

Military Communication Systems, Experience and Applications

Mikko Särelä

Laboratory for Theoretical Computer Science
Helsinki University of Technology
P.B. 5400, FIN-02015 HUT, Finland
mikko.sarela@hut.fi

Abstract

This paper presents use of Ad Hoc Networks in military organizations. It covers the most important things to remember when designing military networks and a short survey of Ad Hoc Networks history. In addition Mobility, Quality of Service and Communications Surveillance and Interference are studied. In military networks all or most parties are mobile and still networks may well consist of hundreds of thousands of nodes. This causes problems for the routing algorithms used within the network. In addition the communication should be hidden behind random noise to make it hard for the enemy to use information of the communications against the organization.

1 Introduction

There are a lot of situations, especially in the military, where timely and assured communication is both difficult and essential. Ordinary mobile communications, such as GSM, require the mobile node to be connected to a non-mobile wired station. In military applications there are many situations, where such infrastructure does not exist. When US special troops start an operation in Afghanistan, they do not

have the benefit of a communications infrastructure that commercial users enjoy in Western world. Similarly for a country like Finland, it is probable that communications infrastructure will be one of the first things destroyed, should a war begin.

In modern combat there is a tremendous need for timely communications. A soldier needs contact with his officer; a driver may need contact with headquarters for driving directions (city combat); a battleship or a carrier needs to communicate with other ships and friendly fighters and with head quarters at home.

The circumstances and requirements differ within the military. Battleships are mobile platforms themselves and a lot of communications takes place within the battleship. In contrast a soldier carrying a radio is also carrying a mobile node. Clearly there is a need for mobile networking infrastructure that is capable of self-organizing dynamically.

The common denominator for those needs is that usually no stationary infrastructure exists, or can handle the communications. A soldier who is working behind enemy lines cannot expect to have static infrastructure for communications. If it did exist, it would certainly be one of the first

things enemy would try to destroy. A battleship could not even have such infrastructure in the first place.

In addition to this most of the wireless bandwidth that exists has been licensed to commercial usage. Most of the free bandwidth resides above 100MHz. Frequencies that are that high propagate badly beyond line of sight (LOS). Military systems will have to be able to co-exist with existing commercial communications and thus will not be able to propagate much beyond LOS.

There is a need for networks that can route information through dynamically changing mobile infrastructure. Ordinary mobile communication systems, such as GSM assume that each node has a direct contact to a stationary gateway that has access to fairly stable communication infrastructure. In military systems users need access to network resources even when no base station is within its LOS. In this situation it is up to other mobile nodes to route the packet to its destination despite quickly possibly quickly changing conditions.

One of the solutions to the problem of highly mobile and dynamic networks is to use Ad Hoc Networks. The idea for them arose in US Department of Defense during 1970s. It has also gained popularity in commercial usage in recent years.

2 Design Parameters

There are some things in which MANETs have great differences to their counterparts. The following paragraphs give an idea what kind of problems must be considered when design-

ing MANETs, especially for military use [1].

Network size is most often used for meaning the amount of nodes in a network. In MANETs it can also be used to represent the size of the geographical area it covers. The size of military Ad Hoc networks is often far greater than the size of its commercial counter parts both in the number of nodes connected and size of the geographical area it covers.

Connectivity means a plethora of things. It can mean the capability of nodes to communicate with each other - directly or indirectly. Or it can be used to signal the amount of nodes directly connected to a node, and whether these connections are bi-directional or unidirectional. It can also mean the capacity of a connection between nodes. In addition the different communication modes that military has for different operations are closely linked to it. Especially EMCON mode, in which a party must keep radio silence, but should be able to receive critical data, is a big challenge for Ad Hoc networking.

Network Topology describes the way network is organized. In MANETs this includes the behavior of nodes (e.g. how and how fast nodes move in MANET). Military networks may change from relatively stable environment to very unstable environment suddenly. For example enemy artillery may destroy some of the mobile nodes, or infantry may scatter around inside a city. In contrast most commercial Ad Hoc networks operate under relatively stable environment, and where short communication break-ups are usually not fatal.

User Traffic describes the properties of the traffic generated by the users. Does the traffic consist of short bursty transmissions, or long transmissions with unchanging data rate? Is the traffic sensitive to loss of packets, or does it require strict delay bounds? Military communication covers a wide spectrum of different messages. Some are time critical, such as requests for air support, or urgent pick up and some have relatively low priority. Most of them have strict requirement for security - that no other than recipient and sender may know what packet contained, and no one may modify it. In addition it should be as difficult as possible for enemy to stop a packet from reaching its destination - even if it has invaded a node inside the Ad Hoc network.

Operational environment means the terrain in which the network operates. Main interest is in things that may prevent line of sight between mobile nodes (e.g. mountains, or buildings in a city). Military Ad Hoc networks should be prepared for active jamming attempts from the enemy. They will also be used under a big variety of environments - from urban, to jungle and mountains to sea and air.

Energy MANETs have no fixed base stations that provide connectivity - all, or most mobile nodes will be involved with routing packets for other actors. Mobile devices are usually small and have scarce energy resources, such as batteries. Thus it is important to design MANETs in a way that minimizes energy consumption.

Regulatory Most of the spectrum that is on the networking wish list is already sold off for commercial operators for different purposes (GSM, TV, etc).

The remaining bandwidth can be found above 100MHz and thus capability of connecting beyond LOS is unlikely.

Performance metrics The designer must understand which requirements are the most important for the users of the system. Only then can the correct performance metrics be chosen - some examples of relevant performance metrics are throughput, delay, protocol overhead, and error rate.

Cost is an important aspect of MANETs if they are going to be taken into use.

Incomplete trust In commercial systems, one can safely assume that trust to a mobile routing node is either 1 or 0. If network operator becomes untrustworthy, word will soon spread and everyone will know it. In military systems the routing nodes may sometimes be untrustworthy, because of enemy jamming, or because they have moved into territory, where they have bad signal to next hop - or they might have been high jacked by the enemy, who has a much resources and incentive to disrupt communications.

One important thing to note is that one cannot separate the design of different layers (as in OSI model) easily, because MANETs are working on the limits of wireless networking. Thus one cannot build an efficient design for transport layer, without considering the way the lower layers operate.

As can be seen there are a number of different problems related to the military perspective of Ad Hoc Networking. In most cases military needs Ad Hoc Networks that work under more diverse conditions, better and more efficiently than civilian world.

3 History

In 1970s packet, when packet switching had proven itself, US military took an interest in putting that into battlefield use. Different branches had their own researches and programs to put packet switching into mobile use in army, navy and air forces. This chapter covers different programs and attempts to increase the mobility of soldiers in different environments.

3.1 DARPA Packet Radio Network

DARPA funded a Packet Radio Network Program, which used broadcast radios for relaying data over multi hop mobile network. Its purpose was to provide for sharing bandwidth and for operation under dynamic conditions [2]. At that time the required radios were heavy and required much energy and had low processing capability. Packet Radio Networks and Ad Hoc Networks are often considered synonyms.

The problems of Packet Radio Networks were addressed in the second generation of Ad Hoc Networks named Survivable Radio Networks during the 80's. One of the main achievements was a small low cost lower power radio that supports sophisticated packet radio protocols [3].

3.2 Army

Army took into packet radio networks late 80's. They made their own version by combining their existing circuit- or broadcast oriented networks with packet oriented routing. The outcome of this development was Single Channel Ground-Airborne Radio System (SINCGARS). It is currently used as

the standard operations radio in the US Army. [4]

3.3 Tactical Internet

In the 1990s US Army developed Tactical Internet (TI), which consists of thousands of mobile nodes. It includes vehicular and man packed radios that act as mobile, wireless and multihop packet radio network running modified commercial Internet protocols. An experiment of that size was needed, in order to test the operability of Ad Hoc Networks in big systems, which Army needs for its operations.

The TI uses open commercial protocols as a basis, because DoD has mandated them as a basis of TI and future communications systems [5]. Thus military can get the benefits of fast paced commercial development of networking - and gain in the interoperability of communications in different branches. The TI uses Open Shortest Path First (OSPF) routing protocol, which is designed for wired and fairly stable networks. It uses periodic Hello messages to find out about its neighbors. As a result the settling times for the network are long [6]. The experiment still demonstrated that the basic requirements for Military Ad Hoc Networks could be satisfied.

3.4 Navy

The Navy has developed a packet radio network for use at sea [7]. It faces a set of its own problems, because often ships that need to communicate are not within line of sight and they are all mobile platforms.

The developed system, named intra-taskforce (ITF) network, uses

high frequency spectrum for connectivity, and frequency hopping against jamming attempts. It is able to provide multi hop connectivity to those nodes not within its own reach.

Navy packet radio also brings another important fact to the front - a mobile node is not necessarily a small device carried around, but may consist of a big network of users on mobile platform. That means that the mobile node operates as a gateway to its own network, while trying to maintain connection to the outside world.

3.5 Air Force

The U.S Air Force has explored the possibility of increasing the connectivity of ground troops through base network provided by network of aircraft. The aircraft above would work as a network, which give connectivity to in places where terrain limits the communications otherwise. These concepts were proven valid in the Strategic Command and Control Communications (C3) experiment. [8]

3.6 Extending Littoral Battlespace (ELB)

The purpose of ELB project was to give Marines communications with the ships using aerial relay. Another important aspect was to make it cheap by using existing commercial products. It used commercial Wave LAN (WLAN) technology from Lucent for links between Marines and aerial relays.

The current version required several modifications to the WLAN technology, including external power amplifier to connect to the aerial relays. Thus it did not achieve the cost effectiveness goals set to it at this point. Also the

ability of the nodes to roam freely in the network was limited. They plan to solve these problems in the next phase of ELB. [9]

3.7 GloMo

DARPA initiated Global Mobile (GloMo) Information Systems program in 1994 to take advantage of rapidly developing Internet infrastructure and technologies. Its aim was to enable same benefits of connectivity that Internet provides to mobile and wireless users anytime anywhere [10]. Specifically GloMo had following five thrusts [11]

1. Infrastructure design, such as computer-aided design tools
2. Untethered nodes that provide low-cost, low-power wireless access with sufficient processing power to support sophisticated network management algorithms
3. Network Protocols and algorithms with robust architectures that can be rapidly deployed
4. End-to-end networking in heterogeneous environments
5. Mobile applications that adapt to varying network connectivity and quality of service (QoS)

The GloMo program has tried several different approaches to networking inside MANET and between MANET and Internet. Two of these approaches are the Wireless Internet Gateways (WINGs) [12] and the Multimedia Mobile Wireless Network (MMWN) [13].

WINGS shows a way for a MANET to be connected to the Internet so that nodes inside the MANET use IP and are visible in Internet - i.e. the MANET is not an opaque network, but visible part of the Internet. WINGS uses flat peer-to-peer network architecture.

MMWN, on the other hand, is based on hierarchical network architecture, where nodes are arranged into clusters [14]. It uses location management, clustering techniques and virtual circuit setup and repair to provide distributed, real-time multimedia applications in a MANET.

4 Open Research Issues

There are a number of open research issues before MANETs fulfill their promise of connectivity in military applications. This chapter is not meant as conclusive report on those issues, but an introduction on most important issues still open.

4.1 Mobility

In military systems most nodes are mobile. This means that data should be transmitted into right receiver wherever he is (and is going to) when the data is sent. The military networks are also big - a military network, possibly fully Ad Hoc, could easily consist of hundreds of thousands of nodes in a large geographical area. This causes great demands for the routing algorithms used.

Military networks also operate under especially hostile environment. It is expected that many of the nodes in the network will be destroyed during operation. In contrast to commercial networks, where problem with a routing node is uncommon happenstance, the difference is great indeed.

The military network should be able to operate even when a big portion of the network has been destroyed - even when the enemy targets the most important nodes of the network. For

that reason bottlenecks are even more dangerous for military networks than for civilian ones.

Routing packets to a mobile node is a difficult problem. One way to solve it is to use Mobile IP [15]. A mobile node (MN) has a Home Agent (HA), which acts as its permanent address. The HA then forwards packets addressed to mobile node to its current location. When mobile node moves from one access point to another, it simply announces its new location to HA.

Unfortunately this approach causes unnecessary delays, consumes bandwidth, and takes up much of network resources. When considering that most traffic in military networks is directed to nodes geographically close to them, it is easy to see that routing everything through HA is folly. It is also a prime candidate to be the critical node destroyed by the enemy.

For these reasons it is preferable for a mobile node to announce its current address to its communication partners and thus allow the route to be optimized. This can be done using a route optimization protocol proposed by Perkins. [16]

Unfortunately the HA usually resides in mobile nodes home network behind firewall. That means if two mobile nodes are communicating with each other, then route optimization causes more trouble than it is worth. [?]

4.2 Quality of Service

Quality of service is a widely used term when speaking about IP-based networks. The United Nations Consultative Committee for International Telephony and Telegraphy (CCITT) Recommendation E.800 has defined QoS

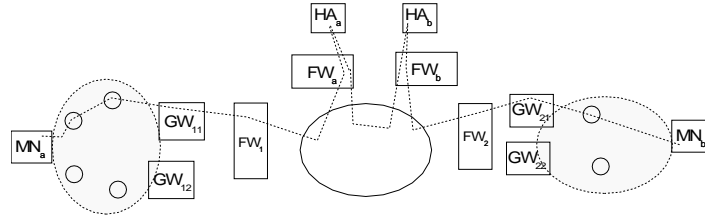


Fig. 1. Two mobile nodes communicating over fixed network

as: “The collective effect of service performance which determines the degree of satisfaction of a user of the service”.

For military networks Quality of Service means that important messages are delivered timely and unaltered into their destination.

For a wide variety of messages guaranteed quality of service is critical - especially so for real-time audio and video. Several methods have been suggested for assuring guaranteed bandwidth in Ad Hoc Networks [18] [19] [20]. This chapter introduces some of them.

There are three basic ways of providing QoS for a network. $\hat{\cup}$ Over provisioning $\hat{\cup}$ Reservation-based engineering $\hat{\cup}$ Reservation-less engineering

Over provisioning means that you add bandwidth until everyone is happy. It is a nice and easy solution, but unfortunately impossible in MANETs, since total bandwidth is limited and cannot be easily increased.

In reservation-based engineering each application in network is promised certain bandwidth according to its request and network policy. An example of this type of QoS is IntServ/RSVP. Typically these protocols require much processing power and memory from the intermediary routing.

An interesting version of reservation-based engineering comes from Candolin, Kari, and Hietalahti [21]. A mobile node (MN) is connected to an access point (AP) (dedicated to bring access to MNs), which is then connected to either another AP or to the gateway (GW). An example of such a network can be seen in Figure 2.

The basic idea is that the GW has certain amount of bandwidth that it can apportion between the AP’s directly connected to it. The AP’s authenticate themselves with the gateway and receive some amount of bandwidth. The AP is then free to redistribute that bandwidth to those APs and MNs that are directly connected to it. For example AP 3 has received 300Kbps from GW and has apportioned 200Kbps to AP6. It can still apportion 100Kbps to another applicant, or keep it for its own communications.

When an MN joins the network it first authenticates itself to the APs it can directly connect to and to GW and then requests for bandwidth. Both the AP and the GW must approve the request through which the traffic must go.

Thus the GW only needs to know how much bandwidth it has apportioned to its direct neighbors and how

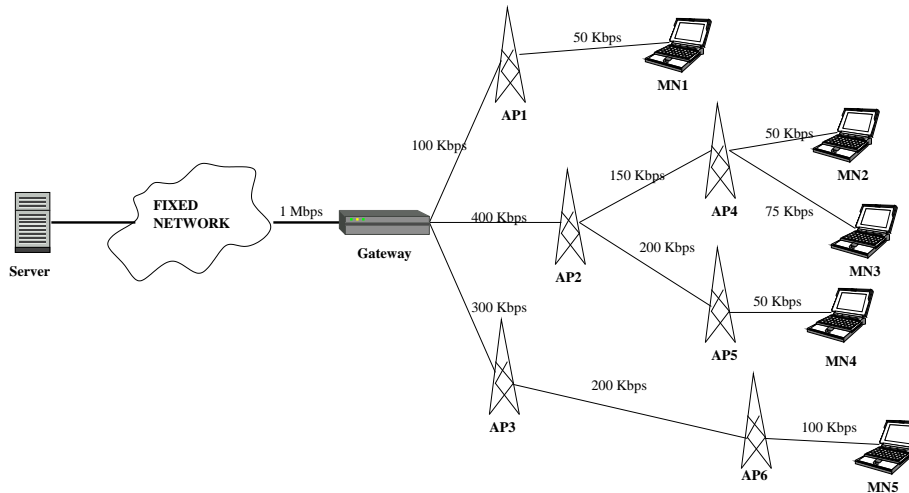


Fig. 2. Nodes and their given capacities

much traffic has been apportioned to each MN. Similarly each AP only needs to know how much bandwidth it has been apportioned (from which APs) and how much bandwidth it has apportioned to other APs and MNs. This reduces the amount of processing overhead required for keeping tabs on who is allowed to send what, but increases it on the other hand, because each packet that is sent must be authenticated by the sender - even the APs just relaying the message must authenticate that the message originated from them.

In reservation-less engineering data is classified into different classes depending on the request of the application and the network policy. These classes may be e.g. 'best-effort' or 'assured'. An example of QoS working in this way is DiffServ.

QoS for Ad Hoc Networks is currently a hot research topic. Many proposals for handling it have been made and much research is still needed for it to be ready for development.

4.3 Communication surveillance and interference

In military operations the enemy is usually monitoring the network traffic for any useful information. And there is a lot to learn, even from encrypted communications. Just from analyzing the traffic, one may be able to locate bottlenecks and other weak points of the network infrastructure for later destruction.

For example the head quarters of a brigade use a lot of bandwidth within the head quarters, and quite much with their battalions. Much more than troops in the field do. The wireless communication signature is different for some critical components of an army.

Similarly the amount of communication goes way up in the front lines, when they are preparing to move into the next wave of an attack. A good rule of thumb is that any big change to the current conditions will cause a surge of communications.

The enemy must not be able to use the presence or absence of communication to determine the location of critical nodes (or troops) or to anticipate a coming operation. Because of that all, or most nodes should keep up a level of random background noise to hide the presence or absence of real communications. This causes problems with battery lifetimes for those devices that are carried around, or are scattered around in the field.

If the trails are uncovered it will also reveal information about the places where transmissions are moved on to the wired network and even about the location of head quarters or scouts moving inside enemy territory.

Even when most things are covered, mere transmissions tell the approximate position of the troops (say a brigade) and also tell the wavelength area they are using. The enemy can then use the latter to jam wireless communications in a critical moment.

5 Conclusions

The field of military communications is full of challenging problems. These problems include a highly dynamic environment, where useful nodes are quite mobile and can easily be destroyed by the enemy. In addition the enemy uses much resources to find out the weak spots of the communications system to shut it down, or to hit the vital organs of the organization.

The use of Ad Hoc Networks in military systems is not one big problem, but a big host of small problems to be solved. These include routing packets to its destination in a big dynamic and mobile network, possibly using positioning data as a help; providing qual-

ity of service for important transmissions; avoiding bottlenecks in the network; hiding the important nodes and units from the enemy; and be resistant to jamming attempts.

The solutions to many of the partial problems can be found already today. The real problem lies in combining all those techniques into one whole system that is resistant to an enemy that is capable and willing to use resources to break it down.

Ad Hoc Networks have the capability of realizing a whole new age for modern warrior - a battlefield, where all relevant and only relevant information is always at hand at the time it is needed. A fight where each soldier can be as efficiently as possible steered toward the maximum effect against enemy.

References

1. Freebersyser, James; Leiner, Berry: A DoD Perspective on Mobile Ad Hoc Networks, Ad Hoc Networking, Addison Wesley, 2001, ISBN 0-201-30976-9
2. Kahn, R. Advances in Packet Radio Technology. Proceedings of the IEEE 66:1468-1496, November 1978
3. Fifer, W; Bruno, F: The Low-Cost Packet Radio. Proceedings of the IEEE 75 (1): 33-42, January 1987
4. Sass, P: Communications Networks for the Force XXI Digitized Battlefield. ACM/Baltzer Mobile Networks and Applications Journal (Special Issue, Mobile Ad Hoc Networking) 4, October 1999
5. Joint Technical Architecture, Version 5.0, September 1997
6. Strater, J; Wollman, B: OSPF Modeling and Test Results and Recommendations, Mitre technical report 96W0000017, Xerox Office Products Division, March 1996

7. Ephremides, A; Wieselthier, J; Baker, D: A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling, Proceedings of the IEEE 75 (1): 56-73, January 1987
8. Frankel, M: Tactical C3 for the Ground Forces, Telecommunications and Processing for Military Command and Control: An Architecture for the 21st Century, AFCEA International Press, Washington, DC, 1986
9. Althouse, E: Extending the Littoral Battlespace (ELB). Advanced Concept Technology Demonstration (ACTD), NATO Information Systems Technology Panel Symposium on Tactical Mobile Communications, June 1999
10. Ruth, R: Global Mobile Information Systems Program Overview, July 1998
11. Leiner, B; Ruth, R; Sastry, A: Goals and Challenges of the DARPA GloMo Program. IEEE Personal Communications, 34-43 December 1996
12. Garcia-Luna-Aceves, J: Wireless Internet Gateways (WINGS). In Proceedings of the IEEE Military Communications Conference (MILCOM '97), November 1997
- 13.
14. Steenstrup, M: Cluster Based Networks, Ad Hoc Networking, Addison Wesley, 2001, ISBN 0-201-30976-9
15. Perkins, C: IP Mobility Support for IPv4, RFC 3220, IETF, <http://www.ietf.org/rfc/rfc3220.txt>
16. Perkins, C: Route Optimization in Mobile IP, Internet draft, IETF, <http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-11.txt>
17. Candolin, C; Kari, H: Complexity of route optimization and mobility management, 2nd Swedish Workshop on Wireless Ad-Hoc Networks, 2002
18. Lin, C; Liu, J: QoS Routing in Ad Hoc Wireless networks, IEEE J. Sel. Areas Commun., vol. 17 (8), p. 1426, August 1999., <http://www.eecs.uc.edu/~guptanis/research/papers/QoS/QoSAdHoC.LinCR.pdf>
19. Royer, E; Perkins, C: Quality of Service for Ad Hoc On Demand Distance Vector (AODV) Routing, IETF Internet Draft, draft-ietf-manet-aodvqos-00.txt, July 2000 (Work in Progress)
20. Sivakumar, R; Sinha, O; Bharghavan, V: CEDAR: a Core-Extraction Distributed Ad Hoc Routing Algorithm, IEEE Journal on Selected Areas in Communications, Special Issue on Ad Hoc Networks, Vol 17, No8, 1999
21. Candolin, C; Kari, H; Hietalahti, M: Providing quality of service in wireless ad hoc networks, 2nd Swedish Workshop on Wireless Ad-Hoc Networks, 2002