

# A DISTRIBUTED TRUNKING MECHANISM FOR AD HOC VHF TACTICAL NETWORKING

Stan Vitebskiy  
Jeffrey A. Kroon

Harris Corporation  
RF Communications Division  
Rochester, NY 14610

## ABSTRACT

*Current tactical communication systems require new approaches to provide adequate support for the growing number of services on a digital battlefield. The RF Communications Division of Harris Corporation has been developing a networking solution to meet these requirements. As a part of this solution, a robust, fully distributed protocol for VHF multi-frequency channel access has been designed. This protocol satisfies the mobility, capacity and integrated voice and data transfer requirements of the tactical environment without fixed infrastructure. This paper presents an overview of the proposed distributed trunking mechanism, including network and node behavior and data movement. Throughput and delay performance of the protocol obtained using OPNET™ network simulation in realistic tactical environments is presented.*

## INTRODUCTION

Modern tactical communications requirements present new challenges to system designers and manufacturers. Current movement towards the digital battlefield drives the need for accommodation of larger loads of data and voice traffic while maintaining connectivity in mobile networks without reliance on the fixed infrastructure. Additionally, users of tactical communication systems now strive to have an access to the same kind of network services which are normally available through the commercial Internet. Therefore new protocols are needed which can be integrated easily with industry standard networking applications and transports while accounting for specifics of the VHF wireless media and the way military organizations use their communication resources. The RF Communications Division of Harris Corporation has been developing networking solution which meets the above challenges. A part of this solution is the novel fully distributed multi-frequency channel access protocol presented in this paper.

There have been a number of media access protocols proposed in the past for application in tactical networking [1-3]. A significant number of these schemes rely on centralized control for bandwidth allocation between different network entities[2,3]. Systems utilizing such protocols become vulnerable due to their single point of failure (base station) and therefore are often unacceptable for application in tactical environments. Among distributed protocols described in the literature, the multiple-access with collision avoidance (MACA)[1] provides collision-free data transfer and efficient solution to the "hidden terminal" problem. However, due to its single frequency implementation it limits the capacity and capability of the networking system.

The protocol presented in this paper does not rely on any fixed infrastructure - it runs independently on each of the networked radios and therefore makes the network tolerant to a single node failure. This protocol addresses the "hidden terminal" problem and uses collision avoidance in the manner similar to MACA while utilizing multiple frequencies. The protocol provides adaptive power and encoding control capabilities, supports simultaneous voice and data transfer, priority based preemption and interruption, and allows nodes to select frequencies in a consistent and robust manner.

The paper is organized as follows. In Section 2, the proposed channel access protocol is described. Section 3 is devoted to the implementation of the protocol model using the OPNET™ network simulation tool. Results of simulations are presented and analyzed. In the final section, the conclusions are drawn.

## PROTOCOL OVERVIEW

The network consists of an arbitrary number of both mobile and fixed nodes, scattered in random fashion over the geographical region of interest. The degree of connectivity between nodes is not known *a-priori* and is

determined by their respective antenna coverage areas. Moreover, the connectivity status may change during the course of network activity due to node movement, failure/recovery or other dynamic factors

In the proposed trunking scheme, a fixed number of radio channels are assumed to be available to the network. All channels are half-duplex, so that none of the nodes can simultaneously receive and transmit. One of the channels is pre-configured to act as a control channel accessible by all network nodes. The rest of the channels are used for voice and data transactions between pairs of nodes (these channels are called "data channels" throughout the text). Access to data channels is negotiated between nodes on the multiple access control channel (see Fig.1). Once a particular data channel has been selected for communication between two given nodes, it becomes inaccessible by any other node in the network, provided the information about channel assignment has propagated to all nodes via the control channel. A node might not have correct knowledge about particular data channel occupancy if at the time of data channel selection it was not listening to the control channel (it could have been down, out of range or involved in another transaction). An efficient channel negotiation mechanism taking into account the above scenario is incorporated into the protocol to avoid a large number of retransmissions and channel renegotiations. After an exchange of data is completed, nodes switch back to the control channel to inform the rest of the network that the channel has been released. Then they continue to listen to the control channel until they decide to start the next exchange. While listening to the control channel, all nodes constantly update their view of the current network state. This information helps nodes in future channel selections.

Control channel negotiations consist of the following steps. On the control channel, the source node broadcasts its channel request to the network. The destination node responds by either agreeing or rejecting to communicate on the requested channel. Acceptance of the channel depends on information the node currently has about the status of the requested channel. If the requested channel is not acceptable for the destination node, then it suggests a different channel and asks the source node to agree on it. This process repeats until the nodes agree on the channel.

Channels available for assignment at every node are divided into two groups. The first group consists of the channels whose status is definitely known, i.e. the

channels that have been released after the last time the node got access to the control channel. In the second group are the channels whose status can not be determined precisely, but that could potentially be free. These are the channels that have been released or occupied before the last time the node switched to the data channel. When engaging in channel negotiations, the source node randomly chooses a candidate channel among the channels in the first group. It starts randomly choosing from the second group only after all the channels from the first group have been rejected by the other party. A destination node accepts the proposed channel if the channel belongs to either of the above two groups in its database, and it rejects the channel if it definitely thinks that the channel is occupied. Whenever a node needs to select a new channel but determines that all of the available channels are busy, it waits until any channel is released or until the maximum channel occupancy time expires, and then assumes that the oldest busy channel it knows of is free.

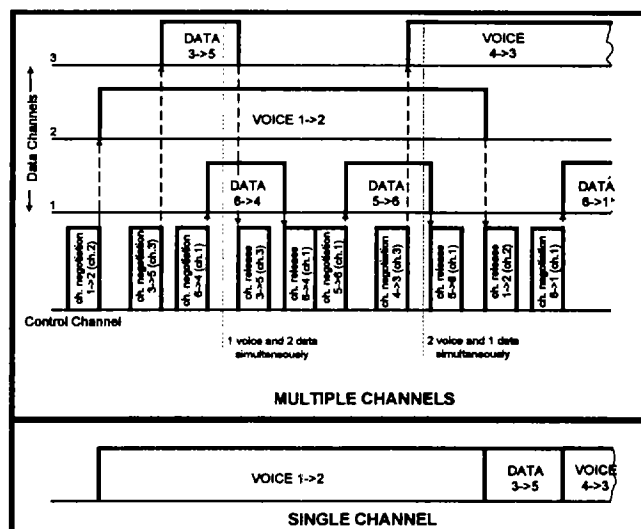


Figure 1. Comparison between distributed trunking scheme (labeled "multiple channels") and single channel multiple access communications. In distributed trunking approach, data channel accesses and releases are negotiated on the control channel, shared by all subnet nodes. This allows for simultaneous voice and data exchanges, improved efficiency, priority preemption and interruption.

If the node waiting for response from its party does not receive it before the time-out, it retransmits its request and waits for the response until the second time-out expires. If the second time-out occurs, the destination node is considered busy or temporarily out of reach. If, instead of the response from the destination node, a request packet of higher priority is received, the node assumes that its request has been lost, and services the received request. The node stops waiting for a response

whenever any information is received that might indicate a non-reception of its request packet by the destination node.

Since the control channel can be accessed simultaneously by multiple nodes, it requires a MAC (medium access control) protocol to maintain efficiency and guarantee fairness of access. Three different MAC protocols were considered for the control channel (Fig.2). In the minislotted CSMA/CA scheme, collision avoidance (CA) exploits the fact that an occurrence of some transmissions in the network can be predicted, and therefore collisions can be avoided. For example, nodes receiving a packet that requires a response and that is not addressed to them, do not start transmission until the destination node has had time to respond. Additionally, time slotting is used to approximately synchronize and redistribute starting times of packet transmissions from different nodes. The duration of every time slot is equal to the packet transmission time plus some number of mini-slots. The duration of a mini-slot is equal to the maximum propagation delay for a given network topology. Since the majority of nodes will start their major slots almost simultaneously, the start of actual transmission is scheduled to coincide with the beginning of a randomly chosen mini-slot within the major slot. Consequently, only packets whose transmission begins at the first chosen mini-slot will experience the collision. Since it is always desirable to favor negotiation that has already been in progress, the first mini-slot of every major slot is dedicated to response packets.

An alternative MAC approach, which eliminates collisions altogether, is time-division multiple access (TDMA) (Fig.2). In this approach, the control channel is divided into *epochs*. Each epoch is in turn subdivided into time slots with a duration twice larger than needed to transmit a control packet. Time slot pairs are numbered in round-robin fashion, and only one node is allowed to transmit in the first time slot of the pair that is assigned to it. Every other time slot in the epoch is dedicated to the transmission of response packets. The larger the subnet, the greater the delay between successive transmissions for a given node. Additional delays are introduced when the data channel is released (Fig.2). In spite of these drawbacks, TDMA's collision-free medium access may outperform CSMA's delay-free access in environments complicated by hidden terminals, constantly changing topology, severe channel fading and interference.

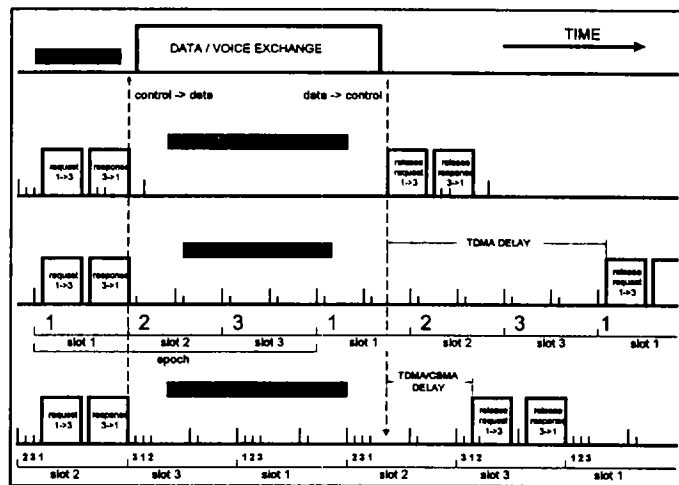


Figure 2. Time allocation on the control channel for three access schemes described in the text: a) CSMA/CA; b) TDMA; c) hybrid TDMA/CSMA. In CSMA/CA, transmission begins immediately if the control channel is unused by other nodes. In TDMA, it starts in the next slot assigned to the transmitter (slot 1). In the hybrid approach, transmission begins in the next slot available and in the mini-slot assigned to the transmitter (slot 3, mini-slot 1) and if the channel is idle.

The third approach combines the features of both *carrier sense* and *time-division* multiple access schemes discussed above (see Fig. 2). The epoch structure is similar to the one in pure TDMA case. However, every pair of time slots begins with a series of mini-slots each of which has a duration equal to the maximum propagation delay in the subnet. The number of mini-slots is equal to the number of nodes and each node is allowed to start transmission only in the beginning of the mini-slot which is uniquely assigned to it. Mini-slots are numbered sequentially in the round-robin fashion and the initial mini-slot number itself changes cyclically from one major slot to another as shown in Fig. 3. This structure is chosen in attempt to guarantee a fair access for all subnet nodes. As time progresses, a node, which was initially privileged by having its mini-slot started before the mini-slots of all other nodes, loses its access priority in favor of those nodes that were disadvantaged by the late mini-slots. As in the case of CSMA, transmission is allowed only if the control channel is idle. This approach eliminates collisions almost completely and does not suffer from large delays. However, it is difficult to implement in practice due to the required node synchronization.

## SIMULATION

Protocol performance was investigated via simulations using the OPNET Modeler [4], a protocol simulation tool by MIL3, Inc. Network topology used in our initial

simulations consisted of 25 fixed nodes occupying an area of approximately 40 km<sup>2</sup>. All nodes were in the line-of-sight (LOS) with respect to each other, and their transmitted power levels (20W) were large enough to provide full network connectivity. A noiseless environment was assumed in order to assess protocol's peak performance in ideal conditions. Arbitrary number of nodes, from 2 to 25, could be enabled to investigate dependence of the protocol performance on the network size. The following parameters were used in simulations: channel bit rate - 16 kbps, modulation - binary FSK, channel bandwidth - 25 kHz, control channel frequency.- 150.1 MHz, channel separation - 100 kHz, switching delay between frequencies - 0.5 msec

One of the parameters of interest characterizing protocol efficiency is a network throughput  $S$  defined as a number of bits successfully received in the entire network per second over the bit rate of one communication channel. It follows from the definition, that the throughput of ideal multi-channel trunked network is bounded by the number of available data channels. The goal of simulations is to determine how well and under what conditions our protocol yields throughput approaching this ideal theoretical bound.

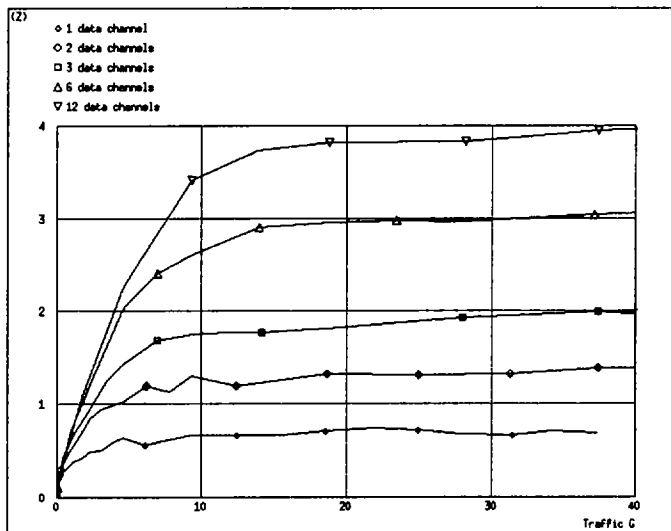


Figure 3. Throughput of 25-node network as a function of total traffic and number of available channels (CSMA/CA control channel).

In Fig 3, the throughput is plotted as a function of network traffic  $G$ , for 25-node network utilizing CSMA/CA protocol on the control channel. The traffic is defined as the total number of bits of raw data generated by all nodes per second over the bit rate of one communication channel. (Note, that in all

simulations, all data packets are assumed to have the same size of 1kb). Curves are plotted for different number of available data channels to demonstrate how trunking is achieved by the protocol. The lowest curve corresponds to the single channel mode of operation of the protocol, or the case when one channel is used for communicating both the control and data packets. In this case, the throughput reaches its maximum of approx. 0.75 for 25 nodes and remains at this level as traffic increases. This result indicates a superior performance of the single channel version of our protocol in comparison with such ubiquitous schemes as ALOHA and slotted ALOHA. The maximum throughput achievable by the latter protocol does not exceed approx. 0.6 in wireless networks [5], and it rapidly decreases with growing traffic. In the multi-channel mode, our results show that the protocol achieves relatively good trunking efficiency. Whenever the throughput saturation level is reached, its value corresponds to approximately a single channel throughput multiplied by the number of available channels. As expected, this result deteriorates when the size of the network and the number of channel increases.

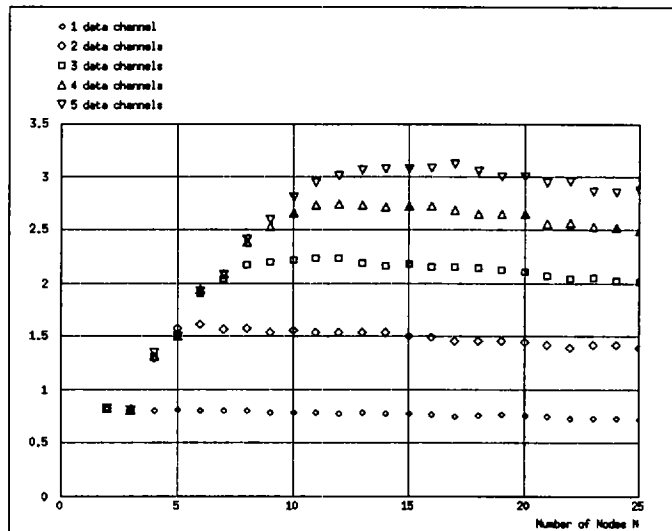


Figure 4. Throughput as a function of number of nodes and number of available channels for fixed network traffic  $G = 10.0$  (CSMA/CA control channel).

In Fig. 4, the throughput is plotted as a function of number of nodes for the fixed traffic  $G=10.0$ . In the single channel mode, the throughput decreases very slowly indicating that for a chosen traffic load and network size range, it always remains close to saturation, though overhead grows both due to the increased number of negotiations and larger slot size. When more channels become available to the network, a

decrease in throughput becomes more prominent due to the growing number of collisions on the control channel,

We also simulated networks utilizing pure TDMA and hybrid TDMA/CSMA on the control channel. As expected, the results for pure TDMA were worse than for CSMA/CA due to the larger delays introduced and smaller bandwidth utilization. In the case of hybrid TDMA/CSMA control channel access mechanism the throughput was very similar to the one achieved by CSMA/CA protocol.

Maximum throughput achievable for a specified load is an important measure of network performance. However, for the protocol to be practical, a number of other parameters should be investigated. Among these parameters are the end-to-end delay experienced by data packets during their transmission between channel access layers on the transmitter and receiver side and the packet loss or fraction of packets expired and discarded by the sender. Additionally, exponentially distributed interarrival times assumed above are not very realistic in tactical environments where diverse traffic sources and hierarchical organization of military units produce quite different traffic patterns.

To simulate our protocols in more realistic conditions we considered a network topology typical for modern infantry's company. Communicating nodes (total number: 22) were assigned to battalion, company, squad and platoon leaders. Digital voice, email, file transfer, GPS position reporting and tactical messaging were modeled as distinct traffic sources. Traffic priority, urgency and origin were taken into account. Digital voice exchanges were performed over connection-oriented links on data channels. Ten data channels were utilized.

	Absolute hourly traffic						
	Email	GPS	FTP	Tact Mesg	Data(total)	Voice	
Traffic (bytes)	253542.4	159974.4	257241.6	811724.8	1482483	23358889	
Throughput (bytes)	253107.2	147558.4	256640	735270.4	1392576	23340237	
% Success	99.82835	92.23876	99.78613	90.58124	93.93536	99.82101	
Delay (sec)	34.94	5.77	58.34	12.43	24.32	3.42	

**Table 1** Hourly traffic, throughput, percentage of success and delay for typical infantry company communication simulation. % of Success is defined as percentage of packets transmitted or percentage of voice calls established before the time-out at the sender.

Results presented in Table.1 indicate that distributed trunking protocol provides means to accommodate a significant amount of voice and data traffic typical for tactical communications and is characterized by small

delays and low blocking and loss probabilities (GPS and Tactical message expiration times were set very small due to their periodicity - thus, relatively smaller percentages of success).

## CONCLUSION

Channel access protocol proposed in this paper utilizes CSMA/CA, TDMA or hybrid TDMA/CSMA on a common access control channel to reserve a number of mutually orthogonal channels for data exchange. The orthogonality is provided both in frequency and time (allowing also a single channel mode of operation). The protocol is fully distributed. Fairness and manageability are maintained by dynamic tracking of network conditions at every node, and through the introduction of mini-slots and priorities. Good network efficiency both in the single and multi-channel modes of operation are demonstrated via OPNET simulations. Results are presented for overall throughput as a function of traffic, number of available channels and network size. It is shown that, for the networks of interest, protocol yields good trunking efficiency and that the throughput remains nearly constant when network size and load increase. Finally, OPNET was used to simulate realistic communications on the infantry's company level and it was shown that the protocol performs adequately in such scenario.

## REFERENCES

- [1] P. Karn, "MACA - a new channel access method for packet radio," Proc. of the 9th ARRL/CRRL Amateur Radio Computer Networking Conference, London, ON, Canada, p.134, Sept. 1990
- [2] D. Awduche, A. Ganz, "MAC protocol for wireless networks in tactical environments", Proc. of MILCOM'96, McLean, VA, pp. 923-927, Oct. 1996
- [3] K.Chen, "Medium access control of wireless LANs for mobile computing", *IEEE Network*, pp. 50-63, Sept. 1994
- [4] OPNET Modeling Manual, © 1989-1995 MIL 3, Inc.
- [5] K. Pahlavan and A. H. Lavesque, "Wireless Data Communications," *Proc. IEEE*, pp. 1398-1430, Sept. 1994.
- [6] D. Bertsekas and R. Gallager, *Data Networks*. Upper Saddle River, NJ: Prentice Hall, 1992.