

The Application of Packet Switching Techniques to Combat Net Radio

BRIAN H. DAVIES AND T. R. DAVIES

Invited Paper

The narrow-band Packet Radio system which is the subject of this paper is a highly flexible and survivable data communications system for the Forward Area tactical environment achieved by applying packet switching techniques to Army Combat Net Radio. The User requirements driving this development are outlined. It is important that this system is not viewed as being in competition with other Packet Radio systems, but as one system or building block in an integrated electronic battlefield, hence the emphasis on internetworking. Important design considerations such as survivability and the ability to operate with random network topologies are discussed. A detailed description of the algorithms for Channel Access, Routing, and Network Control which were developed using finite-state-machine simulation techniques is then given followed by a summary of the simulator performance predictions for various scenarios. Packet Radio is a synergism of signal processing and communications protocols implemented on real-time systems. The signal processing requirements and architecture adopted for signaling in the VHF environment are described in the context of the hardware for a prototype network. Early experience resulting from trials and demonstrations with this network are used to point to refinements in the next iteration of system design.

I. INTRODUCTION

A major problem in providing command, control, and information systems for the Far Forward tactical environment is the difficulty of providing secure and survivable communications. This difficulty is due to the fact that the environment is one which, by its hostile and mobile nature, cannot support a communications infrastructure of base stations and unattended repeaters. The difficulty is further exacerbated by the fact that the communications medium is shared with the enemy and flanking forces.

To date, information in this environment has almost exclusively been exchanged by voice over combat net radio (CNR). Much of this traffic is analog voice using narrow-band frequency modulation occupying 25-kHz channels, while there is substantial use of digitized voice (16-kbit/s continuously variable slope delta modulation) occupying 25/50-kHz channels. A major trend in Forward Area communi-

cations is the increasing use of data, vis a vis voice, for two reasons. First, many of the new computer-controlled weapons systems consist of distributed elements (sensors, command and control posts, and weapons platforms) which require accurate and timely data communications to function effectively. Secondly, there is only a limited amount of the radio frequency spectrum (HF and low VHF) that is capable of supporting mobile tactical communications without the use of a complex mobile repeater infrastructure, which would be expensive in terms of men and logistic support. Consequently, this part of the spectrum is grossly oversubscribed. In this context, data systems have a very much higher information throughput per unit of bandwidth than voice systems. Thus there is considerable pressure to transport as much information as possible by data, thereby increasing channel availability for essential voice command and control. A further consequence of the frequency congestion in the Forward Area is a reduction in the effective range of the radios.

These problems, coupled with the scale of procurement for the Forward Area, have given rise to the following characteristics being required in the next generation of communications systems for this environment:

- 1) more efficient use of the RF spectrum
- 2) ability to operate in reduced radio ranges
- 3) minimum operational overheads
- 4) interoperability with other battlefield data systems
- 5) affordability.

The narrow-band Packet Radio system described in this paper satisfies all five of the above requirements. In summary, Packet Radio, being a data communications system, can accommodate greater numbers of users and transport greater amounts of information than an equivalent digitized speech channel. Packet Radio copes with reduced radio ranges by delivering packets in a number of transmission hops. It is a self-configuring system which automatically adapts to user mobility and changes in radio connectivity, thus relieving users from having to make frequent radio link engineering checks. It is specifically designed as one element in an integrated electronic battlefield. Finally, the

Manuscript received November 20, 1985; revised June 30, 1986. Part of this paper was published in the *MILCOM '83 Proceedings*, October 1983.

The authors are with the Royal Signals and Radar Establishment, Malvern, England.

0018-9219/87/0100-0043\$01.00 © British Crown Copyright 1987

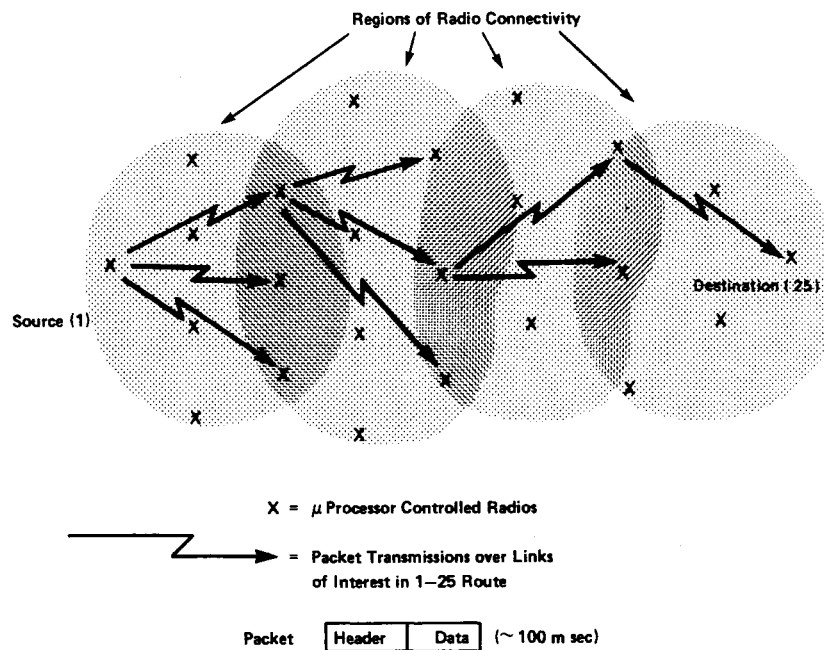


Fig. 1. Basic concepts of Packet Radio.

basic combat net radio can be converted to provide Packet Radio facilities, in addition to those it presently provides, by the addition of a functional module based on signal processing and microcomputer chips. Thus with advances in VLSI technology the costs of this radical new communications system will be an incremental increase in radio equipment costs.

This paper describes the design and development of such a narrow-band Packet Radio system including early experiences with a small prototype network. Section II describes the basic concepts underlying the application of packet switching techniques to the CNR channel including the philosophy of the architectural approach. Section III describes how the system appears to the User and the relevant protocols. A detailed description of the Channel Access, Routing, and Network Control algorithms which were developed using a finite-state machine simulation is given in Section IV. Section V summarizes typical average performance for various scenarios. Section VI describes the signal processing requirements and architecture adopted for the first prototype units, while Section VII highlights the main lessons arising from early experiences with these units. Finally, pointers for future work and a summary are given in Section VIII.

II. BASIC CONCEPTS

In a CNR Packet Radio network a number (2 to 50) of microprocessor-controlled radio transceivers, equipped with burst data modems, share a single narrow-band channel. The transceivers operate in simplex mode and all transmit and receive on the one channel. The channel itself may or may not be frequency-hopped, that is an ECCM issue outside the scope of this paper. The bit rate of the modulation is 16 kbits/s, exactly the same as that employed by digitized speech users, thus making it suitable for use with existing

radio transceivers and frequency allocations. All units demodulate and analyze all transmissions which they receive and source-to-destination transportation is provided by store-and-forward action typical of all packet switched networks. The Packet Radio units automatically configure themselves so that each one is aware of the minimum number of transmission hops to each available destination. This permits automatic and efficient relaying of packets as illustrated schematically in Fig. 1.

A. Fully Distributed Architecture

A number of features of the CNR channel, coupled with a primary design aim of survivability in a rapidly changing and hostile electromagnetic environment (EME), has led to a fully distributed approach to the network architecture in which each unit is functionally identical and there is no central control station. The main task of a control station in a Packet Radio network is to obtain connectivity information, calculate routes, and distribute this routing information to active users. However, the use of a control station, which for efficiency reasons would have to be centrally sited, could constitute a vulnerability. In particular, the control traffic would tend to act as an electromagnetic pointer to the central station making it the focal point of physical or electromagnetic attack, in addition to chance destruction or failure. Survivability of such a system could be improved by the use of a number of control stations, but multistation control is inherently complex, resulting in more control protocols, which in turn make more demands on the limited channel capacity. Fortunately, the basic parameters of the CNR Packet Radio system, with a maximum of 50 units and no more than 10 packets per second on the channel, lend themselves to easy and efficient distributed implementation. A further advantage of the fully distributed approach is that local communications can continue

unaffected should the network become bifurcated into two or more collections of units.

B. CNR Packet Radio in Context of Battlefield Data Communications

There are a number of different types of radio channels that have different applications on the modern battlefield; these include the high-capacity DARPA Packet Radio [1], Packet Satellite [2] channels of various capacities, and the CNR system described in this paper. These systems are not in any sense competing with each other as they offer differing types and grades of service in differing areas of the battlefield. They all have one particular hallmark, namely that they can interoperate with each other, without modification, given a suitable internet architecture. While it is conceivable that these networks could adopt a common network access protocol for a given type of service, the fact that the basic communication resource that is being shared in these networks exhibits very different characteristics means that the basic intranet protocols of channel access, routing, and network control will all be different. If a channel is to be used efficiently under a variety of conditions then these intranet protocols must be matched to communications channel(s) being used; a fact highlighted by Kleinrock in [3].

Certain features of the narrow-band CNR channel have a major impact on the design of the packet switching algorithms:

- 1) The links in a CNR PR network may be subject to very high packet loss rates due to the inherently high bit error rate of the mobile tactical VHF environment and to transmission collisions between neighboring units (hidden terminal problem).

- 2) The semi-broadcast nature of the CNR Packet Radio environment in which a number of possible relayers receive a packet simultaneously is unique to radio-based packet switched systems.

- 3) The all-mobile nature of the units coupled with the possible rapid and dramatic changes in the EME mean that the network designer has almost no control over the topology of the network connectivity.

- 4) The usual mathematical tools for modeling networks assume that they are large enough for the "laws of large numbers" to apply, permitting assumptions such as independence of time of arrival, queue length, etc., at each node. This is patently untrue for this very small channel.

This final feature necessitated a heuristic approach to algorithm design because we did not find it possible to generate a realistic mathematical model which had tractable analysis. In particular, because of the small size of the channel and possible rapid changes in connectivity, we had to investigate the behavior of the network under non-steady-state conditions, and this was only possible using simulation techniques. The design has evolved through and been tested by extensive computer simulations using a finite-state machine representation with the controlling algorithms operating independently for each modeled unit. Despite the heuristic nature of the development, much reference has been made to the literature [4]–[8] on the analysis

of similar but simplified systems and many aspects of the design are practical extensions of well-researched techniques.

III. USER SERVICES

A. Type of Service

A Packet Radio network is capable of providing a number of types and grades of service. We have considered five types of service:

- 1) Unacknowledged Datagram—only requires hop-by-hop acknowledgment and is suitable for sensor information where timeliness of delivery is more important than reliability. This is the baseline service, inherent in the relaying strategy of the routing algorithm. All other services are built up on this baseline.

- 2) Acknowledged Datagram—suitable for highly formatted messages which can be contained in one packet. Currently these services (1 and 2) are built into the terminal handler which is accessed via an RS 232 interface.

- 3) Multiaddress Datagram—the exact nature of this service is still under discussion. Basically it provides an acknowledged datagram delivery to a primary user, and at least one transmission illuminates those units on the multiaddress list. It seeks to emulate the all-informed nature of current CNR operation, should this be required.

- 4) Virtual Call Service—provides a guaranteed delivery of ordered data. Used for database updating, file transfers, etc. Currently, this is provided by TCP/IP [15] protocols, sitting above service 1. In order to permit a number of user projects to use Packet Radio without further software development, an X25 access is being developed, in which special transnet procedures are employed to minimize overheads. This approach to X25 is very much in the original spirit of the protocol as an access protocol, with the network free to implement transnet procedures best suited to the particular network concerned.

- 5) Internetwork Service—the capability for communicating with hosts on different types of networks (see internetworking).

B. Grade of Service

The grade of service is a term used to describe the availability, throughput, average delay, delay dispersion, and accuracy of data transportation being offered to the user. Unfortunately, it is notoriously difficult to predict the performance of the parameters even for packet switched systems in benign environments. Also the grade of service required varies from one type of user and scenario to another. For example, an artillery fire control system may require rapid delivery of data in less than 1 s and would, therefore, have to use a lightly loaded network of no more than few hops, whereas a logistic support unit could accept message delivery times of 10 s, and could thus use a fully loaded network. The grade of service in a Packet Radio network is heavily dependent upon the quality of radio links which may be very variable. The system described below is designed to make the best use of these links.

It is possible to estimate approximate figures for through-

put and average delay given the number of active users and the sharable channel capacity. Discussions with potential users have indicated that the majority of data communications requirements in the Forward Area can be catered for by the use of medium-speed Packet Radio nets based on 16-kbit/s channels. The users' choice of 16-kbit/s channels employing the same modulation system as is currently employed for digital voice has a number of advantages. First, the 16-kbit/s NBFM modulation system has a proven effectiveness when used on mobile links with low-to-low antennas. Second, the users are familiar with the link performance of this system under a wide variety of terrain and electromagnetic conditions, which will greatly help in making optimum use of Packet Radio. Thirdly, it is possible to convert a current Combat Net Radio transceiver into a Packet Radio unit by the use of an applique unit described below. Finally, it permits coexistence with current users of the band, greatly easing the introduction of Packet Radio into service.

C. Internetworking

An efficient automatic internetworking capability provides two types of service enhancement. First, it permits fast and efficient access to information which may be held on databases of other networks. Second, a richly interconnected internet system can be used to enhance the survivability of communications on a single net. This idea of multiply-interconnecting the different communications systems in the tactical environment, in such a manner that automatic and rapid reconfiguration makes best use of the available communication resources, is central to the concept of the "integrated electronic battlefield." It depends for its realization on an internetwork architecture for non-homogenous networks, such as that developed under the auspices of the Defense Advanced Research Projects Agency in the U.S. [9]. The DARPA Internet architecture utilizes an Internet Datagram Protocol which is implemented by all gateways.

The DARPA internet strategy [15] is based on a layered communications architecture which is very similar to the more familiar ISO Open Systems Interconnection model, but is specifically orientated for interconnecting dissimilar types of network in a highly survivable manner. The DARPA Internet architecture is based on the use of a standard gateway. The Internet is thus a super-network in which the gateways play the role of switching nodes and the different types of network are the links between these nodes. The survivability characteristics of this architecture stem from replication of basic networking concepts at the internet level. The cost of such a survivable approach is surprisingly low; any network can be connected without any modifications. All gateways are identical except for the interface modules to the different types of network, and these modules are identical to those realized on all the host computers connected to that network. However, the host computers that require use of the Internet services must implement the Internet Protocol [10] for handling Internet datagrams and the end-to-end protocols for realizing the types of service indicated above. The DoD standard for the virtual call service is called TCP [11] (Transmission Control Protocol). A penalty that has to be paid for the flexibility and survivability of this approach is that of the header overheads of the

TCP and IP which can amount to 50 percent in a 1024-bit packet.

IV. CHANNEL ACCESS, ROUTING, AND NETWORK CONTROL

A. Channel Access

Carrier Sense Multiple Access (CSMA) is a robust multi-access protocol which can be enhanced to operate in the semibroadcast environment with particular benefit when a good capture effect is available, as in FM or direct sequence spread-spectrum systems. The usual drawbacks of CSMA are the dependence of the throughput on the "carrier sensing" time and catastrophic performance under overload conditions [4]. The term "carrier sensing" is used generically here, to indicate a mechanism for detecting friendly transmitting units.

The "carrier sensing" time is the elapsed time from the decision by a unit to transmit to the time it takes friendly users to detect the transmission. It is composed of the times to protect the units receiver circuits and bring its RF carrier up to full power, to modulate that carrier with intelligent unambiguous identification, for this information to transit the battlefield, and be detected by the other users of the network. It is the ratio of this carrier sensing time to the average packet duration, rather than its absolute value, that determines the maximum throughput. Currently in practical systems with average packet durations of 100 ms this ratio can be kept to about 8 percent.

The overload problem is solved by limiting the amount of traffic offered to the network so that the offered load is always less than that associated with peak throughput on the CSMA curves [4]. In fact, it is generally desirable to limit the offered load at some point below that at which the maximum throughput occurs so that the delay performance can be improved. This is the basis by which a tradeoff can be made between throughput and delay performance. The chosen operating threshold will depend on the type of usage required of the network and is intended to be a configuration parameter. Also, this limiting has to be intelligent if optimum throughput is to be obtained with varying numbers of users with varying traffic. This intelligent limiting is achieved by distributed control procedures which monitor the channel's performance.

B. Distributed Channel Access Control

Nonpersistent CSMA exhibits unstable behavior and degraded performance at high offered loads and, consequently, an important design aspect is the distributed control of overall system loading. Each unit generates its own scheduling events and channel access attempts are permitted only at these instants. Units may not start transmitting between schedules even though the channel is idle. There are two types of schedule which we refer to as "continuous" and "special." The continuous scheduler is dominant and runs at a rate which depends on the observed channel loading.

Continuous Scheduler (Fig. 2): This produces "daisy-chained" schedules which are spaced by uniformly randomized time intervals in the range from zero to a maximum as specified by the system parameter T_s . Its effect is to randomize the time distribution of system input irrespective of user characteristics and to limit the input rate

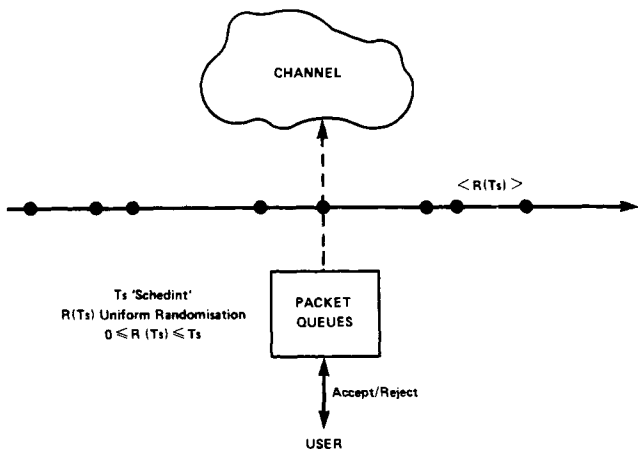


Fig. 2. Schematic of continuous scheduler.

of each unit and, consequently, the system as a whole. The parameter T_s is determined individually by each unit by an adaptive algorithm on the basis of its observation of the channel history.

Adaptive Algorithm: Each unit continuously monitors the channel and records the number of cleanly received packets N_r and the number of "captured" packets N_c (packets resolved from one or more colliding packets by capture switching). The values of N_r and N_c for a suitable integration period are used to calculate the percentage "clash ratio."

$$\text{clashratio} = (N_c / (N_r + N_c)) * 100 \text{ percent.}$$

This is compared with a system control constant "clash control" (found empirically) which corresponds to the desired channel loading and on the basis of the comparison a control action is taken.

- i) $\text{clashratio} > \text{clashcontrol}$; Action: increase T_s
- ii) $\text{clashratio} < \text{clashcontrol}$; Action: decrease T_s

The value of T_s is confined to fall between preset mini-

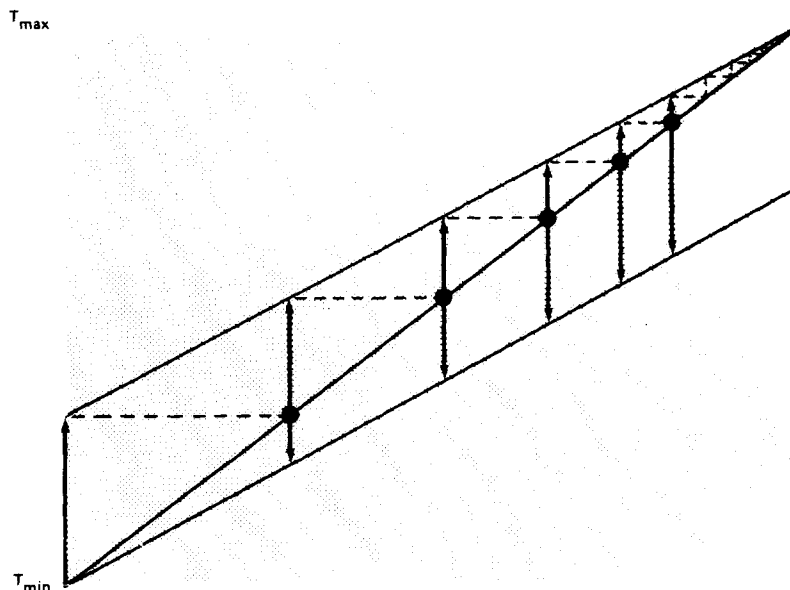


Fig. 3. Dependence of adjustment to scheduling interval T on current value.

imum and maximum limits. The algorithm allows T_s to move towards the required extreme by a function of its separation from that extreme (Fig. 3). This means that the available movement is generally asymmetrical with greater possible travel towards the further extreme. This feature was found necessary to prevent an alternative but undesirable system state in which a few "greedy" users took control of the channel with rapid scheduling at the expense of the remaining units with slow scheduling.

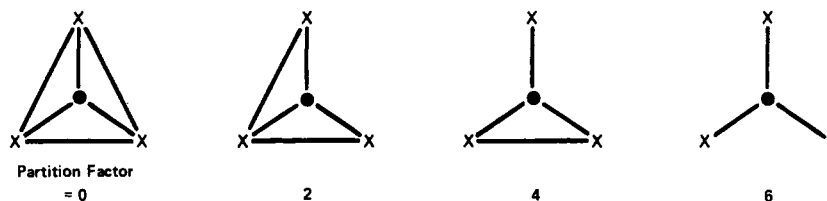
Special Scheduler: This is an event-driven scheduler which is invoked on receipt of packets requiring relay or final hop acknowledgment. Its function is to reduce in-system delays and consequently the schedule always closely follows the originating reception. If the receipt is at its unique destination then the special schedule is immediate. If it is at one of a number of possible relay units then the schedules are staggered by small offsets assigned in the same order as the ascending unique identifiers of the units concerned. This works particularly well for random traffic patterns, where it has the effect of passing a "token" between active users. However, for nonrandom traffic patterns it could lead to hogging between two or more users. (This has not happened in practice because of the significant latency in processing packets.)

C. CSMA-Distributed Control Enhancements for Multihop Networks

If a unit has neighbors which are not fully interconnected then it is likely to be required to perform a relay function and handle extra packets. However, because these neighbors are "hidden terminals" it will also experience an unusually high clash ratio and the adaptive algorithm will cause its scheduling rate to reduce unnecessarily.

By scanning the routing updates received from its neighbors, a unit can determine the number of possible interconnections which do not exist. It can then characterize their interconnectivity by an integer "Partition Factor" as given by:

Nt Total possible Neighbour – Neighbour Links
Nm Number of Missing Links
Partition Factor $\leftarrow (Nm/Nt) \times \text{Max Partition Factor}$



Modification of Scheduling Rate

$$T_s \leftarrow T_s / (\text{Partition Factor} + 1)$$

Fig. 4. Adaptive scheduling modification for hidden terminal effects.

$$\text{Partition Factor} = \frac{(\text{Broken Links} * \text{Max Partition Factor})}{\text{Max Links}}$$

This ranges from zero for full interconnection to “Max Partition Factor” for no interconnection and can be used to modify the scheduling rate as a means of correcting for the effect of hidden terminals on the adaptive algorithm. This modification increases the scheduling rate as neighbors become disconnected, as illustrated in Fig. 4.

In addition, units at the periphery of a network may not “see” any collisions because they have only one link into the network. In order to prevent these units from overloading the channel, each unit broadcasts its scheduling interval in the header of every transmission; each unit then uses the greater of its calculated values and the average of the values being used by its neighbors for controlling its main scheduler.

D. Acknowledgment Strategy

Data packets are assigned unique identifiers (a unique unit identity concatenated with a nonunique local packet sequence number). Acknowledgments are abbreviated and comprise this identifier and the hop count (see “Routing”) to the packet’s destination from the acknowledging unit. This makes it possible to “piggyback” acknowledgments into the first available transmission following the reception of the packets to which they correspond.

E. Retransmission Strategy

The combination of the special scheduler and the piggybacking of acknowledgments means that it is possible to support short retransmission time-outs (the first transmission will include the acknowledgment and is likely to closely follow the originating reception).

Apart from imposing a minimum time-out (preventing retransmission before a round-trip is possible), retransmission packets are simply queued and their transmissions spaced by the scheduler. The adaption of the scheduler under high-load conditions and the additional delays encountered if the retransmission queue builds up both serve as automatic retransmission control procedures.

F. Transmission Packaging

To increase the efficiency of channel utilization, a single transmission may, in fact, comprise of a number of component data packets, a list of abbreviated acknowledgments, and possibly a routing control packet, as illustrated in Fig. 5. Further throughput increases can be obtained by

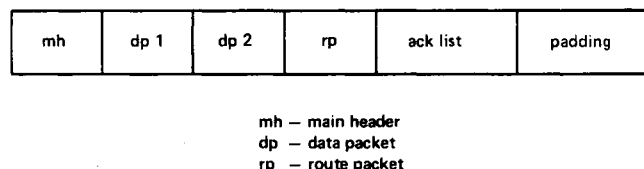


Fig. 5. Transmission packaging.

sending acknowledgments more than once, especially when these can be sent instead of padding at the end of an interleaved block.

G. Network Control

Congestion Control: To further safeguard channel stability it has been found necessary to instigate control actions on the basis of queue lengths. Packets which require handling may arise either as new user-input or be received and require relaying. There are two corresponding controls. All units advertise in their transmissions the total number of relay and retransmission packets they are currently storing.

User Input Control: If the total number of packets stored at a unit (including user-input which has been accepted and queued but not yet transmitted) exceeds a specified maximum then further input from the user is rejected. Furthermore, no packets are taken for transmission from this queue if the relay queue of any neighbor is greater than a given value “queuecontrol.”

Relay Queue Control: Before transmitting a packet which will require further relaying, a unit must examine its record of neighbor queue lengths. If any of them exceed “queuecontrol,” the unit may only transmit if its own relay queue

is greater than or equal to the largest one of the possible relayers.

While the simulations have shown that these control mechanisms are effective in controlling the lengths of the relaying queues, the remote possibility of deadlock is prevented by a time-out-controlled discard mechanism in which packets that have made no progress after a given time (30 s) are discarded.

H. Routing

A basic assumption in our approach to the routing problem is that there are generally a number of units capable of relaying a packet closer to its destination, but because of the variability of the EME it is not possible to predict *a priori* which relayer will successfully receive and decode the packet. Thus the routing as well as the channel access is "contention-based" in the manner described below. There are three main parts to the distributed routing algorithm, a traffic forwarding algorithm, a network measurement algorithm, and a route calculation and dissemination algorithm.

Traffic Forwarding Algorithm: The mode of operation of the traffic forwarding algorithm is illustrated in Fig. 1. In this diagram, the "X"'s represent the Packet Radio units and the shaded areas define regions of radio connectivity. (All units within a region are in direct radio contact with each other.) The arrows indicate the transmission links of particular interest in the delivery of a packet from unit 1 to unit 25. It is assumed that due to the operation of parts 2 and 3 of the routing algorithm that each unit has a distance vector indicating the number of hops to each of the remaining units. Two parameters are included in the packet header to aid traffic forwarding, a unique identifier and the distance from the transmitter to the destination.

Upon receiving a packet not destined for itself, a unit first checks to see if it is a smaller distance from the destination than the last transmitter of the packet. Only if this is the case does the unit put the packet on its relaying queue for subsequent transmission. If a number of potential relayers receive the packet correctly, the first unit to gain access to the channel will cause the other units to remove the packet from their relaying queues (side-stream termination). Each of the relaying stages in Fig. 1 proceeds in a similar manner until the packet reaches its destination. The transmission at any stage may be used as a hop-by-hop acknowledgment for the previous stage (downstream termination). Some unnecessary relaying may occur with this algorithm if possible relayers are out of range of each other. Any unit detecting unnecessary relaying discards the packet. If substantial amounts of unnecessary relaying occurred in practice, it is easy to extend the forwarding algorithm to nominate the next relayer, and only those in direct contact with the nominated relayer would take part in the initial competitive relaying. The nominated relayer is chosen from the routing as being the neighbor with the best quality path to the destination. (This extension to the forwarding algorithm has been implemented in the current prototypes.)

Network Measurement Algorithm: The basic network parameter that is measured is connectivity. The successful

transmission of packets, in both directions, is used to establish a link. The state of the link is continuously monitored using data and routing update packets.

Route Calculation and Dissemination Algorithm: From the traffic assignment algorithm it is apparent that each unit has to determine how many hops away it is from all possible destinations. The basic mechanism it uses to determine these distances is that it identifies those units with which it is in direct contact and, from distance information supplied by these neighbors, it computes its minimum distances to all possible destinations. This repeated minimization algorithm is a modified form of the old Arpanet routing algorithm [12] and a theoretical analysis, including convergence proofs, can be found in [13]. The minimum distance vector is broadcast in all routing update packets to the unit's neighbors.

Note: Like all repeated minimization algorithms, the only way to avoid "oscillation of routing updates" when links go down is to employ "local initialization" as described in Abram and Rhodes [13]. Unfortunately, this has the effect of declaring the destination to be "unavailable" for a significant period while the route is reconstructed from the source via other units. Our policy has been to permit some oscillation of the routing updates but to use consistency checking to damp these oscillations: e.g., if a unit calculated that a neighbor is offering routes with 1, 2, 3 hops to A, B, C, and 5, 6, 7 hops to D, E, F, the latter routes are discarded, because without any unit being 4 hops away, they are impossible!

I. Observations on the Behavior of the Basic Routing Algorithm

The above algorithm works well for slowly changing topologies with good quality links. In developing a scheme to cope under adverse EME conditions, two observations were highlighted by the simulation:

1) If routing updates are event-triggered, rapid connectivity changes could cause the whole of the channel capacity to be taken up with routing update transmissions. This can be prevented by placing a maximum frequency on the rate at which any unit can transmit a routing update. However, this implies that the network will have to perform routing using out-of-date information.

2) Simulations have shown that the hop-counter-based routing scheme still works quite well if the units have a pessimistic picture of the network connectivity. This is because the "hop-counter" information held in the units under these conditions contains "signpost" information as to the direction in which a packet should be relayed. It can also be shown that under congested conditions packets can still reach their destinations in the minimum number of hops.

The above observations led us to develop a "hold down" modification in which the routing tables do not attempt to track fast changes in connectivity, but in which links that have "flaky" or rapidly varying connectivity are labeled as poor quality links. The route calculation algorithm uses poor quality links in hop-counter calculations only if there are no high-quality paths. A route quality factor is used to indicate the number of poor quality links involved.

The use of a minimum time between the transmission of

consecutive routing updates prevents the thrashing associated with simple event-driven algorithms, although the introduction of some hysteresis in the link quality assessment could further reduce the number of routing packets transmitted.

J. Enhanced Routing Algorithm

Connectivity Measurement: The link quality measurement is an attempt to predict the quality of a given link for the next routing update period. In its simplest form this estimate is based on the performance of the link during the last such period:

$$\text{linkquality}(i, j) = \frac{(\text{no. of pkts } r_x \text{ by } j \text{ from } i) * (100)}{(\text{no. of pkts } t_x \text{ by } i) * (100\text{-clashratio})}$$

```
IF linkquality(i, j) < 5/8 THEN linkstate(i, j) = 0 (good)
ELSE
IF 5/8 > linkquality(i, j) > 1/8 THEN linkstate(i, j) = 1
(poor) ELSE
IF linkquality(i, j) < 1/8 THEN linkstate(i, j) = inf (no
link).
```

The linkstate can be thought of as a Kalman filter-like prediction of the state of the link, in that particular direction, during the next update period and as such can use weighted past values in its calculations.

Action on Receiving a Routing Update Packet: An update from a neighbor indicates the number of hops to various destinations, the qualities of the routes, and requests to units whose latest updates it does not possess. (A unit can determine if it is not in possession of a current update, because all transmissions from a given unit "advertise" the sequence number of its current routing update.) It is processed as follows:

a) The entry for the receiving unit is examined to see if the neighbor received this unit's last update. If not, then the "transmit update flag" is set.

b) The unit uses the update to recalculate routes to all other units choosing the minimum hop indications of the highest quality. It notes whether any of the route hops or qualities have changed. If they have changed the unit will broadcast the new update at the earliest opportunity. However, if it has not broadcast an update for T_u (update period) seconds then it sends the new update immediately.

Action When Unit is Idle: If a unit does not have any data packets to send over a routing update period, it forces the sending of a routing update every T_u seconds in order to alert neighbors to its continued existence.

Action When Routing Information Is Incorrect: If units have a pessimistic measure of the number of hops to a destination, the forwarding algorithm will still deliver the packets, possibly with some unnecessary relaying. However, if a unit has too low a value for the distance to a destination, a subsequent relayer may not accept a packet for relaying. This problem is ameliorated by increasing the hop counter in the packet header if no acknowledgment is received after three transmissions. If after seven transmissions no acknowledgment is received, the unit discards the packet.

K. Network Control—Initialization and Self-Configurability

The fully distributed channel access and routing algorithms described above mean that no special actions have

to be taken during initialization. After the lifting of Radio Silence, the units are switched on and the network will self-configure in approximately 2 min, depending on the number of areas of radio connectivity and the quality of the links.

This emphasis on self-configurability, rather than optimum network topologies, is due to the fact that the geographical distribution of radios in the Forward Area is primarily determined by the noncommunications functions of the forces (soldiers are unlikely to travel along the skyline in Forward Area just to improve communications). However, it is possible that existing connectivities will fail to support the data transfer requirements of the users. A privileged command may be entered at any terminal which will result in the display of the connectivity and traffic loadings of the network, thus enabling a Signals Officer to minimally perturb the locations of some users to obtain the required performance. The aim is that the system should require the minimum of human supervision, and when it does require supervisory input, that it presents system status information in an understandable and easily assimilable form. The current RSRE prototype makes extensive use of the graphics facilities available on the standard Digital Equipment Corporation VT100/200 terminals.

V. PERFORMANCE

The RSRE Packet Radio simulator fully implements all the algorithms described above individually for each unit in the network. A two-dimensional connectivity matrix is used to determine which units are affected by the actions of current transmitters. Packet generation is for random source-to-destination pairs.

Hundreds of hours of simulations have been performed on networks with various loadings, topologies, and control parameter settings. A major aspect of the results has been that, although the performance is sensitive to the choice of algorithm, it is not particularly sensitive to the control parameter setting. The main criteria which affect the throughput and delay of such networks will be summarized, followed by particular results for a network subjected to rapid and large changes in connectivity.

The main parameters used in the simulations to which the results refer are as follows:

packet duration	100 units
t_x to r_x switch time	5 units
r_x to t_x switch time	5 units
routing update period	20 000 units
clashcontrol	4 percent
max partition factor	6 (see Section IV-B).

The percentage loadings and throughputs referred to in the next sections are obtained by dividing the total number of delivered bits by the channel bit rate multiplied by the time of the simulation. Thus percentages do not include header or coding overheads. The performance in terms of throughput, delay, and delay dispersion depends upon the ratio of the "carrier sensing" dead time to the average packet duration, network connectivity, and the rate of change of network connectivity. As in all packet-switched networks, there is a tradeoff between loading and average delay. We have not found the performance to be particu-

larly sensitive to the exact setting of the clashcontrol, max partition factor, or routing update parameters.

A. Performance with Single-Hop Topology

The "single-hop" or fully connected network is a special topological case which has significantly better throughput/delay characteristics than others. It obtains full benefit from the co-operative properties of CSMA. When traffic is offered randomly by all users, acknowledged throughput rates of about 60 percent of channel capacity are achievable. This figure is sensitive to the action of the "special scheduler" which permits any unit which has just received a packet for acknowledgment an immediate channel access opportunity. It has been noted that most transmissions are successful on their first attempt and therefore the average delivery time from first transmission is of the order of a few hundred milliseconds. However, in a heavily loaded network, packets will suffer significant pre-transmission delays. The throughput figures have been roughly translated into messages per hour (by assuming 80-byte messages, 20-byte Packet Radio headers, and half-rate Forward Error Control overall) in Fig. 6.

B. Performance with Multiple-Hop Topologies

Although throughput/delay performance for multiple-hop networks depends upon offered traffic patterns and topology, simulations have shown that, for random traffic patterns and topologies with reasonable numbers of relays, the main factor affecting performance is whether or not the topology is static. This effect is quite easily explained. The dynamic changes have two effects:

i) They cause the network to attempt to reroute packets when the routing database information is out-of-date and/or inconsistent. The algorithms to circumvent these problems involve extra transmissions.

ii) Routing updates, which take up some of the channel capacity, are only transmitted when changes occur.

Apart from the dynamics of the topology, the maximum throughput and delay are relatively independent of topology. The main reason for this appears to be that as the connectivity becomes more cellular more units can transmit simultaneously without causing collisions, and thus there is some frequency reuse in nonadjacent areas of connectivity. Acknowledged throughput rates in the range 25-36

percent have been achieved in the static multiple-hop topologies.

C. Performance with Dynamic Topology

The results from the simulations in which rapid connectivity changes have been induced have been most promising. Basically, the link quality assessment time constants are related to the known time that it takes the updates to be disseminated. So unless the connectivity measurement indicates that the link is going to be available for a useful period of time, it is not included in the minimum distance calculation.

Thus the routing tables reflect a pessimistic view of the number of hops required, but when the shorter hop routes are available, the contention-based routing algorithm permits them to be used.

As an illustration of the performance of a network under extremely unfavorable conditions we have taken the case of a 25-unit network where the connectivity can be varied between a 2-hop (good) and 5-hop (bad) scenario, as shown in Fig. 7. The simulation switched the connectivity between these two states at rates between once every 50 time units (half a packet time) and once every 100 000 units. It can be seen from the time constants indicated in the routing algorithm that for most of these switching times routing in-

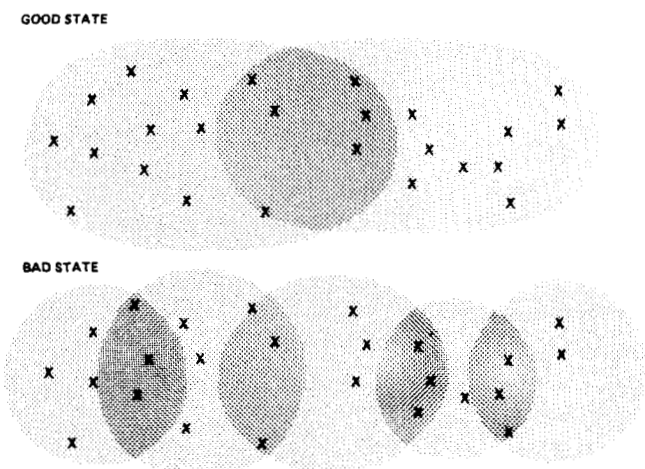


Fig. 7. Two connectivity states used in dynamic performance and evaluation.

State/Topology	Delivered Information (Percentage of Capacity)	Messages/Hour 20 byte header } 1/2 rate 80 byte message } coding
Static, Single Hop	60%	24,000
Static, Multiple Hop	25-36%	10,000-15,000
Dynamic, Multiple Hop	15%	6,000

$$a = \frac{\text{Carrier Sensing Dead Time}}{\text{Average Packet Duration}} = 0.05$$

Fig. 6. Throughput performance.

formation cannot be distributed from one end of the network to the other! The ratio of the time spent in the good and bad states is the same for all simulation runs so that the results can be compared. The ratio used in the example is 25 percent in the good state and 75 percent in the bad state, but the results are maintained for all ratios. Fig. 8 illustrates the throughput, average delay, and lost packets for various accepted loads. The lost packets are those which fail to ar-

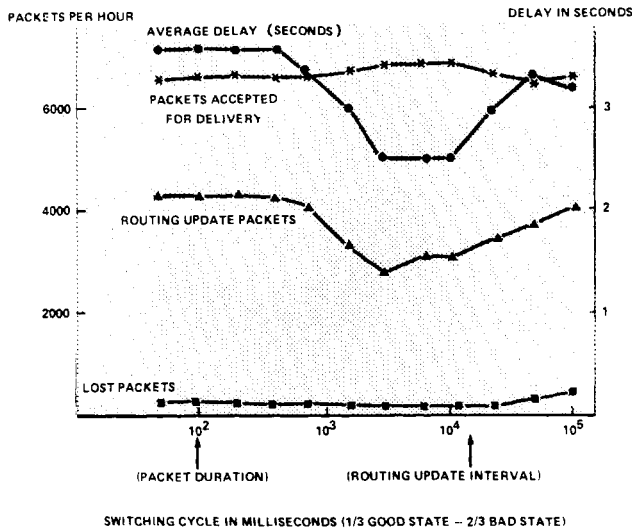


Fig. 8. Performance of dynamic multiple-hop topology of Fig. 7.

rive at their destination because somewhere along the route a unit has transmitted them seven times but, because of confusion in the routing tables, has found no "nearer" unit to accept and relay them. The figures correspond to acknowledged throughput rates of about 15 percent. On a 16-kbit/s channel this corresponds to 6000 80-byte packets per hour including half-rate error control coding and header overheads.

VI. SIGNAL PROCESSING REQUIREMENTS AND ARCHITECTURE

The various functions of the prototype Packet Radio stations are performed in three subunits as shown in Fig. 9. The higher level protocols (routing, internetworking, man-machine interface, etc.) are handled by the station processor, presently a PDP 11-23, with about 60k words of real-time software written in a high-level language, CORAL 66. The critical real-time tasks of the lowest level of protocol, i.e., the signal processing, are carried out by a specially developed burst-data modem. These two together form an applique unit for a vehicle VHF radio set, the CLANSMAN 353. This latter has been modified, by means of a single replacement circuit card, to switch from receive to transmit in less than 5 ms, in order to give efficient channel utilization at high offered load.

Some of the most important system design constraints arise from the requirement for mobile operation in the highly congested radio spectrum to be found in Northern Europe. The combination of the terrain, and the logistic undesirability of the need to rely on extensive well-sighted repeaters, points to the use of the low-VHF band (approximately 30 to 100 MHz) and for the same reasons, most current Army voice communications use this band. This, in turn, has led to the ready availability of radio sets that operate in this band, usually using 25-kHz channeling with either narrow-band frequency modulation or 16-kbit/s digitized speech, and this 16-kbit/s capability has been used as the bearer for the medium-speed Packet Radio system.

The modem has to perform the tasks of synchronization, modulation, demodulation, and error control, and also the more specific tasks of carrier sense and capture switching. It is also particularly important to provide the ability to receive correctly consecutive packets with little or no time between them, something that is notably lacking in many realizations of existing packet systems but very important here in order to maximize the utilization of the small available channel.

In data mode, the radio sets provide a dc-coupled linear

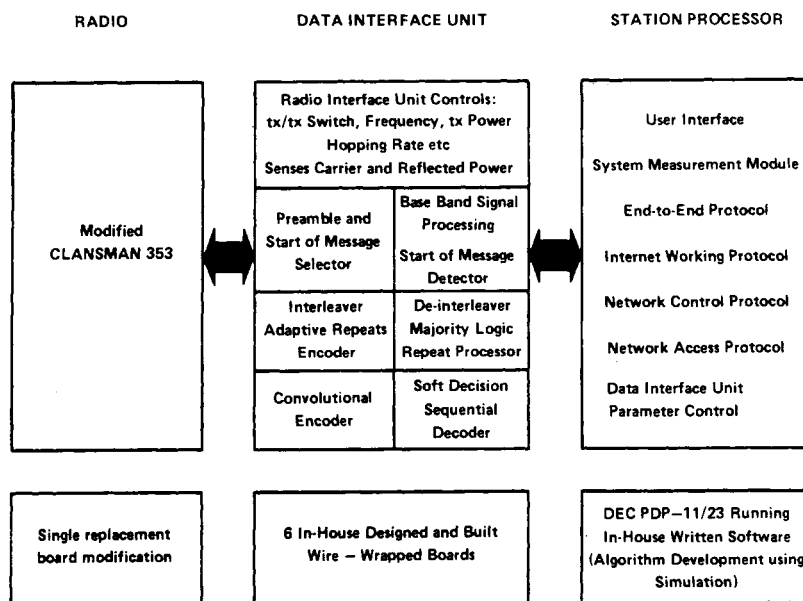


Fig. 9. A flexible prototype tactical data station.

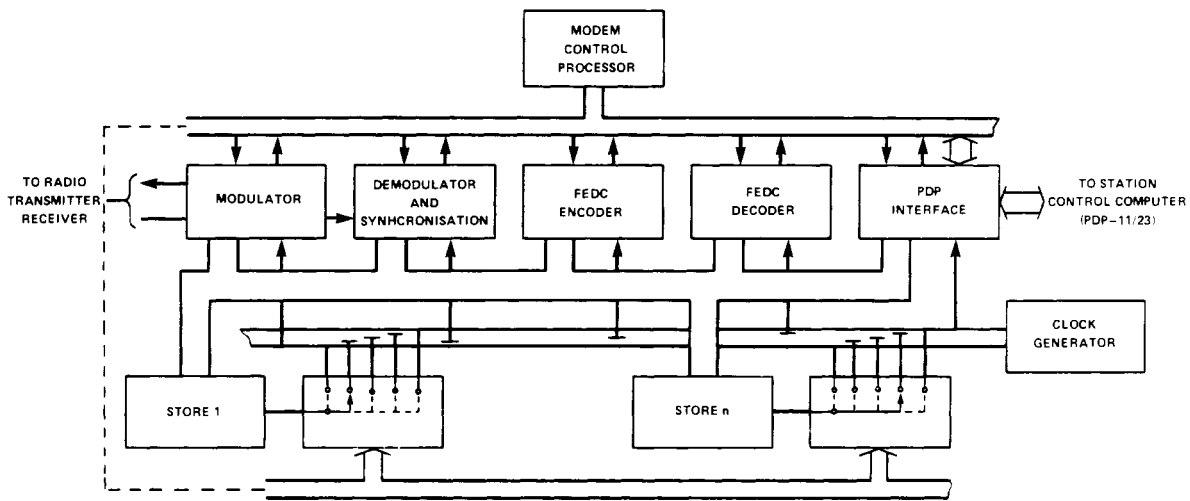


Fig. 10. Packet Radio modem.

FM channel with a bandwidth of some 10 kHz, and this is modulated directly by the bipolar non-return-to-zero bit stream, after filtering by a digital finite impulse response filter. This scheme has the advantage of no error extension or bandwidth expansion, as can happen with partial response, biphasic, or HDB3 coding, and is also highly tolerant of multipath components up to some 20- μ s spread. The message is preceded by a 64-bit synchronization preamble, the length having been chosen to give a suitable compromise between performance in noise, false alarm rate, and fast signal acquisition. The message itself consists of an integral number of 1024-bit blocks up to a maximum of 16 blocks, each consisting of 512 information bits and 512 parity bits, interleaved to a depth of 32. The first block contains in addition a separately encoded indication of the number of blocks in the transmission. The error control system employed is half-rate convolutional encoding of constraint length 47 and sequential decoding [14]. For a two-block message (1024 information bits) this provides a probability of successful decoding of 0.9 at an error rate of 5 percent. This forms the base level of error correction; alternative message structures include two or four repeats and majority voting as an outer code to cope with 10- or 18-percent bit error rates. These alternative message structures are indicated by the use of different synchronization preambles, the three preambles being chosen to be mutually orthogonal.

The incorporation of capture switching requires that the synchronization circuits are kept running all the time, so that in the event of a stronger signal partially overlapping a weaker existing transmission, the demodulator may switch to the larger signal. This strategy falls down when a false synchronization event occurs due to a pattern appearing in a message that is similar to a synchronization preamble. The problem is compounded by the relatively low synchronization threshold (to maximize synchronization probability at high error rates) and also by the tendency for false alarm rates to be higher during random 16-kbit/s traffic than with white noise. Moreover, retransmission of this particular message will cause the same action to occur again. The solution to this problem is, upon an indication of a potential capture, to start a second demodulator running in addition

to the current one. The undetected error performance of the error correction decoder can then be exploited to determine whether or not the capture was genuine. It is even possible to completely recover two packets which overlap by not more than 10 percent, provided that the second one is at least 5-dB stronger than the first.

The signal processing in the modem is all performed digitally; on the receive side the radio receiver output is sampled four times per bit period, i.e., 64k samples/s or every 16 μ s. Many of the operations are bit-oriented, which means that a general-purpose microprocessor is too slow to perform the required tasks, and at the time of the prototype design, signal processing devices such as the Texas Instruments TMS 320 were not available. The prototype was, therefore, constructed in the form of a number of special-purpose hardware units, sharing a common bus under the control of an 8085 microprocessor (Fig. 10). The bus has a 1-bit data path (because so many operations are 1-bit operations, and speed is not a problem at these moderate data rates) and a speed of 2.5 MHz. The processing devices are allocated time slots on the bus in a strict time-division multiple access manner, with the sequential decoder being allocated one cycle in two, and the other devices allocated one cycle in sixteen. The pool of buffers has available to it all the clock phases controlling the bus, and the processor can enable any buffer during any clock phase. By this means, the processor connects a buffer to a demodulator, and when it receives an indication that a message has been received, it can connect that buffer to the different processing devices in turn in accordance with the current modem status (self-test, error measurement, or normal running) and the level of redundancy of that packet as indicated by the preamble. Thus at any instant, there may be a number of packets at various stages in their processing, and a snapshot of the queue for the convolutional encoder might show a packet to be transmitted, and one or more received packets awaiting the first stage of error decoding. The existence of a data path, in addition to control and status, between the control processor and the DMA interface permits an extensive self-test facility.

Current work is directed at implementing the modem on two circuit cards, one to carry out modulation, demodu-

lation, and synchronization, and the other for error control. Each card would consist of a processor and a semicustom support chip; the modulator/demodulator/synchronization is currently being configured as a TMS 320 plus a semicustom correlator chip, to communicate with the error-control unit via dual-port memory. The TMS 320 is not ideal for this particular task, so we will investigate the use of small bit-slice systems and other reduced-instruction set devices, such as the Inmos transputer. A station processor based on a 68000 or similar processor would then complete the applique unit, the key aims being to reduce the parts count, cost, power consumption, and size compared with the current prototypes. The longer-term aim is to produce a battery-powered manpack access unit, which operates a reduced set of protocols (but still needs the full modem functions) and gains access to the main net via the nearest available main Packet Radio station.

VII. EXPERIMENTS WITH PROTOTYPE EQUIPMENTS

Five prototype units incorporating the hardware and software design described above have been constructed. Initially, basic performance assessment and debugging were carried out in the laboratory with the aid of a matrix switching box which permitted computer control of the connectivity on all of the 20 baseband links. These laboratory experiments demonstrated the effectiveness of the contention-based routing algorithm and validated its ability to handle rapid changes in connectivity as predicted by the simulator. Unfortunately, interconnecting at baseband rather than at RF caused the clash detection to be inoperative and failed to show the beneficial effect of RF capture. We now have the development of an RF switching matrix in hand. The laboratory experiments highlighted one area in which the simulator was deficient in detail. Although the simulator did assume that the whole packet had to be received before it could be processed, it then assumed that the processing was performed instantaneously! These early laboratory experiments showed that the combined signal processing and protocol handling produced a significant latency between reception of a packet and the earliest possible transmission of the acknowledgment. This latency was of the order of the shortest packet duration. In particular, this has implications for the special scheduler; it will be relatively easy to enhance the simulator to model this latency.

These laboratory assessments have been followed by a very successful series of mobile field trials and demonstrations. For these trials, three of the units have been installed in standard Army Landrovers, and two in a transportable flatbed cabin. One of the units is usually demounted from the flatbed cabin to a site with fixed wire link to a gateway of the DARPA Internet. Perhaps the most telling feature of these trials and demonstrations was the fact that no "engineering" channel has ever been used. In fact, the mobiles are equipped with a single Packet Radio unit only and it has never been necessary to disconnect the radio from the applique and use it in voice mode. This also bears out the claim made earlier in the paper that Packet Radio often involves less overheads than normal voice operation for the users. These field trials provided confirmation of the mobile communications capability of the network including its ability to adapt to changes in connectivity

generated by units in motion. An unexpected feature of these trials was the ability of the networks to make use of nonsymmetric radio links. Thus packets were often delivered in one hop from a source defined to be two hops away (the routing table only accepts bidirectional links), the acknowledgment from the potential relay terminating the source transmission and that from the destination canceling the relaying attempt. This had not been observed in the simulation because it had always been run with symmetric connectivity data.

A major feature of the demonstrations to-date has been the ability to provide mobile access from remote locations to large computing facilities on the ARPANET, mimicking the ability of field commanders to access powerful C3I databases from the Far Forward area. The TCP/IP protocols permit reliable error-free mobile access to hosts via LANs, satellite, and long-haul networks. Such long-haul access is performed using local echo and line at time transmissions. It is a tribute to the flexibility and robustness of TCP/IP that such access, although involving some overheads, was perfectly acceptable to the operator. In fact, the main problem with mobile use of Packet Radio was entering data correctly via a keyboard. This highlights the desirability of a more sophisticated man-machine interface (MMI) based upon a speech/recognition and synthesis unit.

Interoperability between CNR Packet Radio and the DARPA Packet Radio was effectively demonstrated in trials that occurred over a two week period at the SHAPE Technical Centre in Holland in March 1985. These trials plus a live demonstration at the STC Symposium on Interoperability of ADP Systems [16], involving half a dozen networks attached to the DARPA catnet, highlighted the tactical to strategic communications interoperability and the flexibility that can be obtained by designing networks as members of an internet system rather than as stand-alone systems.

VIII. CONCLUSION

This paper has described the first iteration of system design and development for a narrow-band PR system. The results at all stages have been particularly encouraging. In the second iteration which is based on a commercial procurement of a 25-station unit of suitable size, weight and, power consumption, further refinement and field evaluation of the distributed algorithms will be made.

The algorithms which we have developed have been influenced by the highly mobile and hostile nature of the environment in which systems will be expected to operate. Detailed simulations have been used to evaluate the performance and stability of the algorithms. The channel access and network control strategies as currently implemented are capable of maintaining a useful grade of service over a wide range of operating conditions. In particular, the routing algorithms have been shown to provide a very acceptable level of service when more orthodox algorithms would be generating unsupportable overheads. The strength of the CNR PR, as is the case with the DARPA wide-band PR, stems from the synergism of signal processing and communications protocols; the former, using modern VLSI techniques, to match the latter to what at first sight is a very unprepossessing communications channel.

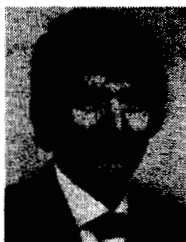
The authors would like to thank J. Jubin of SRI International for helpful discussions (via the DARPA Internet) on the relaying algorithm, the referees for their very helpful comments, as well as M. Hazell and L. Hodge of RSRE for their many contributions to the Programme.

REFERENCES

- [1] J. Jubin and J. D. Tornow, "The DARPA packet radio network protocols," this issue, pp. 21-32.
- [2] I. Jacobs, R. Binder, and E. Hoverstein, "General purpose packet satellite networks," *Proc. IEEE*, vol. 66, no. 11, pp. 1448-1467, Nov. 1978.
- [3] L. Kleinrock, "Principles and lessons in packet communications," *Proc. IEEE*, vol. 66, no. 11, pp. 1320-1329, Nov. 1978.
- [4] L. Kleinrock and F. Tobagi, "Packet switching in radio channels: Part I—Carrier sense multiple access modes and their throughput and delay characteristics," *IEEE Trans. Commun.*, vol. COM-23, pp. 1400-1416, Dec. 1975.
- [5] F. A. Tobagi and L. Kleinrock, "Packet switching in radio channels: Part II—Hidden terminal problem in carrier sense multiple access and the busy tone solution," *IEEE Trans. Commun.*, vol. COM-23, pp. 1417-1433, Dec. 1975.
- [6] —, "Packet switching in radio channels: Part IV—Stability considerations and dynamic control in carrier sense multiple access," *IEEE Trans. Commun.*, vol. COM-25, pp. 1103-1119, Oct. 1977.
- [7] B. M. Leiner, "A simple model for computation of packet radio network performance," *IEEE Trans. Commun.*, vol. COM-28, pp. 2020-2023, Dec. 1980.
- [8] R. R. Boorstyn, A. Kershenbaum, and V. Sahin, "Throughput analysis of multihop packet radio networks," in *Proc. INFOCOM '85*.
- [9] V. Cerf and P. T. Kirstein, "Issues in packet network interconnection," *Proc. IEEE*, vol. 66, no. 11, pp. 1386-1408, Nov. 1978.
- [10] DARPA, *DOD Standard Internet Protocol*, Defense Advanced Research Projects Agency, IEN-128, Jan 1980.
- [11] DARPA, *DOD Standard Transmission Control Protocol*, Defense Advanced Research Projects Agency, IEN-129, Jan. 1980.
- [12] J. M. McQuillan, G. Falk, and I. Richer, "A Review of the development of the ARPANET routing algorithm," *IEEE Trans. Commun.*, vol. COM-26, pp. 1802-1811, Dec. 1978.
- [13] J. M. Abram and I. B. Rhodes, "Some shortest path algorithms with decentralized information and communications requirements," *IEEE Trans. Automat. Contr.*, vol. AC-27, pp. 570-

582, June 1982.

- [14] G. D. Forney and E. K. Bower, "A high-speed sequential decoder: Prototype design and test," *IEEE Trans. Commun. Technol.*, vol. COM-19, pp. 821-835, Oct. 1971.
- [15] B. M. Leiner, R. Cole, J. Postel, and D. Mills, "The DARPA Internet protocol suite," *IEEE Commun.*, vol. 23, pp. 29-34, Mar. 1985.
- [16] B. Leiner and B. H. Davies, "Mobile packet radio interoperability demonstration," in *Proc. 2nd Int. Symp. on Interoperability of ADP Systems* (Shape Technical Centre, The Netherlands, Mar. 1985).



Brian H. Davies received a first class honors degree in physics from the University College, Cardiff, Wales, in 1971. He went on to investigate ionic migration in polycrystalline oxides and received the Ph.D. degree from the University of Wales in 1974.

He then joined the Royal Signals and Radar Establishment (RSRE), Christchurch, where he worked on mobile digital communications at UHF, forward error control for satellite circuits, and software-based

signal processing techniques for which he received the Charles Babbage Award from the IERE in 1980. From 1978 to 1981 he led the RSRE technical contribution to the joint RSRE-DARPA collaborative research agreement on the development and evaluation of inter-networking techniques. Since 1981 he has been responsible for the packet and digital radio programs at RSRE.

Dr. Davies is a member of the Institution of Physics and a Chartered Physicist.



T. R. Davies was born in Cardiff, South Wales, in 1952. He received the B.A. degree in physics from Oxford University, Oxford, England.

He then joined the Signals Research and Development Establishment (now part of the Royal Signals and Radar Establishment), Malvern, England, where he has worked on such topics as signaling codes for digital trunk network, SAW correlators, HF antennas, and digital and analog signal processing

for radio data systems.