Intelligent Tactical IP Router

Mariann Hauge and Svein Haavik

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

7 December 2009

FFI-rapport 2009/01708

1088

P: ISBN 978-82-464-1672-4
E: ISBN 978-82-464.1673-1

Keywords

nettverksbasert forsvar

taktisk kommunikasjonsnett

mobilt ad hoc nett

tjenestekvalitet

internett protokoll (IP)

ruting

Approved by

Vivianne Jodalen	Project Manager
Vidar S. Andersen	Director

English summary

In connection with the introduction of a Network Based Defence (derived from the original Network Centric Warfare term) we envision a definite requirement for a ubiquitous communications network. This network will be based on the Internet Protocol (IP), which today has become the standard also for civilian systems. Differentiated service quality and user priority to prioritize critical traffic flows must also be supported. In a tactical context we see the need for different types of transport networks, primarily radio-based. Assorted radio systems operating in different frequency ranges have distinct, complementary properties. Some radio systems have a long range but low capacity, while others have high capacity but short range. In addition, there are systems relying on an infrastructure, like cellular telephony.

Often, several different radio systems have a connection to the same destination, or several multi-hop routing paths exist from source to destination via many different radio systems. Today there are no good solutions for interconnection of such radio systems in an ad hoc network with often high mobility. Similarly, there are no good solutions to support service quality and priority in such networks. FFI were asked by TRADOK (Norwegian Army Transformation and Doctrine Command) to specify and procure a tactical IP router (termed the Intelligent Tactical IP Router (ITR)) for experimentation with routing and QoS mechanisms for future mobile tactical networks.

This report describes the background and requirement for such a project. It gives a detailed description of the two implemented solutions, in addition to experiences from field testing at Rena Army Camp. The SW platforms are described with the functionality available in Q4 2008. Further development and testing performed in 2009 are not described here. Finally, we outline the need for further development, experimentation/testing and research in this area before such a component is mature for implementation in the Armed Forces.

Sammendrag

I forbindelse med innføringen av et Nettverksbasert Forsvar (NBF) ser man klart behovet for et allestedsnærværende kommunikasjonsnettverk. Dette nettet vil være basert på internettprotokollen (IP) som i dag er blitt standarden også i sivile systemer. Et slikt nettverk må også støtte differensiert tjenestekvalitet og prioritet slik at viktig trafikk får forkjørsrett i nettverket. I taktisk sammenheng ser vi at det er behov for flere ulike sambandsmidler, og da først og fremst radiobaserte. Ulike systemer og frekvensområder har ulike egenskaper som utfyller hverandre. Noen radiosystemer har god rekkevidde men lav kapasitet, mens andre har høyere kapasitet men kortere rekkevidde. Det finnes også systemer basert på en infrastruktur slik som for mobiltelefon.

I mange tilfeller har flere ulike radiosystemer forbindelse til samme destinasjon, eller det finnes flere veier fra sender til mottaker i mange hopp via mange forskjellige radiosystemer. Det eksisterer i dag ingen løsninger for å knytte slike radiosystemer sammen på en god måte i et ad hoc nett med til dels høy mobilitet. Det er heller ingen gode løsninger for å støtte tjenestekvalitet og prioritet i et slikt nettverk. Etter oppdrag fra Våpenskolen for Hærens Samband/TRADOK tok FFI på seg arbeidet med å spesifisere og anskaffe en framtidsrettet taktisk IP-ruter (kalt Intelligent Taktisk IP-Ruter (ITR)) for å eksperimenter med ruting og tjenestekvalitet i mobile taktiske nettverk.

Denne rapporten beskriver bakgrunnen og behovet for et slikt prosjekt. Den gir en detaljert beskrivelse av de to alternative løsningene som er tatt fram, samt erfaringer fra felttest av disse i Regionfelt Østlandet. Systemene er beskrevet med den funksjonalitet de hadde i Q4 2008. Videreutvikling og tester i 2009 er ikke beskrevet her. Til sist skisseres behovet for videre utvikling, eksperimentering/testing og forskning på dette feltet før en slik enhet ansees modent nok for implementering i Forsvaret.

Contents

1 Introduction

In both national and international tactical operations, there is an increasing demand for electronic information, much of which is real-time data that is wanted anytime anywhere. This demand for information is expected to increase even more in future operations. New ways of operating requires information exchange between units that traditionally did not have much interaction. Multinational operations also require efficient information exchange between coalition partners. Thus new operation types and methods need a flexible network infrastructure that is not available in the Norwegian Armed Forces today. To provide high capacity, availability and flexibility in a tactical network, many different transmission media can be used to link the various units and command posts together. Because of the agile movement of the units, these transmission means are normally radio-based, with different data rates and protection abilities, and highly variable availability. The transmission means used in tactical networks have large variations in capabilities and fluctuating availability, thus it is challenging to administer, admit, and route the traffic flows in these networks.

Among others, the Norwegian Army sees the need for a more interoperable and flexible tactical mobile network architecture than the one available today. Therefore The Norwegian Army Transformation and Doctrine Command, Signals Branch proposed to collaborate with the Norwegian Defence Research Establishment (FFI) in a project. The project was to work with industry partners to develop a tactical router demonstrator for flexible dynamic tactical mobile networking. The outcome of this activity is described in this report. The resulting router demonstrators attempt to make intelligent routing decisions in the tactical network, thus the routers are named the Intelligent Tactical IP Routers.

Section 2 of this report presents the background for the project and explains the setting in which we think that the Intelligent Tactical IP Router may serve an important purpose. Section 3 gives an introduction to some of the main networking challenges associated with the wireless mobile tactical domain. Section 4 describes the Intelligent Tactical IP Router and specifies its initial required functionality. A detailed description of the two alternative implementations is given. In section 5 experiences from the initial field tests at Rena Army Camp, of the two router alternatives are given. Section 6 concludes with the need for further work in this area.

2 Background

2.1 Network Centric Operations – Network Enabled Capability

Network Centric Operations was a term coined in the early 2000s for describing a new mode of military operations. This is a comprehensive topic that is not the focus of this report; however it is important to show how the new operational modes can put tough requirements on the communication infrastructure.

Norway as well as NATO and many other countries are making a transition from Platform Centric Operations towards more Network Centric Operations. This transition will put new challenging demands on the communications network architectures, especially in the tactical domain.

An informal group (NBF Think tank) lead by FOHK/J7/CDE was established in October 2004 to discuss the implications of Network Centric Operations in the Norwegian Armed Forces. In [16] some thoughts and high level ambitions for Network Centric Operations from this group are presented. The ambitions stated in this document require a very flexible network infrastructure where all end services ideally shall be available to all cleared users anywhere independent on type of operation and home platform. Efficient data communication towards civilian actors should also be available. Comparable studies in both the USA and NATO have reached similar conclusions.

One commonly agreed mean that can enable a flexible network infrastructure is to make the transition from isolated Combat Net Radio (CNR) networks (that are not easily interconnected with other networks) towards a common network architecture based on the Internet Protocol (IP) protocol suite. Traditional CNR networks are designed to operate as a stand-alone isolated network. The radios usually provide all the functionality on all network layers needed to communicate efficiently with identical CNRs. The protocols used on the different layers are typically non-standard protocols tuned for the specific CNR. In order for a cooperating unit to join the CNR network, this unit must be equipped with the identical CNRs and radio parameters as the other unit. To enable a more flexible network infrastructure, standardised protocols that all network devices support must be used at some level in the network protocol stack. Standardisation with IP at the network layer that allows non-standard device specific protocols at lower layers is one popular solution. If the mentioned CNR network would support IP at the network layer, and IP-based common protocols at higher layers, then this network could be configured to communicate with other IP-based networks via a router/gateway.

The FFI-Report [28] argues for the IP-based network architecture and describes network mechanisms that will be needed in an IP-based network architecture for network centric warfare operations. The FFI-Report [20] studies the migration path needed to convert the current military network to an IP-based network. In [6] NATO suggests a similar approach to ready a coalition network for future Network Centric Operations. In [22] the authors suggest how the efficiency of military operations can be improved by allowing more sharing of electronic data and extended interoperability between platforms and units. Several specific actions for improved interoperability are suggested based on the material available to the Norwegian Armed Forces in 2012. This report also emphasizes that the extended operational collaboration requires a common flexible communication network that is not available in the Norwegian Armed Forces today.

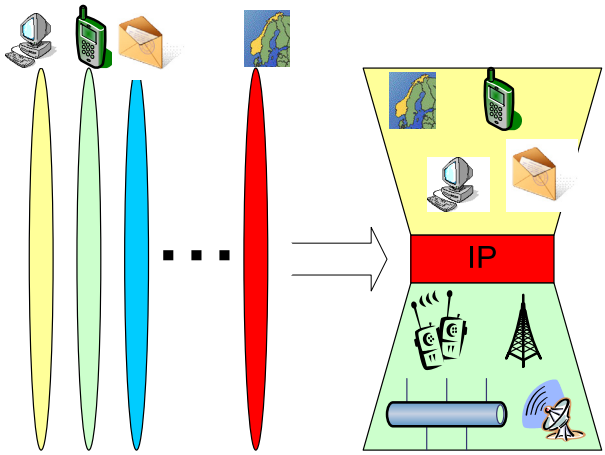

Figure 2.1 This figure shows the transition from platform specific- and application specific-networks towards a common network infrastructure based on the IP protocol suite.

The main goal for the network architecture described in [28] is to achieve a flexible network design with a common network platform with well defined communication services. This can be used to transport all required end user services anywhere and on any underlying infrastructure (e.g., optical fibre, cable and different wireless technologies). As shown in Figure 2.1, the IP protocol suite has been chosen as the mean to provide a common interface for the end user application protocols to the device specific lower protocol layers.

The common network architecture for the Norwegian Armed Forces proposed in [28] is structured in a three-level network topology (see Figure 2.2):

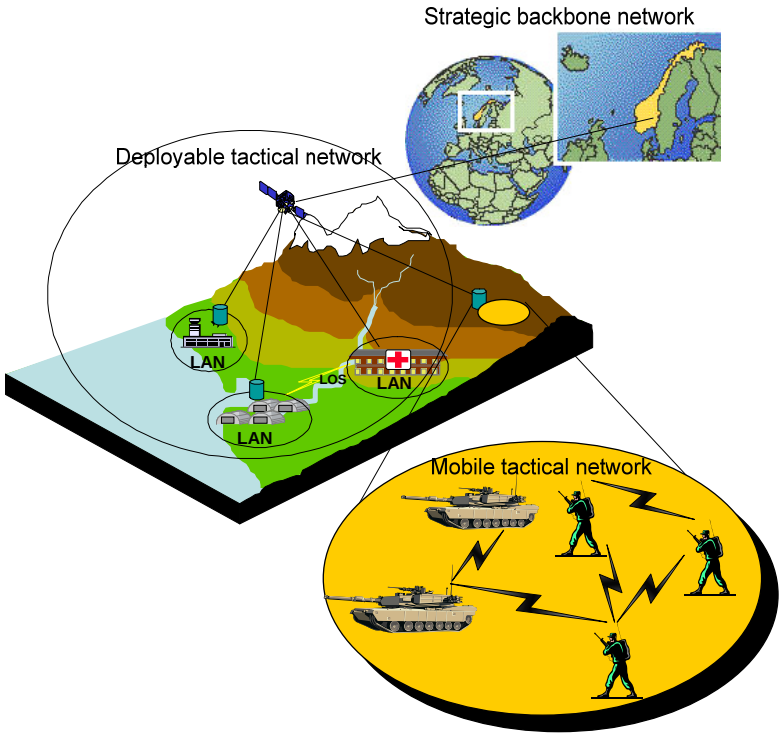

Figure 2.2 This figure illustrates the three-level network topology for the military network architecture.

- On top lies the strategic backbone network with fixed infrastructure.
- The second layer is a deployable tactical network with primarily stationary network infrastructure and one or more long haul access connections to the strategic network.
- The third layer is the mobile tactical network with a high degree of mobility, low data rate and unpredictable operational conditions. It is connected to the deployable backbone network by radio links (e.g., SATCOM, HF or VHF).

The two mentioned FFI reports [20] and [28] discuss the network design of both the strategic-, deployable- and mobile- network levels. However, recommendations in the two reports are mainly given for the strategic part of the network and to some extent, for the deployable tactical domain. The mobile tactical domain is left for future study since many of the required network mechanisms for such networks are not yet mature. In this report we take a closer look at some of the challenges associated with the design of a flexible mobile tactical network. We describe and suggest some mechanisms needed in a network architecture for the mobile tactical networks.

2.2 The Mobile Tactical Network Domain

We see the need to accelerate the work to establish a flexible communication infrastructure in the mobile tactical network. The future forces must be very flexible, and be able to quickly adapt from an ongoing operation to a new one that might be operationally quite different. An efficient, easily configured communications infrastructure is a prerequisite for this. In addition to increased flexibility, new application types are needed in the tactical mobile network (e.g., Situational Awareness (SA) and sensor data), and it is expected that even more data are required in the mobile domain in the future. Thus the communication network must be flexible, have a high capacity and be able to support a variety of data types. The current wireless infrastructure is mainly used for push-to-talk voice traffic and is not able to efficiently support IP data traffic (e.g. Command and Control Information) to mobile units. It is also very difficult to expand the existing (VHF) network with additional wireless capabilities that are not compatible with the VHF network on the physical layer.

To provide a reliable network for different types of operation in varying terrains, the tactical mobile network infrastructure must consist of many wireless networks with different transmission technologies, e.g. long range communication for reach back connections and a higher data rate network for local communication. Robust communication for highly mobile nodes is a requirement. A single transmission technology, e.g. a VHF network, will not be able to support all communication types and data rate requirements. Multiple transmission technologies and routing paths can also improve the network reliability during e.g. jamming attempts.

As new application types are introduced to the mobile network, the network must provide better capacity (higher data rates). Ideally, every soldier in combat should be able to connect to the mobile network. Norwegian military procurement projects for combat equipment often state requirements for robust, high data rate, flexible mobile communication (e.g., SA-data for the squad and distribution of a wide range of sensor data on all command levels). Designing a flexible, highly available, high capacity tactical mobile network is a challenging task.

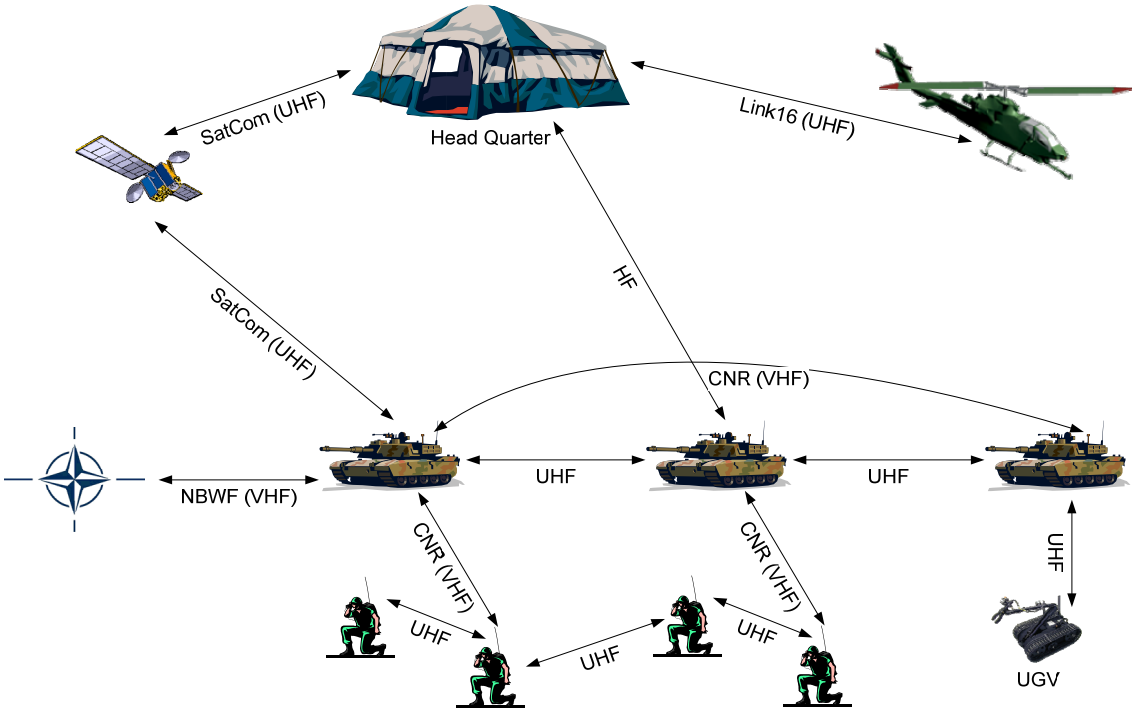

Figure 2.3 The figure illustrates different radio network types that might be used in mobile tactical networks.

The heterogeneous wireless network in Figure 2.3 might for example represent a future platoon network with several connections to a HQ and the deployable network infrastructure as well as access to data from supporting units and coalition partners. In this network all radio types that are available to the unit is used to establish a large common network that is interconnected with the IP protocol suite and thus IP routers on all nodes. As an example, this design allows the platoon leader to automatically utilize radio resources on other vehicles than his own to communicate with the HQ. It is desirable that the heterogeneity of the different radio types is hidden from the users of the network.

We envision the need for an Intelligent Tactical IP Router to make automatic routing decisions in the complex common radio network. This router is a likely component of a dynamic heterogeneous wireless network in a first step towards a Network Enabled Capability. The router should be integrated with the different platforms (e.g., squad leader, combat vehicles, tactical headquarters), and be responsible for automatic and efficient interconnection of the available wireless networks. The Intelligent Tactical IP Router should support prioritization of operation critical traffic, identify the capacity of underlying radio links and take advantage of parallel paths in the heterogeneous network to efficiently exploit all bandwidth resources. The router should also allow for easy incorporation of additional wireless networks. The router may also need to support information security mechanisms to handle confidentiality, integrity and availability, however, information security has not been the focus of the first versions of the router. The Intelligent Tactical IP Router is described in detail in section 4.

Throughout much of this report we use the Army as an example. However, the router is intended to improve tactical networking also for the Navy, the Air Force, the Civil defence and towards Non-Governmental Organizations (e.g., the International Red Cross and Red Crescent). Compatible networking mechanisms in these different disciplines will inevitably also improve interoperability between the different units.

3 Networking Challenges

In this section with the Intelligent Tactical IP Router as the focus, we take a closer look at some of the basic challenges associated with networking in mobile tactical wireless networks:

- Unicast routing
- Multicast routing
- QoS architecture

Network and resource management, network protection and data security are clearly also basic networking elements; however these will not be discussed here. For more information about the protection and security challenges for advanced networking take a look at [18] and [45]. For network security challenges specific for tactical mobile networking, take a look at the outcomes of the GOSIKT (P1070) project at FFI.

The mobile tactical network will be a typical Mobile Ad Hoc Network (MANET) [14]. A MANET is a multi-hop wireless data network. It is a self-configuring network of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily. The network's wireless topology may therefore change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or it may be connected to a backbone, or the Internet.

The three networking subjects (unicast routing, multicast routing and QoS architecture) addressed below are mainly discussed in the context of tactical MANETs. Clearly the mechanism chosen for this domain must interact efficiently with the deployable tactical network, and the strategic backbone network to provide efficient end-to-end services on network paths through any combination of these networks. Efficient and robust connection of MANETs to other networks (also neighbouring MANETs) is also a challenge that has not been well studied. Since the basic network functions for stand alone MANET operation are yet not mature, we choose to focus mainly on these functions in this report, and leave the extra complexity associated with efficient interconnection of the MANET protocols and architecture for later studies.

3.1 Unicast Routing

A consequence of the characteristics of a MANET (e.g., low data rate (compared to fixed network data rates), high mobility, varying channel conditions) is that a routing protocol for such networks needs to handle other challenges than routing protocols for fixed networks. A MANET routing protocol should consume little network resources and at the same time handle rapid route changes

due to node mobility and fluctuating wireless channel conditions. The main focus in MANET routing design has been to find efficient ways to convey routing information and at the same time to make the protocol robust for mismatching topology information. Routing information takes some time to propagate throughout the network, thus the rapid changes in network topology often result in routing information inconsistency between the nodes. Finally, it is challenging to find the correct trade-off between the amount of signalling traffic and the accuracy of the routers' view of the current network topology.

As of today there is no standard for routing in MANETs. Several experimental RFCs exist in the Internet Engineering Task Force (IETF) of which OLSR (Optimized Link State Routing) [12], a wireless extension to OSPF [37] and AODV (Ad hoc On-demand Distance Vector) [38] are the most popular routing protocols. These represent two different classes for routing protocols, the *proactive* type and the *reactive* type. In proactive routing all routers in the network continuously perform routing signalling to maintain a picture of the current network topology. All routers continuously calculate the best route to all subnetworks or all end terminals in the network. In reactive routing, the routers do not calculate any route in the network until a source requests to send data to a destination. When this happens, the router initiates a signalling session to find a route to forward the data from source to destination. Thus in the reactive case, there is no routing activity in the network unless there is traffic in the network. In networks with few, and typically long lasting dataflows, the reactive routing protocols are beneficial. Reactive routing inevitably introduces some delay from the route is requested until the path is found. In networks with much traffic, and short-lived traffic flows, or where short delay is important, proactive routing is beneficial. Proactive routing is also beneficial from a network resource management view since the overhead generated by proactive protocols are more predictable than the overhead from reactive protocols.

There are also a group of protocols that combine proactive and reactive routing (e.g., [42]). These assume that most traffic in the network is local, thus proactive routing is used locally, and reactive routing is used in the infrequent cases where a source wants to talk to a destination outside the local network area.

There is ongoing work in the MANET IETF working group to standardize one reactive protocol and one proactive protocol. Dynamic MANET On-demand (DYMO) Routing Protocol [10] represents the latest for the reactive work, and OLSR version 2 [11] the latest for the proactive work. In addition to these two proposals from the MANET IETF working group, there is ongoing work in the Open Shortest Path First (OSPF) IETF working group to standardize an OSPF interface for mobile ad hoc networks. There are three competing proposals for MANET OSPF [3], [9] and [37]. Mobile Ad Hoc Network (MANET) Extension of OSPF
Using Connected Dominating Set (CDS) Flooding [37] has recently been released as an RFC and will most likely be the chosen proposal for future work towards a MANET OSPF standard.

The mentioned routing protocols all attempt to reduce the routing overhead for mobile networks by using efficient flooding techniques (proactive types) or routing only on demand (reactive

types). The protocols operate independently of the underlying channel type and do not require anything from the underlying protocol layers except for the existence of a functional medium access (MAC) layer and physical transmission layer.

A typical civilian MANET has fairly high data rate (several Mb) and homogeneous links. For military use, where the MANET might have links with very low data rate and the network might consist of heterogeneous links there is a need for more research on routing to design an efficient routing protocol with little overhead. The MANET protocols that are suggested for standardization utilize shortest path routing. In a network with heterogeneous links this will favour long range, low data rate connections and thus put a high load on the low capacity links and leave the high capacity links underutilized. Different routing protocols might be optimal for different network scenarios.

In addition to the mechanisms studied in the ongoing IETF standardization for MANET routing, a routing protocol for mobile tactical networks might also need to take into account the following issues:

- Some cross layer communication with underlying network layers to passively collect topology information from ongoing data traffic to reduce the signalling needed for efficient routing.
- Routing metrics that aim for stable routing paths is needed. This will most likely come at the cost of slightly less efficient routing paths.
- Routing that takes quality of service (QoS) characteristics of the different radio links into account for path calculation might be beneficial both for load balancing in the network and for efficient utilization of the capacity limited mobile tactical network.
- The routing protocols must be expanded to support users that temporarily want to switch to radio silence.
- Efficient interaction between the MANET routing and routing in adjacent networks (e.g., MANET or deployed tactical network) is necessary (gateway functionality).
- Mechanisms to authenticate and otherwise protect the routing information must be integrated with the routing protocol.

An abundance of routing proposals exist that study cross layer enhancements, QoS routing and secure routing for the protocols that are being worked on for standardization. None of these mechanisms have so far been included in the IETF standardization work and will most likely not be included in the first version, maybe never. For efficient routing on networks with heterogeneous links, and routing on networks with nodes in radio silence, very little work has been published.

Two other interesting areas for MANET routing research are hierarchical routing and geographical routing. Hierarchical routing might be more applicable to military networks than to typical civilian MANETs since armed forces are hierarchically organized to follow the chain of command. Furthermore, position information is very important information in tactical mobile

networks, thus the routers position can be assumed to be easily available for a geographic routing protocol.

3.2 Multicast Routing

A large fraction of the traffic on a tactical MANET is envisioned to be group related intended for a group of recipients (e.g., distribution of SA-data, push to talk voice service, and distribution of sensor data), thus efficient data distribution to groups is important. Multicast routing is one mechanism that can realize efficient group communication.

The multicast tree reorganization in MANETs is more frequent than in conventional wired networks, since the multicast protocols have to respond to network dynamics in addition to group dynamics. Consequently, multicast protocols designed for fixed networks do not support the dynamics of MANETs very well. The many multicast protocols suggested specifically for MANETs can be classified in four categories [13]: Tree-based protocols, meshed-based protocols, hybrid protocols, and stateless multicast. In addition to these four types, multicast by means of efficient network flooding is also an interesting approach that has become very popular in experimental tactical mobile networks. Most multicast research treats unreliable multicast distribution, but there is also substantial work on reliable multicast.

The tree-based protocols are based on the IP multicast protocols for fixed networks (e.g., [29] and [41]). These protocols strive to create an optimal multicast distribution tree where the multicast data is distributed to all members with a minimum number of link broadcasts. These protocols are designed to handle some mobility. However, as the node mobility increases, the multicast throughput decreases (and the signalling traffic increases). A basic tree-based protocol is not able to repair broken links quickly enough for a highly mobile network.

Mesh-based protocols (e.g., [30]) were introduced to increase the multicast distribution trees' robustness to node mobility. These protocols introduce some redundancy in the multicast distribution tree; when a link is broken in a mesh tree, the multicast data will (in many cases) continue to flow on a redundant link. This allows the protocol to continue forwarding multicast data while the broken link is being repaired. Clearly the multicast distribution is not optimal on a mesh since the data might travel on parallel paths to the multicast members; however, this inefficiency is traded for better multicast throughput in highly mobile networks.

The hybrid multicast protocols (e.g. [43]) attempt to get the most out of both protocols (tree-based and mesh-based) by combining them.

Stateless multicast (e.g., [26]) makes use of the unicast routing protocol, thus the unicast protocol's robustness to node mobility is important for the performance of this multicast type. No multicast signalling is required, but all addresses of the multicast members must be listed in the header of each data packet. Stateless multicast is therefore efficient only for small multicast groups.

Currently there is no standard or experimental RFC for MANET multicast. The protocol which is a likely candidate to become an RFC, Simplified Multicast Forwarding (SMF) [32], uses efficient flooding for multicast forwarding. In this case there is no need for a multicast routing protocol to maintain a multicast distribution tree. Thus, there is no signalling overhead to maintain a multicast routing table. However, some local (one-hop) signalling is required to identify a subset of a node's neighbours to do multicast forwarding, to get efficient flooding instead of a bandwidth consuming basic flooding. There will clearly also be an overhead due to a high number of redundant packet transmissions; this redundancy is reduced as the density of multicast members increase. The method is very robust for mobility and gives reasonable throughput as long as the overall network load is low enough to keep the packet loss due to data collision on the wireless channel at an acceptable level. SMF is an unreliable multicast protocol. Reliable multicast involves additional challenges.

As for unicast routing, geographic protocols (e.g. [2]), that route on node position is an interesting research area, as is network coding for multicast distribution.

There is not much use of multicast routing in civilian networks due to the difficulties of making an efficient business model with multicast traffic. In multicast routing and group management as defined by IETF, the data source does not know who or how many members each multicast group has. Thus a network service provider does not know how much network resources a multicast service requires. This makes it difficult to define a realistic charging model. Thus, work on MANET multicast will most likely depend on military research. Multicast can be an efficient component in tactical mobile networks. The problematic business model of the civilian world is not an issue. The tactical MANETs have low capacities which lend themselves easily to all techniques that might reduce the traffic load on the network. Multicast does this for group communication, especially for the wireless domain that has an inherent broadcast capacity on the air.

It is impossible to find a MANET multicast protocol that is perfect (little overhead and high efficiency and throughput) for all levels of node mobility, different topologies and traffic patterns. Multicast by means of efficient flooding is a simple and robust protocol group that will suit many military scenarios since these often have a high density of multicast members, and requires robust distribution. Thus, it is useful to put most focus on this multicast type in the initial phase of introducing multicast to tactical MANETs. However multicast MANET protocols are far from mature. As pointed out in [15], multicast research has mainly been performed on isolated uniform networks, thus there is not much experience with multicast distribution to and from uniform networks with multiple gateways. In addition to the multicast mechanisms studied in the ongoing IETF work, a MANET multicast routing protocol for mobile tactical networks might also need to take into account the following issues:

- Multicast on heterogeneous networks where the underlying radio links uses several radio channels with different characteristics. Many of the multicast members have several radio interfaces and can be reached via broadcast on more than one transmission technology. It will be challenging to make an efficient multicast design for such networks.

- Secure multicast solutions are necessary.
- Reliable multicast might be required.
- Multicast distribution to members in *radio silence* must be studied.
- Multicast routing must be enhanced to support several classes of service and be part of the QoS architecture for the mobile tactical network.
- The set of multicast protocols eventually to be used on mobile tactical networks must interact efficiently with multicast in the deployable and strategic networks and must also be able to handle several parallel connections to these networks.

These are all areas where more research is needed.

3.3 Quality of Service

An efficient QoS architecture is very important for tactical MANETs. The networks have low capacity, thus it is envisioned that often the users will want to send and receive more traffic than the network can handle. More network capacity is not easily acquired since there is a shortage of available frequencies in the frequency band that is most beneficial for tactical mobile communication. Equipment cost, equipment weight and battery capacity are other limitations that put constraints on the network capacity. In a military operation it is also likely that the capacity of available radio networks can be reduced either due to malfunction of equipment, jamming of the network or other hostile Computer Network Operation (CNO) activities. When the network capacity is low, it is of utmost importance that mission critical traffic is prioritized by the network at the expense of less important traffic flows. Multilevel Precedence and Pre-emption (MLPP) [4] as originally standardized by The International Telecommunication Union — Telecommunication Standardization Sector (ITU-T)/NATO/US Department of Defence (DoD) should be supported both for voice over IP (VoIP) flows and other dataflows in a packet switched MANET. The idea is that lower-priority flows (both voice and data) may be pre-empted to free capacity for more important flows.

When the data load on a MANET is approaching the maximum capacity, the packet loss ratio increases exponentially. The reason for this is increased packet collision in contention-based radio technologies, and also a higher rate of dropped packets in temporarily full queues in the forwarding nodes for other MAC techniques. With high packet loss, the traffic on the network increases even more due to possible retransmissions at different network levels, which again leads to higher packet loss and so on… Thus it is important to keep the average traffic load on the network below a threshold slightly lower than the theoretical maximum capacity of the network to maintain a stable communication service. Some QoS/traffic management mechanisms must be available to automatically accept, reject and pre-empt dataflows to keep the network load below the threshold.

A tactical MANET must utilize the available network capacity in the best manner possible, which means that a QoS architecture must be supported. In the literature, QoS mechanisms that must be part of a QoS architecture are described in different contexts with different headings. All of the following concepts can be part of a QoS architecture; policy, service level agreements, service

level specification, QoS classes, traffic management, admission control, resource management, QoS management, load balancing, traffic engineering, congestion control, traffic shaping, traffic scheduling, queue management, etc. In this report we have chosen to discuss QoS in the context of a minimal but efficient QoS architecture that divides the QoS operations in two functional entities:

- One entity that does resource management and admission control. This mechanism is needed at the ingress of the network.
- One entity that handles network congestion, packet forwarding, packet prioritizing according to the QoS class and priority required by the different dataflows. This mechanism is needed in all forwarding elements in the network.

Additionally a set of QoS classes must be defined that describe the network requirements (in terms of data rate, jitter, delay, reliability, etc.) needed by the dataflows labelled with the specific QoS class. Flow priorities associated with the role of the end user must also be defined.

Admission control decides if a traffic session that tries to access the network can be supported by the network, thus the admission control must identify the network resources required by the flow associated with a specific QoS class. If there are enough network resources available, the session will be admitted. Thus, there is a need for a resource management mechanism that attempts to estimate the available capacity of the network. If QoS mechanisms are available to support resource reservation, this will be done by the resource manager. However, the prerequisites may change after a session is admitted. A session of very high importance may try to access a fully loaded network. Then, pre-emption of a low importance session may be needed by the admission control. Similarly, due to node mobility, jamming, etc., the network capacity may change over time; this must be identified by the resource manager and acted on by the admission control mechanism.

Short term network congestion due to fluctuations in the radio channel capacities and temporary overload of the network must be handled by the forwarding component of the network routers. This component must also tailor packet queues and packet scheduling to effectuate the delay requirements of the packet's QoS class, and the military priority of the packet. In overload situations this mechanism makes sure that the important traffic is prioritized by the network at the expense of less important traffic that might experience a very high packet loss due to queue overflow.

We have described a simple QoS architecture with a minimum set of mechanisms. The QoS architecture for the Norwegian military communication infrastructure is not yet defined. This architecture might be similar to the conceptual architecture described here, or quite different. No matter how the QoS architecture look like, it is important that the architecture is identical for all three network types (strategic backbone, tactical deployable and tactical mobile). However, the methods used to implement the required functionality might differ substantially within the three network types.

Much work has been done within the IETF to standardize different parts of a QoS architecture. The two main directions which are both proposed standards are Integrated Services (IntServ) and Differentiated Services (DiffServ).

IntServ [8] uses the Resource Reservation Protocol (RSVP) [7] to reserve resources for distinct flows. The source initiates a reservation through a message to the destination. The intermediate routers update the message with information on available resources. If adequate resources are available on the complete routing path the destination responds on the reverse path. The intermediate routers reserve resources for the flow as the response propagates towards the source. This architecture performs resource management and support admission control. Clearly this architecture will induce a lot of signalling overhead in a multi-hop mobile wireless network, with frequent topology changes and varying capacity.

DiffServ [5], [21] defines Per Hop Behaviour (PHB) of aggregate flows. PHB refers to the externally observable forwarding behaviour. It is defined on the basis of the Differentiated Services Code Point (DSCP) value in the Differentiated Service (DS) field of the IP header (also referred to as the Type Of Service (TOS) field). The ingress router codes the DS field in the IP header to values representing priority such as Best Effort (BE), several levels of Assured Forwarding (AF) or Expedited Forwarding (EF). DiffServ performs no resource management or admission control. A Bandwidth Broker (BB) as described conceptually in [35] can be used in conjunction with DiffServ to manage network resources and do admission control. The DiffServ architecture with the BB is also designed for a fairly static network architecture where the network capacity does not change much. More information about the applicability of DiffServ and IntServ in a military context can be found in [28].

For mobile ad hoc networks, no standard exists within the IETF for any of the necessary QoS mechanisms, however there is much ongoing research in the academia and elsewhere. Most QoS models proposed for mobile wireless ad hoc networks are influenced by IntServ and DiffServ. Several of the popular proposals from the academia (e.g., the DiffServ type, Service Differentiation in Stateless Wireless Ad Hoc Networks (SWAN) [1]) assume a contention-based medium access as used by the IEEE 802.11 [23] wireless standard. For most of the current tactical radio networks, this does not apply.

A popular initial approach to QoS congestion control and forwarding, are proposals based on slight modifications of the DiffServ model (e.g., [27]). The DiffServ model is popular since the model acts on DSCP values in the DS field of an IP header. This field is visible also after the dataflow has been encapsulated in an IPSec tunnel. The use of DiffServ approaches will also simplify interconnection with the tactical deployable network and the strategic backbone network.

For resource management to support admission control, polling techniques (e.g., [33]) and QoS resource signalling integrated with the routing protocol are some promising schemes for MANETs. Most existing QoS routing protocol proposals (e.g., [35] and [46]) expect the IEEE 802.11 technology to be used and exploit the characteristics of IEEE 802.11 MAC in the routing

design. Consequently, these proposals can not be directly applied to networks with radio links that are using other physical- and medium access- layers.

In addition to the QoS mechanisms studied in the ongoing civilian research, mechanisms for tactical mobile MANETs should support:

- Dynamic resource management (including resource measurements) to enable the QoS architecture to adapt to the changing network conditions. In tactical networks we expect a large span in instantaneously available network capacity (due to jamming, different transmission technologies, etc.).
- Mechanisms able to perform the necessary QoS functions without imposing much signalling overhead on the low capacity network. This is very important for the narrowband tactical links.
- Mechanisms that can handle heterogeneous radio links based on different radio technologies.
- Nodes in radio silence.
- Transparency to IP security (IPSec) gateways and other security barriers between application and network.
- Tough requirements for traffic priority. In addition to traffic priority to support a specific QoS class (e.g., network delay and jitter) a tactical network must also be able to prioritize traffic based on the payload's importance. These two priority types might conflict.
- The resource management (and possibly resource reserving) mechanisms in the tactical mobile domain must interact efficiently with the mechanisms in the deployable and strategic networks.

These are all areas where more research is needed.

4 The Intelligent Tactical IP Router

With the key challenges for tactical mobile networking in mind, the Norwegian Army Transformation and Doctrine Command, Signals Branch and FFI set out to work with the industry to develop an Intelligent Tactical IP Router (ITR) demonstrator. The ITR should be a cornerstone in our early work to put together a flexible dynamic tactical mobile network. The development phase for the ITR-platform was planned for Q2 – Q3, 2007, ending with a two-week long field test at Rena Army Camp in Q4, 2007.

The ITR was intended to be an experimental platform on which we could propose, implement and test both basic and advanced mechanisms to improve the availability and flexibility in tactical MANET networking. The ITR was not intended to become a product ready for active tactical use. However, experience gained based on ITR test and experimentation might serve as input to specification of network devices for future mobile tactical networks.

The objective for the ITR development was to get a functional router demonstrator that we could use in lab- and tactical field- experiments and thus gain experience on operational requirements for the tactical MANET. At the same time we also wanted to use the ITR to implement and study the efficiency of different technical solutions to support stable mobile networking for several service qualities. The initial ITR-platform will be based on immature MANET mechanisms and thus instable networking is expected, however with time the ITR may evolve to support a stable basic tactical MANET. In addition, more complex mechanisms for future use can be developed and tested on the platform.

4.1 Required ITR Functionality

Initially, basic multicast routing, basic unicast routing and the design of a simple QoS architecture have been the focus for the ITR-platform. With the addition of network protection/security, and network management, these areas are the most important areas to study for early tactical MANET use. The router should be based on IPv4. IPv6 was left for future work.

There are many challenges that must be solved for efficient tactical mobile networking. We chose to focus on routing and QoS mechanisms to support two very important challenges with mobile tactical networking.

- Interconnect all the different radio networks and radio links that are available on a platform at any time, to form one common **heterogeneous tactical MANET**.
- Utilize the common heterogeneous tactical MANET in an optimal manner by the aid of a **QoS architecture**.

In the following sections we describe our requirements to the first version of the Intelligent Tactical IP Router to effectuate support for the two chosen tactical networking challenges.

4.1.1 The heterogeneous tactical MANET

Many military platforms will want access to several different radio networks/links at the same time to provide long range communications, high bandwidth communications, robust communications, etc. Currently these systems are isolated; the end user must choose which radio to use for each application. The ITR should be able to interconnect these networks/links and give the end user a single seamless interface to the common heterogeneous network. The ITR should automatically choose the best path to the destination through the heterogeneous network. This path might traverse several different radio systems in a multi-hop manner, thus the ITR must be able to perform routing on all radio networks/links that form the heterogeneous tactical MANET.

With the ITR-platform we aim to interconnect all available radio resources in one common network that can be used by all applications. Future work might conclude that some tactical radio networks/links are best left isolated and not interconnected in a heterogeneous network, either due to very limited bandwidth, special dedicated use, incompatible security level, etc. However, to utilize the limited radio resources in the best manner it is in most cases best to establish a common network that is available for all applications. Thus for our current work based on ITR-

platform we wanted to interconnect a wide diversity of radio types to gain experience with the performance of the resulting heterogeneous network. The heterogeneity of the network place additional challenges on the network protocols.

The ITR should provide basic multicast support for the heterogeneous network. This is a challenge for several reasons: The different radio networks/links used in the heterogeneous network will have varying support for multicast/broadcast. The systems that support this will in most cases not have compatible multicast protocols and be able to interact. The same challenge applies for unicast routing, however for unicast the penalty for performing e.g., overlay routing to interconnect incompatible systems is lower than for multicast. Another challenge for multicast is the possible large variation in transmission delay on the different radio hops. This can result in unnecessary redundant multicast traffic on the links with long delays (typically the low capacity links).

The ITR was required to support easy addition and removal of interfaces to a radio system on the ITR-platform, and easy reconfiguration of the ITR. It should also be easy to introduce a new type of radio network/link to the ITR-platform. It was also required that the router should support standardized protocols and mechanisms whenever available. Standard interfaces would facilitate interconnection towards other routers either in the deployable tactical domain or integrated with new tactical radio networks that support mobile multi-hop IP routing. Since routing and QoS mechanisms for MANETs are not yet standardized, this requirement had to be interpreted to include support for standard fixed network protocols and possibly the ability to interface popular MANET protocols.

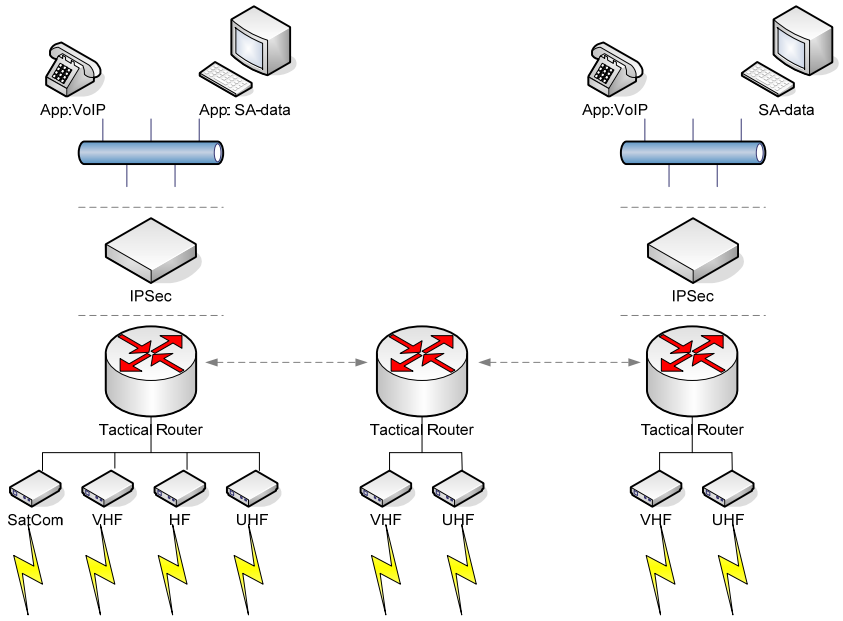

Figure 4.1 This figure show the ITR placed in a network diagram. In this figure we assume unencrypted radio links, thus the router is placed in a black network and an IPSec device isolates the red domain from the black domain.

ITR was required to support at least 4 simultaneous wireless interfaces. These radio networks/links should be supported in the first version of ITR: Harris RF5800H (HF), KDA MRR (VHF), KDA WM600 (UHF), and NERA SATCOM using the Inmarsat Global Area Network (GAN-UHF).

Figure 4.1 shows the ITR in the context of a network elements diagram. In the network example shown in the figure we have a transport network with unencrypted radio links. A red Local Area Network (LAN) can then be isolated from the black network by e.g., an IPSec device. If all radio links have link encryption or are otherwise protected, the ITR can be located in the red network. For the first version of the ITR we have chosen not to focus on information security and do thus not attempt to solve any of the many existing challenges associated with information protection in a heterogeneous multilevel security environment. In future work, interesting security mechanisms can be integrated with the ITR platform to perform some protection of the tactical transport network.

4.1.2 QoS architecture

Given the heterogeneous network as described above, the network capacity could change from several 100 kb/s to a few kb/s when a node moves from UHF coverage to VHF/HF only coverage. Clearly, services (e.g. video) that can be supported on a network with several 100 kb/s will completely jam a network with capacity of only a few kb/s. Thus, the ITR must support a QoS architecture that can handle this extreme dynamics and be able to prioritize the mission critical data traffic in overload situations.

The ITR should be able to store several network routes from source to destination where the different routes might represent support for different QoS characteristics (e.g. bandwidth, delay, jitter and robustness). For the initial tests of the router, we defined a QoS architecture with 6 different QoS classes. All traffic arriving at the router will be marked with one of the 6 QoS classes (see Table 4.1). The QoS classes and the associated applications were chosen to facilitate the analysis of the test results.

QoS class	DS field	Traffic
1	001 010 AF1 001 100 AF1	AF1.1 Routing AF1.2 Administrative traffic
2	010 010 AF2	AF2.1 Short text messages
3	011 010 AF3	AF3.1 SA-data
4	100 010 AF4	AF4.1 Video streaming
5	101 110 EF	EF VoIP
6	000 000 BE	BE Messages w/attachments, other

Table 4.1 The table shows the QoS marks defined for the initial tests of the Intelligent Tactical IP router.

The QoS mark is placed in the DS field of the IP header with DiffServ-like encoding. The router should be able to choose the best path for the dataflows. Different paths might be optimal for flows marked with different QoS classes. Based on the available routes, the router should decide if a path that can support an adequate service quality is available, and thus if the flow can be supported by the network.

The ITR should also be able to prioritize between different traffic types and immediately start dropping low priority traffic when the network approaches congestion and thus maintain fair QoS for high priority traffic. It was envisioned that mechanisms for different types of packet scheduling, and different packet queues associated with the defined QoS classes could be able to handle this. We wanted the different QoS classes to be prioritized in a certain order. For routes with little capacity, QoS class 1, 2, 3 and 6 should be admitted, and prioritized in the mentioned order. For routes with higher capacity, all QoS classes should be admitted and given a share of the available network capacity, however QoS class 5 and 4 should be given a higher priority to keep the transmission delay and jitter of these flows low.

4.2 ITR-platform

An official enquiry listing the requirements mentioned in the previous sections was sent to selected industrial partners [19] in Q1, 2007. The request was for four HW platforms, a copy of the source code and the development framework, and unlimited SW licenses. The ITR-platforms and the source code were meant for experimental use only, by FFI and the Norwegian Armed Forces. We do not have the rights to put the ITR-platforms in operation for normal use.

The technical solutions for the ITR-platform presented in a combined offer from two companies; Thales Norway AS and Kongsberg Defence & Aerospace AS, were selected. In their common offer, they proposed to develop one ITR demonstrator each. In the remainder of this report these companies are referred to as Thales and KDA, respectively. Currently we own four copies of the ITR-platform developed by Thales, and four copies of the ITR-platform developed by KDA.

In the following, the functionality available in the two different ITR-platforms by the end of 2008 is described.

4.3 The Intelligent Tactical IP Router designed by Thales

Figure 4.2 The Intelligent Tactical IP Router designed by Thales is based on a ruggedized PC/104 platform offering four Ethernet ports, two serial ports, one X.25 port and two USB ports

The transmission means used in tactical networks have large variations in capabilities, thus Thales concluded that it could be advantageous to define multiple routing topologies in the heterogeneous mobile network, where each topology represents a specific network characteristic. These topologies are then used to ensure that data packets are only forwarded on topologies supporting the requirements of the dataflow. Topologies can be defined to represent different characteristics of the network, e.g.:

- Network capacity (bit rate)
- Transmission delay
- Robustness
- Security level
- Network segment that coalition partners are allowed to use for transit traffic

The radio networks that were required for the initial field test of the ITR provide a varying degree of network functionality. The MRR (VHF) network has an X.25 data interface [25]. The X.25 network does not perform any IP routing, thus MRR must be connected to the ITR using IP over X.25. The Harris RF5800H (HF) terminals support IP traffic, but offer only static routing. The KDA WM600 (UHF) IP network is able to support static routing, using the OLSR protocol [12] or OSPF [34] routing. The SATCOM (GAN) connection is achieved via a public service provider and the Internet. Thus an IP tunnel had to be established over this connection to hide the public Internet from the private network for the test. Even though many of the radio networks to be used in the test offered an IP service, they did not support a common IP routing scheme. Thus in their ITR-platform Thales chose to establish an overlay network consisting of Generic Routing Encapsulation (GRE) [17] tunnels to hide the differences in the network protocols. To handle the dynamic changes in the network topology for the mobile network, the Open Shortest Path First – Multi Topology (OSPF-MT) [39] routing protocol was selected as the common routing protocol spanning all technologies.

For multicast support, Thales chose to implement a simple flooding mechanism that use the overlay GRE network for all underlying radio networks except MRR where the X.25 broadcast functionality was utilized.

The OSPF-MT routing protocol is able to maintain multiple independent network topologies. This Multi Topology (MT) protocol allowed the design of a QoS architecture with some real time resource management in the Thales ITR-platform. The QoS architecture used a DiffServ-like packet forwarding mechanism, and information from the MT routing tables for network resource management and support for admission control.

The Thales ITR-platform (Figure 4.2) thus aimed for a dynamic QoS architecture and put less focus on minimizing the signalling overhead in the heterogeneous network.

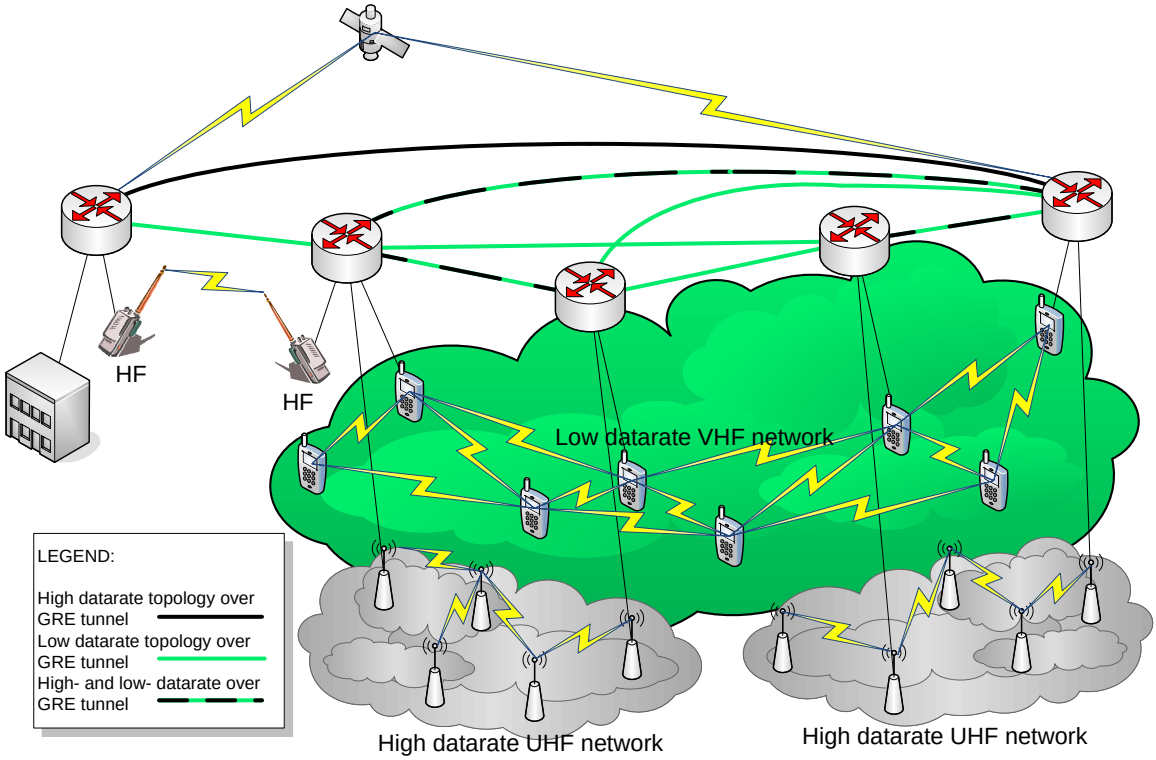

Figure 4.3 Overlay network with Multi Topology routing

4.3.1 Unicast routing solution

The routing protocol implemented in the Thales ITR is based on the IETF standard, RFC 4915 (Multi Topology (MT) Routing in OSPF) [39], which reuses the Type of Service (TOS) field in the OSPF Link State Advertisements (LSA) packets to advertise multiple topologies. The OSPF protocol is designed for use in fixed networks. Its database updates are bandwidth consuming and thus not optimal for low bandwidth networks. Neither is the signalling scheme tuned for highly mobile networks. OSPF will most likely be used in the deployable tactical network and might also to some extent be used in the mobile tactical network, but a MANET protocol should be used in the highly mobile networks. However, the multi topology concept is interesting to study for the

entire mobile tactical networks. Thus Thales chose to provide this protocol for experimenting also in the mobile domain. In future work, multi topology can be implemented also for the mobile extension to OSPF.

OSPF-MT can be set up to maintain network topologies that represent different characteristics of the underlying network or the network location. The radio networks to be used in the initial field test of the ITR represented a large span in bit rate, thus we found it useful to define topologies based on bit rate characteristics for this test. Two network topologies were defined: a low data rate topology and a high data rate topology (Figure 4.3). Each radio link was assigned to one or both topologies based on its data rate characteristics in the following manner:

- Low data rate: MRR (2.5kb/s)[1], RF5800H (9.6kb/s)[1], WM600 (500kb/s)[1], and SATCOM (64kb/s)[1]. The high data rate links are also included in this topology to increase connectivity and network robustness; however the topology can not guarantee more than a low data rate capacity.
- High data rate: WM600 (500kb/s)[1], and SATCOM (64kb/s)[1].

The description of the Thales ITR-platform is made with these example topologies in mind.

The implementation of OSPF-MT was done on the XORP (http://www.xorp.org) open source routing application using the Vyatta (http://www.vyatta.com) Linux distribution (Debian Linux 2.6.20). It offers all major protocols as well as a feature rich Command Line Interface (CLI) for configuration of the router's functionality. In addition to extending the XORP software, the interface towards forwarding tables in Linux had to be adjusted to allow the use of multiple tables. The CLI was extended to support configuration of OSPF-MT information, MT-ids and metrics for each interface.

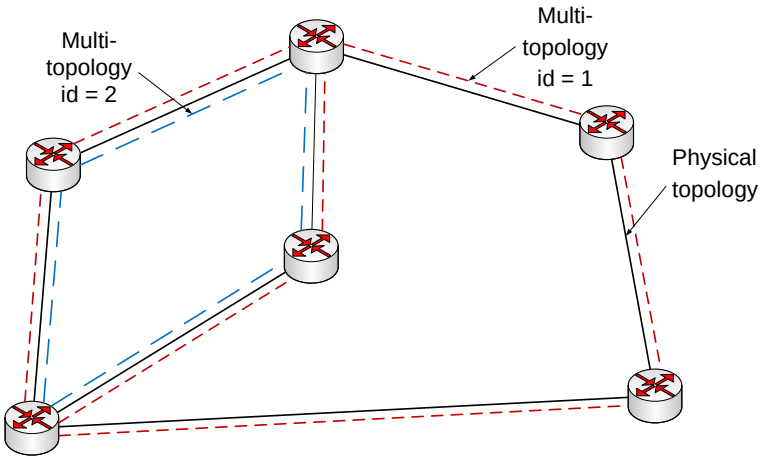

Figure 4.4 Network configured with two topologies.

[1] The data rate given here is the maximum available data rate for the radio configurations applied for the field test. Lower data rates could be experienced during the tests due to co-traffic and difficult channel conditions.

Full compliance with RFC 4915 was not implemented in the first version. The current implementation only supports the Router Link State Advertisement (LSA). However, additional LSA types can be added at a later stage. The implementation supports up to four different topologies, but this can easily be increased if needed. Each topology spans a subset of the physical topology (Figure 4.4). A shortest path first (SPF) calculation is performed for each topology to find the best routes within the topology. Only the links belonging to the actual topology are included in the calculation. The results of the SPF calculation are stored in the forwarding table. Each topology has its own forwarding table, which is used to forward packets marked with a QoS mark that has been linked (in the QoS architecture) with a specific topology.

In addition to OSPF-MT routing, the implementation also supports configuration of static MT routes. Static MT routes are configured using the router's CLI. Both MT-id and MT metric can be configured for the static routes. The static MT routes are only local and not distributed to other OSPF-MT routers.

RFC 4915 [1] only defines how to support multiple topologies within a stand alone OSPF network. The standard does not define how OSPF-MT should be integrated with other routing protocols (e.g., BGP [31] and OLSR [12]) that do not support multiple topologies. Routes imported into OSPF-MT from other routing protocols not supporting multi topology routing have to be classified according to the topology they should be imported into. Similarly, it is necessary to define which routes (from which topologies) to export and which routes not to export when exchanging routes between OSPF-MT and other non-MT capable routing protocols. This may be done through the definition of routing policies. This ability was not implemented in the first version of the ITR.

4.3.2 Multicast routing solution

The radio networks chosen for the field test of the Intelligent Tactical IP router also had varying multicast/broadcast support. The MRR (VHF) network provided an X.25 broadcast service. The KDA WM600 (UHF) network supported the Distance Vector Multicast Routing Protocol (DVMRP) [44]. The RF5800H (HF) had a broadcast service, however for the test network this connection was used as a point-to-point ink. The GAN SATCOM connection was also used as point-to-point link. As was the case for unicast routing, the radio networks did not have compatible multicast protocols. One option for the Thales ITR-platform was to install a multicast protocol on the GRE overlay network already established for the unicast traffic. The drawback with this solution was that the inherent broadcast characteristic of a radio network with a common channel would not be utilized. We required that the broadcast support of the MRR network should be utilized. Thus, Thales implemented a non-standard multicast/broadcast mechanism for the ITR-platform.

The multicast/broadcast mechanism was implemented in the Click Modular Router Framework (http://read.cs.ucla.edu/click). The implemented protocol was a standard flooding protocol with some extra functionality tailored for a heterogeneous network with large variations in link delay. A flooding protocol does not maintain a multicast distribution tree; it simply forwards a received

multicast packet on all interfaces except the interfaces where the packet has already been received. For interfaces to a multi-hop radio network with a shared common channel, the packet must also be forwarded once on the interface where it has been received.

The multicast/broadcast function was tailored to use the X.25 broadcast support of the MRR network, and used the GRE overlay network for all other links. In a heterogeneous wireless network that consists of several radio networks based on different transmission technologies there is a large variation in transmission times for the different link types. It is difficult to do efficient flooding of multicast packets on such networks. To improve the flooding efficiency it is useful to be able to configure a forward delay on selected links to allow a multicast packet to propagate a long latency link prior to the delayed arrival of an identical packet on a short latency link. This is done to avoid jamming of the long delay links (e.g., MRR) with superfluous multicast packets. In Figure 4.5 a multicast packet arrives at node A. Next the packet is forwarded on both radio interfaces of node A. The packet arrives at node B on the short delay link before it has been received on the long delay network. Node B does not yet know that the packet already is transmitted on the long delay network, thus node B forwards a superfluous packet on this network. This jamming of the long delay (often low capacity) network can be avoided if node B delays the multicast packet some time before it performs a forward on the long delay network. If the multicast packet has been received from the long delay network during the delay, then the packet will not be rebroadcast on this network. Thales implemented such delay functionality in the flooding engine for the ITR-platform.

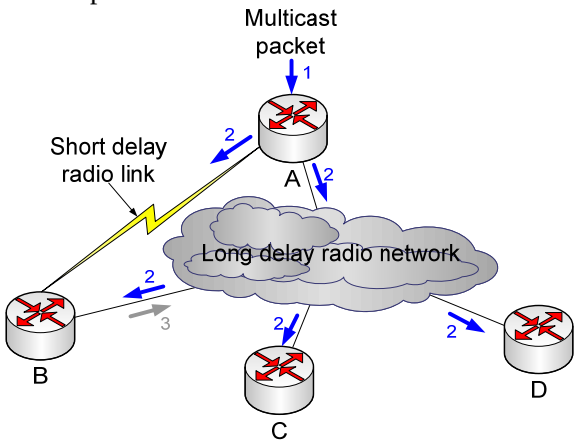

Figure 4.5 The figure shows the flooding of a multicast packet in a heterogeneous network with two different radio interfaces.

4.3.3 QoS architecture

The OSPF protocol is capable of taking into account link costs (data rates), when selecting the "best" route. However, standard OSPF is not able to filter traffic based on application requirements. Instead it selects one route between the source and destination for all types of traffic. The characteristics of a mobile tactical network might vary substantially depending on available radio equipment and available network connectivity. Some of the links in a mobile tactical network might have very limited data rates, and are unable to support the data rate requirements of high data rate applications (e.g. video streaming). Other links have long

forwarding delay and can not support applications that require short delay (e.g., Voice over IP). Thus we needed a QoS architecture to ensure that only data traffic that could be supported by the current tactical network topology was allowed to enter the network. The QoS architecture should dynamically block the network for traffic that could not be supported, and thus maintain good service quality for traffic that could be supported. The architecture should also make sure that high priority traffic was prioritized in situations with limited network capacity.

A solution offering a combination of QoS mechanisms based on the DiffServ architecture and OSPF-MT routing based on the packets' QoS mark was selected to support the QoS and traffic control requirements for the Thales ITR-platform. For the initial tests of the ITR, two OSPF-MT topologies were configured as described in section 4.3.1. Table 4.2 shows how the QoS marks defined for the initial tests were associated with the two OSPF-MT topologies.

In this architecture, an IP packet was forwarded on the topology associated with the packet's QoS class. If a destination address was available only in the low data rate topology, packets marked with a QoS mark requiring high data rate transmission (e.g. video) could not be forwarded over this topology, and the packet was dropped at the source. Other topologies can be created to represent other important network characteristics.

QoS class	DS field	Traffic	Low data rate topology	High data rate topology
1	001 010 AF1 001 100 AF1	AF1.1 Routing AF1.2 Administrative traffic	X X	X X
2	010 010 AF2	AF2.1 Short text messages	X	X
3	011 010 AF3	AF3.1 SA-data	X	X
4	100 010 AF4	AF4.1 Video streaming	-	X
5	101 110 EF	EF VoIP	-	X
6	000 000 BE	BE Messages w/attachments, other	X	X

Table 4.2 This table shows how the QoS classes and topologies used in the field test at Rena Army Camp were associated.

The QoS mechanisms based on DiffServ differentiate the service level for different classes of traffic and divide the data rate between the classes. By adding Multi Topology class-based routing, traffic is prevented from entering the network, unless a route supporting the application's QoS requirements is available end-to-end. This might improve the network utilization. Traffic is stopped at the network edge if an end-to-end route capable of supporting the traffic is not available. Using traditional IP routing protocols, the traffic might in the worst-case traverse the entire network just to find out that the host is only reachable through a very low data rate link not able to support the application's requirements.

The applications' packets were classified by marking the IP DS header field and classification was done by the IP-tables functionality in Linux. In addition to supporting OSPF-MT routing,

QoS mechanisms were configured to support service differentiation and rate control. The Linux traffic control (TC) tool was used for queuing and scheduling mechanisms to implement the DiffServ-like scheme. This environment can also be used to prioritize selected traffic flows. For the first version of the Thales ITR-platform, multicast traffic and unicast traffic was handled separately with independent queues and schedulers.

More information about the Thales ITR-platform can be found in [40].

4.4 The Intelligent Tactical IP Router designed by KDA

Figure 4.6 The Intelligent Tactical IP Router from KDA is based on a ruggedized PC/104 platform offering three ports for Ethernet or serial (RS232) connection, one port for Ethernet or serial (RS422)connections, and 4 ports for Ethernet connections only.

The radio networks that were required for the initial field test of the ITR provide a varying degree of network functionality. The MRR (VHF) network has an X.25 data interface. KDA also has access to an optional proprietary X.28-like [24] Packet Assembly/Disassembly (PAD) interface in MRR, that can be used for IP traffic. This PAD interface was used for the MRR connection to the KDA ITR-platform. The other networks required for the test (Harris RF5800H (HF), KDA WM600 (UHF) and SATCOM (GAN)) has the network functionality as described in chapter 4.3.

KDA designed the ITR-platform with interconnection of different protocols in mind. The purpose was to avoid using an overlay network whenever possible to prevent the overhead associated with the overlay tunnels. KDA also focused on minimizing the routing overhead on the low bit rate links and thus decided to use several different routing protocols in the heterogeneous network. These protocols were configured to support some exchange of routing information. GRE tunnels were used to establish an overlay on the links that could not run the chosen protocols by KDA, or where the radio's network protocols could not interconnect to these protocols.

For multicast, the DVMRP protocol supported by the KDA WM600 (UHF) radio was chosen as the common protocol and an overlay was established where this protocol was not supported. For QoS a straight forward DiffServ-like architecture was chosen.

The KDA ITR-platform (Figure 4.6) thus aimed for low routing overhead for unicast traffic in the heterogeneous mobile network and put less focus on the QoS architecture.

4.4.1 Unicast routing solution

The KDA ITR-platform is based on the Gentoo (http://www.gentoo.org) Linux distribution. This distribution is popular for use in embedded devices. Gentoo allows a detailed configuration of available Linux functionality and thus supports the possibility to build a ITR with a small footprint that can be run on small devices with little storage space and limited memory.

The routing protocol suite is based on the Quagga (http://www.quagga.net) daemon. Quagga offers all major protocols. Furthermore, there are two other daemons installed, these are OLSR (http://www.olsr.org) and TDP (Taclan Discovery Protocol). TDP is a nonstandard routing protocol developed by KDA. It is a low overhead protocol intended to be used on low bandwidth links. TDP works well for one-hop radio links, but is not intended to be used as a stand-alone protocol on dynamic mobile multi-hop networks. Both of the two mentioned routing daemons are exported as plug-ins to the Quagga core router. This means that some routing information can be imported and exported between the different protocols.

In Q4 2008, the KDA ITR-platform was updated to support IPv6 in addition to the original IPv4 protocol to prepare the router for experimentation with future IPv6 tactical networks. The TDP protocol and the drivers for the PAD interface to the MRR radio were also updated for IPv6. Additionally, an implementation (http://hipserver.mct.phantomworks.org/ietf/ospf) of one of the three suggested MANET extensions to OSPFv3 (IPv6), the MDR proposal [37], has been installed in the Quagga router base on the ITR-platform.

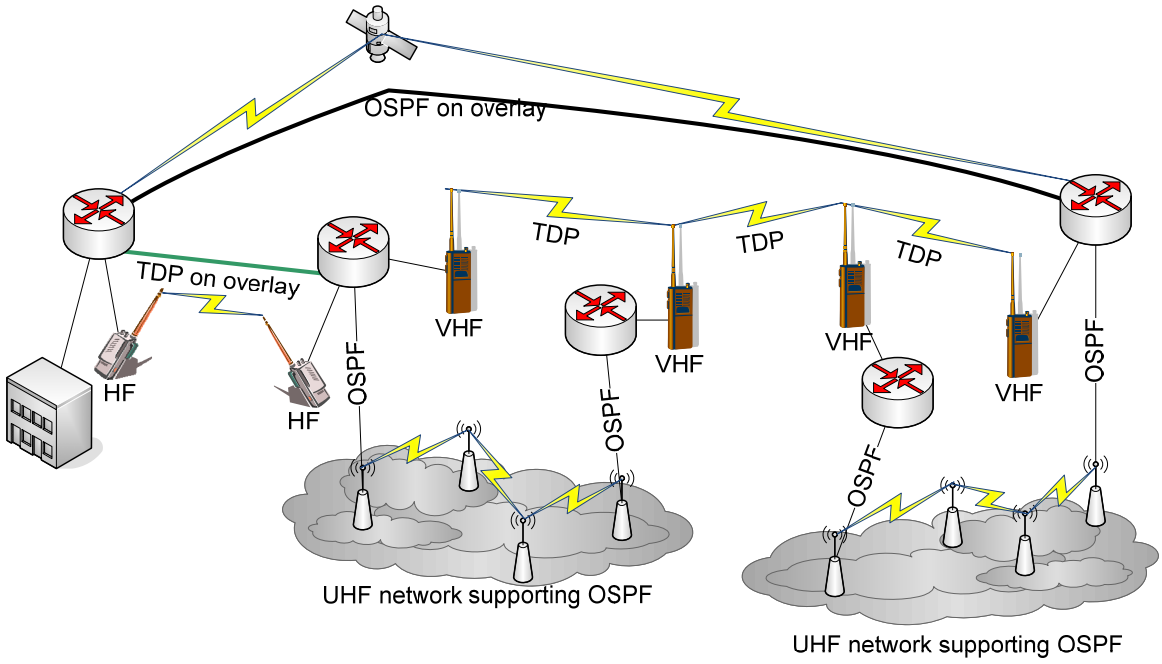

Figure 4.7 This figure shows the routing configuration in the KDA ITR-platform for the test network in the initial field test of the ITR.

KDA chose to configure two different unicast routing protocols for the heterogeneous network in the initial field test of the ITR. The TDP protocol was chosen for the low data rate connections MRR (VHF 2.5kb/s) and RF5800H (HF 9,6kb/s). OSPF was chosen for the higher data rate connections WM600 (UHF 500kb/s) and SATCOM (64kb/s). When MRR's PAD interface is utilized, the MRR radio links are seen as a one-hop data connection, thus TDP can be run directly on this link; there is no need to create an overlay tunnel. The HF radio is connected at the network layer and supports only static routing, thus an overlay GRE tunnel running TDP had to be established to include the HF link in dynamic routing. Both WM600 and the KDA ITR-platform support OSFP, thus OSPF was chosen for the link between ITR and WM600. For the SATCOM connection an overlay tunnel had to be established to hide the Internet from the private network used in the test, and OSPF was chosen to run on this overlay (Figure 4.7).

4.4.2 Multicast routing solution

The radio networks that were required for the field test of the Intelligent Tactical IP router also had varying multicast/broadcast support. For KDA use the MRR PAD has a broadcast data service at link-layer level. The KDA WM600 (UHF) network supported DVMRP. (This protocol was introduced to the KDA WM600 (VHF) radios to support the ITR tests.) The HF and SATCOM connections were used as point-to-point links. Similarly, as was the case for unicast routing, the radio networks did not support any compatible multicast solutions. KDA chose to run the DVMRP protocol in the ITR network.

DVMRP can be characterized as a broadcast and prune multicast routing protocol. This means that IP multicast packets are forwarded to all possible receivers (flooded) and then unwanted data traffic is pruned back to the minimum tree necessary to reach all of the current receivers. Graft and prune messages are used to handle new- or leaving multicast members. Periodically the multicast tree is refreshed with a new flood and prune activity. One tree is created and maintained for each source. This protocol is not optimal for MANET use where the network topology changes frequently; however it provides a functional multicast service for the heterogeneous network that could be experimented with in the field. Since WM600 supported this protocol, and MRR PAD had a broadcast service, the inherent broadcast characteristic of the radio networks could be utilized. For HF and SATCOM, an overlay had to be used, however these radios were used as point to point links, and thus a broadcast functionality was not needed.

The different transmission delay characteristics for the heterogeneous network were not taken into account for this solution. Thus some unnecessary packets were sent on the long latency links (MRR and HF) for every refresh of the multicast routing distribution tree.

In the Q4 2008 release from KDA, the SMF protocol implementation from Naval Research Lab (NRL), nrlsmf (http://cs.itd.nrl.navy.mil/work/smf/index.php) was also made available for the ITR-platform. This is an interesting multicast option for tactical mobile use that we will study closer in due course.

4.4.3 QoS architecture

The OSPF protocol is capable of taking into account link costs (e.g., available data rate), when selecting the "best" route. However, standard OSPF is not able to filter traffic based on application requirements. Instead it selects one route between the source and destination for all types of traffic. The same holds for the TDP protocol. A careful configuration of link cost for the different link types in a heterogeneous network can provide an aggregated cost for the complete network route. This aggregated cost can support a resource manager and admission control for a heterogeneous network. As an example: if the link cost represents the data rate of the link (low cost = high data rate) then the aggregated cost for a route gives an indication of the available data rate end-to-end. With this method it is impossible to know whether the route represents a long route (many hops) with high data rate links, or a short route (few hops) with low data rate links. However, for a limited network size the threshold on the link cost from source to destination might be used to block or accept traffic associated with a QoS class that requires high data rate support. The aggregated cost is a single value, thus it is not possible with this method to maintain several routes with different QoS characteristics to the destination. For the field test of the KDA ITR-platform, the aggregated link cost was used by OSPF and TDP to find the lowest cost route from source to destination. The cost value was not used to support admission control.

The applications' packets were classified by marking the IP DS header field and classification was done by the IP-tables functionality in Linux. The KDA ITR-platform uses the Linux traffic control (TC) tool for rate control, queuing and scheduling to implement a DiffServ-like QoS scheme. This environment can also be used to prioritize selected traffic flows. Additionally, TC and IP-tables functionality were used to block traffic types associated with a QoS class that was not allowed to traverse a certain link type in the heterogeneous network. This blocking was done according to Table 4.3 for the radio types to be used in the initial field test at Rena Army Camp. This blocking ensures that the low data rate links are not congested with high data rate traffic; however it does not stop the traffic flow from entering the network in a situation where the low data rate link is not at the first hop. In this case the traffic is dropped when it reaches the low data rate link.

QoS class	DS field	Traffic	VHF (2.5kb/s)	UHF (500kb/s)	HF (9,6kb/s)	SATCOM (64kb/s)
1	001 010 AF1	AF1.1 Routing	X	X	X	X
	001 100 AF1	AF1.2 Administrative traffic	X	X	X	X
2	010 010 AF2	AF2.1 Short text messages	X	X	X	X
3	011 010 AF3	AF3.1 SA-data	X	X	X	X
4	100 010 AF4	AF4.1 Video streaming	-	X	-	-
5	101 110 EF	EF VoIP	-	X	-	X
6	000 000 BE	BE Messages w/attachments, other	X	X	X	X

Table 4.3 This table shows how the defined QoS classes are allowed (X) or dropped (-) at the different radio links used in the initial field test at Rena Army Camp.

5 Field Test at Rena Army Camp, October 2007

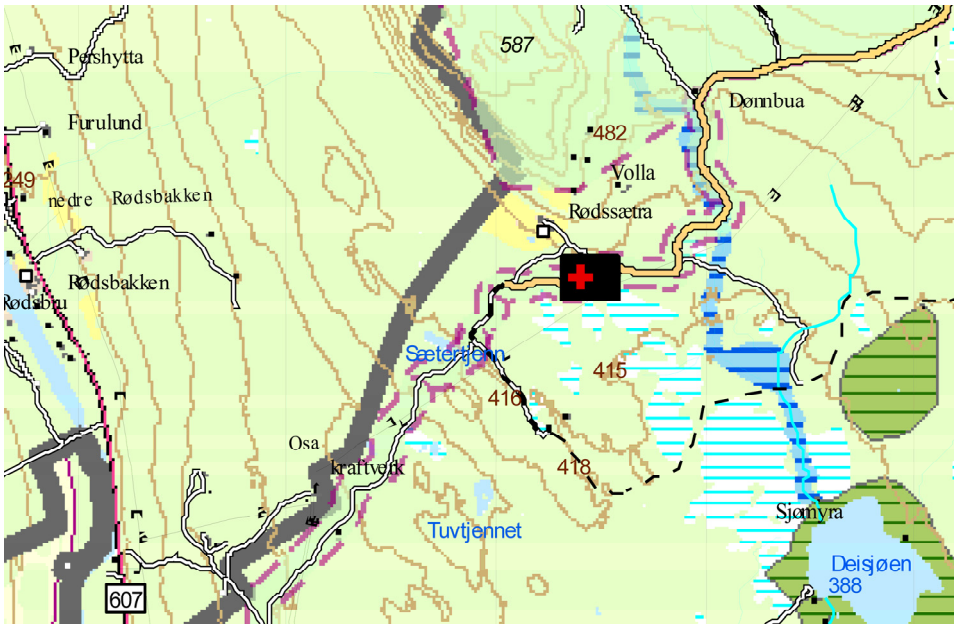

Figure 5.1 This map shows the area around Rødssætra (near Rena Army Camp) where we did the field tests of the Intelligent Tactical IP Router in October 2007.

The two Intelligent Tactical IP Router platforms were tested in a two week long field trial (one week for each platform) at and around Rødssætra near Rena Army Camp in October 2007 (Figure 5.1). The main objective of the tests was to see how well the chosen routing and QoS architecture could utilize a heterogeneous wireless network made up by radio networks/links using different transmission technologies (and thus a large variation in maximum data capacity and transmission delay). Due to mobility and fluctuating channel conditions, this network would also have rapid topology changes. We wanted to verify the claim that carefully configured mechanisms to support service qualities might improve network throughput while maintaining an adequate service quality for important high priority traffic. A second objective was to study how well the chosen protocols and implementations were able to accurately represent the network topology of the mobile wireless test network.

In the first version of both the KDA- and Thales- ITR-platforms, many of the chosen protocols and QoS mechanisms were standardised solutions designed for the Internet. Thus these protocols and mechanisms were intended for high data rate fixed networks and not for mobile heterogeneous low data rate tactical networks. The reasons for this choice of protocols were threefold:

- Time and cost constraints. Much open source code is available for the popular standardized Internet protocols, whereas very little stable code is available for MANET proposals that are not yet standardized.
- In the first years to come, there will not be an abundance of squad networks and platoon networks to interconnect, thus the Intelligent Tactical IP router might be applicable for

use higher up in the tactical hierarchy where the network mobility is lower. In these positions, the choice of solutions might be the correct ones.

- The Intelligent Tactical IP Router must be able to interact efficiently with standard protocols and QoS mechanism in a deployed tactical network, thus these solutions must also be supported by the ITR.

The IP routers that must be deployed in the tactical network in the first years to come to start the migration from the current e.g., X.25 based network to an IP based network, will most likely be based on carefully configured routers with standard Internet protocols. In due course, as the experience with tactical mobile networking increases, solutions tailored for mobile narrowband use will be introduced. Thus, in the field test of the experimental ITR we also wanted to gain experience with the use of carefully configured Internet protocols for routing and QoS in a tactical MANET.

In the first release of the ITR-platforms many standard protocols for unicast, multicast routing and QoS handling were used. These were adapted for mobile, low bandwidth use by careful configuration of the protocol parameters. In current and future research involving the ITR-platforms we intend to introduce more experimental components tailored for tactical MANETs.

5.1 Test Configuration

Four different radio technologies were used in the field trial: Harris RF5800H (HF), KDA MRR (VHF), KDA WM600 (UHF), and NERA SATCOM using the Inmarsat GAN (Global Area Network). In the test scenarios, we used a network of 5 nodes, each equipped with a ITR. The network consisted of 4 mobile nodes and one fixed headquarter (HQ) node. The Intelligent Tactical IP Routers were set up with the network interfaces as shown in Figure 5.2. All vehicles were equipped with GPS. Vehicle 4 was also equipped with a sensor (video camera).

A key point for the experiment was to make use of several network mechanisms to enforce an adequate service quality for the test applications. We used DiffServ-like coding to classify the traffic in 6 different QoS classes. We used the DS field of the IP header to mark the dataflows with the correct QoS mark. Some of the applications used in the test supported QoS marking of the data packets. The remaining traffic flows were marked by us for the test with the IP-tables functionality in Linux. Table 4.1 shows the traffic types used in the test, and how these were classified. QoS class 4 is used for video streaming. We included this bandwidth-consuming application in our experiment to test how the different mechanisms supporting service quality, were able to cope with a high traffic load.

Many of the existing applications used by the Norwegian Armed Forces in the tactical field do not support QoS configuration. It is evident that this will be supported in due course, however to be able to perform field tests with QoS focus at the present time we chose to use some experimental applications with tactical functionality for the tests.

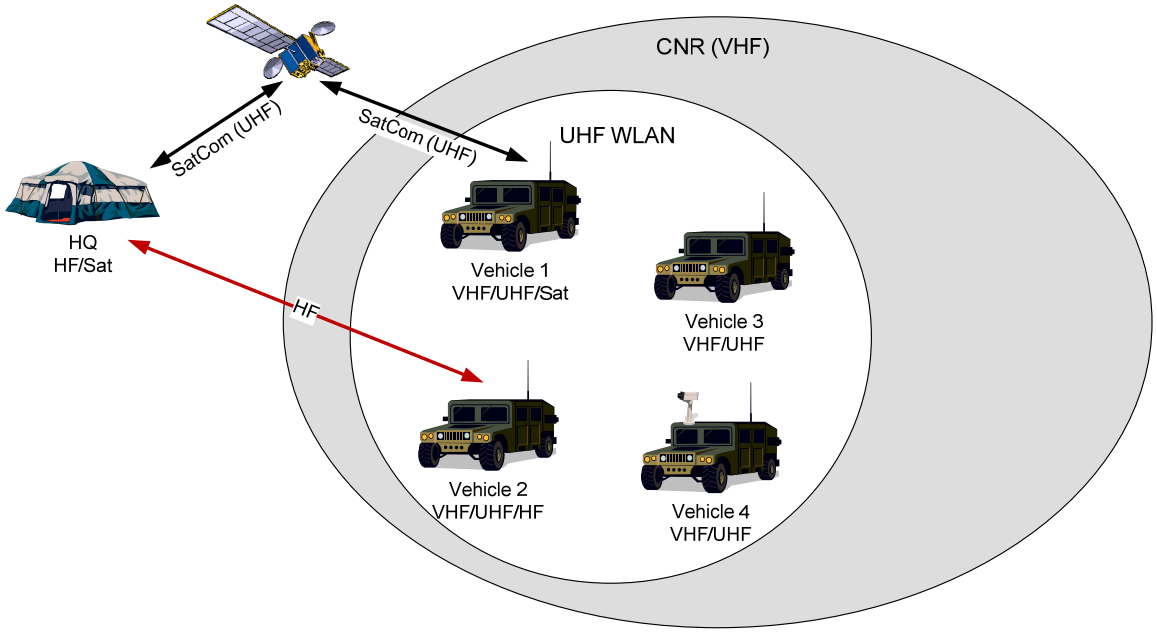

Figure 5.2 Ruggedized Intelligent Tactical IP Routers were installed in four vehicles, and an office version was used in the HQ

Our test network consisted of wireless networks that ranged from a common gross channel capacity of 2.5 kb/s (VHF) to 500 kb/s (UHF) (Table 5.1). QoS class 4 (Video streaming) required at least 100 kb/s and QoS class 5 (VoIP[2]) required approximately 7 kb/s for a full duplex connection. Clearly, it was not possible to support video and VoIP on the low data rate links, and the QoS architecture had to block these QoS classes on the low data rate links.

In the Thales ITR-platform the QoS architecture was supported by the aid of OSPF-MT. In the test, we wanted to maintain OSPF-MT routing for two network topologies; one high data rate topology, and one low data rate topology. Table 4.2 shows how the different QoS classes and applications were mapped to the two topologies. Table 5.1 shows how the different wireless networks were associated with the two network topologies. The low data rate topology spans both the high and low data rate links whereas the high data rate topology only includes the high data rate links. The best path within each topology was calculated based on the OSPF metric associated with each link. With this setup, the routing tables in each ITR would tell if a traffic flow labelled with one of the 6 QoS classes could be supported on all links from source to destination. If there was no support, then the traffic flow was blocked in the ITR at the source.

In the KDA-platform, a blocking filter was implemented in each ITR. When a traffic flow labelled with a QoS class arrived at a ITR, the ITR identified the next hop for the flow on its way to the destination. If the next hop link was a link type that did not allow the specified QoS class, then the traffic flow was blocked. Thus the traffic did not overload the low bandwidth links.

[2] The VoIP application used was a free experimental application from US Naval Research Lab. We used the MELPe 2400 codec. With IP header overhead and full duplex connection this application required a data rate of approximately 7 kb/s.

However, the traffic (which was now garbage for the network since it could not be delivered to the destination successfully) might have traversed several high bandwidth links on its way to the limiting low bandwidth link.

Wireless network	Channel capacity[3]	Channel type	QoS class supported	OSPF-MT topologies
HF	9.6 kb/s	Point to point channel	1, 2, 3 and 6	Low Data rate
VHF	2.5 kb/s	Common channel shared among 4 nodes	1, 2, 3 and 6	Low Data rate
UHF	500 kb/s	Common channel shared among 4 nodes	All	High and Low Data rate
SATCOM	64 kb/s	Packet switched service	All except 4	High[4] and Low Data rate

Table 5.1 Approximate channel capacity for the wireless networks (based on different transmission technologies) used in the field test, configured QoS class support and their associated routing topologies.

The other mechanism we used in order to support traffic priority and service quality was the TC environment in Linux. This mechanism is available in both the Thales- and the KDA- ITR-platform. For each network interface we defined a traffic shaper, whose purpose was to keep the traffic transmitted on the interface below a certain threshold, to avoid network congestion. We used the queue configuration at each interface to implement packet scheduling (and thus QoS class priorities) and packet drop-precedence.

We defined two different queue architectures, one for the low data rate interfaces, and one for the high data rate interfaces. For the low data rate interfaces (VHF and HF) we chose to use a strict priority queue with no fairness in the packet scheduling to ensure that the highest priority traffic types were given enough resources, and to utilize the available data rate in the best manner possible. For the high data rate interfaces (UHF and SATCOM) we used the hierarchical token bucket (HTB) queuing structure for Linux, and associated a share of the shaping data rate to each of the QoS classes.

5.2 Test Scenarios

The test network represented a challenging case for automatic traffic priority and routing dynamics since the end-to-end network capacity could change from a comfortable data rate of 500 kb/s to a very restrictive data rate of 2.5 kb/s in no time, due to e.g. vehicle mobility. The scenarios we defined focused on situations where one or more of the vehicles moved and lost

[3] The data rate given here is the maximum available data rate for the radio configurations applied for the field test. Lower data rates could be experienced during the tests due to co-traffic and difficult channel conditions.

[4] The SATCOM link was allowed in the high data rate topology with the additional constraint that we did not allow QoS class 4 (video streams) on this link

connection to one of the radio networks, and had to automatically switch to another wireless network based on a different transmission technology. The heterogeneous network was operated as a flat network, where all vehicles and the HQ were part of a single domain. This was done to study how a detailed knowledge of the complete network topology could improve network utilization. Six scenarios were defined for the field test. Figure 5.3 and Figure 5.4 show two representative ones. The following scenario description and observations are valid for both the Thales and the KDA ITR-platforms unless explicitly stated otherwise.

The Situation Awareness (SA) application was operational on all platforms (including the HQ) in all scenarios. This application was configured to send position updates every 30 sec to a multicast group address. All platform operators sent one text message to all other platforms (vehicles and HQ) during each test. One VoIP flow and one unicast video stream were maintained for each test. The video stream was compressed to an average of 100 kb/s. The full duplex VoIP connection required less than 10 kb/s. The tests were run with a controlled traffic distribution. We placed a high load on the network, and had to rely on the QoS mechanisms to prioritize among the flows, and choose network routes in the best manner.

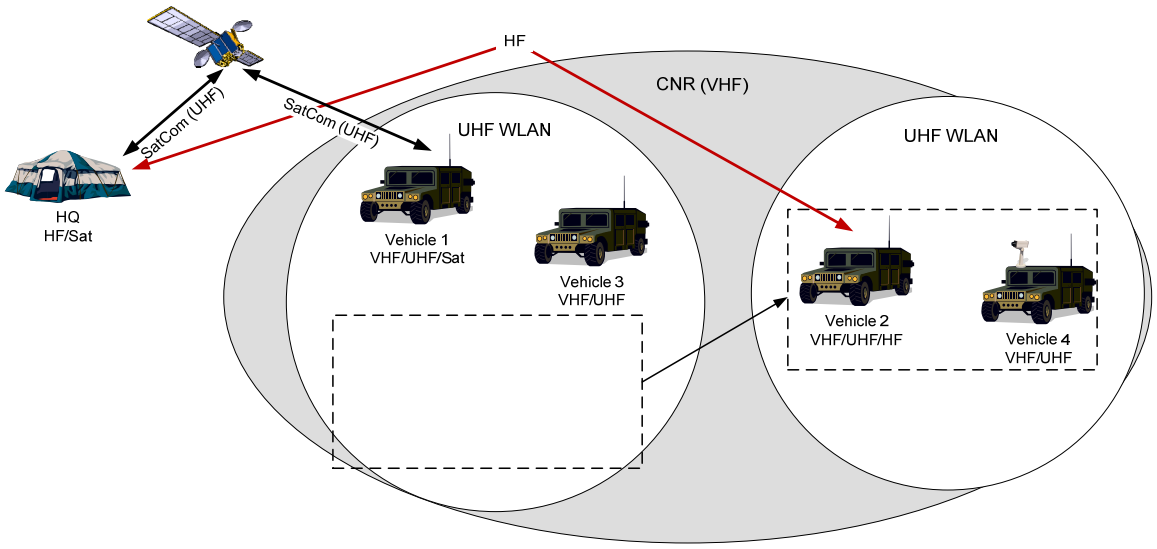

Figure 5.3 Two vehicles on a temporary task communicate with their home unit and with the HQ.

Figure 5.3 represents a scenario where a group of two vehicles is sent on a temporary mission and needs to maintain connectivity with its home unit and the HQ. Communication with the remainders of the home unit must automatically change form UHF to VHF as the group is leaving the UHF coverage. Communication with the HQ must change from the VHF and SATCOM path to the HF connection. The group can communicate internally using the UHF network. In this scenario the SA-data was sustained fairly well. We observed a somewhat lower quality on the position updates in the HQ than in the vehicles. In this scenario we sustained two voice connections, one connection between vehicle 1 and 3, and one connection between vehicle 2 and 4. The voice quality on these connections was quite good; even when vehicle 2 and 4 were driving (together) away from the home unit. The video connection between vehicle 4 and

vehicle 2 experienced high packet losses as the vehicles were moving, but improved when the vehicles in the group stopped at the end position. The text messages were received within an acceptable timeframe. However, some of the messages were automatically retransmitted to the nodes reachable only on the low data rate channels.

Figure 5.4 represents a scenario where a reconnaissance vehicle is sent on a mission and needs to maintain connectivity with its home unit and the HQ. Communication with the home unit must automatically change from UHF to VHF, and finally to a two hop HF and SATCOM path via HQ. The connection to HQ has to change from the UHF and SATCOM route, to the HF link.

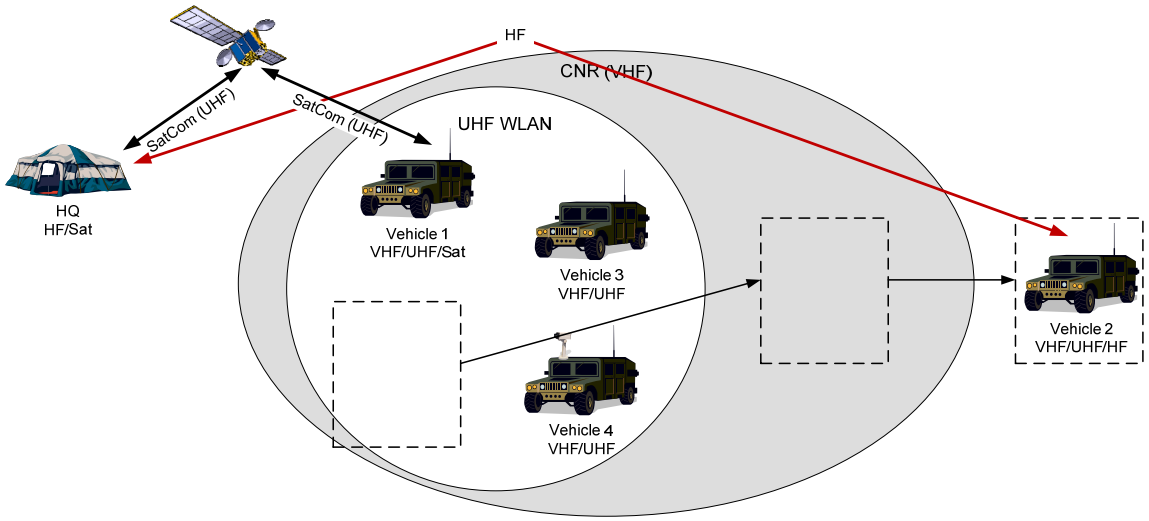

Figure 5.4 A reconnaissance vehicle communicates with the home unit and with the HQ.

When the reconnaissance vehicle reached its end position, all traffic between this vehicle and its home unit had to traverse the HF connection to the HQ. When this happened, we observed degradation in the quality (packet loss) of the SA-data service. However, we were able to sustain a general picture of the whereabouts of the nodes. During this scenario we sustained a VoIP connection between vehicle 2 and vehicle 3 while vehicle 2 was driving away. The VoIP application we used did not time out, thus we were able to talk on and off, as the high data rate routing path was present or lost as the vehicle was driving out of range. We started a VoIP connection between vehicle 4 and the HQ when the other VoIP connection was permanently broken. Now the VoIP connection was sustained on the SATCOM link, which also transported all application traffic (SA-data and some text messages) between the reconnaissance node and the home unit. The VoIP connection experienced some packet loss, but it was possible to maintain a conversation. The quality of the video stream from vehicle 4 to vehicle 1 was acceptable.

5.3 Observations

The observations presented in this report are based on the perceived quality of the services we ran on the test network, as observed by the personnel operating the different platforms. Both ITR-platforms were prototypes where functionality had been prioritized before rigorously testing, thus we encountered some problems due to instability of the ITRs. We also spent much time to find

the correct configuration of the radio links/networks for use with IP traffic. We observed very instable channel conditions for the UHF network in the test terrain. The UHF network was set to use a very low transmission power, due to some co-location problems with this network with high transmission power. Thus the routing information for both the KDA and Thales ITRs, and the topology information for the Thales ITR varied often. This situation made it a challenging task for the test personnel to keep track of the current network connectivity and the observed service quality at the same time. However when the routers were operating correctly, and the radio links/networks were configured correctly, the overall impression of the network performance in all scenarios was good.

For the Thales ITR-platform we reduced the packet rate of the OSPF-MT Hello protocol on the low data rate links to one per minute, thus it may take up to three minutes for the heterogeneous network to detect loss of a low data rate link. The loss of a low data rate link (HF or VHF network) meant (in most cases) that the vehicle was outside the range of any connection to the home network. We felt that long detection times were acceptable for this situation, since it was more important to keep a low signalling load on these channels. The high data rate topology converged quickly because the high data rate links used the default OSPF Hello protocol parameters with Hello interval of 10 sec. For the KDA ITR-platform the TDP was used for routing on the low capacity links. We maintained a higher Hello rate for this protocol (e.g., an interval of 20 sec for HF and 30 sec for VHF).

For the Thales ITR-platform we did experience some difficulties with OSFP-MT on the low data rate HF and VHF links. Synchronizing the OSPF Link State database took a long time over the low data rate links. During the synchronization there was no capacity left for other traffic. This observation came as no surprise, as we had expected to experience several difficulties with the use of protocols intended for fixed Internet in a low data rate tactical MANET. We also observed some unexpected route losses on these links, probably associated with a problem with the Linux driver. Thus this was not a routing problem, but a bug in the implementation.

For the KDA ITR-platform, we observed oscillation in the routing table, the OSPF protocol and the TDP protocol did not cooperate well. At the end of the test period, this problem was solved. We also experienced problems with the multicast protocol. The DVMRP instance that ran in the ITR-platform did not communicate with the DVMRP instance that ran in the UHF network, thus we had to configure an overlay network for multicast also on the UHF network.

The HF radio showed unpredictable transmission delays. The radio was optimized for maximum throughput on a stand-alone HF connection. This optimization is not optimal when the HF link is integrated into a heterogeneous network running a routing protocol with periodic short messages.

Every 30 sec during the tests we fetched a snapshot of the main routing table, the topology tables and the status of the queues (throughput, length, dropped packets etc.) for the different QoS classes. We also stored all data packets sent and received by the PC operated by the test personnel on each platform. From these logs we observed that all data traffic was marked with the correct

QoS class. The queue logs and the snapshot of the routing- and topology- tables verified that the network handled the QoS classes as expected.

We did not run any of the test scenarios with the QoS mechanisms disabled to validate an improvement in network operation and service quality with the QoS mechanisms enabled. Such a test is better performed on a simulator or in a lab environment for simpler quantification of the results.

6 Conclusion

We argue that it is smart to combine wireless networks with different transmission technologies to create a heterogeneous tactical network. This network may seamlessly sustain different communication needs, e.g. long range communication, local high data rate communication and reliable communication. The heterogeneous network may also improve robustness due to an increased number of redundant routes and different radio technologies. However, it is challenging to build a stable and highly available heterogeneous mobile wireless network that support different service qualities and allow mission critical traffic a higher priority. Much more research and experimentation is needed to reach this goal.

Obviously routing protocols intended for fixed high data rate Internet is not optimal for the long range low capacity tactical links. However, with the two Intelligent Tactical IP Router-platforms we have demonstrated the possibility to interconnect a wide range of radio types using standard protocols as a first step, while protocols designed for mobile tactical use become more mature. We have also shown how standard DiffServ-like mechanism for QoS handling can be very useful also for mobile tactical use. DiffServ-like mechanisms combined with multi topology routing provide a flexible QoS architecture that can adapt to changing network topologies.

We intend to continue our research and experimentation with the ITR-platforms in the future. In short term we want to gain experience and collect operational requirements through experimental use in different military units and for different military disciplines. In longer term we want to experiment with, and do research on technologies for future advanced tactical networking, with the Intelligent Tactical IP Routers as an experimental platform. Based on experience from the field test, future work on routing and QoS must involve research on mechanisms that improve the stability of the heterogeneous network (possibly at the cost of some resource efficiency).

References

[1] G.-S. Ahn et al., "SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks," *in proceedings INFOCOM*, New York, USA, pp. 457-466, 2002.

[2] B. An and S. Papavassiliou, "Geomulticast: architectures and protocols for mobile ad hoc wireless networks," *JPDC*, vol. 63, no. 2, pp. 182-195, 2003.

[3] E. Baccelli et al., "OSPF MPR Extension for Ad Hoc Networks." *draft-ietf-ospf-manet-mpr-03.txt* (work in progress), Nov. 2008, http://www.ietf.org.

[4] F. Baker and J. Polk, "Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite." *RFC 4542*, 2006, http://www.ietf.org.

[5] S. Blake et al., "An Architecture for Differentiated Services." *RFC 2475*, 1998, http://www.ietf.org.

[6] M. Booth et al., *NATO Network Enabled Capability Feasibility Study*, Version 2.0, NATO Unclassified, 2005.

[7] R. Braden et al., "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification." *RFC 2205*, 1997, http://www.ietf.org.

[8] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: an Overview." *RFC 1633*, 1994, http://www.ietf.org.

[9] M. Chandra and A. Roy, "Extensions to OSPF to Support Mobile Ad Hoc Networking." *draft-ietf-ospf-manet-or-01.txt* (work in progress), Sept. 2008, http://www.ietf.org.

[10] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing." *draft-ietf-manet-dymo-15.txt* (work in progress), Nov. 2008, http://www.ietf.org.

[11] T. Clausen, C. Dearlove, and P. Jacquet, "The Optimized Link State Routing Protocol version 2." *draft-ietf-manet-olsrv2-07.txt* (work in progress), July 2008, http://www.ietf.org.

[12] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol." *RFC 3626*, 2003, http://www.ietf.org.

[13] C. d. M. Cordeiro, H. Gossain, and D. P. Agrawal, "Multicast over Wireless Mobile Ad Hoc Networks: Present and Future Directions," *IEEE Network*, vol. 17, no. 1, pp. 52-59, 2003.

[14] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations." *RFC 2501*, Jan. 1999, http://www.ietf.org.

[15] C. Danilov et al., "MANET Multicast with Multiple Gateways," *in proceedings MILCOM*, San Diego, CA, USA, 2008.

[16] G. Enemo, *NBF Tenketank - Resultater pr april 2006*, FFI/Notat-2006/01225, 2006.

[17] D. Farinacci et al., "Generic Routing Encapsulation (GRE)." *RFC 2784*, 2000, http://www.ietf.org.

[18] B. H. Farsund, O. I. Bentstuen, and T. Gjertsen, *(U) Sikkerhetsutfordringer i Forsvarets Informasjonsinfrastruktur*, FFI/Rapport-2006/03926, Begrenset, 2006.

[19] FFI, *Forespørsel om tilbud på 4 stk taktisk ruter*, 6.2.2007.

[20] T. Gjertsen et al., *(U) Migrasjon av Forsvarets Kommunikasjonssystemer*, FFI/Rapport-2005/00290, Begrenset, 2005.

[21] D. Grossman, "New Terminology and Clarifications for DiffServ." *RFC 3260*, 2002, http://www.ietf.org.

[22] O.-E. Hedenstad et al., *(U) Prosjekt 1092 NbF Implementeringsplan - anbefalte tiltak*, FFI-rapport 2008/01350, Begrenset, 2008.

[23] IEEE, "*IEEE 802, part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*," 1999.

[24] ITU-T, *DTE/DCE interface for a start-stop mode Data Terminal Equipment accessing the Packet Assembly/Disassembly facility (PAD) in a public data network situated in the same country*, Recommendation X.28, 1997, http://www.itu.int.

[25] ITU-T, *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit*, Recommendation X.25, 1996, http://www.itu.int.

[26] L. Ji and M. S. Corson, "Explicit multicasting for mobile ad hoc networks," *MONET*, vol. 8, no. 5, pp. 535-549, 2003.

[27] B. C. Kim et al., "A QoS Framework Design Based on Diffserv and SNMP for Tactical Networks," *in proceedings MILCOM*, San Diego, USA, 2008.

[28] Ø. Kure and I. Sorteberg, *Network Architecture for Network Centric Warfare Operations*, FFI/Rapport-2004/01561, 2004.

[29] A. Laouiti et al., *Multicast Optimized Link State Routing*, INRIA, Research Report RR-4721, 2003, http://www.inria.fr/rrrt/rr-4721.html.

[30] S. J. Lee, W. Su, and M. Gerla, "On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks," *MONET*, vol. 7, no. 6, pp. 441-453, 2002.

[31] K. Lougheed and Y. Rekhter, "A Border Gateway Protocol 3 (BGP-3)." *RFC1267*, 1998, http://www.ietf.org.

[32] J. Macker, "Simplified Multicast Forwarding for MANET." *draft-ietf-manet-smf-09.txt* (work in progress), July 2009, http://www.ietf.org.

[33] A. Mohammad, O. Brewer, and A. Ayyagari, "Bandwidth Estimation for Network Quality of Service Management," *in proceedings MILCOM*, Orlando, FL, USA, 2007.

[34] J. Moy, "OSPF Version 2." *RFC 2328*, 1998, http://www.ietf.org.

[35] D.-Q. Nguyen and P. Minet, "QoS support and OLSR routing in a mobile ad hoc network," *in proceedings ICN/ICONS/MCL*, Mauritius, 2006.

[36] K. Nichols, V. Jacobson, and L. Zhang, "A Two-bit Differentiated Services Architecture for the Internet." *RFC 2638*, 1999, http://www.ietf.org.

[37] R. Ogier and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding." *RFC 5614*, 2009, http://www.ietf.org...

[38] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing." *RFC 3561*, 2003, http://www.ietf.org.

[39] P. Psenak et al., "Multi-Topology (MT) Routing in OSPF." *RFC 4915*, http://www.ietf.org.

[40] B. Rossow, I. Sorteberg, and M. Hauge, "Multi-Topology Routing in Resilient Tactical Networks," *in proceedings RTO-MP-SCI-187 Symposium on Agility, Resilience and Control in NEC*, Amsterdam, The Netherlands, 2008.

[41] E. M. Royer and C. E. Perkins, "Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol," *in proceedings MobiCom*, Seattle, WA, USA, pp. 207-218, 1999.

[42] W. Shaochuan, T. Xuezhi, and J. Shilou, "AOHR: AODV and OLSR Hybrid Routing Protocol for Mobile Ad Hoc Networks," *in proceedings ICCCAS*, Guilin, China, pp. 1487-1491, 2006.

[43] C. C. Shen and C. Jaikaeo, "Ad Hoc Multicast Routing Algorithm with Swarm Intelligence," *MONET*, vol. 10, no. 1-2, pp. 47-59, 2005.

[44] D. Waitzman, C. Partridge, and S. Deering, "Distance vector multicast routing protocol." *RFC 1075*, 1988, http://www.ietf.org.

[45] E. Winjum, *Er ruting og tenestekvalitet i IP-nett sikkert?*, FFI-rapport 2006/03914, 2007.

[46] H. Zhu and I. Chaotic, "Admission control and bandwidth reservation in multi-hop ad hoc networks," *Comput. Netw.*, vol. 50, no. 11, pp. 1653-1674, 2006.

Abbreviations

AF	Assured Forwarding
AODV	Ad hoc On-demand Distance Vector
BB	Bandwidth Broker
BE	Best Effort
CLI	Command Line Interface
CNO	Computer Network Operation
CNR	Combat Net Radio
COTS	Custom Off The Shelf
DS	Differentiated Service
DSCP	Differentiated Services Code Point
DVMRP	Distance Vector Multicast Routing Protocol
DYMO	Dynamic MANET On-demand
EF	Expedited Forwarding
FOHK	Fellesoperativt hovedkvarter
GAN	Global Area Network
HF	High Frequency (3MHz – 30MHz)
HQ	Head Quarter
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
LAN	Local Area Network
LSA	Link State Advertisement
MAC	Medium Access
MANET	Mobile Ad Hoc Network
MDR	MANET Designated Routers
MLPP	Multilevel Precedence and Pre-emption
MRR	Multirolle radio
MT	Multi Topology
NBF	Nettverksbasert forsvar
OLSR	Optimized Link State Routing
OSPF	Open Shortest Path First
OSPF-MT	Open Shortest Path First – Multi Topology
PAD	Packet Assembly/Disassembly
PHB	Per Hop Behaviour
QoS	Quality of Service
RFC	Request For Comments
RSVP	Resource Reservation Protocol
SA-data	Situation Awareness data
SDR	Software Defined Radio
SMF	Simplified Multicast Forwarding

SPF	Shortest Path First
TC	Traffic Control
TDP	Taclan Discovery Protocol
TOS	Type Of Service
ITR	Intelligent Tactical IP Router
UHF	Ultra High Frequency (300MHz – 3GHz)
VHF	Very High Frequency (30MHz – 300MHz)