FFI-rapport 2009/01894

NATO Narrowband Waveform (NBWF) – overview of link layer design

Vivianne Jodalen, Bjørn Solberg and Svein Haavik

Norwegian Defence Research Establishment (FFI)

28 March 2011

FFI-rapport 2009/01894

1175

P: ISBN 978-82-464-1927-5
E: ISBN 978-82-464-1928-2

Keywords

Taktisk radio

VHF/UHF

NATO STANAG

Combat Net Radio

NATO Narrowband Waveform (NBWF)

Approved by

Torunn Øvreås	Project Manager
Eli Winjum	Director of Research
Vidar S Andersen	Director

English Summary

This report is an updated and final version of a draft report distributed to the NC3B SC/6 AHWG/2 in September 2009. We have kept the same report number in order to avoid confusion.

In coalition operations NATO has a need for a standardized, interoperable combat net radio waveform at VHF and UHF. Work is currently ongoing in NC3B SC/6 AHWG/2 to produce such a Narrowband Waveform (NBWF) standard. NC3A, CRC in Canada, FFI, and now also Kongsberg are taking part in this work. FFI has the responsibility for producing the link layer specification of the standard. The work has been going on since 2007 through the projects 1088 “TIPPER” and 1175 “Gjennomgående kommunikasjon for operative enheter”.

This report presents a technical overview over the link layer design, and the considerations that underpin the design. It also adresses the impact of the requirements and the physical layer on the link design.

In short, the link layer offers simultaneous voice and data services, where the channel capacity is exploited efficiently at any time. Multicast voice (Push-To-Talk) is the most important service, and the establishment of a multicast voice connection will pre-empt data traffic. When multicast voice is not activated in the network, the channel can be exploited efficiently to send data or unicast voice. All nodes in the network get a minimum dedicated channel access to send data or management information. Channel access to send data is based on contention where data with high priority will have the largest probability of accessing the channel. The link layer offers both a reliable and an unreliable packet data service for unicast connections and an unreliable service for multicast.

FFI together with Kongsberg are now producing a final specification of the link layer in the form of a NATO STANAG. Simulations to validate the concept and tune parameters also remain to be done. In addition, a Head STANAG will be produced that describes the relationship between different parts of the NBWF (physical, link and network layers) and the interconnection with other networks.

Sammendrag

Dette er en oppdatert og endelig versjon av en FFI rapport som ble distribuert til NC3B SC/6 AHWG/2 i september 2009. Vi har beholdt det samme rapportnummeret for å unngå forvirring.

Nato har behov for en standardisert, interoperabel nettradio bølgeform på VHF og UHF til bruk i internasjonale operasjoner. Gjennom NC3B SC/6 AHWG/2 arbeider NC3A, CRC i Canada, FFI og i den senere tid også Kongsberg, for å ta fram en slik Narrowband Waveform (NBWF) standard. FFI har ansvaret for å definere link-laget i standarden. Arbeidet har pågått siden 2007 gjennom prosjektene 1088 ”TIPPER” og 1174 ”Gjennomgående kommunikasjon for operative enheter”.

Denne rapporten presenterer en teknisk oversikt over link-lags designet, og de vurderinger som er lagt til grunn for designet. Den beskriver også føringer på designet gitt av kravspesifikasjon og fysisk lag.

Kort beskrevet forteller rapporten om et linklag som tilbyr samtidige tale og datatjenester, der kanalkapasiteten utnyttes mest mulig til enhver tid. Multicast tale (Push-To-Talk) er den viktigste tjenesten, og kanalressurser stilles til rådighet for denne på bekostning av datatrafikk i nettet. Når multicast tale *ikke* er aktiv, kan kanalen utnyttes i stor grad til datatrafikk eller unicast tale. Alle nodene i nettet får en minimum fast tilgang til kanalen slik at de kan sende data eller nødvendige kontrollmeldinger. Tilgangen til kanalen for å sende data baserer seg på konkurranse der data med høy prioritet har størst sannsynlighet for å vinne kanalen. Linklaget tilbyr både en pålitelig og upålitelig pakkedatatjeneste for unicast og kun en upålitelig tjeneste for multicast.

FFI sammen med Kongsberg er nå iferd med å produsere endelig spesifikasjon av linklaget i form av en STANAG. Det gjenstår også simuleringer for å validere konseptet og bestemme parametere. I tillegg jobbes det med en Head STANAG som beskriver forholdet mellom flere deler av NBWF (fysisk, link, nettverkslag) og sammenkobling med eksterne nettverk.

Contents

1	**Introduction**	**7**
1.1	Aim and Scope	7
1.2	Background and relevant references	7
1.3	The need for the NBWF	8
1.4	The NBWF (L) component and ambition level	9
2	**Considerations on NBWF radio subnets**	**10**
2.1	General	10
2.2	Main link layer protocol issues	10
2.3	NBWF physical layer	11
2.4	Security	15
3	**NBWF services**	**16**
3.1	Voice and data transfer	16
3.1.1	Voice communications	16
3.1.2	Transparent data communications	17
3.1.3	Packet data communications	18
3.2	RBCI (Radio Based Combat Identification)	18
3.3	The NBWF reference model	19
4	**Considerations for the MAC design**	**22**
4.1	Physical layer modes – implications for the MAC design	22
4.2	Voice over the NBWF subnet	22
4.3	TDMA frame structure	24
4.4	Relaying of voice and data	26
4.5	Voice and data capacity considerations	29
4.6	Data over the NBWF subnet	32
4.6.1	Random Access data	33
4.6.2	Reserved access data	34
4.7	Selective call	36
4.8	Types of time slots and TDMA frame structure – summary	37
4.9	Quality of service (QoS) functionality	38
4.10	RBCI	39
4.11	Time synchronization	40
4.12	Network management	40
5	**Outlook**	**41**
	References	**42**

Abbreviations 44

1 Introduction

1.1 Aim and Scope

The aim of this document is to provide a technical overview of the framework for the link layer design that will be proposed as part of the NATO standardized Narrowband Waveform (Land), ambition level 1. The waveform is currently in development, and various parts of it are developed by different organizations within NATO countries. This document describes the main services offered by the link layer and the protocols that are needed in order to realize the services. Ongoing simulation efforts at FFI will refine the protocols, but the detailed protocol specification as a result of these simulations is not within the scope of this document. Any discussion and feedback from industry or organizations on our proposal is welcome.

The intended audience of this document will be members of the SC/6 AHWG/2 with technical background. A first draft of this document (without an FFI reference number) was released to the group at the Helsinki meeting in September 2009. This report is the final version which describes *all* major parts of the link layer of the Narrowband Waveform (Land), ambition level 1. There has also been changes to the physical layer design which is reflected in this document.

1.2 Background and relevant references

Over the last few years, much work has been undertaken by the NC3B SC/6 and NC3A to establish wireless reference architectures for NATO. The architectures serve as structures for the communication standards that need to be developed (or are already in place) in order to achieve interoperability between nations.

Reference [1] "Wireless Reference Architecture – non SATCOM (WiRA)" has been developed to support the NATO common funding Capability Package CP0A0101. This architecture addresses the Beyond-Line-Of-Sight services between static elements (NATO headquarters), deployed NATO force elements and the first level of national headquarters. Other architectures address other parts of the communications infrastructure.

There exists no NATO common funded CP for the land tactical domain. Traditionally, force elements in this domain have been equipped with national systems that have not been interoperable with any other nations' systems. This is no longer satisfactory because of the force structures and operational requirements of today. Wireless interoperability needs to be enhanced also in the land tactical domain and at lower echelons of the command structure. So, despite that there exists no CP in the land tactical domain, a reference architecture for this operational scenario has been developed by NC3A. Two NC3A Technical Notes exist that document this work:

Reference [2] “Wireless communications architecture (Land): Scenarios, requirements and operational view”, presents the operational views of this architecture and lists requirements such as which services are needed, data rate, quality of service and security. The requirements have been deduced from a set of NATO scenarios.

Reference [3] “Wireless communications architecture (Land): System and Security Views” presents the systems views of the same architecture. It describes the variety of communication elements that are likely to be found in the wireless land tactical domain in the future, how they should interact, and which elements are needed but remains to be developed. One of the elements that are identified as needed, but not yet existing, is a standardized narrowband waveform with long range capabilities. This narrowband waveform (from here called NBWF) is the topic of this document.

From [2] and [3], operational and system requirements for the NBWF have been deduced. They are reflected in reference [4] together with a description of the ambition level for the waveform, and a subdivision into a NBWF Land component and a NBWF Air component.

The list of requirements in [4] is long, and to us it seems unlikely that all of the requirements can be met within a single waveform constrained to 25 kHz. For instance, we do not believe that a subnet consisting of 250 nodes (requirement 2.04.03) can support mobility management (requirement 2.09.12) and adaptive interior routing and packet relay (requirement 2.09.03). Therefore, our proposal for a NBWF concept makes some prioritizations between the requirements listed in [4]. Simulation studies will show how the basic services can be implemented in the best way, and what the limits for successful operation of these services are.

1.3 The need for the NBWF

Interoperability between multi-national task forces and coalition forces operating within weapon range of one another is a key requirement in the land tactical domain. For frequency bands such as HF and SHF Satcom, NATO standards have been developed that provide the necessary interoperability. For the VHF frequency band frequently used in the land tactical domain, the only standard is S4204 that provides unsecure voice and low data rate only. In the UHF band, S4236 HaveQuick II and S4372 SATURN exist and will be used in the future for tactical operations. There is nevertheless a need for a new non-tactical waveform in the UHF band that can be used for military air traffic control. This new waveform would replace the S4205.

From the information exchange requirements and operational view in [2] it is clear that *a range* of communication systems is needed having different characteristics such as range, throughput, spectrum and infrastructure requirements. One system, maybe the system that will be required in most of the operational scenarios, is that of a *medium range*[1], *low capacity* communication for voice and basic data services such as friendly force tracking and targeting. The range of this

[1] In [3] this system is described as *short* range, low throughput

system is roughly defined as distances from a few kilometres to tens of kilometres, covered typically by UHF and VHF communications. Low capacity is typically less than 64 kbps.

So, because there is a requirement for interoperable communications in the VHF/UHF communication bands, a narrowband waveform for this purpose needs to be standardized. *Interoperability* is the new key functionality that the NBWF will provide compared to fielded systems today. Other new functionality such as higher data rates and improved networking is also desirable, and will be included.

The architecture in [3] describes radio nodes of different complexity ranging from a simple radio node providing a few services and one RF bearer, to a complex radio gateway providing multiple services over multiple RF bearers and networking functionality between them. The NBWF is present in all of these radio nodes/gateways, and is thus a main component in the system architecture. In another system view in [3], the NBWF is shown as an interface component between all levels of command ranging from brigade headquarters down to the sections. In this aspect the NBWF is also an important component.

The system architecture in [3] lists some key technologies that are assumed to be important in the development of a future tactical wireless capability. Common, secure, net-ready waveforms are the first on the list together with software defined radio implementations. The NBWF is mentioned particularly as the first goal towards increased capability for a NATO coalition tactical network.

1.4 The NBWF (L) component and ambition level

The NBWF shall be a tri-service waveform. However, the operational requirements come from the land-tactical domain, and the NBWF shall primarily complement or replace existing CNR waveforms. It shall work at both VHF and UHF frequencies, but we assume that the long range capability of VHF is the most interesting for the pure land domain. For ground-air communications (air-traffic control) UHF frequencies will be used. Because of the longer propagation times expected between an air platform and ground, and also other requirements to networking, the waveform design may be different for the air component of the NBWF. We distinguish therefore between the NBWF Land (L) and Air (A) waveform. The focus of this report and the link layer design at FFI is on the NBWF (L).

Reference [4] defines a base level of ambition for the NBWF (L) in order to bound the requirements for the first version of the waveform. Higher levels of ambition can be reached later by an evolution of the waveform. The base level of ambition includes:

- a waveform supporting secure voice and data services, friendly force tracking and radio based combat identification
- operation on a single RF channel of 25 kHz bandwidth
- basic networking capabilities

2 Considerations on NBWF radio subnets

2.1 General

An NBWF subnet shall provide secure voice and data services to the radio nodes participating in the subnet. In order to achieve this, the protocols on the antenna interface needs to be standardized and be common to all participating nodes:

1. The physical waveform design (such as e.g.: type of modulation, FEC, synchronization, training sequences, physical level PCI, frame construction, misc radio parameters)

2. COMSEC (such as e.g.: crypto system, keys, PCI e.g. IV exchange)

3. Link layer protocol (such as e.g.: MAC , ARQ)

4. Network protocol (such as e.g.: routing protocols, header compression)

5. Radio network radio management protocols (such as e.g.: net entry/exit)

All these protocols must be specified in detail in order to provide interoperability at the radio channel level, which is a main target of the NBWF development. To some extent these protocols will interdepend, in particular if high overall protocol efficiency is desired. In particular, there will be a tight relationship between the MAC protocol and the physical layer protocol.

Reference [5] presents a draft specification proposal for the *physical layer* of the NBWF. In order to achieve interoperability on the air it must be complemented by all relevant aspects of point 2 – 5 in the above list, in which case the final NBWF specification becomes a true *networking* waveform specification.

Moreover, terminal functionality like voice coding and possibly a TCP proxy, which may be implemented in the radio, must obviously also be subject to specification/standardization.

2.2 Main link layer protocol issues

FFI has undertaken a task of proposing a link layer protocol for an NBWF subnet. The link layer protocol must be able to handle both voice and data traffic from various applications. The data traffic from all applications is based on IP, but it may have widely differing characteristics as to message (and packet) length, importance (priority) as well as different requirements for packet delivery delay and reliability. The MAC protocol is responsible for the sharing of the physical channel between the various nodes with traffic to send. The transmission on the channel will be bursty. Various classes of MAC protocols were considered initially [6]. However, the real-time nature of the voice traffic leads to a tight requirement on end-to-end transfer delay. Since it is difficult to achieve this tight value for a stochastic MAC protocol (e.g. a random access protocol), it was decided that the MAC protocol should be based on a TDMA structure with a suitable reservation mechanism. We propose that the TDMA protocol should have the following characteristics:

- be fully distributed, i.e. no “master” node used
- provide efficient operation in multi-hop as well as single-hop environment both for voice and data traffic
- provide a minimum data capacity C_{min} to any node in the subnet
- be scalable to different subnet sizes
- allocate the additional available capacity according to the priority of the traffic waiting to be served in the various nodes
- make sure that the subnet capacity is used for the transfer of the highest priority traffic even under high load conditions by pre-empting lower priority traffic
- share available data capacity on a fair basis
- provide a rapid set-up of voice time slots after a push-to-talk operation
- enable the transfer of digitized voice without introducing unacceptable end-to-end transfer delays
- minimize the “idle time” of the time slots, i.e. minimize the relative time the capacity of a time slot is not used due to an ongoing reservation/release process or due to “confusion” as to its usage
- handle dynamic data rates and dynamic message lengths efficiently

These requirements have strong influence both on the choice of the TDMA frame parameters as well as the protocol for allocation/de-allocation/control of time slots. The price paid for dynamic resource allocation will be increased signalling traffic.

The link layer is responsible for delivering the data packets between any two nodes in the subnet. The importance of a safe packet delivery will vary between the different applications and therefore both a reliable and a non-reliable service should be provided by the link layer.

Another factor that will have strong influence on the TDMA protocol is the properties of the physical layer. Before we proceed with the link layer discussion, we summarize some of its key qualities that are of importance to the higher layers of the NBWF protocol.

2.3 NBWF physical layer

Reference [5] presents the last draft (Draft 4) of the proposal for a STANAG for the NBWF physical layer. The physical layer draft proposal is of a generic nature, enabling more uses of it than only for the NATO NBWF. The NATO NBWF will constitute one “profile” of its use, and the profile will be defined in terms of a parameter table.

Figure 2.1 illustrates the structure of the generic physical layer waveform proposal, as applied to a secure burst transfer of a MAC PDU.

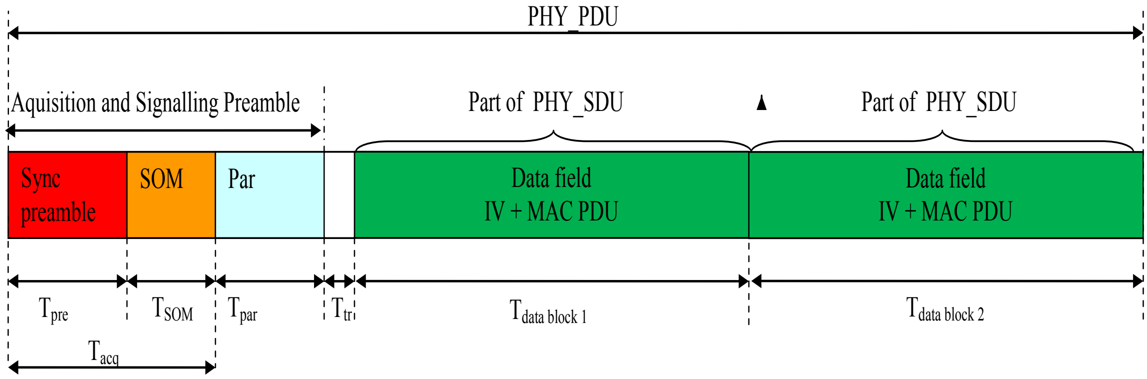

Figure 2.1 The structure of the NBWF physical layer burst waveform

A physical layer PDU comprises the following fields:

- The sync preamble field, the main purpose of which is to allow receivers to extract frequency information of a burst transmission. It consists of a CW signal and the duration is 1.5 ms (T_{pre}).

- The Start Of Message (SOM) field, the purpose of which is to define the end of the acquisition field and start of information data. Additionally the SOM provides symbol timing and phase reference. Two SOM words are defined; one indicates a regular transmission and the other one indicates the presence of a short transmission burst. The duration of the SOM is 2.1 ms (T_{SOM}) and it is transmitted at the lowest symbol rate.

- The Par field comprises physical layer PCI, i.e. protocol information that is needed to secure a successful reception of the data field of the burst, such as data rate, interleaver length, burst length, and the possible use of midambles. The length of this field is 12 information bits which is block coded using a Golay (24, 12) code. The block code is sent twice resulting in a net code rate of ¼. The duration of the Par is 1.6 ms (T_{par}) and it is transmitted at the lowest symbol rate. This field is absent in case of a short transmission burst. A slightly different PAR which includes some parity bits for error check is currently considered.

- The transition field does not carry information, but is included to allow for some changes in the signal processing in the receivers (changes in decimation/interpolation/filters). To our understanding, the need for this field is caused by a change in symbol rate between the Par field and the data field. The duration of the transition field is 0.1 ms (T_{tr}).

- The data field comprises the information to be transferred by the physical layer, i.e. the MAC PDU and the crypto initialization vector (IV). The data rate (and the symbol rate) can be chosen for each individual burst as specified by the Par fields.

In the current version [5] of the physical layer there is no midamble defined that can be used for accurate channel estimation and equalization. However, the need for midambles is possibly there, particularly at the higher data rates, and this is currently being considered.

The generic physical layer allows a reinsertion of the sync preamble field and the SOM, if this is required because of a very long burst duration. The reinserted preamble and SOM is transmitted at the lowest symbol rate and it enables frequency tracking and resynchronization. There is no need for resynchronization of the NBWF because of the short time duration of a slot and the relatively few number of slots that can be merged. This will limit the burst durations.

The “family” of waveforms and user data rates offered by the NBWF physical layer draft 4 specifications [5] are shown in Table 2.1 along with the associated symbol rate on the channel. The modulation is Continous Phase Modualation (CPM) concatenated with a convolutional encoder. Also shown in this table are simulated values of the required E_s/N_0 for a block error rate of 0.1 using non-coherent detection and an interleaver (block) duration of 12 ms [7]. Corresponding E_b/N_0 and SNR in 25 kHz bandwidth are calculated. All modes comply with the requirement of 99% power within 25 kHz, but not with the spectral mask of S4204 Edition 3 (requirement 2.07.03 of [4]).

Mode	User Data rate [kbit/s]	Channel symbol rate [ksymbol/s]	E_s/N_0 [dB] @ BLER = 10^{-1}	E_b/N_0 [dB] @ BLER = 10^{-1}	SNR [dB] in 25 kHz BW @ BLER = 10^{-1}
N1	20	30	1.7	3.5	2.5
N2	31.5	42	6.95	8.2	9.2
N3	64	80	13.1	14.1	18.2
N4	96	128	17.55	18.8	24.6
NR	10	30	-0.7	4.1	0.1

Table 2.1 Summary of the data rates (within the data field) of the proposed modes in [5], along with simulations of communications efficiencies. BLER is Block Error Rate.

The NR mode has been designed to operate at very low SNR values achieving long range coverage. This mode will not be used for the NBWF.

We note that there is a fairly strong SNR requirement at the two highest rates. This means that the radio range of these modes will be quite noticeably reduced as compared to the range at the lowest bit rate.

The reduction of radio range with increased data rate implies that more connections will be multihop when rates are increased, provided that the NBWF physical subnet coverage shall be similar to current VHF CNR networks in operation. For example, the SINCGARS CNR radio has maximum planning range [8] of 10 – 40 km for digital voice using a 50 W vehicular node. The use of dedicated relay stations increases the SINCGARS communications beyond this, if needed.

The following exercise aims at estimating the achievable ranges of the NBWF modes. Since the radio range is heavily influenced by the actual topography of the link; range values presented in the following will be indicators based on empirical data from [9].

Reference [5] offers a model for calculating the path loss. However, calculating the radio range of existing tactical VHF radios using this model seems to give highly exaggerated values. For this reason we have instead used the Egli model [9] to estimate the median range of the various modes. The median propagation loss is normally assumed to vary with distance according to $d^{-\gamma}$, d being the distance between the radio nodes. In the Egli model, the exponent γ has the value of 4.

The radio range estimates presented in Table 2.2 for the various NBWF modes are based on the Egli model in [9]. The referenced Egli paper also includes empiric information on the statistical variation of the propagation loss which we use in the table. An AWGN channel is assumed, i.e. no dispersion due to multipath occurs. The (theoretical) SNR data of Table 2.1 have been used. The following assumptions apply:

Carrier frequency: 60 MHz (approximately midband in tactical VHF frequency range)
Transmit power: 50 W (vehicular)
Effective antenna gain = 0 dBi
Antenna heights: 2.5 m
Effective receiver noise factor: 13 dB

Mode	User Data rate [kbit/s]	SNR [dB] in 25 kHz BW @ BLER = 10^{-1} 2)	"Egli" median range at 60 MHz, vehicular 50 W, rural [km]	90% probability of higher range than [km]	10% probability of higher range than [km]	Egli median range relative to the range at lowest rate (mode N1)
N1	20	2.5	22,0	13,1	36,9	100 %
N2	31.5	9.2	15,0	8,9	25,2	68 %
N3	64	18.2	8,9	5,3	14,9	40 %
N4	96	24.6	6,1	3,6	10,2	28 %
NR	10	0.1	25,2	15,0	42,3	115 %

2) Simulated values from [7] and calculated in table 2.1

Table 2.2 Estimates of radio range for the proposed NBWF modes

In an unknown topography, the range must be treated like a probabilistic parameter. Therefore, Table 2.2 also presents estimates of the 10% and 90% quantiles for the range distributions in addition to the median range. We notice that there is an approximate 1:3 ratio relationship between these quantiles. The last column presents the median ranges as a percentage of the median range of mode N1. This metric is independent of the assumptions made for estimating the absolute range, and, in fact, only relies on the propagation loss to follow a $d^{-\gamma}$ relationship and that γ has the value of 4 (if γ is less than 4, the relative range at higher data rates will be even further reduced).

A legacy CNR radio may have a sensitivity of -116 dBm for a 16 kbit/s digital voice mode at BER = 0.1. With the above assumptions, this gives a range performance similar to that depicted for mode N1. However, NBWF mode N4 must be expected to offer a range of approximately 1/4 to 1/3 of the range of 16 kbit/s digital voice in a legacy CNR.

2.4 Security

According to the requirements in [4] the NBWF (L) shall support secure voice and data with information confidentiality up to NATO/Mission/National SECRET. It shall provide traffic flow security at a defined minimum level and other non-confidentiality protection such as authentication. Finally, it shall support encryption standards external to the waveform in line with NATO's encryption modernisation programme (for instance SCIP or NINE).

This subject has been discussed in the AHWG/2 with the consultation of security experts in NATO, and a policy paper for the security aspects of the NBWF has been produced [10]. It states that both the information domain and transport domain needs protection, but the protection requirements are different for the two domains and they should be separated.The information domain is protected by properly chosen COMSEC and the transport domain is protected by Air Interface Encryption at the link level. The latter includes protection of radio net and control information, in addition to protecting the information data being sent.

The following figure illustrates the security architecture chosen for the NBWF. A basic security level is provided by the radio node itself, typically up to NATO Restricted. This will protect both the information content and the radio control information up to for instance the Restricted level. It requires sufficient number of bits in the PCI of the MAC layer to be reserved for (parts of) a crypto initialization vector[2] (IV). If this protection level is sufficient also for the information being sent over the NBWF subnet, no other protection mechanisms are needed. If a higher level of confidentiality is needed, the protection needs to be provided externally to the NBWF waveform, for instance through an external SCIP or NINE device.

This basic security constitutes an air interface encryption (AIE). The AIE provides only a protection of the radio waveform over the air, and no protection in the data network of which the NBWF radio node may be a part.

[2] The crypto IV is necessary in order to generate the key stream used for encryption/decryption.

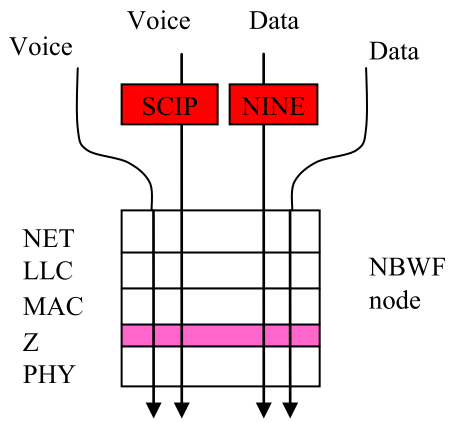

Figure 2.2 Illustration of security architecture for the NBWF

3 NBWF services

3.1 Voice and data transfer

The prime services offered by an NBWF subnet are secure voice and data transfer. The traffic will be generated by and terminated by various Command and Control end user applications using standardized (and not application-specific) communications interfaces, wherever possible. Applications may run internally or externally to the radio node.

3.1.1 Voice communications

The following types of secure (up to NATO restricted) voice services are provided:

1. Multicast voice (point-to-multipoint, PTT)
2. Unicast selective call (point-to-point, PTT)

In our design of the NBWF link layer we have given priority to the multicast voice service which will have advantages over the unicast selective call service.

The NBWF node must, according to the requirements [4], support the following vocoders without transcoding:

1. STANAG 4591 MELPe @ 2 400 bit/s
2. G729D @ 6 400 bit/s
3. STANAG 4209 CVSD @ 16 kbit/s

In addition, we propose that a voice service based on the STANAG 4591 MELPe @ 1200 bit/s vocoder should be considered as an option for use in situations where a longer voice delay is permitted.

The STANAG 4591 MELPe 2 400 bit/s vocoder is the default vocoder used by the NBWF. The G729D and the STANAG 4209 CVSD vocoders are primarily intended for communications with terminals in subnets where STANAG 4591 coding is not an option. The use of these latter two vocoders may result in decreased radio coverage in the NBWF subnet compared to that of MELPe transfer, since the use of higher data rates at the physical layer may be required.

We propose to use *a transparent data service* for the transfer of speech, by a suitable allocation of the time slots of the TDM structure of the channel. This gives the most efficient use of the gross capacity of the time slots, avoiding the extra protocol overhead of a packet data service. Therefore, even though the speech transfer takes place by transmitting bursts in reserved time-slots, there will be no VoIP formats on the air interface. However, it is presumed that the VoIP formats may be used at the user interface as required.

The 2 400 bit/s MELPe coded voice is organized in frames comprising 54 bit, with frame duration of 22.5 ms. The algorithmic delay of the coder/decoder function is about 45 ms. The output of the voice coder can be either streamed or packetized. In the latter case the MELPe frames are octet aligned, and a higher rate than 2 400 bit/s is required at the physical layer.

According to the requirements in [4], the NBWF shall also be capable of supporting external encryption standards such as SCIP and NINE. In future communication networks we anticipate that external SCIP devices will be able to communicate across the NBWF subnet by establishing a SCIP over RTP session [18] with the local NBWF node. The RTP packets containing the SCIP information arriving at the local NBWF node will have to be unwrapped and transmitted as MELP speech using the transparent data service described in the previous sections. SCIP point-to-multipoint traffic will be sent in reserved timeslots for multicast voice, and SCIP point-to-point traffic will be sent in timeslots appropriate for selective calls (described in chapter 4).

Current SCIP devices running the circuit switched "blank and burst" mode will have to reserve a transparent data transfer service described in the next section.

The SCIP protocol will have to be run in a mode with pre-placed keys, since the NBWF subnet will not have enough resources to handle capability exchanges and negotiations between the end terminals.

3.1.2 Transparent data communications

Note:
There are no explicit requirements for a transparent data transfer service stated in [4]. By transparent data transfer service we mean a transfer of a bit stream at a specified rate, delivering the received bit stream with or without bit errors, and with no constraints on the duration of the bit stream. This type of service is a very basic physical layer service, and is offered by essentially all present VHF CNRs. We propose that this transparent data service is made available for use by an external terminal for special applications for which an IP packet service is unsuitable or inefficient.

A secure transparent data transfer service is offered at the following data rates:

1. 1.2 kbit/s
2. 2.4 kbit/s
3. 6.4 kbit/s
4. 16 kbit/s

These rates are the *user data rates* which are lower than the channel rate of the burst transmitted on the air. The MAC protocol will assign the capacity according to the TDMA protocol. The transparent data service is proposed as a half duplex service in order to economize with the available capacity in a NBWF subnet. A half duplex transparent data transfer service will probably be adequate to serve applications like circuit switched SCIP and the transfer of speech traffic with coding according to G.729D (6.4 kbit/s) or STANAG 4209 (CVSD @ 16 kbit/s).

3.1.3 Packet data communications

A secure (up to NATO restricted) packet data transfer service based on IP will be available. This IP service will serve different data applications, including, but not limited to, situation awareness, targeting and messaging systems. Higher confidentiality levels must be provided by node-internal or external IP crypto devices such as NINE, or by application layer security.

The following type of secure (up to NATO restricted) packet data services is provided:

1. IP unicast ("point-to-point")
2. IP multicast ("point-to-multipoint" with the destination group specified by a dedicated address)
3. IP radio broadcast (a packet transmission from one node to whichever neighbour node that can receive the packet). This type of service is per definition not subject to relaying and is limited to communication to neighbouring nodes.

Support of Quality of Service (QoS) shall be provided. However, restrictions will apply compared to general IP networks, due to the inherently low capacity of the NBWF subnet. QoS policies of an NBWF subnet should as far as possible be harmonized with those of the tactical area network.

The IP multicast and radio broadcast services will be based on a non-ARQ link protocol and, hence, offer only non-reliable packet transfer. The IP unicast service offers both a reliable packet transfer (i.e. using ARQ link protocol) as well as a non-reliable packet transfer.

3.2 RBCI (Radio Based Combat Identification)

The purpose of RBCI is to identify friendly forces within an area that is a weapon target. RBCI is a "last second" action of a weapon deliverer to make sure that friendly forces are not attacked. If a friend is identified within the area, the weapon delivery is immediately aborted. The nodes in the NBWF subnet shall be able to respond to an RBCI interrogator signal, without having dedicated hardware for this purpose. The time delay requirement for an interrogation and response is as short as 1 second (to be confirmed). This strong requirement is set by the vulnerability of a helicopter being the weapon deliverer (and interrogator). The previously called NC3B SC/7 AHWG/5 (Air-to-surface Identification Group) is working on the requirements for RBCI.

There may be many NBWF subnets on the ground, so the interrogator is not affiliated to any one subnet. The interrogator can not be assumed to be synchronised to the subnets, so the whole process is unsynchronized. The NBWF protocols will interrupt their normal communications mode in order to search for an interrogation at a separate channel. This must occur often enough to make sure that an interrogation can be detected and a response sent within one second. After a brief search interval the NBWF node will return to its normal communications mode unless an RBCI interrogation signal is detected. In the latter case the responder function will remain active and in control of the radio until the RBCI response is sent.

The main issue for the NBWF design concerning RBCI is how RBCI can be accommodated by the NBWF subnets on the ground. That will be described in this document. A second issue is whether the RBCI interrogation and response can be conducted using the NBWF waveform itself. An important question here is if resilience against jamming is required for the RBCI exchange. If that is the case, the NBWF (L) fixed frequency waveform is not adequate. This topic will not be described further here.

3.3 The NBWF reference model

A reference model for the NBWF and associated external entities is shown in Figure 3.1. This reference model is described in more detail in [16]. The figure shows the services of the NBWF and protocols at different OSI layers. NBWF service access points are located at the red horizontal line. Protocols above the red line can be implemented internally or externally to the NBWF node, and are *not* part of the NBWF specification. However, they are needed in order to interface applications to the NBWF. For instance, the stripping of RTP packets (comprising SCIP) arriving at the Ethernet interface of the radio and the conversion to MELPe packets to be sent over the NBWF, will take place in the protocol entity called MV Applications (or SC Applications) in the figure. The voice service is split in two different services; multicast voice (MV) and selective call (SC), due to their different treatment at the MAC layer.

The reference model is divided into a user plane, a control plane and a management plane. They all share the same Base MAC, AIE and PHY layer. Protocols of the control plane connect/disconnect links and share the resources according to QoS policies. Protocols of the user plane delivers the user data according to requirements set by the applications, and protocols of the management plane does the same with management data such as routing information.

In the figure the term "Connection Oriented transport" has been used. This refers to a reserved access to the channel where the reservation has been confirmed by one-hop neighbours in the network. In the rest of the report the term "reserved access" is used, instead of "connection oriented".

The reference model has been used in the implementation of the simulator [12], [13], [14] and [15].

A glossary is included here for help, but for further understanding of the reference model, we refer to [16].

3aPDP - 3a Packet Data Protocol
CAC – Call Admission Control
CO – Connection Oriented
CL – Connectionless
FA – Fixed Access
IPoA – IP over Air
LLCM – Logic Link Control Management
LLCU – Logic Link Control User data
MV – Multicast Voice
SAP – Service Access Point
SC – Selective Voice
TD – Transparent Data

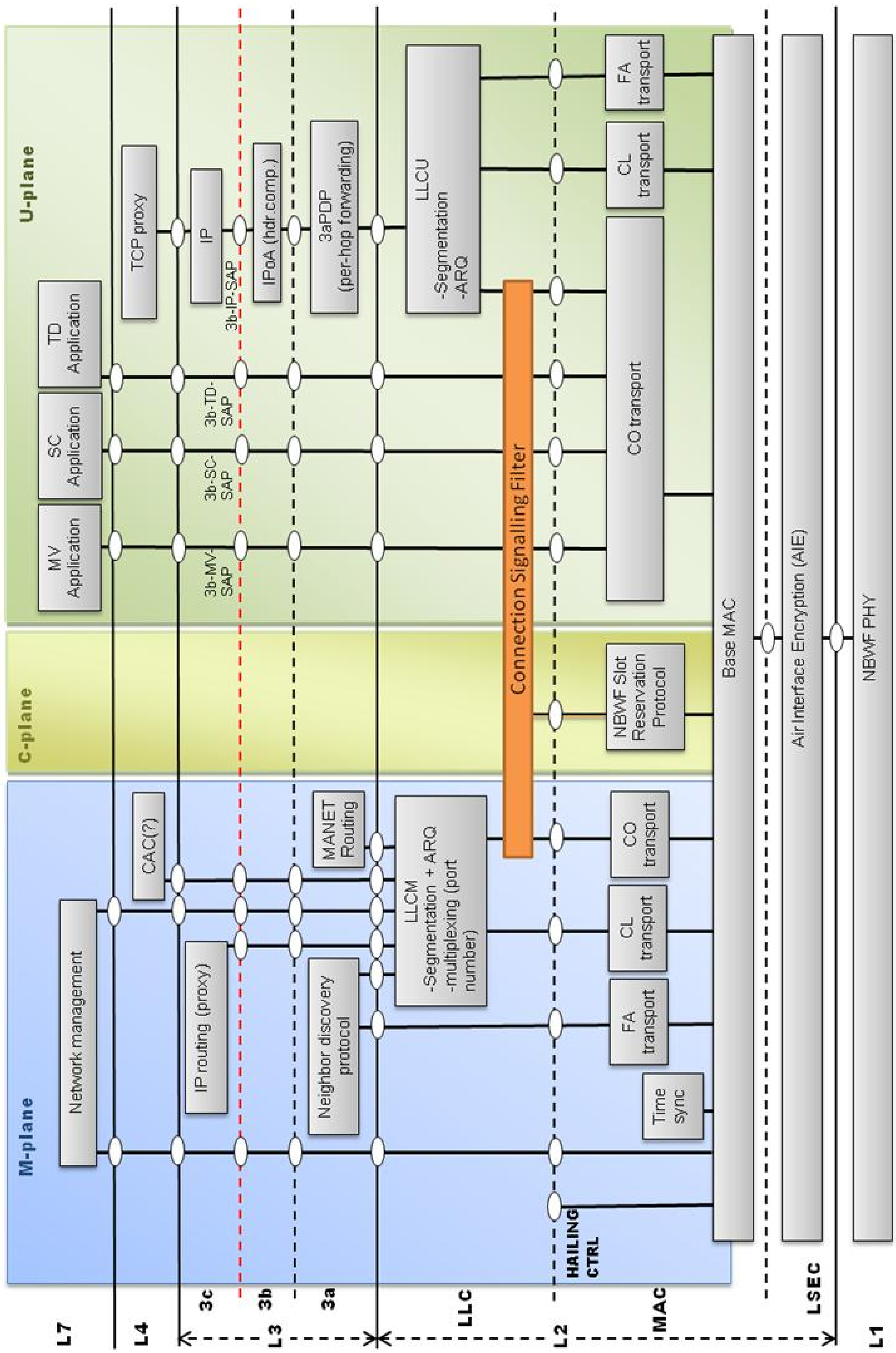

Figure 3.1 Reference model for the NBWF

4 Considerations for the MAC design

4.1 Physical layer modes – implications for the MAC design

The range performance and data rates of the proposed set of waveforms were described in Section 2.3. There is a large difference in the radio range of the N1 (20 kbps) mode and the N4 (96 kbps) mode. The N1 mode will reach three to four times as far as the N4 mode, which means that several relays will be needed for the N4 mode in order to cover the same operational area as the N1 mode. However, the transmission time is shorter for the N4 mode. To compare the two modes we calculate the time required to transmit a ~200 ms segment of MELPe encoded speech (2.4 kbps). Taking into account the time required for the physical layer PCI (shown in Figure 2.1) we find the time duration to be 32 ms for N1 and 13 ms for N4. If the whole operational area is just covered by one transmission of N1, the N4 will need to be relayed several times depending on whether it is a unicast to one particular node or a multicast destined for several nodes, and the duration of the transmission will be n times 13 ms. We see that with more than one relay, it will be advantageous to use the N1 mode, and with such a large range difference between the N1 and the N4, many relays will probably be needed. Mobility of the nodes will increase the need for management traffic, and more so for the N4 mode than for the N1 since network topology changes will occur more frequently for the N4 mode. Thus the traffic load (including management) will be higher when using the N4 mode.

We conclude that for broadcast/multicast traffic it is particularly wise to use the lowest data rate to reach as many nodes as possible in one radio hop. The conclusion is different if the topology of the subnet is such that all nodes can be reached in one hop by using a higher data rate, but we believe this is not a typical characteristic of an NBWF subnet.

The N1 mode is a robust mode similar (or better) in range performance to legacy CNRs at the same data rate. This mode satisfies the requirement to the NBWF to offer propagation ranges similar to current VHF capabilities [10, paragraph 1.01.15]. Only 1-2 relays are needed to reach a large geographical area (> 50 km). We believe that this mode will be frequently used because of its range performance. We have therefore based our MAC design on this mode, and aimed at optimizing protocol functions for this 20 kbps mode. However, other modes at the physical layer can be used with our MAC as well, but the efficiency of the MAC protocol becomes lower for these modes. It makes sense to provide the highest efficiency for the mode with the lowest capacity. For unicast traffic, adaptive data rate will be possible.

4.2 Voice over the NBWF subnet

The transfer of secure voice is a delay sensitive service, even if the voice transfer is operated on a push-to-talk basis. The maximum end-to-end voice transfer delay within an NBWF subnet is required to be either 250 ms ([4], para. 2.01.08) or 500 ms ([4], para. 2.0.2.05). Voice and data traffic must be handled by the subnet "virtually simultaneously"[3] in order to comply with both

[3] We use the term "virtually simultaneously" loosely to indicate that fragments from both services are handled well within the transfer delay requirements

voice and data delay requirements. Simultaneous transmission of voice and data also leads to a better utilisation of the channel since voice does not require all of the capacity at the physical layer. For the NBWF MAC layer, these requirements lead to the choice of a reservation protocol based on TDMA.

The voice traffic is transferred in periodic bursts in reserved time slot(s) within a TDM frame structure. This means that the voice traffic needs to be packetized at some protocol level. The allocation of time slots provides a channel with some latency, but with very low (or no) *variation* in the latency. The information transferred in the time slots is the output of the vocoder preceded by some PCI from the NBWF protocols. We propose *not* to use IP technology for wrapping of each voice packet (i.e. voice burst) on the channel. Although feasible, this would only increase the necessary PCI to be transferred, by adding PCI generated by protocols at layer 3 and above to each transmission. To save PCI, we propose to only add necessary PCI from the MAC and the crypto IV to the voice information transmitted in each burst.

This approach does not prevent that *interfacing* of the radio can be done according to VoIP standards. In this case, the coded voice in standard VoIP packets may be unwrapped and, if necessary, transcoded using a low rate vocoder (such as G729D or STANAG 4591). Then the voice payload will be transmitted in the allocated time slots, but without any PCI from the IP layer and above. Any IP PCI that needs to be known by the NBWF receiver node (e.g. to reassemble the received voice to VoIP packets) is transferred in an initial control packet. Hence an NBWF radio is able to operate with either analogue or VoIP interface signals.

An NBWF subnet is required to transfer voice with different vocoders [4] operating at data rates of 2.4 kbit/s (STANAG 4591), 6.4 kbit/s (G.729D) and 16 kbit/s (CVSD, STANAG 4209). We assume this means that any NBWF subnet shall be able to allocate sufficient time slots to provide the required capacity of these vocoders, given that this capacity is available. The number of time slots needed per frame (and per hop) used for handling one voice call will depend on the data rate of the vocoders, the selected transmission mode (with rates as defined in Table 2.2), and is also to some degree influenced by the PCI added by the NBWF protocols. This is subject to a discussion later.

Voice communication and data applications shall share the capacity of the NBWF subnet. We assume that the major portion of voice traffic will be broadcast/multicast, in which case relaying will always be required in multihop topologies. If time slots are permanently allocated for the multicast voice service, significant parts of the subnet capacity would be wasted during periods with no voice activity. In order to avoid this loss, we propose a scheme where only a basic capacity for a rapid call setup signalling is permanently allocated. For selective voice calls (point-to-point) there is no fixed capacity allocated for call setup signalling, and the signalling must compete with data reservations.

The purpose of this signalling is to allocate/de-allocate the time slots necessary for the transfer of the coded voice. If necessary, it will pre-empt the data traffic that use time slots which will be required for the voice traffic. The PTT action preceding every talk spurt triggers a signalling sequence allocating dynamically time slots for the sender node and, if applicable, the relay node(s). At the end of the PTT action the signalling is completed and the dynamically allocated time slots will be de-allocated. Upon arrival of the next talk spurt, which normally is generated from another source node, a new signalling sequence will be exchanged, resulting in a new and possibly different allocation of time slots for the source/relay nodes of this next talk spurt.

The signalling procedure which consists of an RTS signal from the sender node and a number of CTS signals from one-hop neighbours, also ensures that the two-hop neighbours of the sender node become aware of the ongoing talk spurt, and make them refrain from transmitting in the occupied time slots.

This signalling procedure for the allocation of time slots for each talk spurt needs to be very efficient in order to achieve a short time delay from the PTT action until the channel resources for the voice transfer is allocated. This delay requirement, as given in [4], is 250 ms, which is a value that may be hard to achieve in some subnet topologies.

4.3 TDMA frame structure

Since the voice application is very important in the NBWF subnet, the frame structure of the TDMA protocol has been chosen based on the maximum tolerable delay of voice (~250 ms, ref [4]) and the MELPe frame length (22.5 ms at 2400 bps).

The voice will be subject to a burst transmission as governed by the TDMA protocol. In each burst the data information will be preceded by an acquisition and signalling preamble field (see Figure 2.1). The duration of this field is approximately 8 ms. Assuming a burst transmitted at the 20 kbit/s rate (mode N1) and comprising a payload of exactly one MELPe frame (54 bits), the on-air duration of the payload would be 2,7 ms. Adding the duration of the preamble field, the transmission would be highly inefficient. For this reason one transmission burst will have to comprise several MELPe frames. The more MELPe frames packed in a burst, the higher efficiency will be obtained. However, the speech transfer delay will also increase. Therefore, the number of concatenated MELPe frames per burst must be limited according to the delay that can be tolerated.

If we choose the MELPe frame length of 22.5 ms as the basic slot size and a buffering time of nine slots in our TDMA protocol, we get a burst repetition rate of 202.5 ms. The transmission time is about 37 ms (assuming 20 kbit/s mode and some protocol overhead). With an additional 45 ms algorithmic delay this represents a total voice delay of almost 300 ms on a half duplex link without relaying. The cost of a relaying process will in addition be $n \cdot 22{,}5$ ms where n is the number of time slots needed to send the buffered voice (i.e. n=2 for the 20 kbit/s mode).

The choice of nine slots in a TDMA frame makes sense also when transmitting 1200 bps MELPe. Six longer MELPe frames (each 67.5 ms represented by 81 bits) can be fitted into two time slots *every other* TDMA frame of 202.5 ms (using the 20 kbit/s mode). However, a delay of 500 ms must then be tolerated.

When nine 2400 bps MELPe frames are buffered and then sent, the time to transmit them depends upon the physical layer data rate and the protocol overhead at the link and physical layer. If the data rate is sufficiently low, two time slots are needed in order to transmit nine MELPe frames.

The offered link data rate of a connection using *one single slot* per TDMA frame can be calculated as follows:

Duration of acquisition and signalling (PHY PCI) T_1= 8 ms [4]
Available time for data transmission: 22.5 ms – 8 ms = 14.5 ms
Physical layer data rate: R_1
Number of bits transmitted at R_1=20 kbps (N1): 20 kbps · 14.5 ms = 290 bits
Of these, approx 100 bits (K_2) are assumed to be crypto IV and link PCI
User data transmitted per 22.5 ms time slot T_s: 290 – 100 = 190 bits
TDMA frame duration: T_f=202.5 ms
Link data rate R_2: 190 bits/202.5 ms = 938 bps

The formula that expresses the link data rate R_2 as a function of the number of slots merged (n) is as follows:

$$R_2 = \frac{(n \cdot T_s - T_1) \cdot R_1}{T_f} - \frac{K_2}{T_f}$$

The formula assumes optimum length interleavers. The link layer data rate versus the number of merged time slots for various physical layer data rates is shown in Figure 4.1. The required link data rates for the various vocoders are also shown in the figure. Thus, if 20 kbps is the data rate used at the physical layer, *two* time slots are needed in order to service the 2400 bps STANAG 4591 voice. Also at 32 kbps data rate, two time slots are required, whereas for 64 kbps one time slot is sufficient. For the other vocoders mentioned in Section 3.1.1, the required link data rate is higher, and the relationship between the number of required time slots and the physical layer data rate can be seen in Figure 4.1.

[4] This is an estimate

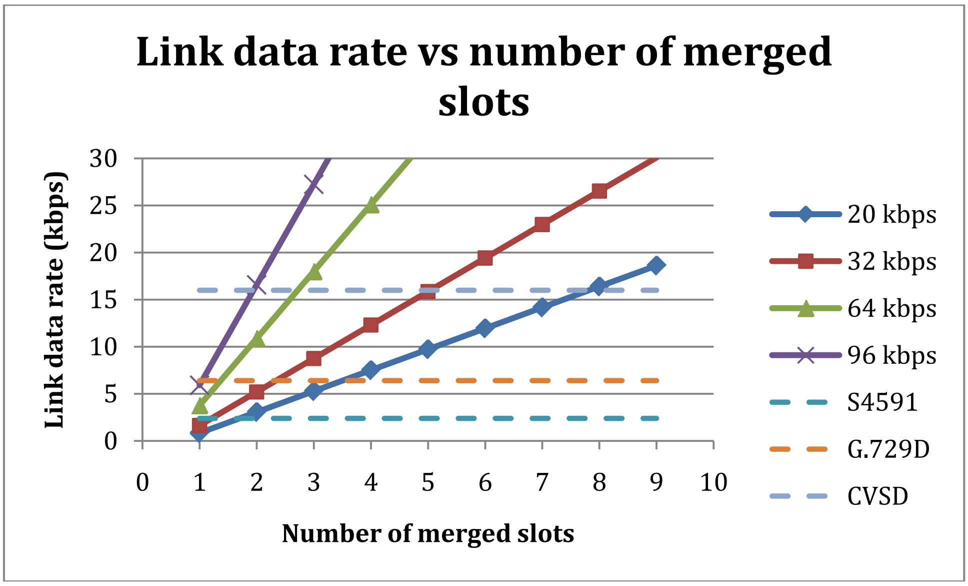

Figure 4.1 Link data rate as a function of the number of merged time slots.Required minimum link data rates for different vocoders shown as dashed lines

4.4 Relaying of voice and data

Automatic relaying of voice in a multihop environment without the need for dedicated relay nodes is a highly desirable feature that the NBWF MAC protocol should aim for. This functionality is not available in any CNR subnets today, and dedicated relay nodes must be set up in order to extend the radio range of the subnet. Automatic relaying will be a very complex protocol due to the real time delay requirements, limited bandwidth and the mobile environment. We are not sure if such a protocol is feasible within 25 kHz bandwidth, and extensive simulations are needed to provide the answer. In order to arrive at a draft MAC protocol specification earlier, we propose a simpler solution with dedicated relay(s) for voice. This is more in line with current CNR solutions with two distinctions: 1) We use TDM relaying instead of FDM relaying which means that relaying is done on the same frequency and only one radio is needed for the relaying, and 2) *any* NBWF node can act as a voice relay if it is configured to do so.

We have chosen the TDM type of voice relay since this approach is closer to the final goal of automatic relaying. Frequency resources are saved by the TDM type of relay, but there will be less capacity for data services on the channel, since relaying will occupy time slots. Another advantage is better network connectivity and it is possible to transmit point-to-point traffic directly between two nodes (provided that the topology allows this) thus avoiding activating the relay.

The relay node can be a full member of the subnet, generating and receiving traffic, provided that its role as a relay node is not in conflict with its role as an ordinary subnet member. There may be, for instance, a conflict between the combat task of a node and the desired geographical position of a relay node. However, the need for only one radio makes this a more flexible solution than the current use of traditional FDM relays.

In the longer term, automatic relaying of voice without a dedicated relay should be investigated and added to the protocol specification, if possible. This will not be further described in this document or in [11].

Data will be routed in the subnet over multiple hops according to the dynamic routing tables maintained at the nodes, and the fixed relay for voice will have no specific role in this, except for being a frequently used node for routing. The protocol stack used when IP packets are routed in the NBWF subnet and when digital voice is relayed according to the description in Section 4.2, is shown in Figure 4.2 and 4.3 respectively. Figure 4.3 does not show the protocol stack at the interface to the voice generator since that will depend on whether the voice codec/SCIP application is implemented internally or externally to the NBWF node. The data application in Figure 4.2 is assumed to come from an external terminal.

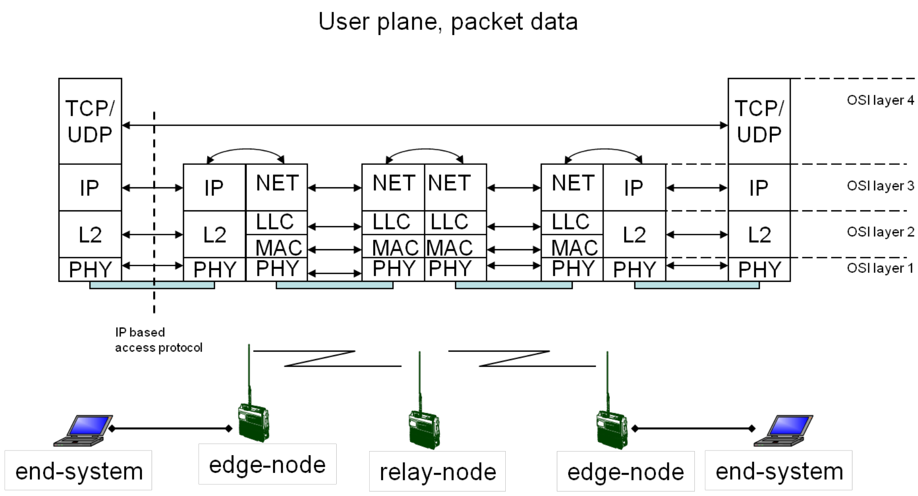

Figure 4.2 Protocol stack for routing of data traffic

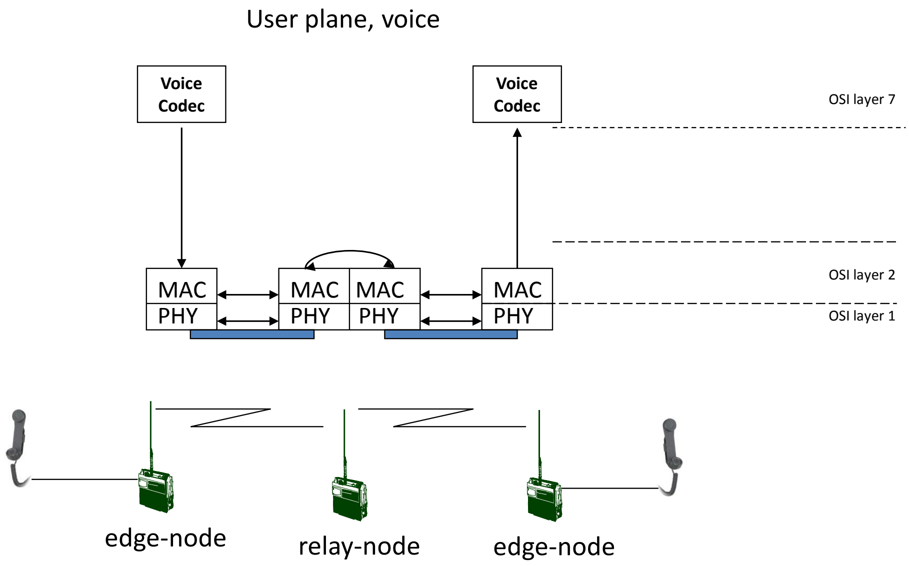

Figure 4.3 Protocol stack for relaying of digital voice

Voice packets are transferred over a connection established end-to-end, and the lifetime of the connection is approximately the same as the call holding time. Data packets using reserved slots are transferred over connections established hop-by-hop, and the lifetime of a connection is identical with that required to send the maximum packet size (1500 bytes) over one radio link. Data packets using non-reserved slots are sent as pure datagram packets contending for slot capacity. Data transmissions will be further described in section 4.6

A small NBWF subnet is shown in Figure 4.4 with node C set up as a relay node for multicast voice at a geographically favourable spot. We assume that all nodes in the subnet can hear a radio broadcast from node C using the most robust waveform at 20 kbps. A second relay node can be added if further range extension is needed. In that case we assume that all nodes can hear at least one of the relays at 20 kbps. If a node nevertheless is in a position where no relay can be heard, it will not be able to take full part in a multicast voice session. However, it may be able to talk locally to its radio broadcast neighbours and send and receive unicast data through them.

Figure 4.4 also shows simultaneous multicast voice and IP traffic being sent over the subnet.

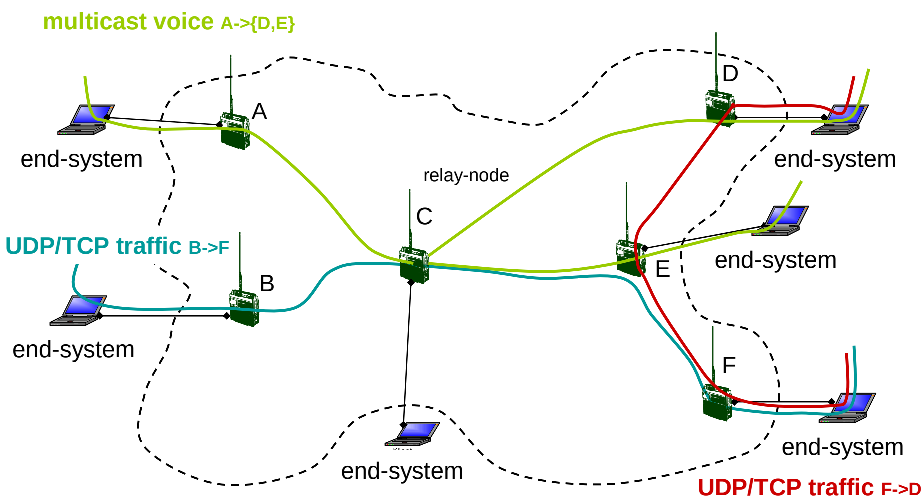

Figure 4.4 NBWF subnet with node C set up as a relay node for multicast voice

4.5 Voice and data capacity considerations

In Section 4.3 it was concluded that the transmission of MELPe at 2400 bps requires two timeslots per TDMA frame when using a physical layer data rate of 20 kbps. Relaying of the voice requires another two time slots. Of the nine timeslots available in a TDMA frame, only five slots then remain for sending data (including network control information). It is even possible to add a second voice relay within the frame structure which will use another two time slots. Then only three time slots remain for data and control. This represents a minimum capacity for data traffic.

The available capacity for sending data traffic thus depends on the following factors:

- The data rate of the vocoder used (number of bits buffered in 202.5 ms)
- The data rate at the physical layer, and the time duration of the physical layer PCI
- Number of dedicated relays in the subnet
- Link layer PCI

From these factors the number of slots required for multicast voice is determined, and the rest of the slots are available for sending data. A gross data rate available for data is $R_1 \cdot d/9$, where R_1 is the physical layer data rate and d is the number of time slots available for sending data. Taking the physical layer and link layer PCI into account, the link layer data rate is less, and a formula for R_2 was given at page 25. It can be seen from Figure 4.5 that protocol efficiency will increase if the available time slots are merged, instead of using each slot individually.

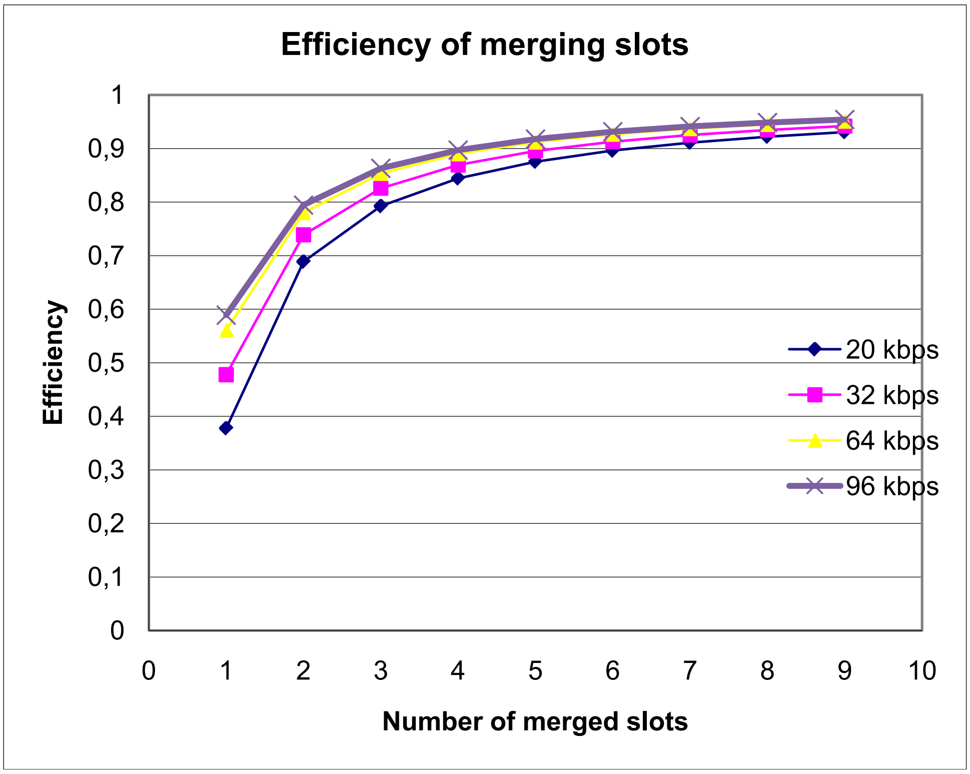

Figure 4.5 Data protocol efficiency if time slots are merged. Link layer PCI is here 120 bits.

A minimum capacity C_{min} should be reserved for any node in the subnet as stated in Section 2.2. This capacity could be used by the node e.g. for sending IP-traffic such as control traffic and/or situational awareness data. Since the number of nodes in the subnet can be large (>10), each node can not be assigned a fixed time slot in each TDMA frame, but have to share two (or more) slots with all other nodes in the subnet. Each node gets regular access to these slots at time intervals longer than the duration of a single frame. The MAC protocol accommodates this by a superframe structure on top of the frame structure. In the following we call this *fixed access* data.

The fixed access data capacity for all nodes is part of the total data capacity. So for each TDMA frame, two time slots are reserved for sending fixed access data on an alternating basis between the nodes. The rest of the time slots that are not used for voice are available for other IP traffic. We have looked at the available data capacity in Table 4.1, given the vocoder used, the number of voice relays in the subnet and the physical layer data rate. The physical layer data rates come from the three waveform modes N1, N2 and N4 in [5]. For the calculation of the link data capacity we have used a link layer PCI of 120 bits (15 bytes). This link layer PCI includes crypto IV.

The sixth column shows the total available link data capacity if *all* remaining data slots are used individually and not merged. The seventh column shows the total available link data capacity when two slots are merged and used for the fixed access data, and the rest of the available slots are merged and used for other IP traffic.

The last column shows the median communication range of the voice, taken from Table 2.2 in Section 2.3. An unrealistic assumption here is that the relays are placed exactly at the radio broadcast range, which gives an optimistic estimate of the network multihop range.

Vocoder and number of dedicated voice relays	PHY data rate (kbps	Number of multicast voice slots	Number of remaining data slots	Gross data rate of remaining data slots (kbps)	Link data capacity when remaining slots used individually (kbps)	Link data capacity of 2 merged slots fixed access + rest of slots merged (kbps)	Network range (km) for voice at 60 MHz, 50 W (based on Egli i sec 2.3)
S4591, 2.4 kbps	20	2	7	15,6	5,9	12,8	22
	32	2	7	24,9	11,9	21,2	15
	96	1	8	85,3	50,3	76,6	6
S4591, 2.4 kbps, 1 relay	20	4	5	11,1	4,2	8,3	44
	32	4	5	17,8	8,5	14,1	30
	96	2	7	74,7	44,0	65,9	12
S4591, 2.4 kbps, 2 relays	20	6	3	6,7	2,5	3,9	66
	32	6	3	10,7	5,1	7,0	45
	96	3	6	64,0	37,7	55,2	18
S4591, 1.2 kbps	20	2	7	15,6	5,9	12,8	22
	32	1	8	28,4	13,6	24,7	15
	96	1	8	85,3	50,3	76,6	6
S4591, 1.2 kbps, 1 relay	20	4	5	11,1	4,2	8,3	44
	32	2	7	24,9	11,9	21,2	30
	96	2	7	74,7	44,0	65,9	12
S4591, 1.2 kbps, 2 relays	20	6	3	6,7	2,5	3,9	66
	32	3	6	21,3	10,2	17,6	45
	96	3	6	64,0	37,7	55,2	18
G.729D, 6.4 kbps	20	4	5	11,1	4,2	8,3	22
	32	3	6	21,3	10,2	17,6	15
	96	2	7	74,7	44,0	65,9	6
G.729D, 6.4 kbps, 1 relay	20				Not possible		
	32	6	3	10,7	5,1	7,0	30
	96	4	5	53,3	31,4	44,6	12
G.729D, 6.4 kbps, 2 relays	20				Not possible		
	32				Not possible		
	96	6	3	32,0	18,8	23,2	18
CVSD, 16 kbps	20				Not possible		
	32	5	4	14,2	6,8	10,5	15
	96	2	7	74,7	44,0	65,9	6
CVSD, 16 kbps, 1 relay	20				Not possible		
	32				Not possible		
	96	4	5	53,3	31,4	44,6	12
CVSD, 16 kbps, 2 relays	20				Not possible		
	32				Not possible		
	96				Not possible		

Table 4.1 Voice and data capacity considerations. (The subnet range when relays are used is based on the maximum range for each hop, thus representing a very optimistic subnet range)

Conclusions from studying the table are:

- Relaying of voice is very ”expensive” in the sense that several time slots are occupied by the voice, and little capacity is left for data
- When a node has data to send, it should attempt to use *all* slots available to achieve an acceptable data rate. If only one time slot is used, the link data rate will be low and the resource utilization poor. (For instance when there is a MELP 2.4 voice session without relaying going on, the link data capacity per node would be: 5.9/7 = 0.8 kbps at 20 kbps PHY data rate, 11.9/7 = 1.7 kbps at 32 kbps and 50.3/8 = 6.3 kbps at 96 kbps).
- Even though a relatively high link data capacity (50-70 kbps) can be achieved by using the 96 kbps physical layer mode, the range performance of this mode is probably not satisfactory for multicast/broadcast services.
- Direct support of the high rate vocoders G.729D (6.4 kbps) and CVSD (16 kbps) over the NBWF subnet is possible only to a limited extent. The 20 kbps mode with its good range performance can only be used with the G.729D vocoder for half duplex traffic without any dedicated relays. Then 4.2 kbps is left for data. Even when using higher physical layer data rates, relaying of the voice is difficult.
- For the 1.2 kbps S4591 voice, buffering 202.5 ms voice is just above the limit to fit into one time slot for 20 kbps, therefore two slots are necessary. This then gives no capacity gain by going from 2.4 to 1.2 kbps MELP. However, if a longer delay of the voice can be tolerated, two time slots can be used every other frame, thus using only half of the capacity used for 2.4 kbps MELP. This will allow more capacity to be used for data traffic.

4.6 Data over the NBWF subnet

As stated in the last section every node gets a fixed access data capacity. The interval between each fixed access for a node depends on the total number of nodes in the subnet, but is limited to a maximum interval. Time slots that are not reserved for multicast voice or fixed access data, dynamic time slots, are available for reservation by any other node on a temporary basis. The number of dynamic time slots available is variable, depending on whether a multcast voice session is ongoing and the type of voice codec used. Dynamic time slots can be used for:

- *Random access data*, which means that the node may access the channel during a contention window, without any reservation. There is a chance of collision so this service should be used for short packets with a requirement to low delay but no requirement to a reliable delivery.

- *Reserved access data*, which means that the node reserves a number of timeslots for a period, similar to the reservation made for multicast voice. Reserved access should be used when there is a requirement on a reliable delivery and when the IP packets are large.

- *Selective call*, which means that in most cases a point-to-point voice connection is established between two nodes in the network. This may occur simultaneously with an ongoing multicast voice talk spurt. Selective call will be treated in section 4.7.

The interaction between the voice and data protocols will be subject to intensive simulations using our discrete-event simulator [12], [13], [14] and [15]. The following description may therefore be changed in the future as a consequence of the simulation results.

4.6.1 Random Access data

Data can be sent using a pure random access protocol. If a node perceives time slots other than the multicast voice signalling slots and the fixed allocation slots to be free, it can transmit data without any reservation. A slotted p-persistent CSMA type of protocol is used within the time interval perceived by the node to be free.

The contention window starts after the multicast voice (MV) signalling time slots. The length of the window is dynamic and depends on the number of neighbour nodes, traffic load and network queuing at different priorities. The contention window may stretch beyond one TDMA frame, but comprising only dual use (multicast voice and data) and general use time slots, not the multicast voice signalling slots or fixed access slots. Within the contention window the CSMA contention slot size is approximately 4 ms which corresponds to the duration of the sync preamble and the SOM.

The data to be sent will have different military priorities, and we have assumed four classes of priority. Within the contention window, the highest priority traffic will contend for access from the start of the window and the lower priority traffic will start their contention in later parts of the window. The start of the contention periods for the different priorities is dynamic and based on the perceived network queue at the different priorities. If there is no high priority traffic at any node, the lower priority traffic will be allowed to contend for access earlier in the contention window. This dynamic adaption of contention period relies on nodes being able to exchange information about their queue status.

Figure 4.6 illustrates the contention window and the contention periods for the different priorities. If a high priority packet (pri 1) arrives at the MAC layer after the end of its contention period it will be allowed to contend with lower priority packets. The same applies to the lower priority packets arriving too late for their contention periods. The RTS signal has the duration of one time slot so the last time to send it is at the beginning of the last time slot before the fixed access (FA) time slots.

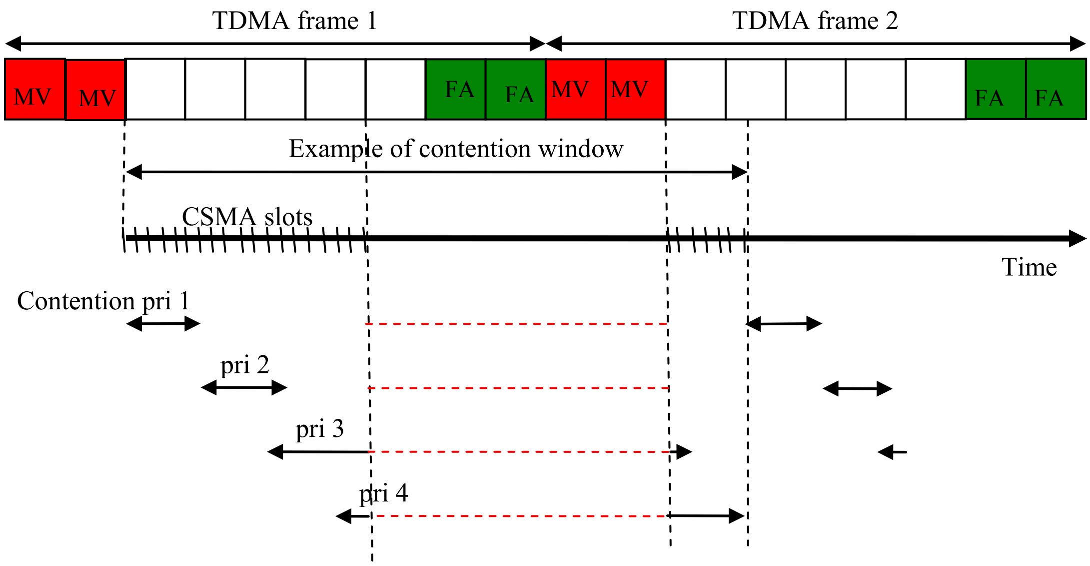

Figure 4.6   Contention window for reserved access data

The random access data packet will contend with the reservation signalling for reserved access data (next section).

The amount of data to be sent using random access is limited to what can be fitted into the free time slots of one TDMA frame (corresponding to one segment in the last section). No segmentation is therefore performed prior to random access data transmissions, and there is a maximum size of the packet that can be sent using random access. If a collision occurs, the complete data packet may be lost and no retransmissions are attempted. Random access data will therefore be used only for small data packets where low latency is more important than safe delivery.

The details of this access protocol has not been studied yet.

4.6.2 Reserved access data

For the reservation of capacity for sending data traffic the same CSMA-based contention protocol described in section 4.6.1 is used. RTS/CTS signaling is sent during the contention window and will contend for access with random access data . Unlike the reservation scheme for voice, no time slot is reserved on a permanent basis for such signaling.

The reservation is similar to the reservation made for multicast voice. For unicast traffic the confirmation of the reservation is made only by the single recipient node that will route the packet on to its final destination. With this confirmation signalling the recipient node informs its neighbours that it is receiving a data packet. The confirmation is done immediately after the RTS has been received. For multicast traffic a number of one-hop neighbours are selected by the transmitting node to confirm its reservation. The nodes that are selected to confirm are among those that need to receive the packet either because they are destination nodes or because they are selected as relay nodes. The confirmations will be done sequentially after the RTS has been received. This RTS/CTS procedure is basically the same for multicast voice and data, except that the voice signaling takes place in dedicated slots.

A node is allowed to reserve *all* of the available time slots for a certain amount of time, to obtain the highest link data capacity as seen from Table 4.1. The maximum reservation time is currently set to be approximately the time duration of one 1500 bytes IP packet sent at the lowest physical layer data rate (can be several IP packets if larger physical layer data rates are used). After the transmission of the maximum IP packet (or several smaller packets), the time slots are de-allocated and released for other nodes to use. If the node has more data to send, a new reservation must take place through contention with other nodes.

The maximum reservation time will be subject to simulations, but we wish to make this short enough to avoid the use of pre-emption of an ongoing packet transmission. That is, if a data packet with a higher priority arrives for transmission, it will have to wait for the current transmission to finish. When the reservation is released it will contend for access. Assuming an ongoing multicast voice session requiring two timeslots, and an ongoing data transmission of a 1500 bytes data packet using the remaining five slots at 20 kbps data rate, the duration of the data reservation is 1,5 s. This represents the longest waiting time for a new reservation to be made, assuming that retransmissions due to imperfect receiving conditions are not required. If the multicast voice was set up with a relay requiring four time slots, there would be three time slots left for data transmission and the duration of the reservation would be 2,7 s.

The reservation may be used to send both unicast and multicast data. However, we believe that the multicast traffic is likely to consist of short packets, making random access (described in section 4.6.1) more suitable. The proposed reservation scheme for data will be subject to simulation studies.

As described in section 4.2, multicast voice will pre-empt the data traffic that use time slots which will be required for the voice traffic. If there are time slots left for still sending data after the MV pre-emption, the node owing the reservation may continue to transmit using only those time slots now available. At the release of the MV traffic slots, the reserved access data transmission may again use the maximum number of time slots. This requires a flexible segmentation of IP packets at the LLC layer. (Also the fact that the selected physical layer data rate may change during a transmission requires a flexible segmentation procedure). The segmentation is flexible down to each individual byte, and the bytes being sent in a segment are addressed in the link layer PCI. An IP packet is divided into a number of segments dependent on the size of the IP packet, the available number of timeslots to be merged, and the physical layer data rate. The segmentation function is only active when using reserved access data. For random access data (next section) we assume the packets are small enough to fit into the available slots for data within one TDMA frame.

The LLC layer offers both a reliable and an unreliable unicast service to the network layer. For multicast, only an unreliable service is offered. If a reliable unicast service is selected, the transmitting node will request an acknowledgement from the recipient (1-hop neighbour) at appropriate times selected by the transmitting node. The cost of reversing the transmission and sending an ACK is high, so several segments should be acknowledged simultaneously. The channel reservation made by the transmitter for sending data will also be used by the recipient for sending the ACK (time duration of ACK is one time slot of 22.5 ms). The ACK acknowledges each transmitted segment individually and requires retransmissions if segments are received in error. Retransmissions will extend the reservation time required to transmit the complete IP packet. However, it is necessary to limit the maximum allowed reservation time to a few seconds. If the error rate is high, decreasing the physical layer data rate for the retransmissions is one action that can be implemented (but need not be standardized). The ACK contains, in addition to the selective acknowledgements, advice on which data rate the transmitter should choose based on the measured channel conditions at the receiver.

If an unreliable service is selected by the network layer, the LLC layer segments and transmits the IP packet (or transmits several smaller IP packets) without requiring acknowledgements. If multicast traffic is served, only an unreliable service is offered by the LLC layer, and no acknowledgements are sent from any of the recipients. A low physical layer data rate with high robustness is then preferred.

4.7 Selective call

In the NBWF network a selective voice call between two nodes can be established simultaneously with, and independent from, any ongoing multicast voice call. The selective call may also include more than one recipient node. Whereas the multicast voice has a reserved time slot for signalling and is able to pre-empt ongoing data transfers, the selective call will have to contend for channel resources. A selective call can only be established if sufficient channel resources (time slots) are available. Two slots are needed to transmit 2.4 kbps MELP voice, and more slots are needed for other vocoders.

We limit the selective call to be established in general use (GU) time slots only (described in the next section). This in order to prevent pre-emption of selective calls when multicast voice is activated. The number of GU slots available depends upon the number of dedicated relays in the network configuration. If there are two relays, there exists only one GU slot and a selective voice call is not possible at all. With one relay, there are three GU slots and a selective call without relaying is possible (assuming a MELP 2.4 vocoder). In a NBWF net without relays five GU slots are available, and in principle a selective call with relaying can be established. However, we assume there is no need for relaying in this network since there will be no relaying of the MV. So a one-hop selective call is the only offer in the NBWF network when two slots are reserved for superframes (see next section).

A selective call will be established by dialling a number and the following reservation signalling will be equal to the reservation signalling for data. The selective call signalling will contend for access in the same contention window as the data reservation signalling. When the reservation is made, the reservation will be used for a half duplex exchange between the originating and terminating node until the end of the conversation.

A pre-emption mechanism must be available in order to pre-empt an on-going selective call.

4.8 Types of time slots and TDMA frame structure – summary

The frame structure of the NBWF waveform is illustrated in Figure 4.7. A superframe structure lies on top of the frame structure, and the number of frames in a superframe is configurable, depending on the actual number of nodes in the subnet and the required ”static” capacity for each node.

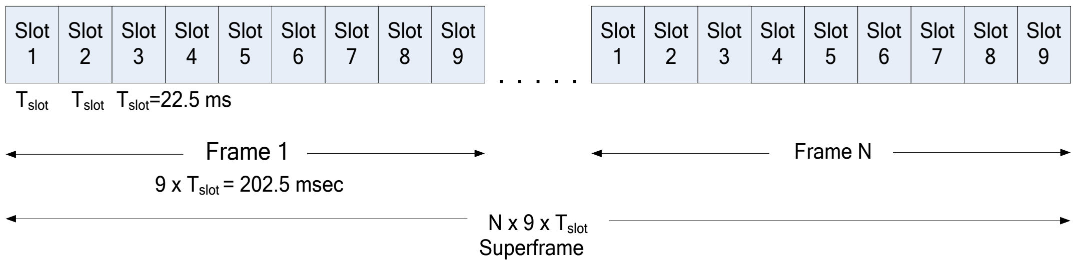

Figure 4.7 Frame structure of the TDMA protocol

There are two categories of time slots within each frame; *fixed* and *dynamic*. Fixed time slots are those that are reserved on a permanent basis for MV signalling or through the superframe structure. The allocation of fixed time slots is not changed from one frame to the next. The only way to change this allocation is through the subnet management system. The rest of the time slots are dynamic, meaning that their allocation may change from one frame to the next. Table 4.2 gives an overview of the different categories of time slots and their usage.

Category	NAME	Usage
FIXED	MV	MV signalling or MV transfer only
	SF	Superframe allocation
DYNAMIC	DU	Dual use (MV or data pre-empted by MV)
	GU	General use (data or selective call)

Table 4.2 Different types of time slots

1. *MV - Multicast voice.* These slots are reserved on a permanent basis for multicast voice signalling only. As a minimum, one slot of this type is always allocated for networks serving multicast voice. Additional MV slots may be allocated through the management system when voice relays are configured. We recommend one additional MV slot to be allocated per relay. The fixed MV slots are used for rapid signalling to reserve the required additional slots needed for MV transfer.

2. *SF - Superframe allocation.* A number of time slots are reserved on a permanent basis to be allocated through the superframe structure. These slots are used to guarantee a minimum data capacity for each subnet node. The use of this capacity is for each subnet node to decide.
3. *DU - Dual use.* These slots are available for dynamic reservation by any node for data transmission. In case of an MV call setup, a pre-emption will take place, and the slots are used for MV for a period. MV always has priority over data in these slots.
4. *GU - General Use.* These slots resemble DU slots in some respect, but they are never subject to pre-emption by MV. These slots may only be used for data or selective call.

A node that performs a data reservation at a time when no MV session is active may reserve both DU and GU time slots. Should an MV session be initiated, the DU slots will be pre-empted, but the node will keep all of its GU slots. This situation has impact on the segmentation function of the link layer, in order to handle dynamic segment sizes.

An example of the time slot utilization in a TDMA frame is shown in Figure 4.8. In this example the subnet is set up with one fixed relay node, and two slots are reserved for superframe allocation. When a multicast voice is set up, any dual use slots in use are pre-empted and reserved for MV transmission.

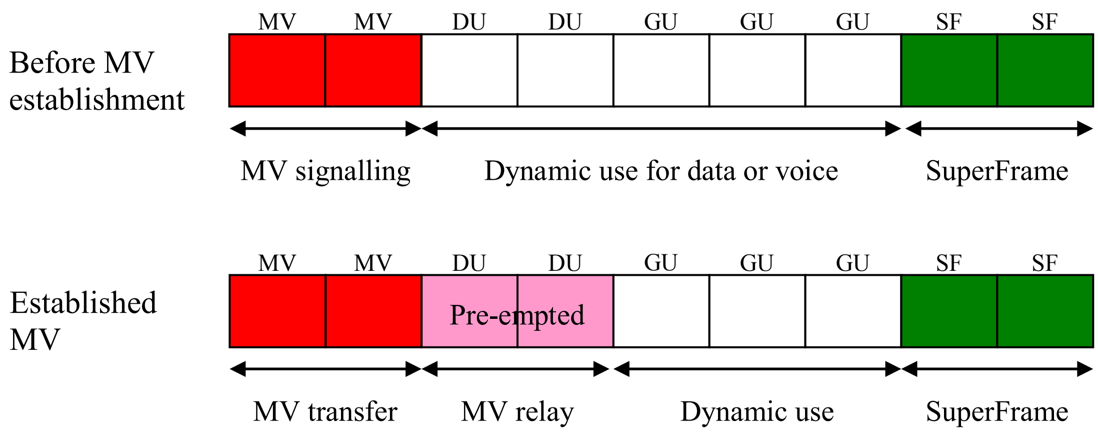

Figure 4.8 TDMA frame of a subnet with one multicast voice relay node

4.9 Quality of service (QoS) functionality

Here follows a summary of the QoS mechanisms at the link layer of the NBWF subnetwork, even though they have been described in earlier chapters. By QoS mechanisms we mean resource control mechanisms that facilitate different priorities to the different applications or users.

- For multicast voice a fixed signalling slot is always available, and no other application is allowed to use this slot. This enables a rapid setup of a MV connection at any time.
- When a MV connection is set up, on-going data transmissions using dual use slots may be pre-empted by the MV. This hands over the necessary channel capacity to the MV

connection. The data transmission that was pre-empted is allowed to use the rest capacity of the channel, and will get the dual use slots back when the MV is finished.

- Each radio node may be allocated a small fixed channel capacity for sending data. This is achieved through a superframe TDMA structure where each node gets access to the channel in fixed slots once every superframe. This fixed capacity will allow the nodes to send for instance network management data without collisions.
- The data applications using the NBWF subnet will request a certain QoS from the subnet. Based on that requirement the appropriate link layer service will be provided; a connectionless service or a connection-oriented service. For the latter, a selective ARQ protocol can be used in order to provide a reliable service.
- Channel capacity can be reserved for sending data or selective voice calls similar to the reservation for MV. However, there is no fixed signalling slot for data/selective call reservations. Reservation signalling must contend with random access data. Channel reservation reduces impact of collisions, while still keeping flexibility and dynamic resource allocation amongst the nodes.
- There is a limit to the allowed reservation time for sending data, typically corresponding to the transmission of one 1500 bytes IP packet at the lowest physical layer data rate (20 kbps).
- There is a contention window for data and selective call access. High priority selective calls and data have precedence over lower priority data and contends in the first part of the window while lower priorities contend in later parts. The size of the contention window is dynamic, and will be regulated according to the traffic queues at the different priorities. Higher priority data is not allowed to pre-empt on-going lower priority data transmissions.
- Selective calls are only established in General Use time slots in order not to be pre-empted by multicast voice.
- Pre-emption of selective calls is allowed. The pre-emption signal will be sent in Fixed Access time slots or through a separate data reservation in free time slots.

4.10 RBCI

The purpose of an RBCI service was described in Section 3.2. RBCI may be quite resource consuming for the subnet, and the RBCI service is activated in the NBWF subnet through a management procedure when needed. In the absence of distinct requirements for RBCI, we only sketch how the RBCI service can be implemented.

Each node leaves the NBWF subnet for one time slot every frame (or every other frame) to search for a hailing request at the RBCI frequency. The choice of time slot for RBCI will be done individually by each node based on its perception of free time slots and the traffic situation. The choice of time slot may vary from frame to frame. A node will choose a time slot for RBCI based on the following criteria:

- a free time slot
- if no free time slot is available, a slot with traffic that does not concern the actual node (or is a duplicate received due to MV relaying)
- if no free time slot is available, and the traffic in all time slots concerns the actual node, a slot with the lowest priority traffic

If no hailing is received on the RBCI frequency, the node will return to the NBWF subnet and continue the communication. If an interrogation is received, the node must perform relevant actions according to the RBCI protocol. A proposal for an RBCI concept is sketched in [19].

4.11 Time synchronization

In many NBWF networks an external source for time synchronization such as a Global Navigation Satellite System (GNSS) will be available. However, such an external source can be unavailable and the NBWF shall not be dependent on the availability of such external signals. In case a GNSS is available at all nodes, this will be used as the common time reference in the network. If a GNSS is *not* available, a common network time reference must be established and maintained according to a sync exchange protocol between the nodes. This is not yet defined.

In order to perform satisfactorily the NBWF nodes must be time synchronized to within 1.5 msec.

The NBWF subnets on the ground will not be time synchronized with aircrafts delivering weapons, unless a GNSS is available at both ends. For the RBCI exchange, the interrogation from the aircraft will take place over a relatively long period of time (~500 ms according to the proposal in [19]) to facilitate the NBWF node on the ground to receive the hailing signal with the required probability. Synchronization is then achieved by the reception of the sync preamble of the hailing signal. If the RBCI exchange is based on a hopping waveform, the synchronization will be more complex.

4.12 Network management

A number of management protocols needs to be defined for the NBWF. These are not part of the link layer specification, but they may put some requirements on the link layer, and are mentioned here for completeness:

Radio Silence of NBWF nodes is not listed as a requirement in [4], but should be considered for inclusion. Services provided to a node in radio silence needs to be defined.

Late Net Entry allows nodes to join and become a member of the net. This includes acquiring initial network parameters.

Network split and merge allows the network to be divided into several networks consisting of a smaller number of nodes and to rejoin into a larger network again.

5 Outlook

This document has described at a high level the design of the link layer and the considerations that underpins it. The design of the link layer and also the NBWF in general is by no means fixed at this point in time (March 2011). FFI has put much effort into building a discrete event simulator that reflects the characteristics of the proposed data link layer (and also the physical layer), and this has not been used to any extent yet. The simulator will be used in the year to come to validate the proposed link design and to tune link layer parameters. The simulations will for instance investigate

- The robustness of the reservation signalling scheme for voice
- the contention based link access for data and priority handling
- interactions between the data link protocol and multicast voice

It is expected that the link layer design may change based on these simulations.

References 6, 11-17 and 19 in addition to this report have been produced at FFI as documentation of the link layer and simulator development. From the spring of 2011, FFI focuses on producing the final STANAG documents which will comprise a Link layer STANAG and a Head STANAG. The Head STANAG will describe the relationship between the different parts of the NBWF (physical layer, link layer, network layer) and the interconnection to external networks.

The next step for the link layer is the development of prototype software. FFI does not have resources to undertake this task, and industry must be involved. Presently, NATO HQ Staff is investigating the possibility of establishing a multi-national project that will develop those parts of the NBWF still missing and also develop software prototypes.

Hopefully the NBWF ambition level one will lead to an *interoperable* fixed frequency combat net radio waveform implemented on a wide varity of software defined radio platforms in the battlefield. In addition to being standardized and interoperable, it should not be inferior to legacy combat net radio waveforms. In that sense, the NBWF will need to be developed further with an EPM capability. Work is ongoing at the physical layer, and the link layer needs to be reconsidered in light of this. Also for air-ground applications the link layer (and physical layer) of the NBWF must be reviewed.

References

[1] Kallgren D, Bastos L, Winkler M, Boogaart A, “Non-SATCOM Wireless Reference Architecture, Edition 1”, NC3A Technical Note 1221, 2006

[2] Street M, Szczucki F, “Wireless Communications Architecture (Land): Scenarioes, Requirements and Operational View”, NC3A Technical Note 1246, 2006

[3] Boogaart A, Oudkerk S, Street M, Szczucki F, “Wireless Communications Architecture (Land): System and Security Views”, NC3A Technical Note 1247, 2007

[4] Barfoot R, “Requirements for a Narrowband Waveform” Version 0.4, NATO AC/322(SC/6-AHWG/2)M(2008)0003, Aug 2008

[5] Vigneron P, “Technical standards for narrowband physical layer of the NATO networking enabled communications waveform and VHF propagation models, Draft 4”, NATO/SC6/AHWG2, March 2010

[6] Bråten L E, Hauge M, Voldhaug J E, Øvsthus K, “Medium access for narrowband wireless ad-hoc networks - requirements and initial approaches, FFI/Rapport-2008/01313, 2008

[7] Brown C, “Block error rate results for NBWF modes”, nov 2010

[8] SINCGARS planning range: www.gordon.army.mil/sigbde15/25u/25u10/25u1CTDF/25u12/25u12h05.ppt

[9] Egli J J, “Radio propagation above 40 MC over irregular terrain”, Proceedings of the IRE, Oct 1957, pp1383-1391

[10] NATO, “Security Principles for Narrow Band Waveform Radios”, AC/322(SC/6-AHWG/2)N(2010)0012-ADD1, Sept 2010

[11] Haavik S, “Initial link layer protocol design for NBWF – Input to NATO SC/6 – AHWG/2, FFI-Rapport 2009/01895, 2011

[12] Berg T J, “The design of an initial NBWF network simulator”, FFI-Rapport 2008/01921, 2008

[13] Libæk B, Berg T J, Voldhaug J E, “Enhancements of the narrowband waveform (NBWF) network simulator”, FFI-Rapport 2009/01765, 2009

[14] Berg T J, “The design of an initial LLC data protocol for the NBWF simulator”, FFI-Rapport 2011/00537, 2011

[15] Libæk B, Solberg B, ”A simulator model of the NATO Narrowband Waveform Physical layer”, FFI-Notat 2011/000533, 2011

[16] Libæk B, Berg T J, “A reference model for the NATO Narrowband Waveform”, FFI-Notat 2011/00532, 2011

[17] Haavik S, Libæk B, “Link layer design for a military narrowband radio network”, NATO RTO IST-092, Wroclaw, Polen, Sept 2010

[18] SCIP 214.2 “Secure Communication Interoperability Protocol (SCIP) over Real-time Transport Protocol (RTP), Jan, 2010

[19] Haavik S, Libæk B, “A proposal for Radio Based Combat Identification (RBCI) – input to NATO SC/6 AHWG/2”, FFI-Rapport 2009/01983, 2009

Abbreviations

AHWG	Ad Hoc Working Group
ARQ	Automatic Repeat Request
BER	Bit error rate
C-plane	Control plane
CNR	Combat Net Radio
COMSEC	Communications Security
CP	Capability Package (NATO funding)
CSMA	Carrier Sense Multiple Access
CTS	Clear To Send
CVSD	Continuous variable slope delta modulation
EPM	Electronic Protection Measures
EW	Electronic Warfare
FA	Fixed Access
FDM	Frequency Division Multiplexing
FEC	Forward Error Correction
FFI	Forsvarets forskningsinstitutt (Norwegian Defence Research Establishment)
HF	High Frequency
IP	Internet Protocol
IV	Initialization Vector
LLC	Link Layer Control
MAC	Medium Access Control
MELPe	Mixed Excitation Linear Predictive, enhanced
MV	Multicast Voice
NBWF	Narrowband Waveform
NBWF(A)	Narrowband Waveform Air component
NBWF(L)	Narrowband Waveform Land component
Par	Parameter register
PCI	Protocol Control Information
PDU	Protocol Data Unit
PHY	Physical layer
PTT	Push To Talk
QoS	Quality of Service
RF	Radio Frequency
RBCI	Radio Based Combat Identification
RTP	Real-time Transport Protocol
RTS	Request To Send
SCIP	Secure Communication Interoperability Protocol
SDU	Service Data Unit
SHF	Super High Frequency
SNR	Signal to Noise Ratio
SOM	Start of Message
STANAG	Standard Agreement (of NATO)

TCP	Transport Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple access
VHF	Very High Frequency
VoIP	Voice over IP
U-plane	User plane
UHF	Ultra High frequency