contain special information on the command and control of
military forces and will also be disseminated throughout the
network. However, unlike track reports, these messages
are not sent out on a regular basis at fixed intervals. Rather,
they are sent out randomly as the tactical situation dictates.

Point-To-Point Command and Control Messages

In addition to the broadcast command and control mes-
sages, the network will contain point-to-point command and
control messages. These messages are intended only for a sin-
gle recipient, and are called directed messages.

PROTOCOL ISSUES

Typically, the functions implemented in the Transport Layer
include:

a. Packetizing and reassembly.
b. Host-to-host error control.
c. Host-to-host flow control.
d. Connection management.

The design of each of these functions is dependent on the
characteristics of the traffic handled by the network. Thus,
the unique characteristics of tactical data impact the design of
these functions such that different solutions are appropriate
than those developed for use in conventional networks.

Packetizing and Reassembly

In a packet switched network, long messages are broken
down into smaller units called packets. These packets are then
routed independently, in a store and forward fashion,
throughout the network. Packet switching is suited for the
transmission and reception of bursty computer data. With
this type of data, packet switching efficiently utilizes the
channel bandwidth, and improves message delay when com-
pared to circuit switching. Packet switching can also enhance
survivability, since packets can be quickly routed around
failed or destroyed network components.

Packet switching is also suitable for the types of tactical
data discussed here. In some instances, message switching
may be appropriate. However, the use of a store and forward
switching technique for tactical data should improve effi-
ciency of channel utilization efficiency and network surviv-
ability as compared to circuit switching.

Host-To-Host Error Control

Error control (acknowledgment) protocols are used in
packet switched networks to ensure message delivery when
packets are lost due to channel noise, failure of the routing
protocol, or any other reason. Two types of error control pro-
tocols are common in packet switched networks. Hop-by-hop
acknowledgments are used to recover from packets lost
between nodes within the transmission path of the packet.
This type of error control will compensate for channel noise.
It will not, however, recover from other errors such as the
failure of the routing protocols to deliver packets to their
intended destination(s). Thus, a host-to-host error control
scheme is required to fully guarantee the delivery of all mes-
sages to their destination(s).
Conventional network protocols, such as the ARPANET Transmission Control Protocol (TCP), implement a host-to-host error control protocol utilizing positive acknowledgments (PAK's). With this protocol, every time a packet is transmitted by its source node, a copy is stored. The source node then waits for a PAK from the destination node. If this PAK is received within a suitable time out period, the copy is discarded. Otherwise, the copy is used to retransmit a duplicate packet to the destination. This procedure continues until the destination node successfully receives a copy of the packet and delivers a PAK to the source.

This method of error control is suitable for a network such as the ARPANET which utilizes only directed messages. However, the positive acknowledgment scheme is not suitable for use with nondirected messages such as target track and nondirected command and control messages. The use of positive acknowledgments with nondirected messages will generate large amounts of overhead, resulting in poor network performance. For example, in a tactical network containing 40 nodes each nondirected message will generate 39 PAK's, whereas in the ARPANET, each message generates a single PAK regardless of the size of the network.

Conventional networks such as the ARPANET can attempt to minimize the overhead generated by acknowledgments by piggybacking the PAK's onto normal message traffic. However, overhead is still generated, and if techniques can be developed to minimize the number of acknowledgements generated, overhead will be reduced. Also, even with piggybacking of PAK's, special acknowledgment messages will have to be transmitted if a normal message is not ready to be transmitted by the acknowledging node. This would degrade throughput, and may be inappropriate in tactical situations in which one or several nodes may be purposefully keeping message transmissions to a minimum.

Thus, with the use of PAK's alone, large amounts of acknowledgments will be generated in tactical networks, causing congestion and degrading message delays, response time, and message throughput. New error control protocols are called for. This paper will describe new error control protocols which have been developed for use in tactical networks. The type of protocol presented differs for the three message types: target tracks, broadcast command and control messages, and directed command and control messages.

**Host-To-Host-Flow Control**

Flow control protocols are implemented to ensure that a sending node will not transmit data faster than the receiving node can process and utilize it. Some sort of flow control protocol will likely be required for use in tactical networks. However, this subject will not be addressed here, but rather will be left as a topic for future research.

**Connection Management**

Connection management protocols exist for a variety of reasons. They facilitate the orderly exchange of information required to initialize error control, flow control, and other functions. They also facilitate the reliable transfer of data, ensure the orderly termination of data transfer, and provide for recovery from catastrophic events such as host crashes.

For two primary reasons, a connection establishment protocol is not well suited to tactical data. First, tactical data is characterized by short inquiry response type messages rather than by long sessions of message exchange. In this environment, it is not necessary nor efficient to expend the large amount of overhead required to establish a connection just to deliver a short message. Second, a connection establishment protocol is not suitable to a tactical network's use of large amounts of nondirected messages. In order to deliver a non-directed message using a connection establishment protocol, a connection must be established between the source node and all other network nodes. Thus, large amounts of overhead will be expended to establish these connections. Also, a separate copy of the message will be generated for each connection. For example, in a network of 40 nodes, 40 separate connections would be required just to deliver a short broadcast command and control or target track message, and 40 separate copies of the message would be generated. This is wasteful of channel bandwidth, a limited resource in a tactical environment.

Thus, the use of a connection establishment protocol for the types of tactical data discussed here is inappropriate. Rather, a connectionless protocol is called for. This connectionless protocol should take the form of a reliable datagram service. That is, the connectionless protocol merely transmits individual packets (datagrams) to the intended destination(s) and ensures their reliable delivery. This guarantee of delivery is established by error control protocols.

In a similar study of protocol issues for another tactical network, the Army Battlefield Information Distribution (BID) system, M.T. Liu and L.D. Umbaugh came to a similar conclusion, although they did not develop any protocols [3].

**NEW ERROR CONTROL PROTOCOLS**

As explained above, the characteristics and requirements of tactical networks call for the development of new host-to-host protocols. These new protocols will take the form of a reliable datagram service. The tactical messages will be simply transmitted as datagrams using suitable error control techniques. The design of the error control protocol will be different for each of the three types of tactical data. The datagram service is already provided by the Network, Data Link, and Physical Layers. This paper concentrates on the presentation of new Transport Layer error control protocols. These new protocols, described below, used in conjunction with the existing routing, multiple access, and other Network and Data Link Layer protocols, form a family of new reliable connectionless host-to-host protocols.

**Point-To-Point Command and Control**

**Message Error Control**

The one area of commonality between tactical and conventional networks with regard to error control involves directed command and control messages. These messages have a single source and destination node, and the use of positive acknowledgments is suitable. A block diagram of the protocol is given in Figures 1 and 2.

**Non-directed Command and Control Message Error Control**

A new error control protocol has been designed for the nondirected command and control messages. This protocol was designed using the following assumptions:

a. Broadcast command and control messages are generated at each node at random times.

b. Guaranteed delivery is essential.
A negative acknowledgment (NAK) scheme was designed to ensure delivery of the target track messages. This scheme is presented in Figures 3 and 4.

The basic concept underlying this error scheme requires command and control messages originating from each source to be numbered sequentially. Thus, a missing message can be detected when messages arrive out of sequence. For example, suppose node D receives nondirected command and control message 15 from source node S, and then at a later time receives number 17 as its next message. Node D then concludes that message 16 is missing and transmits a negative acknowledgment for message 16 back to node S. This NAK is either routed as a special directed message, or piggybacked upon a regular directed command and control message intended for node S and ready for transmission at node D. Upon the receipt of this NAK, node S retransmits the command and control message to node D. This retransmission of the broadcast command and control message does not, however, need to be routed again as a nondirected message, but rather is routed as a directed message. With this protocol, acknowledgments are generated only by nodes which missed a particular message. This should produce much less overhead than with the use of positive acknowledgments since it is likely that most nodes will have received the message correctly and only a few will not.

There are a couple of protocol details which deserve additional comment. First, there exists the possibility that the NAK's themselves can be lost. Thus, the NAK's need to be
MESSAGE RECEIVED OVER COMMUNICATION CHANNEL

DUPLICATE?

YES

DISCARD

NO

SEND PAK TO SOURCE NODE

SEND MESSAGE TO HOST

Figure 2. Point-To-Point Command and Control Message Error Control

retransmitted at regular intervals until a retransmission of the command and control message is eventually received. In a sense, the receipt of the retransmission acts as a positive acknowledgment of the NAK. A suitable choice for the time out period between transmission of the NAK’s is the same time out period used by the directed messages, which use the positive acknowledgment error control technique. Second, a node cannot sense that a nondirected command and control message has been lost until a later message is received. Using the example given above, node D does not realize that message 16 is missing until message 17 is received. If message 17 is much later than message 16, then the retransmission of message 16, and its eventual delivery to node D is excessively delayed. Thus, it is essential that each node originate some sort of broadcast message on a regular basis which integrates with the same numbering scheme used by broadcast command and control messages. A solution to this is to require each node to occasionally transmit a “Heart Beat” message. These messages are generated by each node on a regular basis and thus ensure timely retransmission of lost broadcast command and control messages.

Target Track Acknowledgment

A new error control protocol was also developed for the target track messages based upon the following assumptions:

a. Target tracks are initiated at each node with random starting times.

b. Following the initial target track, updates are generated at fixed intervals of duration Ttt, where Ttt is much larger than the average delay required for the delivery of each message to all nodes throughout the network.

c. Delivery of each target track message is desirable but not essential since tracks are updated on a regular basis.

A negative acknowledgment protocol was also implemented for the target track messages. This protocol is presented in Figures 5 and 6, and described below.

Upon the receipt of the initial target track report, the expected time for the next update Tu is computed as follows:

\[ Tu = t + Ttt \]

where

\[ t = \text{the current time} \]

\[ Ttt = \text{update interval} \]

This requires knowledge of Ttt, which can either be carried as overhead on the target tracks, or established apriori for various classes of targets.

If the next update is received reasonably close to Tu, no action is necessary. If however, at time Tu + Tnak, where Tnak is a grace period to accommodate random fluctuations

38.5.4
Figure 3. Broadcast Command and Control Message Error Control

In message delays, the next update has not been received, the node assumes the message has been lost and a NAK is generated and sent to the source node. Upon receiving the NAK, the source node retransmits a copy of the target track, this time in the form of a directed message to the node from which the NAK was received.

No error control is implemented for the initial target track report. Error control, however, is established for all of the updates once an initial report is received. Thus for some nodes, one or a few target track reports may be missed prior to the establishment of error control. If it is a requirement to guarantee delivery of the initial target track report, two solutions are immediately evident. One solution is to use positive acknowledgments for the initial report, and then switch to the more efficient use of negative acknowledgments for all of the updates. A second solution is to use flood routing (every node relays the message) for the initial track report, not implementing host-to-host error control for this single report, and relying on the link error control to ensure delivery. Pure flooding does not allow messages to be lost due to routing failure and a reliable link error control protocol will ensure delivery of flood routed messages to all nodes.

Unlike with the nondirected command and control error control protocol, the node missing the track report does not repeatedly transmit NAK’s until the track report is received. Rather, only one or a few NAK’s are generated depending on the frequency of the updates. In most cases, a single NAK will result in the timely reception of the missing target track report. However, if the target track still is not received following the transmission of a few NAK’s, the node merely waits for the next update.

**SUMMARY**

Tactical networks differ from conventional networks, such as the ARPANET, in several aspects. In particular, tactical networks handle track report messages, broadcast command
and control messages, and point-to-point command and control messages. These messages possess characteristics very different from the types of data commonly found in conventional networks. The track reports and broadcast command and control messages are nondirected in that they are not directed to any one particular node, but are disseminated to all nodes. Also, these tactical data types will possess many short inquiry response types of messages.

Conventional host-to-host connection establishment protocols which use positive acknowledgements, such as the ARPANET Transmission Control Protocol, are not suitable for these types of tactical data. Rather, new reliable connectionless protocols are needed. An alternate to the use of TCP is to use a datagram protocol and implement error control based upon the use of negative acknowledgements in conjunction with the conventional approach of relying primarily on the use of positive acknowledgments. These new protocols will greatly reduce the amount of overhead generated in tactical networks and thus improve overall network performance.

**BIBLIOGRAPHY**


Figure 5. Target Track Message Error Control
Figure 6. Target Track Message Error Control