FFI RAPPORT

SUBNET RELAY; a mobile wireless ad-hoc network

Lars Erling Bråten, Jostein Sander, Jan Erik Voldhaug

FFI/RAPPORT-2007/00901

SUBNET RELAY; a mobile wireless ad-hoc network

Lars Erling Bråten, Jostein Sander, Jan Erik Voldhaug

FFI/RAPPORT-2007/00901

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
P O Box 25, NO-2027 Kjeller, Norway

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
N0-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER FFI/RAPPORT-2007/00901	**2) SECURITY CLASSIFICATION** UNCLASSIFIED	**3) NUMBER OF PAGES** 34
1a) PROJECT REFERENCE FFI-II/1088/912	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE** -	

4) TITLE
SUBNET RELAY; a mobile wireless ad-hoc network

5) NAMES OF AUTHOR(S) IN FULL (surname first)
Bråten Lars Erling, Sander Jostein, Voldhaug Jan Erik

6) DISTRIBUTION STATEMENT
Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

	IN ENGLISH:		IN NORWEGIAN:
a)	Subnet relay	a)	Subnett rele
b)	Mobile ad-hoc	b)	Mobilt ad-hoc
c)	Wireless Internet	c)	Trådløst Internett
d)		d)	
e)		e)	

THESAURUS REFERENCE:

8) ABSTRACT

Subnet relay (SNR) is a realisation of a mobile narrowband ad-hoc network produced by Rockwell Collins Government Systems Canada. The product is mainly developed for maritime users providing Internet protocol connectivity between vessels. It may be used by both the air force and the army to create an interconnected low mobility network. An SNR node controller can utilise existing HF, VHF or UHF narrowband radio equipment, existing link encryption devices as well as modems resulting in relatively low deployment costs. Applications such as e-mail utilising XOmail and chat over Netmeeting have been successfully tested at FFI in laboratory environments. The maximum UDP throughput obtained in a two node network was about 60 kbit/s when utilising a 76.8 kbit/s modem over a 25 kHz UHF channel. For a degraded radio link introducing packet errors, the TCP performance enhancing proxy significantly improved the throughput. FFI follows the standardisation attempts of SNR in NATO AHWG VUHF. The lacking support of IPv6, as well as the fact that Rockwell Collins is not willing to publish the TCP performance enhancing proxy, might require substantial additional effort before a STANAG may be accepted. In addition there are a number of minor issues, such as definition of quality of service classes and the ability to handle merging and separation of networks that require further work. FK-KKIS and NDLO plan to test SNR in an operation scenario, possibly including interoperability tests with the Dutch Navy. FFI will continue the work on characterisation of SNR networks with a larger number of nodes and further investigate the link encryption issues encountered in the current trials.

9) DATE	**AUTHORIZED BY** This page only	**POSITION**
2007-02-26	Vidar S. Andersen	Director

ISBN 978-82-464-1129-3

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

CONTENTS

SUBNET RELAY; a mobile wireless ad-hoc network

1 INTRODUCTION

Communication between vessels from different nations is traditionally provided by multiple satellite communication links via National Defence Headquarters. Rockwell Collins Goverment Systems Canada (formerly IP Unwired) has, on behalf of the AUSCANNZUKUS countries, developed a concept for Internet protocol (IP) communication between vessels. The systems intended operating frequency is in the UHF band, however, narrowband operation at lower frequencies, such as HF, is possible. The ad-hoc network concept is called Subnet relay (SNR), and it appears to become a maritime de-facto standard within the AUSCANNZUKUS countries (1). SNR has been tested at several sea trials, and the AUSCANNZUKUS countries aim at implementing it before 2009. The SNR concept has recently been presented to NATO ad hoc working group on VHF and UHF issues for possible standardisation and is described in ACP200, Maritime Tactical Wide Aarea Networking (2). General comments to the drafted Standardisation agreement (STANAG) may be found in Annex A, where it is concluded that further work is required before it is agreed within NATO to standardise this mobile ad-hoc network. SNR may increase range as well as improve connectivity between vessels compared to traditional point-to-point links, see Figure 1.1.

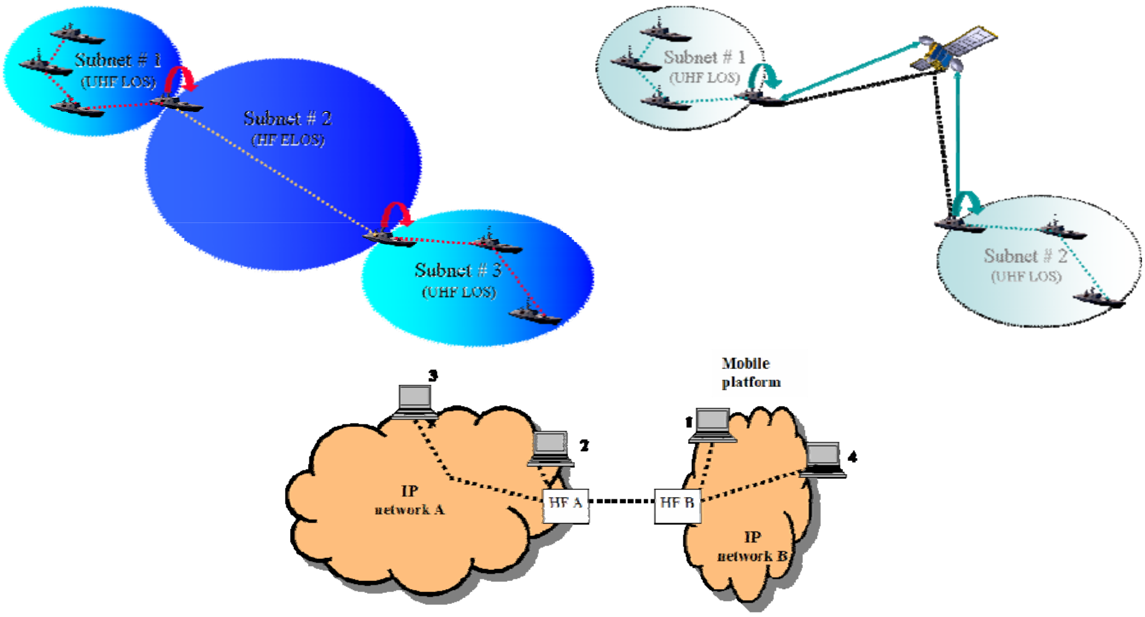


Figure 1.1 Routing within and relaying between IP sub networks

The Norwegian Navy and the Norwegian defence research establishment (FFI) consider SNR to be an interesting communication system, and are now exploring the possibilities of the system through lab trials. The Norwegian Navy will later perform over-the-air testing. At a NATO Sub Committee 6 Ad Hoc Working Group (SC6/AHWG2) 2006 meeting in the UK, representatives of the Royal Netherlands Navy and TNO-Telecom expressed interest in the

SNR as well, and cooperation between TNO and FFI has been established. The objective of FFI is to investigate the performance of:

- SNR functionality on UHF radio bearers with up to 25 kHz bandwidth
- SNR functionality on HF radio bearers with up to 3 kHz bandwidth
- Bridging to STANAG 5066
- Military Message Handling System (MMHS) over SNR
- The effect of COMSEC equipment on SNR

In addition we would like to look into
- Chat and possible VoIP over SNR
- Connection to Norwegian Defence Digital Network (NDDN)
- SATCOM bridging of two or more SNR networks
- Interoperability of SNR with other communication systems

The SNR equipment provided by Rockwell Collins consists of a SNR node controller and a HF/VHF/UHF modem that may give data rates up to 96 kbps in 25 kHz or 256 kbps in 100 kHz bandwidth for UHF[1]. For HF the data rates are 9.6 kbps in 3 kHz and 19.2 kbps in 6 kHz. Other modems may be used instead of the modem provided by Rockwell Collins. Existing radios, crypto equipment and antennas on board the vessels may be used as is. SNR operates on a single frequency with typically 4-20 nodes in a network using distributed TDMA as access protocol with spatial time slot reuse. It has a distributed architecture, it is a self-organising network, however, it is not self-configuring. Other characteristics of SNR are:

- Standard use of IPv4 protocols
- Dynamic slot assignment – adaptable to traffic load at the nodes
- Single nodes may come and go in the network (functionality for groups missing)
- Relay and routing
- Different SNR networks can be linked via for example a satellite link

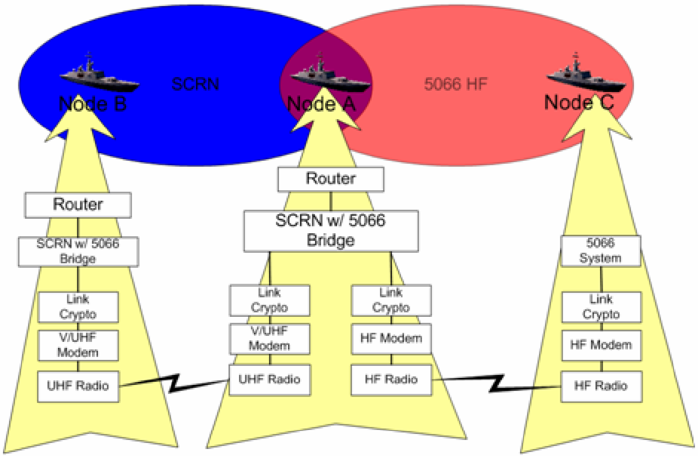


Figure 1.2 An SNR node can act as a bridge between an HF 5066 system and a SNR node.

[1] The current generation of SNR equipment is limited to 76.8 kbit/s within a 25 kHz channel.

Additional features include

- Bi-/uni-directional links (bi-directionality is not assumed)
- Reliable/unreliable link service (both TCP and UDP)
- Data compression built in
- Parameterised design enabling different equipment types (radio, modem, encryption) and network topology (number of nodes, types of traffic)

The SNR concept is not limited to maritime environments. It may also be used to connect for example maritime forces with land forces, as well as internally within stationary or slowly moving land forces. It is one of the first commercial ad-hoc networks designed for IP connectivity at sea, and it seems that several nations are cooperating on developing network with similar characteristics. If wider frequency bandwidths were available, for example at higher frequencies, a number of alternatives systems would be of interest as well.

2 DESCRIPTION OF SUBNET RELAY

A SNR node consists of a node controller and a modem, with optional link encryption between the controller and the modem. The modem audio output is then connected to a radio (half or full duplex) forming a single frequency network. Normally a router is connected to the node controller, enabling local area networks (LANs) to be interconnected by the SNR communication system. SNR forms a mobile ad-hoc networking with:

- Ability to use multiple, standard military LOS/ELOS bearers with existing encryption equipment, radios, and antennas
- Combined relaying (layer 2) and routing (layer 3)

Single nodes (typically ships) may connect to the network given that they utilise the same operation frequency, parameter set and encryption. Functionality to include a new group of nodes with an already existing network (merging of networks) is not included in the current version of the system. The same applies to cases where a group of nodes (ships) separates into smaller groups, where the system would not automatically form new subnetworks operating at different frequencies. The self organising property do not include self configuration, that is, the users have to agree on a set of parameters to utilise given the variety of radios and modems in the group. Selection of proper parameter sets will become an issue for NATO standardisation, if it is decided to develop a Standard agreement (STANAG) for Subnet relay. Radio silence may be implemented by hindering the modem to send information, either from the graphical user interface or from the user interface on the modem itself.

A picture of the first generation SNR hardware is given in Figure 2.1.

Figure 2.1 SNR reconfigurable 1st generation hardware (controller, modem or HF channel emulator)

The 2nd generation hardware, available from 2006, includes a front panel for parameter setting. 3rd generation hardware will probably be available during 2007, including features such as shock and vibration certification and built in bridging to STANAG 5066. In addition, an option for a 70 MHz intermediate frequency radio interface enabling 100 kHz wide channels and improved throughput as well as half rack versions will become available. The latter is useful when deploying several SNR node controllers on a vessel to improve throughput or implement different security domains.

2.1 Routing and medium access

Mobility and dynamic bandwidth provisioning is provided by the main elements working together, see Figure 2.2:

- Routing element: Optimised link state routing-like (OLSR-Like), covers range between one and five hops.
- MAC Element: Time division multiple access (TDMA) based scheme called Distributed slot reservation media access (DSRMA). DSRMA covers routing range of N^2 neighbours.
- Router protocol covers remaining range according to routing protocol, see the Section 2.3.

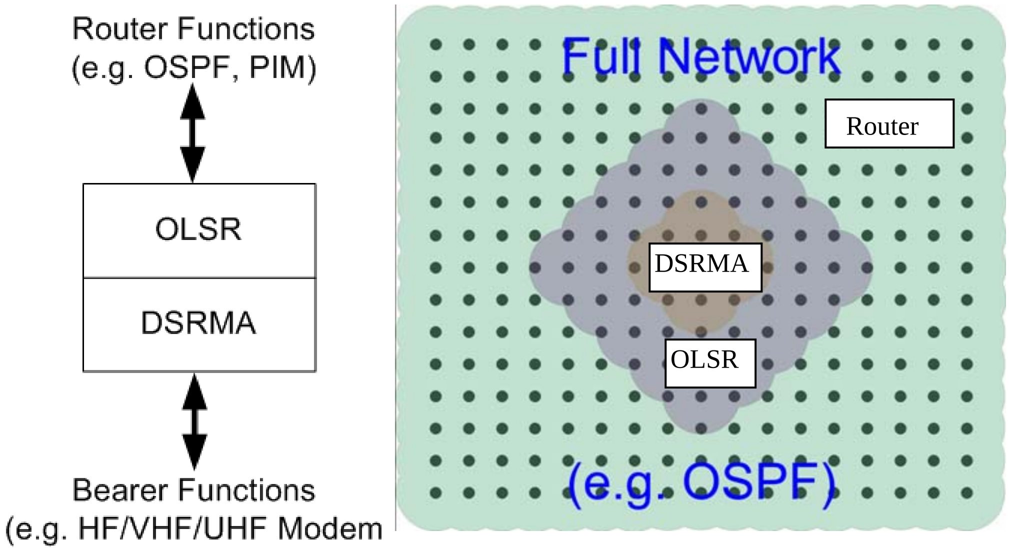


Figure 2.2 SNR routing. DSRMA routing in the middle, OLSR within the larger SNR network

TDMA is utilised to avoid on-air packet collision with the nearest neighbours. The non-centralised implementation of the slot allocation algorithm is called DSRMA, see Figure 2.3.

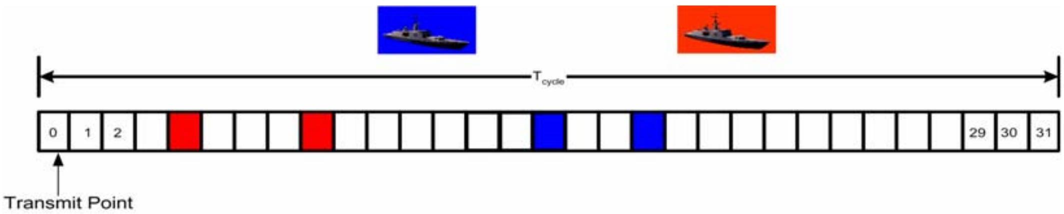


Figure 2.3 TDMA slot reservations in SNR

Slots are assigned according to traffic load (and other factors) and can be pre-allocated and merged for efficiency enhancement. As the traffic buffer fills up, the node will request more slots. As the buffer empty, the node will release some of its slots. When a node reaches one of its slots, it transmits. The TDMA scheme ensures that interference normally is on an acceptable level, however, for HF sky wave interference tests indicate that a larger TDMA cell may improve performance (3).

The number of time slots in a cycle is partly determined by the number of SNR nodes in the network. Each node requires at least one slot per cycle to be active in the network. In addition, at least one random access (RA) slot is required to facilitate joining of new SNR nodes. The slot allocation algorithms try to satisfy two conflicting constraints: spread slots throughout the cycle to ensure minimum latency, and group slots together to allow slot merging and efficient data transfer.

Accurate timing is obtained from a GPS receiver, an accurate on-board time source or via an available Network time protocol (NTP) server. A GPS time reference will often be available onboard ships. To reduce the dependence on GPS availability and ensure network operation when GPS is not available, due to for example terrain obstacles or jamming, some navies have decided to purchase accurate time sources that require about yearly adjustment.

2.2 Mesh topology creation

Upon activation, an SNR node needs to discover if a mesh network is already present. If no network is detected, the node will initiate a new one. In the passive approach the network discovery is based on the reception of beacon messages, whereas in the active approach probing messages are sent. The discovery phase, based on initial active or passive scanning, results in basic connectivity between the nodes in the SNR network. The SNR nodes then form the mesh network by associating with the neighbouring nodes (5).

2.3 IP Layer Routing

Routing is essential to allow communication between SNR nodes. Two types of IP routing protocols are considered by the IETF MANET working group:

- Proactive routing protocols, where nodes periodically exchange routing tables and maintain the entire topology of the network, with each node knowing the shortest path to each node in the network. Examples include Destination sequenced distance vector (DSDV) and Optimized link state routing (OLSR).
- Reactive routing protocol, where routes are established on-demand. Examples include Dynamic source routing (DSR) and Ad-hoc on-demand vector (AODV).

Proactive algorithms, such as OLSR, are useful in small networks due to low overhead from route maintenance. Reactive algorithms are preferable when the network size is large (5). The Optimised link state routing (OLSR) protocol for mobile ad-hoc networks is tailored to the requirements of a mobile wireless LAN. OLSR provides optimal routes (in terms of number of hops). The key concept used in the protocol is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. In OLSR, link state information is generated only by nodes elected as MPRs. An MPR node may choose to report only links between itself and its MPR selectors (4).

- Each node elects a set of one-hop neighbours, MPRs through which all of its two-hop neighbours can be reached
- A node that selects a MPR is called a multipoint relay selector (MPRS).
- Each MPR is responsible for disseminating the list of nodes which have selected it as an MPR
- Nodes build up routing tables which allow them to determine relay paths to nodes which are beyond their two hop neighbourhood

2.4 Priority schemes and QoS

SNR currently implements quality-of-service (QoS) according to:

- Link layer packets are prioritised
- Relayed traffic always has priority over other traffic of the same priority level
- 15 priority levels possible
- 4 currently defined
    - Network topology data has highest priority (15)
    - Router data (OSPF, PIM, IGMP) (13)
    - TCP proxy control (6)
    - TCP, UDP (5)

The implementation does allow different QoS for different traffic or applications, although this is not implemented, partly due to lack of Internet Engineering Task Force (IETF) and NATO standards in this field. SNR does not seem to support DiffServ/IntServ/MPLS in its current implementation, neither does the proposed STANAG produced by Rockwell Collins.

2.5 IP Traffic Manager

During initial sea trials the Transmission control protocol (TCP) traffic throughput was an issue. This is as expected, as most TCP implementations are not tailored for long delay narrowband links with transmission errors. A TCP performance enhancing proxy (PEP) was introduced (May 2004), called ‘IP traffic manager’ or IPTM by Rockwell Collins. IPTM transports the data in the stream across the wireless domain using a protocol designed specifically for the wireless media in use. On the destination side, the TCP stream is re-established between destination-side IPTM and actual destination. IPTM is transparent to standard TCP operation. Currently IPTM resides on same hardware platform as SNR.

Future military communication is expected to implement security on the network layer (COMSEC) by utilising IpSec end-to-end encryption. The SNR links are characterised by limited bandwidths, long delays and non-negligible bit error rates. All of these characteristics degrade the throughput of TCP/IP communications. Performance enhancing proxies provide perhaps the best solution to this problem, but PEPs provide no benefit if the TCP headers are encrypted (7). Further investigations are required to find a common solution applicable to several or all of the military wireless networks.

2.6 Overhead

Each packet accepted from the network interface of the controller is wrapped with a link-layer header (1). The format of the first link-layer header is shown in Table 2.1.

Bit Field	Number of Bits
Frame Type	4
Priority	4
Source Address	8
Destination Address	8
Relay Address	8
PDU ID	16
PDU Length	16
Hop Count	3
Spare	2
Compress Flag	1
ACK Flag	1
Fragmentation Flag	1
Fragmentation Offset	8

Table 2.1 Link Layer PDU Header, first part

Each IP packet get a 10 Byte header in front on the link layer from the first header and about 9 Byte from a second header, implying increased overhead for short packets. In addition there are a number of control packets originating from for example the medium access control (1). The IP version 4 header is 20 Bytes long. UDP has a 8 Byte header while TCP has a 20 Byte header. These headers represent (necessary) overhead in the system, and the end-user traffic throughput will therefore depend on the chosen TCP and UDP packet lengths. The Ethernet maximum transmission unit (MTU) is 1500 Bytes, and the sum of header lengths (IP plus UDP or TCP and possible headers from higher layers) and payload will often be equal to or less than 1500 Bytes. Normally the application selects a suitable packet size depending on the service to be offered to the user. Voice over IP would, for example, require a short packet length to reduce time delays of individual samples, whereas file transfers would benefit from larger packets and reduced overhead. Transmission bit errors affect larger portions of the data transfer if utilising long packets. The SNR equipment implements link layer automatic repeat-request (ARQ) on a hop by hop basis if a reliability flag is set (1).

3 MEASUREMENTS AND RESULTS

The objective of the current trials is to characterise the SNR ad-hoc IP network with respect to traffic capacity obtainable over a 25 kHz wide UHF radio channel. Throughput and packet delay are therefore measured as function of input traffic load. Results are shown for selected combinations of TCP and UDP traffic with SNR controller parameters such as slot length and maximum slot merging.

3.1 Measurement set-up

The operation of the SNR node controller and modem does not require any particular operation frequency. However, the channel bandwidth is of importance for the system throughput. The currently supported modulation and coding schemes (often called waveforms) are listed in

Table 4.3 (Annex C). The main utilisation until now has been single frequency operation with a 25 kHz UHF channel, although HF operation with somewhat lower bandwidths is possible as well.

The current measurement set-up includes one link only, enabling characterisation of a single link SNR network, see Figure 3.1. The radios are connected together with a combination of attenuators and a power divider. Additional routers are inserted between the node controllers and user PCs.

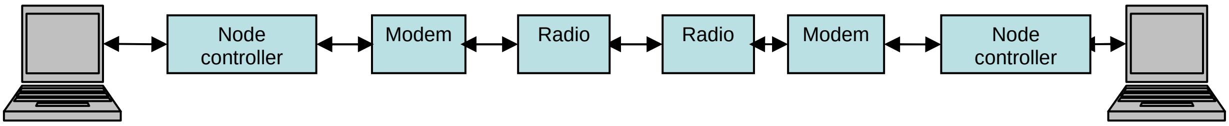


Figure 3.1 Laboratory test set-up

The XD432U8 UHF radio from Rohde & Schwarz is one interesting alternative for the Norwegian Navy, see Figure 3.2.

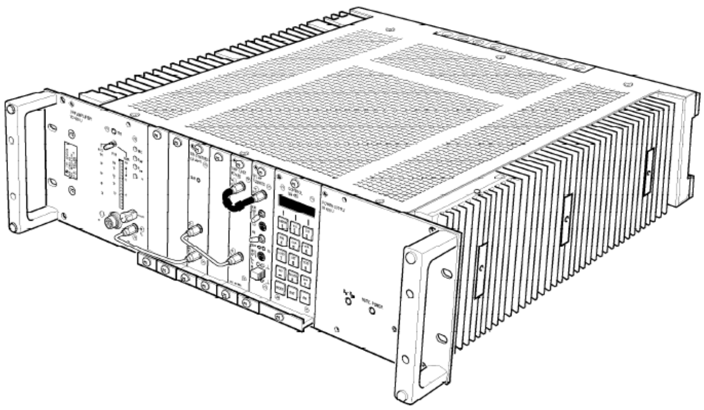


Figure 3.2 UHF radio XD 432U8 from Rohde & Schwarz

This radio is able to operate with near 25 kHz bandwidth when employing amplitude modulation through connector X29 located on the back. Pins 4 and 12 are used for push to talk, pins 3 and 15 for wideband input to radio and pins 6 and 15 for wideband output from radio. It must be ensured that the crypto card in the radio, containing connector X29, has jumper X11 in the correct position to enable modulation of the wideband output signal.

The SNR system may utilise legacy bulk encryption devices to ensure privacy within the ad-hoc network. Encryption is also required to ensure that only friendly forces participate in the network, as SNR does not offer any authentication of the nodes. In the current trials, we have investigated the connection of a BID 1650 (British Inter Departmental) device between the modem and the node controller using a RS232 synch serial protocol. Work is still ongoing to get the SNR equipment to interwork with the encryption device. The Ministry of Defence in the UK have been asked to share information on this, and other issues, from their extensive trials. However, the information has not been made available for FFI yet.

The parameter settings during trials for the node controller and the modem are based on recommendations from Rockwell Collins and are listed in Annex B and C respectively. The main parameters are given in Table 3.1.

Parameter	Value	Parameter	Value
Mod&Cod	VUHF V2	**Receive delay**	140
Modem rate	76.8 kbit/s	**Tx delay opt**	110
Crypto	None	**Slot overlap**	110
Min holdoff	500	**Slot length**	705
Radio overhead	40	**Slot allocation**	Deterministic
Modem interl.	25	**Num RA slots**	2
Modem overh.	40	**Slots per cycle**	25
Slot guard time	40	**Max slot merge**	4
Transmit delay	110		

Table 3.1 Parameter settings for test scenarios

We employ the VUHF IPU V2 modulation and coding format running at 76.8 kbit/s modem transmission speed. It should be noted that not all of the parameters are described in the user manual, and it is therefore somewhat challenging to understand the implication on system performance of the relatively large number of parameters.

A weakness of SNR is that the parameters are radio dependent. According to Rockwell Collins the problem can be overcome by setting parameters suitable for the worst radio you expect to participate in the network. Despite using a radio with faster switchover time between transmit and receive than Rockwell Collins did in their testing, we still found the need to adjust the recommended parameter settings in order to obtain error-free communication. The slot overlap parameter had to be reduced from 140 ms recommended by Rockwell Collins to 110 ms in order to avoid significant packet loss.

3.2 Traffic measurements

The resource allocation algorithm introduces transient behaviour in the measurements. The initial allocated number of slots per user depends on the preallocation method chosen; we have by default used so called deterministic preallocation, see Annex B for a description. At the end of the measurements, the queue size decreases and less slots are allocated. The measurements were performed by generating traffic sequences of 7 minutes, and analysing only the middle 5 minutes of received traffic to obtain steady state results with minimal influence of the transients at the start and end of the measurement runs.

3.2.1 UDP measurements

We have measured UDP characteristics of the SNR nodes by utilising *mgen* software (8) running on a PC with Linux operating system. Measurements have been validated using the

Smartbits 600 from Spirent Communications. Mgen measures throughput in terms of user data, while Smartbits 600 measures layer 3 throughput including UDP and IP headers. In the following, measurement results generated by mgen only are reported.

3.2.1.1 UDP packet size

Initially, four UDP payload sizes were tested to see the influence of the additional header overhead(s): 222, 472, 972 and 1472 Bytes, where the latter corresponds to a full Ethernet frame. The measured throughput between two SNR nodes is given in Figure 3.3 with corresponding parameters shown in Table 3.1.

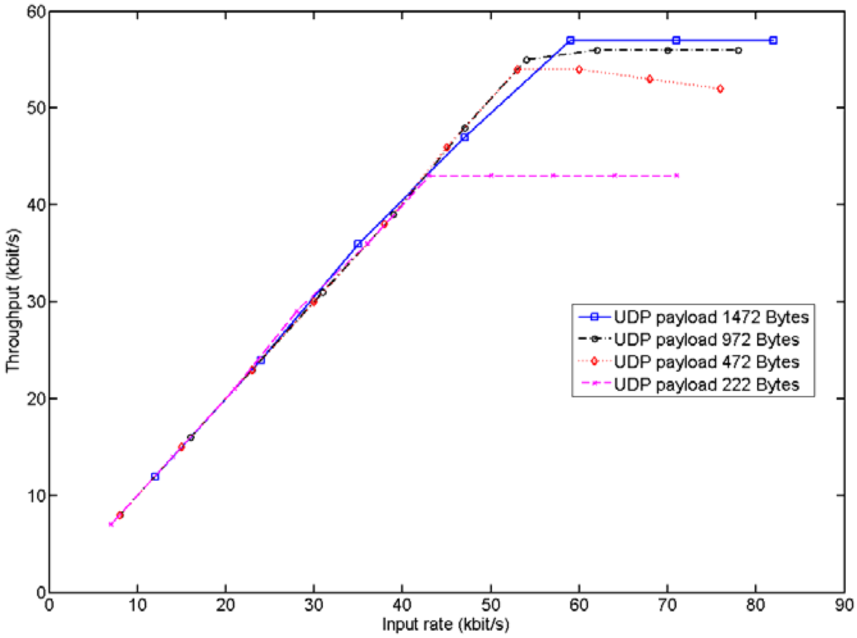


Figure 3.3 Throughput as function of input rate for different UDP payload sizes

The maximum throughput is significantly lower for an UDP payload of 222 Bytes. For the other cases, however, the impact of the packet size does not significantly affect the maximum throughput.

3.2.1.2 Slot merging

The influence of slot merging on throughput is shown in Figure 3.4, utilising a UDP payload of 1472 Bytes and a medium duration slot length of 705 ms.

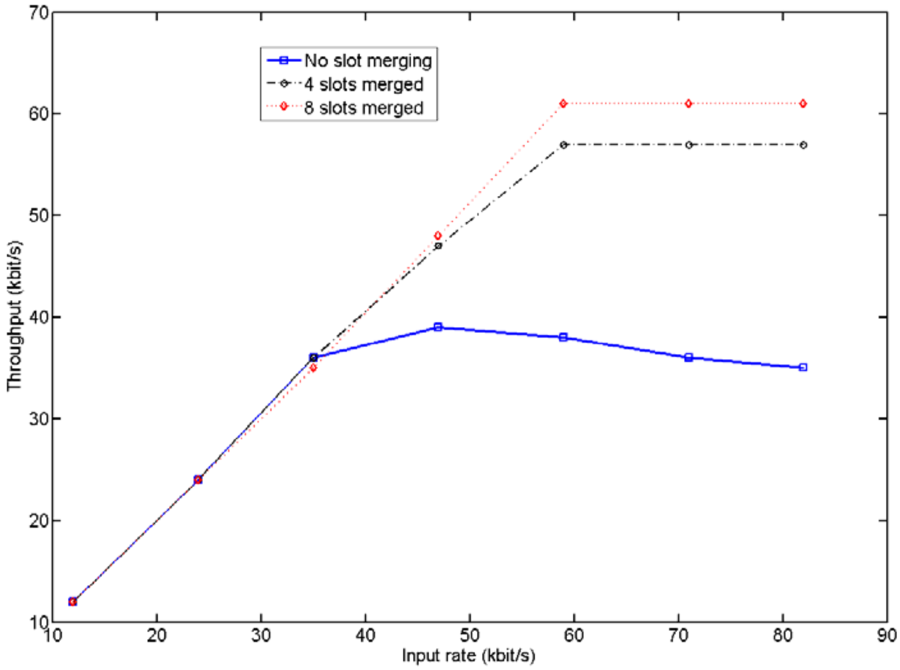


Figure 3.4 Influence of slot merging on throughput, slot length 705 ms

The amount of slot merging significantly influences the throughput for slot lengths of 705 ms. We see that allowing merging of more slots results in higher throughput. There is, however, a penalty in the form of increased roundtrip delay. At input rates exceeding the capacity the throughput is actually found to decrease somewhat with increasing input rate for the case with no slot merging. The corresponding average packet delay is shown in Figure 3.5.

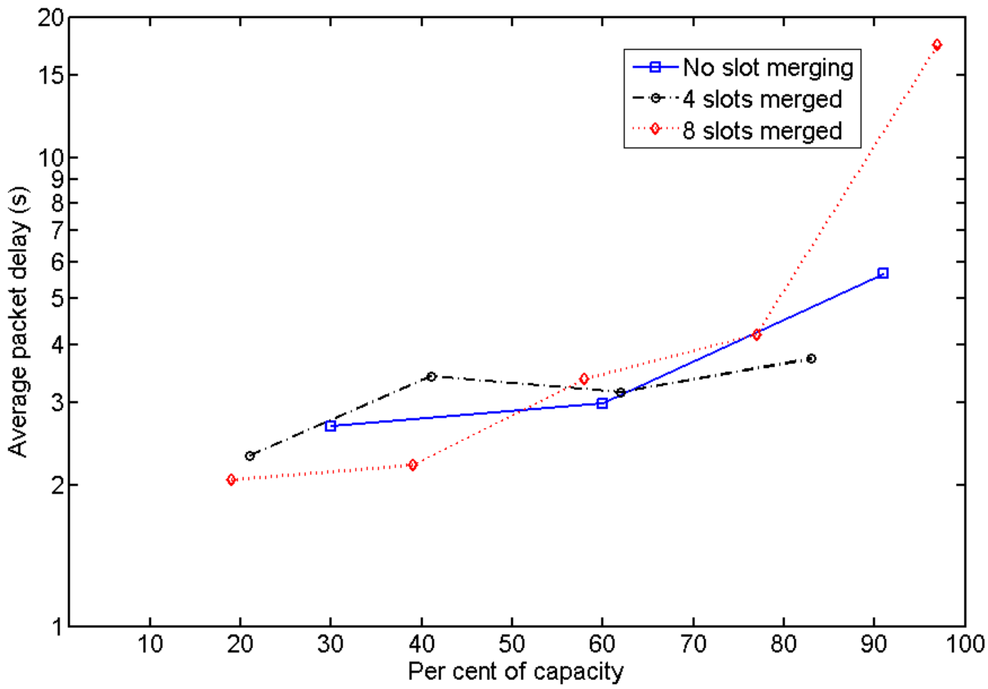


Figure 3.5 Influence of slot merging on average packet delay, slot length 705 ms. Per cent of capacity is found by dividing the input rate by the max throughput for each case.

At low to moderate throughput, the average waiting time is in the range of about 2 to 4 seconds for these unidirectional traffic flows. The significant increase in average packet delay in case of a maximum of 8 merged slots when the throughput is close to the capacity limit may be caused by the slot allocation algorithm. The time evolution of the packet delay from the start of the measurements is shown in Figure 3.6.

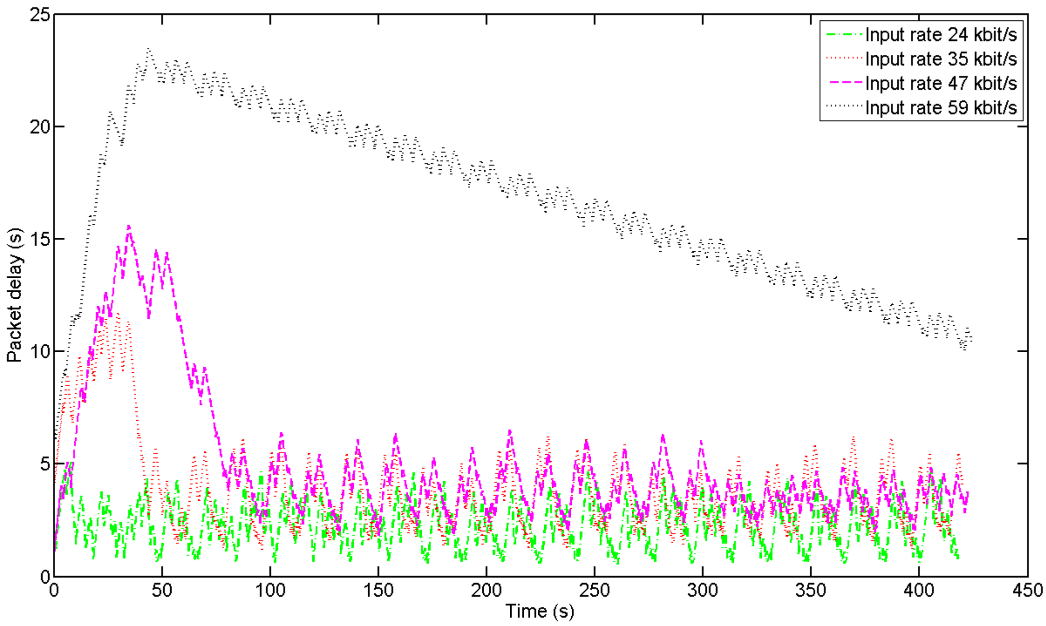


Figure 3.6 Packet delay as function of time, maximum 8 merged slots, slot length 705 ms

For input bit rates below the capacity, the initial delay increases until a sufficient number of slots per cycle is allocated. Thereafter, the length of the transmit queue decreases and the delay decreases towards the steady state value of a few seconds. The rate of time delay decrease depends on the difference between the input bit rate and the maximum throughput. The input bit rate of 59 kbit/s is very close to the capacity for this case, and we see from Figure 3.6 that the delay for this input rate decreases slowly.

Slot merging enables less overhead as only one preamble is required for the merged slots. For a short duration slot of 380 ms, the effect of enabling merging of four slots is about a threefold increase of the transmission capacity, see Figure 3.7. The resulting capacity difference by increasing the maximum number of merged slots from 4 to 8 is also significantly higher than for the medium duration slot length of 705 ms, see Figure 3.4. It should be noted that combining 380 ms time slots with no slot merging produced some rather strange behaviour. It seems from our measurements that once the transmit queue is filled up, which happens quickly in this case as the system throughput is limited by short time slots, instead of just discarding some new packets and carrying on, transmission comes to a complete halt. Once the sender queue was full, no further packets made it to the receiver in this particular case. This implies that not all of the measurements shown in Figure 3.7 are based on 5 minutes of received data. This behaviour has been reported to Rockwell Collins, who have not yet been able to provide us with an explanation.

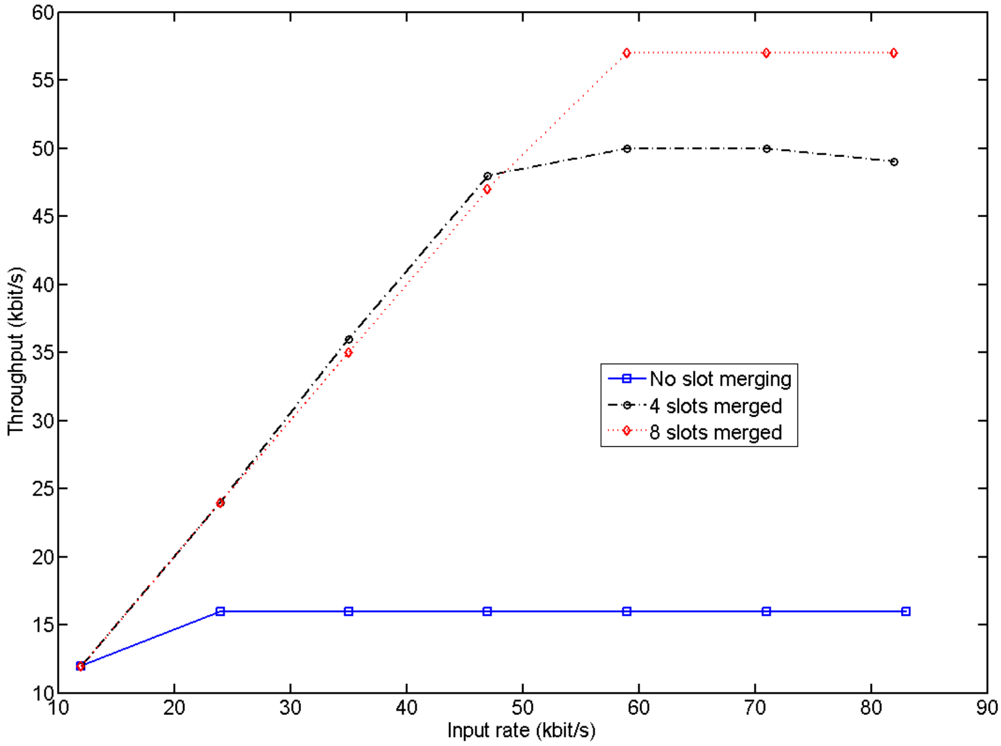


Figure 3.7 Influence of slot merging on throughput, slot length 380 ms

The resulting throughput variations for a slot duration of 980 ms and varying degree of slot merging is shown in Figure 3.8.

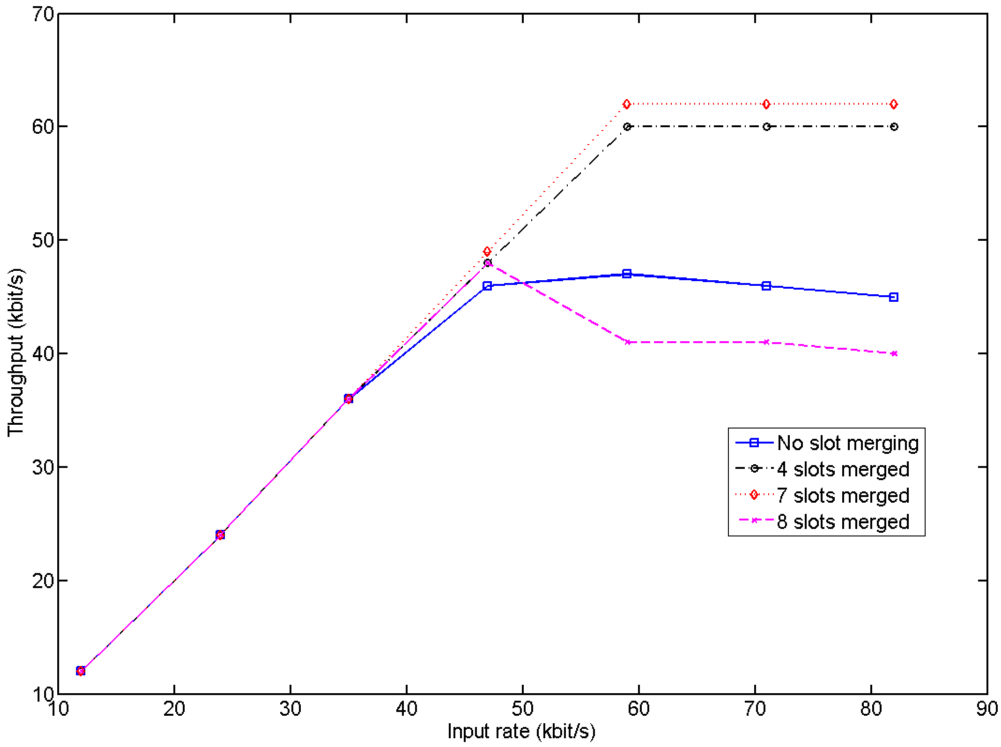


Figure 3.8 Influence of slot merging on throughput, slot length 980 ms

It is interesting to observe the significant decrease in throughput at high loads for the case of maximum 8 slots merged. The system is not able to handle merged slots of this length

(980ms/slot · 8 slots). The receiving node controller buffer overflows, and packets are discarded. To illustrate this effect we have included the case 7 merged slots in this test. We see that the system is able to handle 7 merged slots of length 980 ms, but not 8.

The limited number of trials indicates that about 4 merged slots results in a reasonably good performance irrespective of packet length.

3.2.1.3 Influence of slot length

The influence of the controller slot length on available throughput is shown in Figure 3.9. The maximum slot merging parameter has been set to 4 for this test.

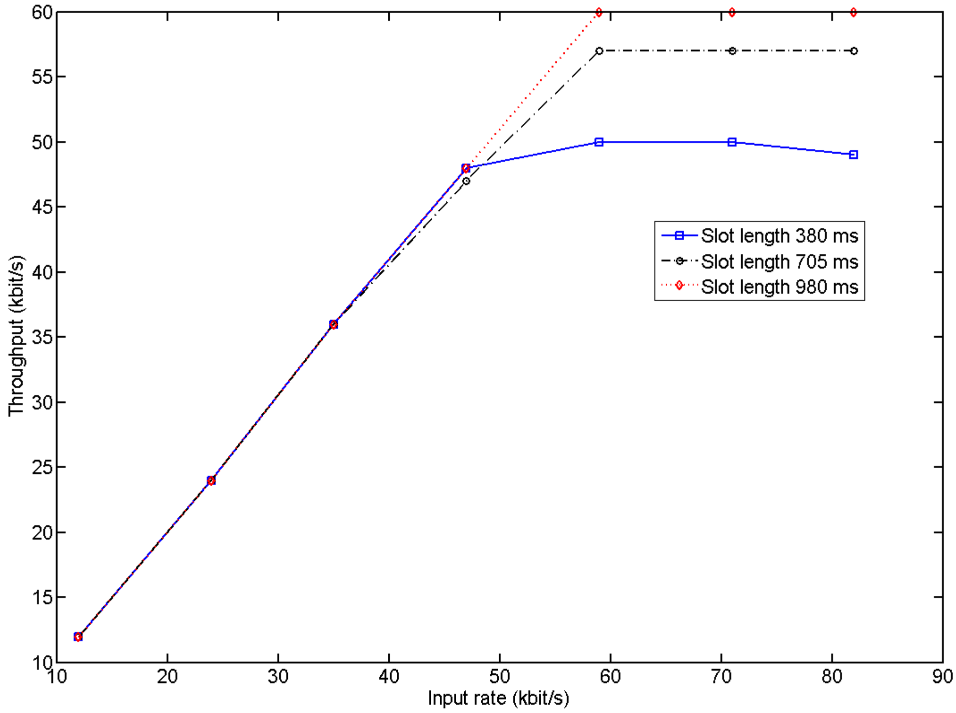


Figure 3.9 Influence of slot length on throughput, max slot merging of 4

The available throughput increases with increasing slot length, and the medium slot duration of 705 ms results in about 10 kbit/s higher maximum throughput than the shortest duration. By increasing the slot length further, a slight increase in throughput is observed. However, the average packet delay, displayed in Figure 3.10, clearly displays the time delay penalty by applying long duration merged slots during normal operation conditions.

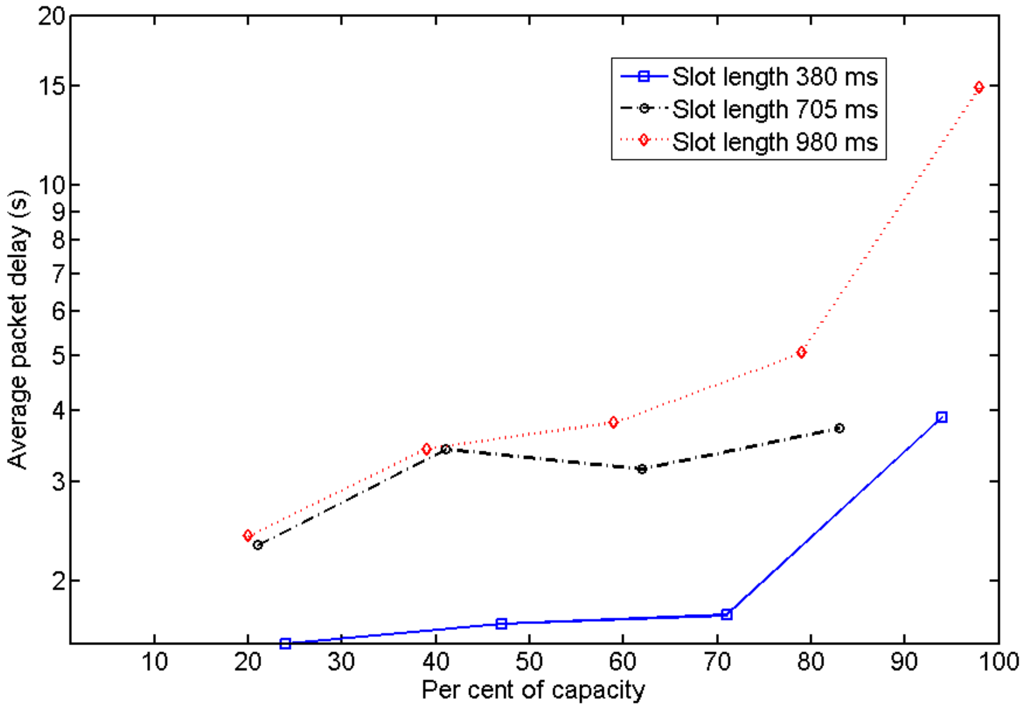


Figure 3.10 Influence of slot length on average packet delay, max slot merging of 4

Another factor that will influence the selected slot duration is the requirements from the application, or offered service. The UDP payload size may be of importance as well, if for example, avoidance of packet segmentation by selecting an appropriate slot duration improves the quality of service. Normally the end user is not directly involved in selecting such parameters. If the sub-network is utilised for specific applications for the majority of time, optimisation may be useful.

3.2.2 TCP measurements

The performance of SNR when utilising TCP traffic, commonly used by many Internet applications, was measured utilising the software tool Iperf (9) running on server and client computers with Linux operating system. SNR includes a TCP performance enhancing proxy, called IP traffic manager (IPTM) by Rockwell Collins. Measured TCP throughput for different combinations of node controller parameters are shown in Figure 3.11.

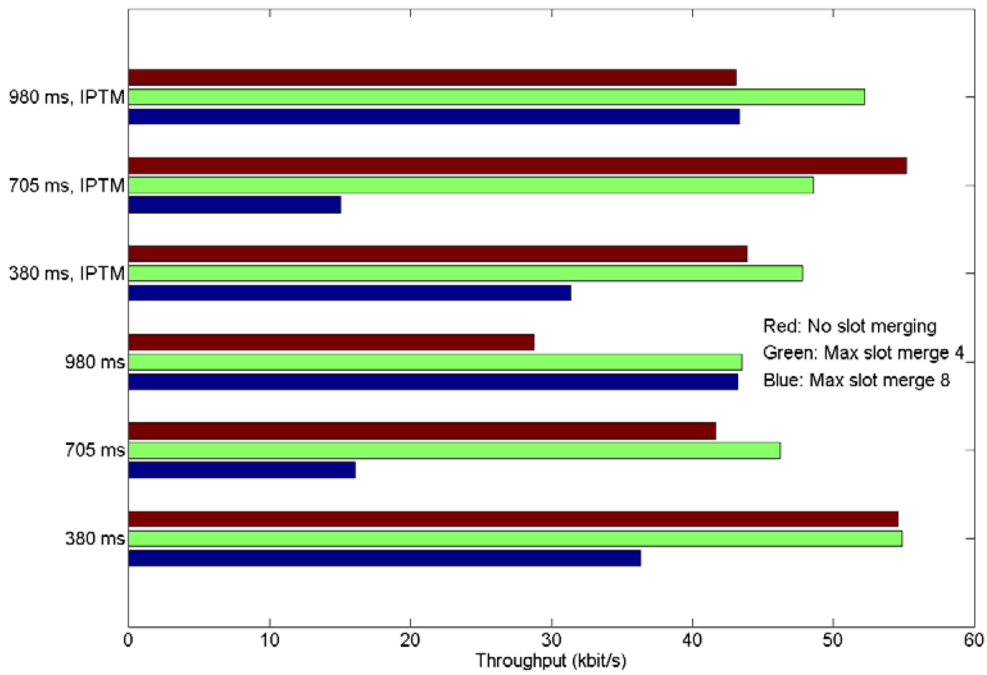


Figure 3.11 TCP throughput, single error free link

No great difference in throughput is observed between the cases with and without IPTM. We see that without IPTM, 380 ms slots give the best throughput. This is reasonable, as shorter time slots make the system quicker, i.e. the TCP acknowledgements arrive faster. For slots of long duration the IPTM increase throughput, while for short slot times the throughput is actually somewhat higher when not employing the IPTM.

Once we introduce some errors in the form of packet losses into the system, however, the situation becomes different, see Figure 3.12.

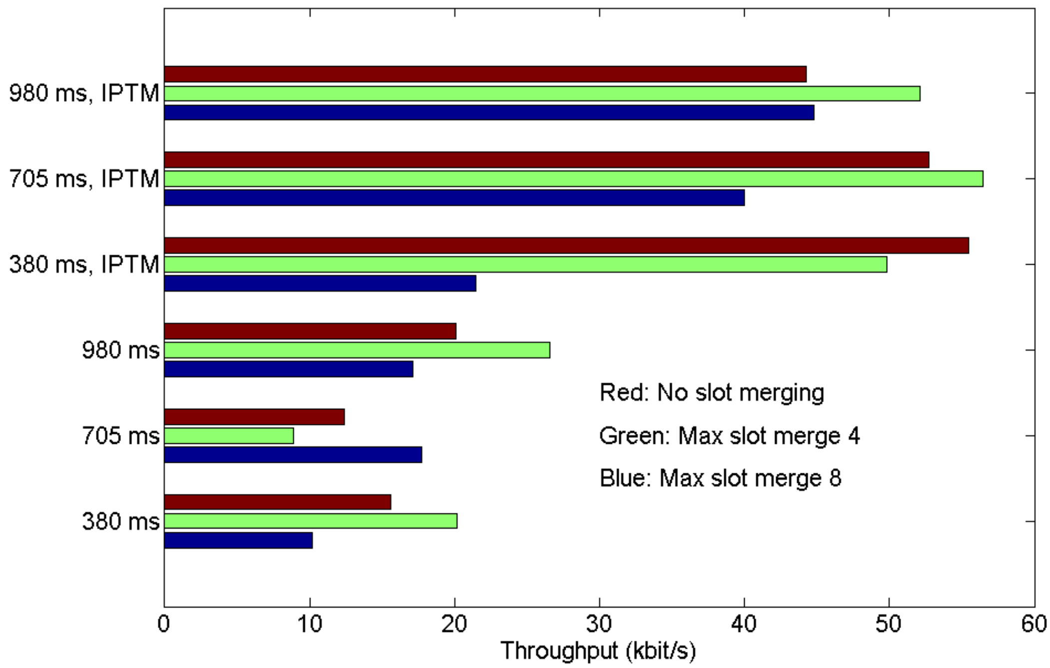


Figure 3.12 TCP throughput, single link with packet errors

Rather than a perfect channel, we now have about 1 per cent random packet loss. As expected, there is a clear improvement in performance when using IPTM compared to when not using it. The highest throughput is generally obtained for a maximum slot merging of 4, irrespective of slot time duration. This is in line with the results obtained for UDP.

3.3 E-mail, chat, and voice over IP

The chosen applications for generating application type traffic is mainly the NATO Military Messaging Handling System (MMHS) for handling of formal military messages, as well as chat and VoIP functionality provided by for example Netmeeting. Voice capabilities of the SNR system are also of interest, although the limited throughput due to the narrowband channels might become a challenge.

Currently only a limited number of different application tests have been performed. XOmail worked well utilising UDP transport and one mail server per node. Multicast require necessary functionality to be implemented in the external router. Chat seems to work well, with a slight delay that probably is acceptable for the users. Netmeetings VoIP solution in the two node setup resulted in good voice quality, although the significant time delay degrades the end user experience.

4 CONCLUSIONS

Subnet relay is an interesting concept closing the gap between network enabled capabilities and practical wireless communications at sea. SNR enables range extension and IP connectivity for a group of ships at UHF frequencies. These are all desirable factors for the Norwegian Navy as well as other countries.

SNR seems to become a de facto standard in parts of the NATO fleet, although no STANAG has been formally approved. There is an ongoing cooperation between the Netherlands and Norway on testing of SNR equipment and investigation of standardisation possibilities. The NATO group handling standardisation aspects of SNR, the VUHF Ad Hoc Working Group, has concluded that the proposed STANAG from Rockwell Collins is currently not suitable for standardisation and that further work is required if it is decided to standardise a maritime ad-hoc network. In addition to required changes of more editorial nature, the lacking support of IP version 6, as well as the fact that Rockwell Collins is not willing to publish the “IP traffic manager”, might require substantial additional effort before a STANAG may be accepted. In addition there are a number of minor issues, such as definition of quality of service classes and the ability to handle merging and separation of networks that require further work.

Initial measurements of the performance of the narrowband system have been carried out at FFI. So far tests have been limited to a 2-node network, so relaying and routing aspects have not been evaluated. The preliminary results indicate reasonably good performance when selecting a proper parameter set. These parameters are subject to standardisation as well to ensure interoperability within NATO as they depend on characteristics of the radios and modems utilised. With a 25 kHz wide channel and a modem providing 76.8 kbit/s, the maximum application throughput obtained between two SNR nodes was about 60 kbit/s and the average packet delay exceeded about 2 seconds. For a degraded radio link introducing packet errors, the TCP performance enhancing proxy significantly improved the throughput. When increasing the number of nodes in the network the available throughput for each node will decrease, especially if relaying information between nodes is required to obtain connectivity. In a long term perspective traffic demand is expected to increase and alternatives with higher capacity may become required. However, SNR includes multi-hop functionality and enables use of existing hardware on board vessels with a resulting minimum integration cost when deploying the system onboard ships.

FFI plans to continue the investigation of SNR in cooperation with TNO in the Netherlands, including more extensive laboratory trials as well as field trials during manoeuvres. There have been efforts to get access to extensive trials performed by the UK, which might progress the work further as well.

References

(1) NATO AHWG VUHF input document from IpUnwired (Now Rockwell Collins), Technical specification to ensure interoperability of subnet relay node controllers.

(2) MARITIME TACTICAL WIDE AREA NETWORKING (MTWAN), ACP 200(A), AC/322(SC/6-AHWG/1)N(2005)0027

(3) M. Jorgenson, C. Reichelt and T. Johnson, “Operation of the dynamic TDMA subnet relay system with HF bearers,” IEEE Mil. Com. Conf., 17-20 Oct. 2005, vol. 1, pp. 338 – 343.

(4) RFC 3626, Internet Engineering Task Force, “Optimized Link State Routing Protocol (OLSR), www.ietf.org.

(5) S.M Faccin, C. Wijting, J. Kenckt, A. Damle, “Mesh WLAN networks: concept and system design,” IEEE Wir. Com., vol. 13, issue 2, April 2006, pp. 10 – 17.

(6) XOmail, Internet page http://xomail.com/

(7) J. Oetting, K. King, “The impact of IPsec on DoD Teleport throughput efficiency,” IEEE Mil. Com. Conf., vol. 2, 31 Oct. - 3 Nov. 2004, pp. 717 – 721.

(8) Multi-Generator (MGEN), Naval Research Laboratory, Internet page http://cs.itd.nrl.navy.mil/work/mgen/index.php

(9) Iperf, National Laboratory for Applied Network Research, Internet page http://dast.nlanr.net/Projects/Iperf/

A COMMENTS ON PROPOSED SNR STANAG

The draft Subnet Relay (SNR) STANAG was developed by IP Unwired some time ago and submitted to NATO Sub-committee 6. IP Unwired was acquired by Rockwell Collins in 2006, and is now Rockwell Collins Government Systems Canada, hereafter denoted as RC.

SNR enables an early entry to network based capabilities for mainly maritime, but also land and air forces. SNR is able to utilise commonly deployed radio equipment (HF - UHF) and bulk encryption equipment (only limited IpSec capabilities) and is considered as a useful extension of radio communication capabilities by operative personnel. The AUSCANNZUKUS nations have been involved in development and testing of the equipment, and several of them are now in the process of ordering SNR nodes in relative large quantities for their navies.

A.1 General comments

According to RC, the proposed STANAG is sufficient for independent implementation of the SNR system, including both the controller part and the proposed modulation and coding format for spectrum efficient communications. The proposed STANAG enables manufacturers to optimise their concepts within the system specifications, and care has to be taken to ensure interoperability. One such example is that RC has decided not to include the so called “IP traffic manager” as they consider this as a competitive advantage.

A system standard in the form of a STANAG may require independent implementations to ensure interworking of the equipment. The proposed STANAG seems to be on a “fast track”, and time limitations may hinder such interoperability tests with other vendors.

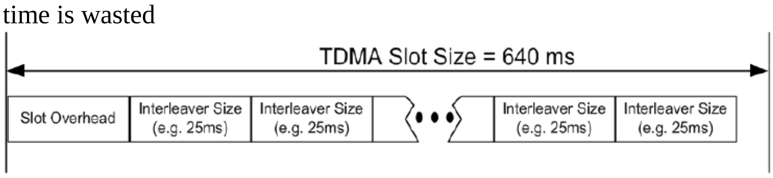
- RC has continued development of SNR and is willing to update the proposed STANAG if asked to do so. One new feature is the ability to include airborne SNR nodes, requiring handling of so called “advantaged nodes”.
- The performance enhancing proxy (PEP) is not included.
    - This is required for efficient TCP/IP communications on the narrowband SNR network and is in practice needed for a number of applications (HTTP, SMTP,...).
    - Without specifying the PEP, SNR will have a significant interoperability problem.
    - IpSec combined with PEP is an issue that require further work
- The proposed modulation and coding approaches (waveforms) from RC should be harmonised as long as possible with the ongoing work on narrowband VHF communications including aspects such as frequency hopping.
- Quality of services classes are not defined, but the system is prepared for it
- The SNR system will not be able to divide a large network into two or more smaller networks if groups of ships separate. It is unsure whether it is able to join two existing networks operating at the same frequency or if interference will degrade the performance.

A.2 Conclusions

It might not be necessary to standardise SNR. If it is decided to produce a SNR STANAG, additions to the specifications as well as interoperability test with different implementations may be required. This will require development of the missing components in the proposed STANAG, or some form of agreement with RC.

B SNR NODE CONTROLLER PARAMETER SETTINGS

Parameter	Value	Description
Data rate	76800 bit/s	Modem data rate
Crypto type	None	
Min Data Holdoff	500 μS	Minimum time to wait for CTS after RTS is asserted on the Sync Serial before transmitting in micro-seconds. Setting this to a value greater than 0 will ignore any glitches on the CTS line up to the given time. Note: this parameter is currently limited to 10,000 us, this limit may be modified in future releases.
Radio overhead	40 ms	The time, in milliseconds, taken by the radio to prepare for transmission of modem traffic. It is the largest of either: 1. The Radio Frequency (RF) Ramp-down time plus the RF Transmit to Receive Switching Time; or 2. The RF Ramp-up time plus the RF Receive to Transmit Switching Time.
Modem interleaver	25 ms	The time required, in milliseconds, to fill the block modem interleaver. This parameter is used in the calculation of the TDMA slot size and setting limits on Tx Delay Optimization and Slot Overhead (when activated).
Modem overhead	40 (2 preambles)	The time required, in milliseconds, to transfer the modem preamble. This parameter is used in the calculation of the TDMA slot size.
Slot guard time	40 ms	A time, in milliseconds, used to account for uncertainties in the system. Includes all elements of uncertainty like the maximum time synchronization jitter from various processing functions, propagation delay, etc.
Transmit delay	110 ms	The time, in milliseconds, introduced on the transmit side by the modem and crypto unit (if applicable). Includes: 1. Tx Crypto Synch Processing Delay - the time required by the crypto unit to process the crypto synch sequence. This does not include the time required to transmit the crypto synch sequence (which is the Crypto Synch Seq Overhead); 2. Tx Modem Interleaver Delay - for block interleavers, this value is the same as Modem Interleaver ; and 3. Tx Modem Audio Buffer Fill Delay - the time required to fill the audio buffer of the modem. This value is dependent on the modem and the waveform being used.
Receive delay	140 ms	The time delay, in milliseconds, introduced on the receive side by the modem and crypto units (if applicable). It includes: 1. Rx Crypto Synch Processing Delay – the time required by the crypto unit to process the crypto synch sequence. This does not include the time required to transmit the crypto synch sequence (which is the Crypto Synch Seq Overhead); 2. Rx Modem Interleaver Delay – for block interleavers, this value is the same as Modem Interleaver 3. Rx Modem Audio Buffer Flush Delay – the time required to flush the audio buffer of the modem. This value is dependent on the modem and the waveform being used.
Tx delay opt	110 ms	The time, in milliseconds, before the beginning of the OTA slot, that an SNR unit will begin to transmit. This is done to maximize transmission efficiency. The

		value can range from 0 (no optimization) to a maximum of the Tx Delay (maximum optimization).
Slot overlap	110 ms	The amount of time, in milliseconds, that a received STU from slot N-1 can overlap into the transmitting unit's slot N. This overlap is allowed when the transmission delay optimization mode is used. If the STU is not received within the slot overlap time after the previous slot has ended, the STU is assumed to be out of synch and is discarded. The value goes from the Transmit Delay Optimization value to the sum of: 1. The SCRN Module Tx Processing Delay – the time in milliseconds required by the SCRN Module to process a STU; 2. The Tx Crypto Synch Sequence Processing Delay – the time, in milliseconds, required by the Tx Crypto to process the crypto synch sequence; 3. The Tx Modem Interleaver and Audio Buffer Fill Delay – the time, in milliseconds, introduced into the transmit stream by the Tx modem to account for the interleaver and to fill the audio buffer 4. The Rx Modem Interleaver and Audio Buffer Flush Delay - the time, in milliseconds, introduced into the receive stream by the Rx side of the modem to account for the interleaver and to flush the audio buffer; 5. The Rx Crypto Synch Sequence Processing Delay – the time, in milliseconds, required by the Rx Crypto to process the crypto synch sequence; and 6. The SCRN Module Rx Processing Delay – the time in milliseconds required by the SCRN Module to process a received STU; Each SCRN module will have to overlap incoming and outgoing transmissions to ensure the slot timing OTA is maintained. As such, there is an allowable overlap for an incoming transmission for the preceding slot. This value is the Slot Overlap. If a transmission is received that is not within the Slot Overlap, the STU is considered out-ofsynchronization and is discarded.
Slot length	350, 705 and 980 ms	The Over-the-Air (OTA) slot length in milliseconds.
Slot overhead ratio		This variable is automatically calculated based on the other parameters. It is the ratio of the total slot overhead to the maximum size of the data portion of the SNR Protocol Data Unit, otherwise called the Slot Transmission Unit (STU). The overhead includes all protocol overhead of the STU as well as the Crypto Synch Sequence, Radio, and Modem Overheads, and the Slot Guard Time.
Quantization error	0	The modem interleaver is a fixed size, as is the TDMA slot. As shown in the figure below, if the slot overhead plus an integer number of modem interleavers does not fit exactly within the TDMA slot size, then in every slot, there is a period of time at the end of the slot in which nothing is transmitted. As such, this time is wasted  The quantization error, a calculated value, is the percentage of the wasted time compared to the overall slot size. In the example of the figure, the quantization error is 2.3% (i.e. (640 mod 25)/640). Once the interleaver size is entered, the

		user should try to set the slot size to minimize the quantization error value.
Time source	Garmin 16	Used to select the GPS type connected to the SCRN Module.
Ignore valid flag	Enabled	If Disabled - the Valid flag in the sentence from the GPS will be checked and if the GPS indicates that it does not have a valid fix, SCRN will NOT process the sentence. If OFF - the sentence will be processed, although the GPS may not have a valid fix.
Ignore NMEA errors	Enabled	Errors in the NMEA string are detected using a checksum at the end of the string. Some GPS receivers do not use a correct checksum. Enabling the “Ignore NMEA Errors” will allow the use of NMEA data with a broken or incorrect checksum.
Compression	None	Used to set the level of compression used by the SCRN Module. Level 9 gives highest compression and, thus, highest data throughput, whereas level 1 gives you lowest compression, and lowest data throughput.
Slot allocation	Deterministic	1. No Preallocation: Maintains the minimum amount of slots to stay in the SNR network. Example: an 8 slot cycle with 2 active nodes will only take 2 slots and leave 6 open when this is enabled 2. Half Preallocation: Will randomly divide half the available slots among active nodes in the SNR network. Example: an 8 slot cycle with 2 active nodes will allocate 2 slots for each active node 3. Full Preallocation: Will randomly divide available slots between all active nodes in the SNR network. 4. Deterministic: Makes the best use of over the air time by actively allocating sequential slots to active nodes to easily merge slots and reduce overhead. This is the recommended setting.
Tx que TTL	120	Time to Live for packets in the Transmit Queue of the SCRN module in seconds.
Num Ra slots	2	Random access slot – a slot that can not be chosen by a node in the network. It allows for others to join the network by transmitting in the RA slot. Typically 2.
Num slots/cycle	25	This lets the user limit the time required to complete a cycle. The number of SCRN modules allowed to exist in the SNR space is limited by the slots per cycle. Eg. if RA= 2 and num Slots/Cycle=12, 10 SNR nodes will be the maximum.
Neighbour sense	3 of 5	X of K is the minimum times a new node's transmission (X) is heard out of a maximum (K) in order for it to be a valid neighbor. Eg. if neighbor up is set to "2 of 3"; a new neighbor node has to be heard at least 2 times out of a maximum of 3 transmissions for it to be added to the subnet.
IPTM	Enabled	IPTM more than doubles SCRN TCP throughput over HF/VHF/UHF wireless bearers. It is wholly transparent to both the source and destination stations’ and requires no modification of software on end workstations, routers, or other network equipment. For the initial release of IPTM, all nodes on a subnet must either have IPTM enabled or disabled.
V1 compatibility	Disabled	Forces 32 slots/cycle, does not allow slot merging, as well as some other aspects that are limited in V1 of SNR. Basically it allows compatibility with original version 1 of SNR.
Slot merging	Normally enabled	Enabling this feature will allow the SCRN module to merge available slots in the SNR timing cycle when there is not high demand for over the air time. This allows for faster transfer of large files due to reduced overhead from individual

		slots and removes the need to wait for the SCRN module to wait for its turn in the TDMA cycle.
Max merges slots	0, 4, 7, 8	This limits the number of merged slots, when Slot Merging is enabled.
Logging menu		Enable this feature to log errors and other information performance and troubleshooting the system.

Table 4.1 B SNR node controller parameter settings

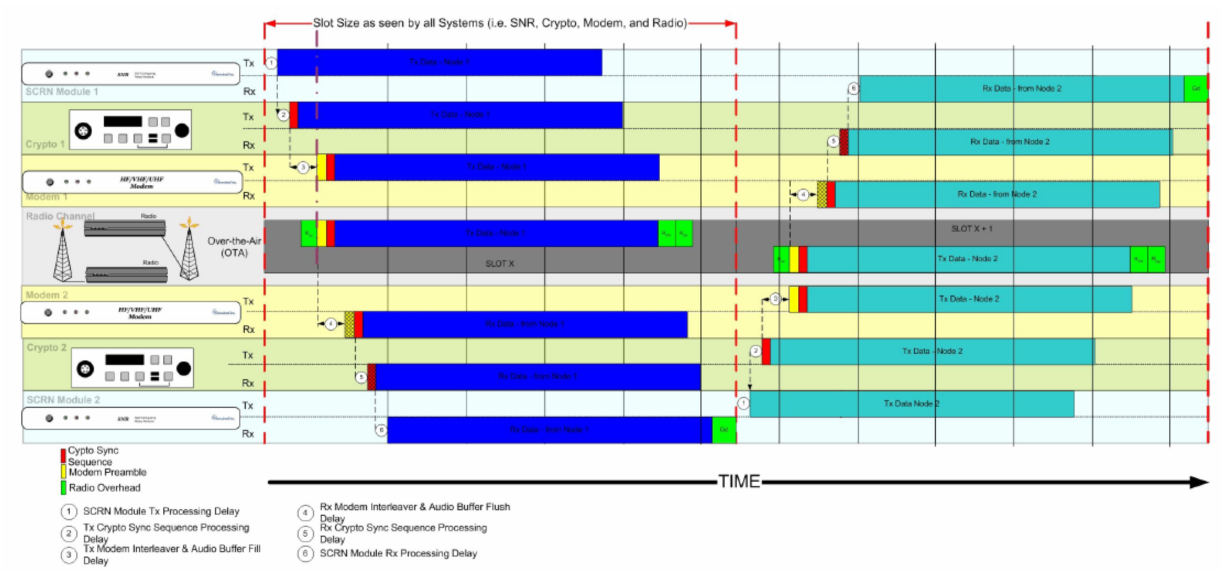


Figure 4.1. The SNR System Timing Structure without Optimization

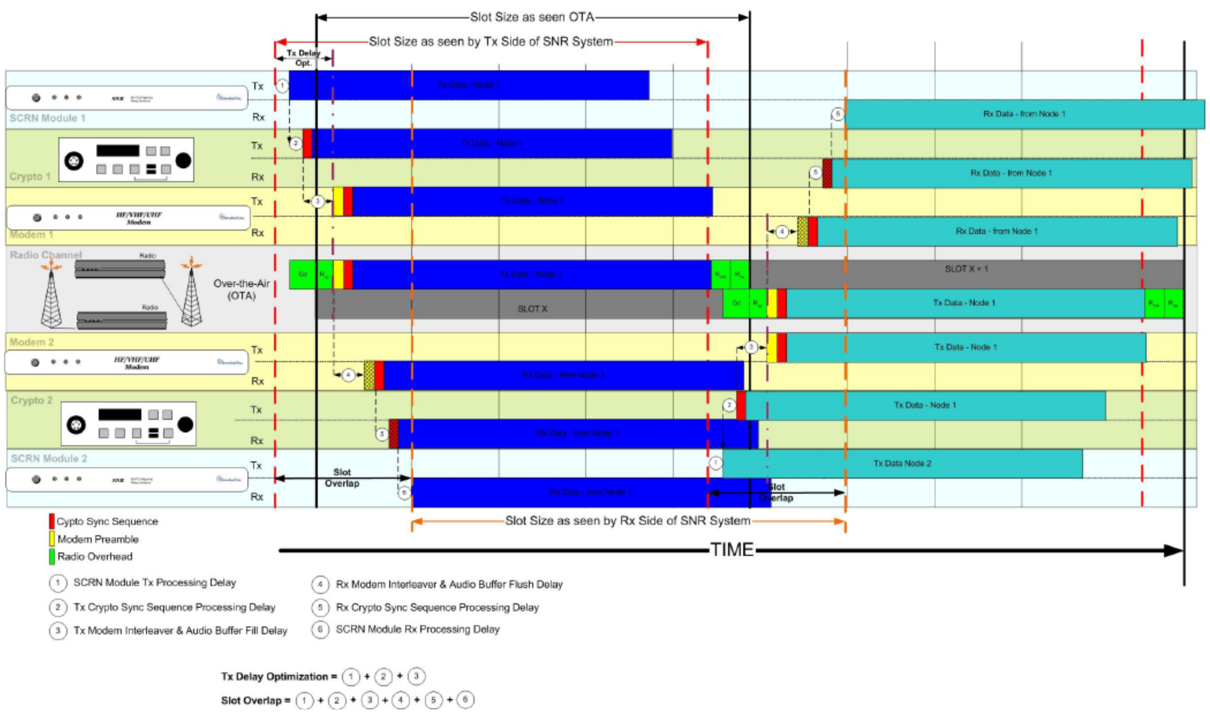


Figure 4.2. The SNR System Timing Structure with Optimization

C SNR MODEM PARAMETER SETTINGS

Parameter	Setting
Waveform	VUHF IPU V2
Tx interleaver length	Very short (25 ms)
Tx constellation	Normal
Receiver autobaud	Full
Loop mode	No loopback
Data interface	Synchronous
Data invert	Normal
Preamble length	2 (preambles)
Duplex	Half
Frequency tracking	Enable
Data source	External
Optional EOM	On
Max message duration	0
Drop out time	Medium
Min ALC setup time	0
Power level	-13 dBm (XD 432U8 Rohde & Schwarz)
Key line hang time	0
DTR behaviour	Ignore
DCD behaviour	VDP
Synch TX clock	Internal
COTS asynch mode	Disable
ADC gain	Normal
BER test	1000

Table 4.2 Modem settings

Waveform	Description
Mil-Std 188-110A	These waveforms provide rates from 75 bps to 2400 bps with convolutional coding and 4800 bps in an uncoded form. These waveforms form the basis of the STANAG 4539 mode from 150 bps to 2400 bps, albeit with relaxed performance specifications.
Mil-Std 188-110B	These standard waveforms specify high data rate, autobaud HF waveforms in Appendix C (for single channel operation) and Appendix F (for dual channel or ISB operation). In a single channel, this standard specifies data rates of 3200, 4800, 6400, 8000 and 9600 bps, protected by a convolutional code, or 12.8 kbps in an uncoded mode of operation. In two channel operation (i.e. ISB operation), data rates of 9600, 12800, 16000 and 19200 bps are supported. These autobaud waveforms and the single channel variants form the basis of STANAG 4539
STANAG 4285	This waveform is used by NATO at 300 bps for the BRASS naval broadcast. It provides data rates of 3600, 2400 and 1200 uncoded and 2400 to 75 bps coded. This waveform does not provide an autobaud capability and both transmitter and receiver must agree on the data rate and interleaver settings before transmission begins.
STANAG	This is a very robust 75 bps HF data waveform. It will operate effectively almost 10 dB below

4415	the noise floor in a noise dominated environment, nearly 40 dB below the level of a tonal interferer, and tolerate extremes of delay and Doppler spreading. This waveform is also included as the 75 bps rate of STANAG 4539.
STANAG 4529	This waveform is a derivative of STANAG 4285 which was developed for use in narrower 1240 Hz channels. The narrower occupied bandwidth was achieved by reducing the baud rate of the STANAG 4285 waveform from 2400 baud to 1200 baud and changing the filtering to reduce the occupied bandwidth. Achievable data rates are half of those with STANAG 4285.
STANAG 4539	This is the best all-purpose HF data waveform provided with the IPU modem. It offers very robust performance at 75 bps and high throughputs at 9600 bps, with those and all intermediate data rates protected by a convolutional code with a variety of interleaver settings. 12.8 kbps is available in an uncoded form. The autobaud capability available for all rates allows the transmitter to select a data rate and be confident that the receiver will be able to decipher the message without knowing the data rate or interleaver setting in advance. If your application does not require that you use a particular waveform to be interoperable with some existing system, this is the waveform that we recommend using.
Commercial Airborne Waveform	This waveform has been designed to work in the narrower bandwidths available in the Aircraft bands (2.4 kHz vice 3 kHz). Operating at an 1800 baud rate, rather than the more commonly used 2400 baud, this waveform provides an autobaud capability with data rates from 75 bps to 8000 bps (9600 bps uncoded). A selection of interleavers and a powerful constraint length 9 convolutional code ensure data integrity.
Commercial Maritime Waveform	This waveform was designed to support legacy maritime radios which may have extremely narrow passbands. Operating at a symbol rate of 1440 baud, this waveform provides an autobaud capability with data rates from 75 bps to 6400 bps (7680 bps uncoded). A selection of interleavers and a powerful constraint length 9 convolutional code ensure data integrity.
Programmable FSK	This waveform is provided for interoperability with legacy equipment which uses FSK modes of operation. Although not nearly as effective as the serial tone modes, FSK modems remain in operation worldwide and this mode allows the user to communicate with these older devices.
IP Unwired V/UHF HDR V1	This waveform is designed to provided high data rate digital data service using legacy radios which support wideband (>21 kHz) audio inputs. This waveform provides an autobaud capability in supporting data rates from 2.4 to 76.8 kbps. A selection of 4 interleavers is available: 40 ms, 160 ms, 640 ms and 2.4 s. Taken together with the constraint length 9 convolutional code used to ensure data integrity and the adaptive equalizer to mitigate the effects of multipath and fading, this waveform provides new capabilities in fading environments for legacy equipment.
IP Unwired V/UHF HDR V2	This waveform is very similar to the previous waveform. As with that waveform, this one is designed to provided high data rate digital data service using legacy radios which support wideband (>21 kHz) audio inputs. This waveform also provides an autobaud capability in supporting data rates from 2.4 to 76.8 kbps. Again, a selection of 4 interleavers is, available, but with slightly different options: 25 ms, 100 ms, 400 ms and 1.6 s. Taken together with the constraint length 9 convolutional code used to ensure data integrity and the adaptive equalizer to mitigate the effects of multipath and fading, this waveform provides new capabilities in fading environments for legacy equipment. Relative to the previous waveform, this waveform provides slightly more protection against time dispersion effects and slightly less against rapid fading or Doppler spreading.

Table 4.3 Currently supported modem waveforms