Student Research Project

Design and analysis of network addressing algorithms used for data communications in narrow band radio system

written by
cand. Dipl.–Ing. Dominik Lieckfeldt

Tutor:

Dr.–Ing. Hans-Dietrich Melzer (University of Rostock)
Dipl.–Ing. Thomas Kaltenschnee (Rohde & Schwarz GmbH + Co. KG)

Institute for Telecommunications and Information Technology
University of Rostock

Munich, 6. Juni 2005

Problem analysis

The objective of this student research project is to analyze and design aspects of the ISO OSI layer 3 with regards to the special requirements of network addressing in a radio network.

The conceptual formulation comprises two subtasks. The design and analysis of a statics addressing scheme and the analysis of a routing mechanism for the project TacSys. Both subtasks shall fulfill particular requirements that also have to be found. This student research project will be further divided into the following subtasks:

1. Investigation of the recently existing functionality of the tactical radio protocol stack and of the radio device.

2. Analysis of different radio net topologies .

3. Working out the requirements for a radio based network layer with regards to different radio and radio net addressing modes.

4. Design and analysis of an addressing scheme which meets the found requirements.

5. Analysis and evaluation of a bandwidth efficient routing algorithm which can be used for tactical nets.

The first step will be to analyze TacSys with respect to the requirements it has to meet and its application scenarios. Furthermore, the existing functionality of the RS-IRP stack and the radio device M3TR© has to be examined. Then the addressing capabilities of the radio unit will be investigated and compared with typical TacSys nets. Furthermore other existing addressing schemes will be considered as well. Thereby the requirements for the addressing scheme to be created will be found.

The last part will be finding and evaluating a suitable ad hoc routing algorithm. The evaluation will contain a simulation via Matlab© which has to consider the special conditions within TacSys nets that differ from usual simulation approaches in the area of ad hoc routing.

Abstract

This student research projects provides an approach for the RS-IRP network layer addressing scheme for the RS-IRP protocol stack of the Rohde & Schwarz project TacSys which especially considers the bandwidth restriction in the V/UHF frequency bands as well as the given addressing capabilities of SECOM-H and SECOM-V. In addition, RS-IRP network layer addressing can be used in conjuction with the radio remote control interface of M3TR© to further decrease the protocol overhead of RS-IRP.

Furthermore, this work shows that the ad-hoc routing protocol AODV can be used for tactical nets and provides a basic Matlab© simulation which is used to evaluate parameters of AODV.

Preface

This document was written at the company Rohde & Schwarz where I worked at the radio system development department 2WFE which is responsible for the development of applications for tactical communication. Recent projects included applications for data file and e-mail exchange and situational awareness amongst other things.

The department itself consists of several teams. I worked in the protocol development team that was concerned with implementing layer 2 and 3 algorithms for digital communications using the tactical radio M3TR© (Multiband, Multirole, Multimode Tactical Radio) which was developed by Rohde & Schwarz.

This document is divided into four parts. The introduction informs the reader about the general structure of the whole project and presents basic information about the used equipment, e.g. the facilities provided by M3TR©. The reader can find detailed information about the equipment.

The main part describes the process of analyzing the given tasks, of finding an adequate solution and of putting it into practice. In chapter 4 conclusions will be drawn and an outlook for potential next steps will be given. A list of abbreviations and acronyms and additional information can be found in the appendix.

Contents

List of Figures

1 Introduction

Large communication networks are only possible if a reasonable addressing scheme is used. The most common example is the world wide web. Growing in size and connecting people all over the globe it has become an import source of information. The addressing scheme defined in the Internet Protocol (IP) provides the facility to route information along different paths and over multiple intermediate stations. The IP addressing scheme allows to limit the propagation of traffic by introducing subnets. Furthermore addressing of more than one endpoint is possible as well.

The mentioned features are not only desirable for large scale nets but also for radio networks. The special conditions that occur due to propagation of radio waves in the HF, V/UHF frequency bands along with requirements for tactical radio nets demand for a special way of addressing participating units (`PU`). This work is an approach to combine already existing facilities with an addressing scheme that fulfills the requirements and provides for simple routing capabilities.

This section describes the TacSys(Tactical System) project in the business area 2 of Rohde & Schwarz and gives a survey of the project´s system architecture in general. The reader will find information not directly concerning the concept of the network layer but supporting the general idea of the whole system.

Throughout this document the `ISO OSI` reference model is used to classify and structure the project´s components. Those are a proprietary protocol stack including a radio unit and an application providing the functionality to remotely monitor and control the radio.

The main objective of the project is to support a flexible and efficient communication as well as to take into consideration the special military requirements like radio silence, protection against jamming or detection and interception of radio communication.

1.1 About Rohde & Schwarz and TacSys

Both company founder Dr. Lothar Rohde and Dr. Hermann Schwarz studied in the physico-technical institute of Jena and finished in 1931. As they both were greatly interested in RF measurement they kept in contact to experiment with electrical discharges in gases. Their ongoing research resulted in their first joint measurement instrument in 1931, a precision frequency meter for wavelengths of 6 to 3600 m. In August 1933 the scene was set: a vacant apartment at num-

Figure 1.1: Company founders Dr. Lothar Rohde and Dr. Hermann Schwarz.

ber 36 Thierschstrasse, about 120 sqm in size, was converted for their purpose and became the first place of business of the "Physikalisch-technisches Entwicklungslabor" Dr. Rohde und Dr. Schwarz, or PTE for short.

Today Rohde & Schwarz is a company with an international presence in the fields of test and measurement, information technology and communications. For 70 years the company group has been developing, producing and marketing a wide range of electronic products for the capital goods sector. The company is headquartered in Munich, employs about 6150 people worldwide and has subsidiaries and representatives in over 70 countries around the world. Rohde & Schwarz also develops systems for secure radio communication. By using software-defined radios the facilities of such systems are expanded and include voice and data transmission along other services such as e-mail and radio-link to internet.

1.1.1 Description of the TacSys system

This section provides a detailed view on TacSys which is a project of the department 2WFE at Rohde & Schwarz (see figure 1.2 for an arrangement of 2WFE). Starting with an overview of the structure of 2WFE and continuing with a closer look at the requirements and concerns of TacSys, this section will finally focus on the description of the protocol stack RS-IRP which main purpose is to provide optimized data transmission over the radio unit M3TR©.

The department 2WF consists of two main subdivisions: a marketing and sales and a system development devision. Whereas the former is concerned with customer relations and marketing and sales of 2WF´s products, the system development department 2WFE deals with application design and protocol development. 2WF provides products for end-users which are mostly found in the military sec-

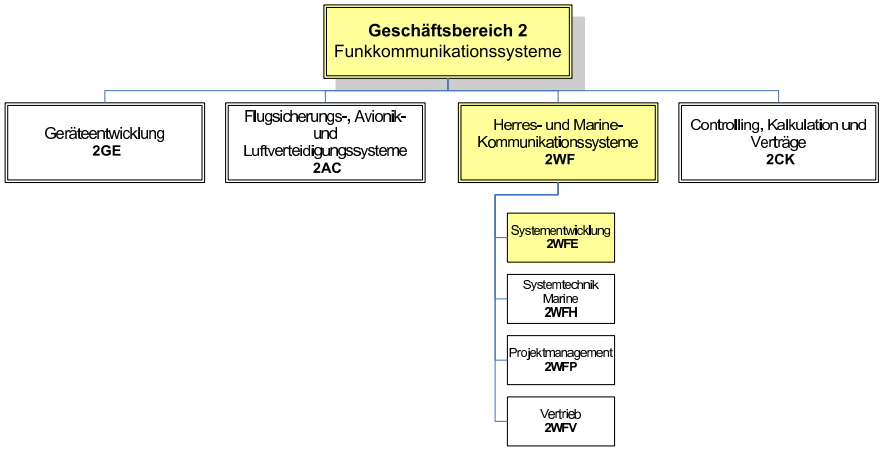

Figure 1.2: Arranging 2WFE in the business domain 2 of Rohde & Schwarz

tor. In recent years, the need for solutions which combine modern communication services with security requirements has strongly grown in this sector. 2WF uses Rohde & Schwarz military radio systems such as M3TR© or XK 2000 as a basis for application and protocol development.

TacSys is project which has the objective to provide secure, flexible, mobile and ergonomic communication solutions for military use. Using the M3TR© as radio set, applications such as E-Mail, SMS and Video amongst others shall be provided to the customers. TacSys is divided into layer 2 and 3 protocol development and application specific design. As shown in figure 1.3 the protocol stack shall provide service access points which allow the applications to use the underlying functionality.

The protocol stack which is referenced as RS-IRP implements parts of the `ISO OSI` layer 2 and 3. The addressing and routing aspects of the Network Layer are subject of this student research project, whereas layer 2, which is divided into Logical Link Control and Media Access Control, is already implemented in a basic version which is further being enhanced. The latter provides secure and non-secure data link communication along with adaptive data rate control functionality. Furthermore it supports quality of service (QoS) mapping and channel access algorithms which provide fair (CSMA) and priority controlled access (dynamic TDMA).

The radio unit M3TR

The Rohde & Schwarz M3TR© is a multi-band, multi-mode software-defined radio which provides line-of-sight (LOS) and beyond-line-of-sight (BLOS) communication. It covers the spectrum from M/HF (Median Frequencies/High Frequencies) to the UHF (Ultra High Frequencies) frequency bands[1]. The wide range

[1]see (5) for a classification of the used frequency bands

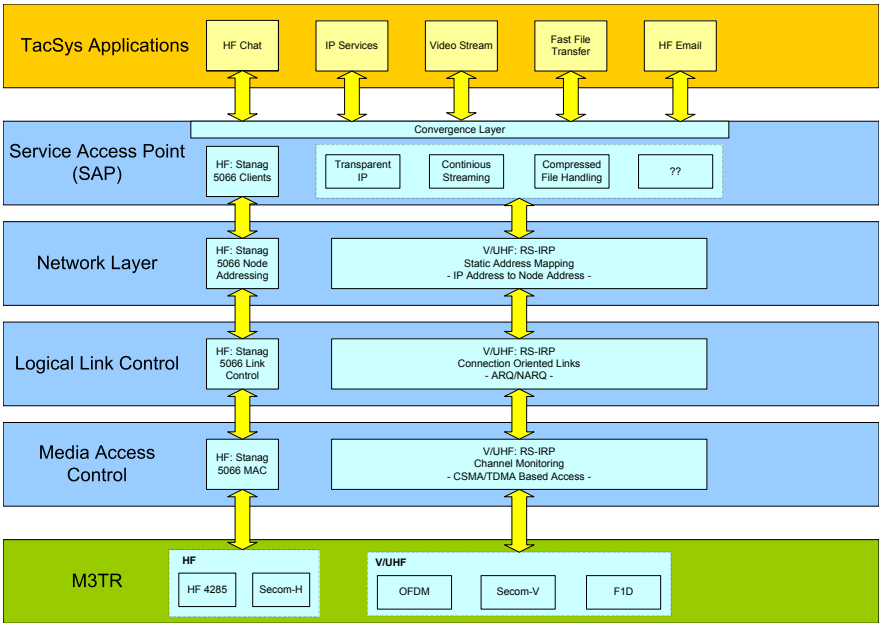

Figure 1.3: TacSys project structure.

of usable frequencies of the M3TR© meets various national and international regulations, thus providing global operation in changing missions and environments.

Its transmission capabilities include the military waveforms ALE according to MIL-STD-188-141B, STANAG 4285 and SECOM-H for BLOS and SECOM-V for LOS communication. Furthermore a high data rate communication mode using OFDM is also available. The integration the Communication Security layer (COMSEC) and the compatibility to various external COMSEC devices provide protection against detection, interception, jamming and spoofing.

As will be further explained, the M3TR© provides functionality which correspond to `ISO OSI` layer 1,2 and 3. Nevertheless, there is, for example, no ARQ (Automatic Repeat Request) functionality implemented nor a channel access algorithm. That is why additional radio protocol parts have to be developed that add this functionality.

Survey of M3TR© ´s transmission modes

This section shall briefly inform the reader about the used transmission techniques. For an in depth view of this topic (4) are recommended.

SECOM-H is a slow frequency-hopping spread spectrum transmission mode which is used for communications in the M/HF frequency bands, i.e. 1,5 MHz - 30 MHz. Slow means that the hopping rate equals the symbol rate. The available bandwidth W is divided into many smaller "frequency-slots" of bandwidth B. Every other time interval T_c another frequency is

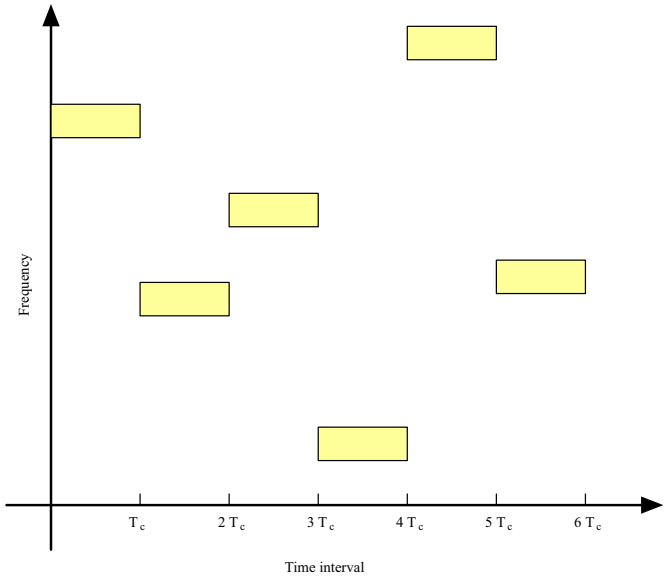

Figure 1.4: Example of a frequency sequence in SECOM-H mode.

selected by a pseudo-random algorithm to transmit data during communication . The pseudo-random algorithm is responsible for security aspects and determined by a specific key hopset combination along other parameters which must be known to both sender and receiver. Stations not knowing this combination can not follow the communication and might not even be capable of recognizing that there is transmission.

The hopset is the pool of frequencies that are available for hopping. A crypto algorithm choses the actual frequency for each hop. This provides the facility to generate hopping sequences that have none or few common frequencies allowing multiple users to access the same bandwidth W with minimal interference. In addition it allows for establishing different communication channels, i.e. one for all stations to listen on and private channels for actual point-to-point or point-to-multipoint connections with own key-hopset-combinations. Furthermore, it also provides the possibility to divide `PUs` into member of a specific net, subnet or multi-point-group. However, stations included in such a communication have to agree upon key-hopset-combination. Therefore a so called link setup (`LSU`) is required before every data transmission.

SECOM-H provides data rates up to 2,4 $\frac{kbit}{s}$ (3 kHz radio channels) with forward error correction.

SECOM-V is a fast frequency-hopping spread spectrum transmission mode which is used in the frequency range from 30 MHz to 108 MHz and 121 MHz to 512 MHz. SECOM-V provides data rates up to 9,6 $\frac{kbit}{s}$ with forward error

correction are possible.

OFDM is a multi-carrier transmission mode which spreads the data over multiple adjacent frequency channels. The M3TR© provides OFDM transfer data rates of up to 72 $\frac{kbit}{s}$ (25 kHz radio channels).

SECOM and COMSEC

The Rohde & Schwarz development SECOM (SECOM-V for the VHF and UHF bands, SECOM-H for HF) is a frequency hopping transfer method. It provides secured communication and network features.

SECOM introduces an own addressing scheme which allows for hierarchical net topology. This also includes that header information is added to every data packet send.

Within one SECOM-V net, several subnets and sub links can be established simultaneously in point-to-point, point-to-multipoint and broadcast mode. Network synchronization and access can be planned and controlled individually for each user.

The COMSEC part of the SECOM Enhanced Protection Methods (EPM) is based on a crypto algorithm developed by Rohde & Schwarz. The method uses key lengths of up to 256 bits (approx. 107 variants).

Interfaces

The M3TR© can be accessed via RS232 and RJ45. The protocols developed for TacSys use the RS232 as bidirectional, asynchron interface to receive and to send byte-oriented data and to remotely control the radio and its parameters.

Radio remote control (radio remote control) provides access to the parameters of M3TR© and allows for establishing logical links. This is important for SECOM-V and SECOM-H mode because a link setup (`LSU`) is performed at the beginning of every communication. It is used for temporary time synchronization of the calling and the called `PU` (or `PUs` in case of multicast) which includes agreeing upon a unique sequence of hopping frequencies. That is why the following communication can not be overheard by other members of the net. Further, the created symmetric link can be used as long as the communication lasts.

A software module which allows for monitoring and changing radio parameters has been developed by the author.

1.2 Outline of the main part

The main part of this student research project is divided into three chapters. The first chapter, chapter 2, is about static addressing in tactical networks and begins with an analyzis and considerations of the relevant requirements: Section 2.1.1

presents the requirements the radio net addressing scheme to be created has to meet and section 2.1.2 analyzis the addressing capabilities of SECOM-H and SECOM-V transmission modes of M3TR©. The section 2.2 investigates whether STANAG 5066 addressing can also be used for RS-IRP with regards to the previous investigations. The last part of this chapter which is section 2.3 presents an approach for a network layer addressing scheme for the RS-IRP protocol stack which is the conclusion of the consideration of this chapter.

The second chapter of the main part, chapter 3, covers the investigation of tactical radio nets with regards to ad-hoc routing. This chapter motivates why routing is also interesting for tactical radio nets and further investigates the promising ad-hoc routing protocol AODV. Section 3.1 presents the relevant requirements (section 3.1.1) for this task and introduces the main aspects of AODV (section 3.1.2). Section 3.2 deals with the simulation of AODV using Matlab©. Here the model of the simulation is explained (section 3.2.1) and the measured metrics are introduced (section 3.2.2). The final section of this chapter, section 3.3, presents the conclusions of the previous sections and evaluates the results of the simulation.

The last chapter of the main part, chapter 4, provides a summary and evaluates the results of the main part. In addition, an outlook is provided that outlines what can be done to further investigate the given task and to improve the simulation.

2 Discussion of static addressing schemes

This chapter provides a closer look at addressing issues related to RS-IRP. Starting with a short introduction why to use network addresses within TacSys this chapter explains a potential solution for the given subtask and its lead-through.

In general, the network layer according to the ISO OSI protocol stack shall provide end-to-end connectivity. This requires that packets may make several hops at intermediate PUs while propagating through the net. Inorder to support routing there must be an addressing scheme that uniquely identifies source and destination of a communication[1].

One of the main objectives of TacSys is to interoperate with existing communication infrastructure, e.g. LANs, satellite links etc. This demands for network-wide unique addresses to provide data transfer between nets and within nets over multiple hops. The interoperability and networking capability respectively becomes more and more one of the main demands of customers. Nevertheless, it has to be pointed out that this demand for interoperability has different importance for the HF and V/UHF communications respectively.

In contrast to the HF communication part of TacSys, typical tactical nets consist of 5 to 10 PUs that use SECOM-V or OFDM in the V/UHF frequency bands. However, the number of nodes per net may change as a consequence of specific customer requirements. The PUs of one net can be either vehicles with build in M3TR© plus tx amplifier or man-packs, i.e. M3TR© with light-weight rechargeable battery carried by a person. Both types of PUs have different transmission ranges and velocities according to their antenna and the power of the tx amplifier. It shall be possible to have PUs within tactical nets that have an interface for accessing to a LAN. These stations shall also be capable of being connected to more than one other tactical net. Thereby they can work as a relay between these nets and the local area network. This allows for routing messages from one of the PUs of radio net 1 to LAN 192.168.110.x directly or to LAN 192.168.120.x via radio net 2 (see figure 2.1).

[1] (7), p. 339

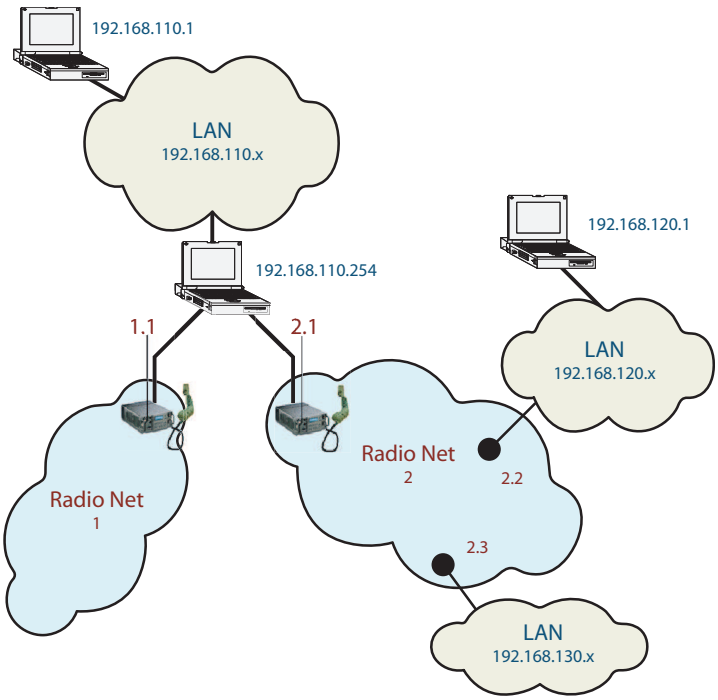

Figure 2.1: Application scenario. RS-IRP nets are embedded within local are networks.

2.1 Requirements and analysis

The first task was to design and create an addressing scheme which fulfills particular demands that also have to be found during this work. It has to be mentioned that finding the requirements during the development of the project was not as easy as it seems. It is common that most military customers are reluctant to state clear and detailed requirements before they explicitly decide on a sales order. Therefore, some important parameters for this work, e.g. maximum RS-IRP net size, could not be easily ascertained.

In the following the found requirements will be presented. The next section will focus on considering already existing addressing schemes and evaluating them with regards to the found requirements. As the HF protocol stack uses an implementation of STANAG 5066[2], the STANAG 5066 addressing scheme will be considered to be reused within RS-IRP.

The STANAGs (Standardized NATO Agreements) are standards used within the NATO to ensure interoperability and define modern radio waveforms and ARQ protocols that shall be used in NATO alliances. STANAGs that cover less critical topics (cipher algorithms,for instance, are excluded here) can also be used by non-NATO countries and organizations.

[2]see 1.3

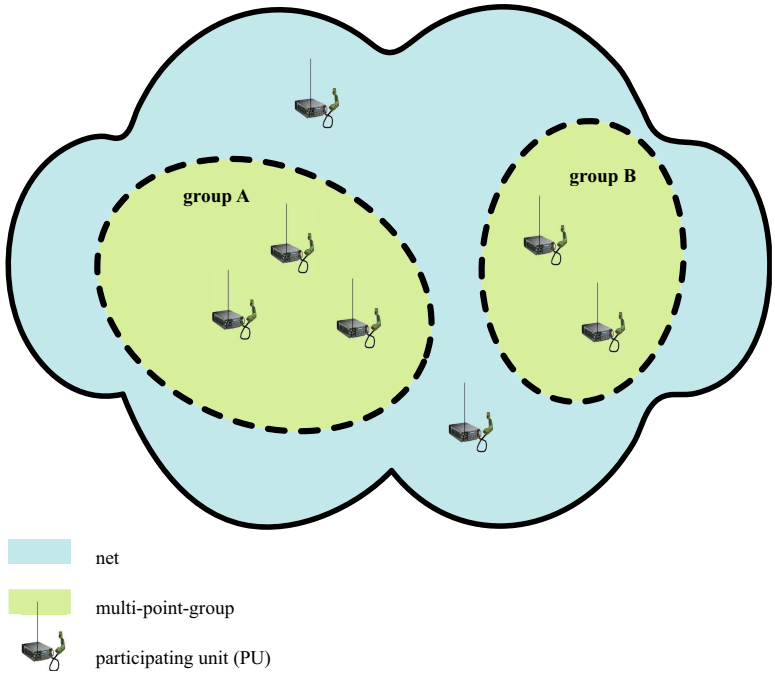

Figure 2.2: Net topology supported by SECOM-V

2.1.1 Requirements

Besides other high-level requirements, the addressing scheme to be created has to consider the bandwidth restrictions of the transmission channel.

As with all radio communication systems the transmission modes have limits regarding the provided bandwidth. Therefore the amount of bits spend for layer 3 addresses has to be minimized. Hereby a trade-off has to be found between the features that shall be implemented and the bandwidth consumption of the layer 3 addressing scheme.

Another design goal is that the addressing scheme to be created should be easily displayable. Both developers and system-users are familiar with IP addresses, for example. Therefore it is desirable that the RS-IRP addresses can be displayed in a similar way.

The high-level requirements are:

- The addressing scheme to be created shall allow for point-to-point, point-to-multipoint(i.e. multicast) and broadcast transmissions.
- The addressing scheme to be created shall be compatible with the addressing schemes of SECOM-V.
- It shall be possible to use the addresses in conjunction with radio remote control.

- It shall consider different tactical network architectures with regards to characteristics of V/UHF frequency bands.

2.1.2 Analysis of radio and radio net addressing schemes

Actually there are 2 SECOM addressing schemes, one for SECOM-H and one for SECOM-V. The only difference between them is address space and the supported net topology. In both modes uni-, multi- and broadcast is possible.

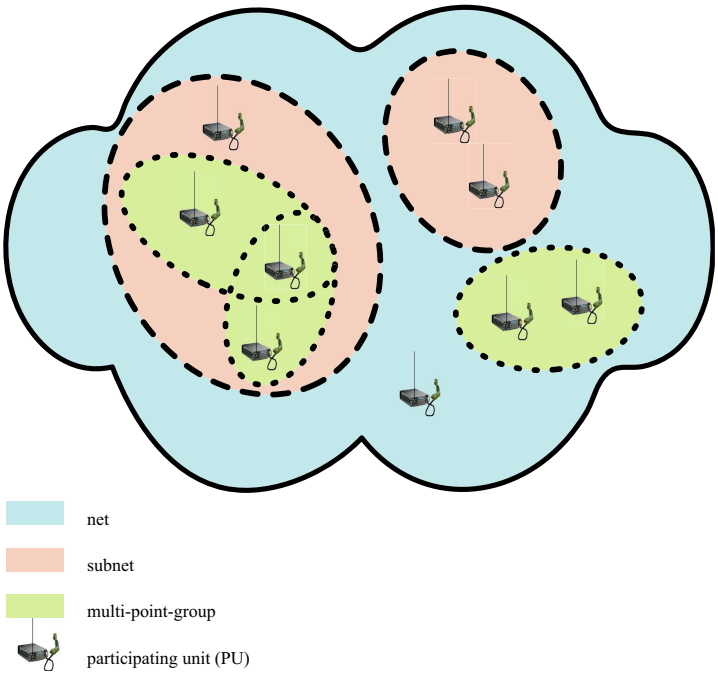

Figure 2.3: Net topology supported by SECOM-H

In SECOM-H mode the `PU` can belong to `GROUP`s, `SUBNET`s and `NET`s, whereas in SECOM-V there are `NET`s, `GROUP`s and `PU`s along with `NET-GROUP`s. `NET-GROUP`s consist of `NET`s that can be synchronized to minimize the interference between them. However, they have no impact on addressing.

As shown in figure 2.3, in SECOM-V overlapping of `GROUP`s is supported. However, this feature is not needed for RS-IRP nets and will therefore not be supported in the RS-IRP addressing scheme. Both SECOM addressing modes support multicast to all `PU`s of one `GROUP` and broadcast to all `PU`s of a `NET`. These will be one of the key features for the RS-IRP addressing scheme to be created.

2.2 Stanag 5066 addressing

Because of their achievable transmission ranges, the HF frequency bands are still very important for military communications. Therefore one part of

STANAG 5066 defines a global addressing scheme which allows to arrange units hierarchically. According to STANAG 5066 addressing the world is separated into regions. Each region contains nations and/or organizations which again consist of classes of units, i.e. different unit types. The nations are the accepted independent states of the world according to NATO. The last part of STANAG 5066 addresses identifies a single unique unit. Figure 2.4 gives a schematic of STANAG 5066 addresses along with an example. Because STANAG 5066 defines addresses that are

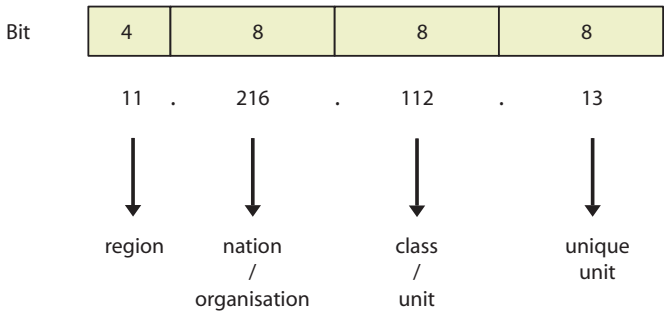

Figure 2.4: STANAG 5066 addressing scheme.

globally unique, the address distribution is controlled by JITC (Joint Interoperability Test Command)[3].

As RS-IRP applies to small, tactical nets using V/UHF only a fraction of the address pool provided by STANAG 5066 would be used. Furthermore a standardized layer 3 addressing scheme is likely to be not optimally adapted to the given application scenarios of RS-IRP. In contrast to the HF communication part of TacSys, RS-IRP does not focus on global interoperability but on internetworking with connected LANs for example. Some customers explicitly do not want a V/UHF communication system that uses a common addressing scheme. The conclusion is that a global addressing scheme is an optimal approach for HF communications regarding the considered applications but not suitable for tacical networks. That is why a proprietary addressing should be created that optimally meets the given requirements.

2.3 RS-IRP addressing

As SECOM-H and SECOM-V nets differ in their topology, the RS-IRP addressing scheme uses their common features as a basis. Therefore SECOM-V subnets are not support. This is also reasonable because RS-IRP nets consist of about 5 to 10 `PUs`. Therefore it is sufficient to arrange `PUs` in `GROUP`s and `NET`s.

RS-IRP addresses consist of three parts: `LinkID`, `NetID` and `NodeID`. The `LinkID` indicates if the following address shall be interpreted as a `GROUP` ad-

[3]For further information see: http://jitc.fhu.disa.mil/it/register.html

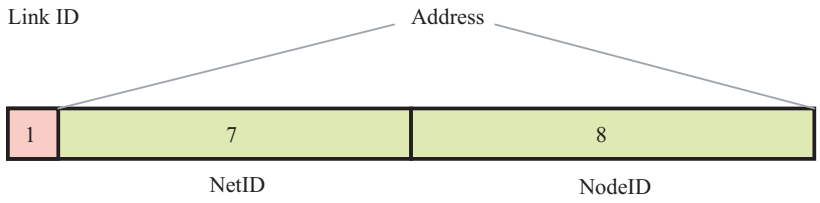

Figure 2.5: RS-IRP addresses.

dress (multicast) or as a point-to-point address referencing one single `PU` (see figure 2.5).

The `NetID` and `NodeID` indicate the `NET` and the single `PU` or `GROUP` respectively. In every `NET` a special address is reserved for the `NodeID` field to allow for broadcasts in that `NET`.

As mentioned earlier, it is yet not possible to get detailed information on the needed address space. Therefore the number of bit spend for RS-IRP address size as shown in figure 2.5 has to be optimized when this information is available.

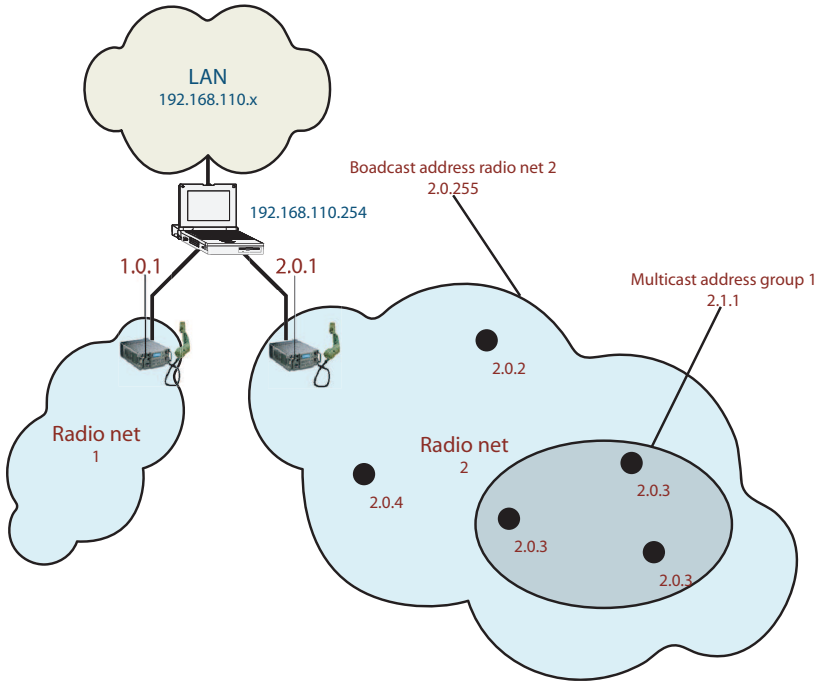

Figure 2.6: RS-IRP addresses.

This addressing scheme allows for an integration of the radio remote control (RRC) part of TacSys in the addressing process. RS-IRP addresses could be translated to SECOM radio addresses by the network layer. Thereby it would be possible to pass these addresses to the RRC module which then can initiate a `LSU` to the indicated `PU` or `GROUP`. This would allow for a reduction of the protocol

header overhead introduced by the network layer header because address information would not be needed for this communication as long as the physical link exists. Furthermore, using radio remote control to establish links has additional advantages that are related to the use of SECOM:

- it is possible to have multiple connections using the same bandwidth but with different hopping sequences at the same time. However, this only applies to SECOM-V due to the hopset length and is limited to a small number of parallel links.
- it is possible to have connections within one net that can not be overheard even by other members of the net.

This addressing scheme can be displayed in dotted decimals. Therefore the different parts of RS-IRP addresses can be separated as figure 2.6 shows.

3 Discussing ad hoc routing concept

This chapter deals with considering ad-hoc routing concepts for RS-IRP nets. The questions will be answered why routing functionality is desirable for RS-IRP and how a suitable ad-hoc routing algorithm can be evaluated before actual its implementation. Furthermore, the Ad-hoc On-demand Distance Vector routing protocol (AODV) will be explained and further considered throughout this chapter. The evaluation includes a simulation using Matlab© which will be discussed in detail in the second part of this chapter. Finally, the results of the simulation will be evaluated and conclusions for RS-IRP will be drawn.

3.1 Requirements and analysis

While communications in the HF frequency bands have a potentially large range, V/UHF transmissions are limited to LOS. It is desirable to extend the transmission range of the SECOM-V and OFDM modes. Currently, for SECOM-V with 9,6 $\frac{kbit}{s}$ a radio range of up to 20 kilometers and for OFDM with 64 $\frac{kbit}{s}$ a radio range of up to 10 kilometers can be achieved[1]. These values apply to man-packs which consist of the M3TR© with a rechargeable battery and a short antenna. The above mentioned range will be the basis for further considerations, although there can also be vehicles in RS-IRP nets which use more powerful equipment and therefore have a larger radio range.

The transmission range could be extended, for instance the tx power could be increased or the antenna could be adapted to the transmission. There is equipment for both alternatives but the extra weight introduced by an tx amplifier or the decreased flexibility and the higher risk of being spotted when carrying a larger antenna make them unappropriate. RS-IRP nets shall apply to small, flexible and mobile tactical radio nets.

Another way to extend the transmission range is to implement routing functionality. Thereby some or all `PUs` of a net can be used as relays to forward packets in case a specific destination is not within direct radio range.

During the development of the Internet many routing protocols and algorithms have been proposed. However, they apply to different scenarios which are more

[1] these are average values taken from an internal evaluation of M3TR© transmission characteristics

focused on the avoidance of fully meshed networks without reducing the number of potential connections. Conventional networks, as the internet, have different characteristics with regards to wireless networks: They are fixed regarding their topology, have a hierarchical order and use wired circuits as transmission media. But the conditions for wireless (ad-hoc) networks are very different: Wireless ad-hoc networks are[2]

- decentral (no given hierarchy)
- not stationary (changing infrastructure)
- dynamic (no constant node membership)
- limited to narrow bandwidth
- battery-powered (limited lifetime of `PUs`)

With this background, it is clear that different approaches were needed to develop sophisticated routing mechanisms for wireless networks, i.e. ad-hoc networks.

The development of routing algorithms for ad-hoc networks is a relatively new area of research. The most promising RFC regarding ad-hoc routing is *RFC: 3561 Ad hoc On demand Distance Vector routing (AODV)*. There are also some military standards concerning this topic. For example *Mil Std 188-220B* defines a routing mechanism which applies to military standards but also has some drawbacks: It defines periodical updates of the routing information of every node which would increase the net load and affect the radio silence requirement. Furthermore, *Mil Std 188-220B* contains various other functionality that is not needed for RS-IRP.

Therefore another solution has to be found which

- does not need periodical updates of routing information
- routing messages introduce minimal overhead
- can handle changes of net topology in wireless (ad-hoc) networks

As AODV fulfills these requirements and performed well in various evaluations it will be further considered. Therefore section 3.1.2 gives a description of AODV. Thereafter in section 3.2 the simulation of AODV using Matlab© will be explained and its results in section 3.3 considered.

[2] taken from (6)

3.1.1 Requirements

As with all radio based communication systems the bandwidth is limited. The M3TR© provides data rates up to 2,4 or 9,6 $\frac{kbit}{s}$ for secured transmissions in HF or V/UHF and up to 72 $\frac{kbit}{s}$ for plain communication using OFDM in V/UHF. To transmit a maximal amount of application data, the overhead introduced by routing messages shall be small in comparison to the available bandwidth.

In contrast to the large possible range of radio communication in HF, V/UHF communication is limited to LOS transmissions. Therefore routing functionality is needed to extend this range by use of intermediate stations (hops).

To further decrease the possibility of being discovered due to radio transmissions, the routing algorithm used for RS-IRP shall not rely on periodical updates of routing information and thereby support radio silence.

The routing protocol shall consider the special condition in tactical radio networks with regards to the characteristics of the V/UHF frequency bands.

3.1.2 Ad Hoc On Demand Distance Vector Routing (AODV)

AODV is one of the "oldest" ad-hoc routing protocols proposed by the Mobile Adhoc Networks working group (MANET). Developments started around 1998 and lead to AODV's proposal as ad-hoc protocol by Charles E. Perkins and Elisabeth M. Royer in 1999 (1). Since, there were 13 draft versions until its submission as RFC 3561 (3). Until draft 5 the multicast feature was integrated and further specified in the extension MAODV (2).

AODV can be called a "pure on-demand route acquisition system"[3]: information to establish and maintain routes is only stored by `PUs` that are part of an active route. Although there are optional periodical updates defined, AODV does not need them because the routes are build on-demand. Those updates can be used to provide each node information about which `PUs` are directly reachable, thus decreasing the latency regarding path setup.

AODV uses sequence numbers which, similar to timestamps, provide information on the freshness of routing messages. This guarantees that there are no loops in routes. A proof for this can be found in (1). Each route request can be identified uniquely which reduces the processing and broadcasting of the corresponding messages during propagation through the net.

A `PU` can collect information about its adjacent nodes by interpreting the layer 3 address of any broadcast message it receives. Especially `HELLO` messages are supposed for this matter. This message type has the same structure as `RREP` messages with the `TTL` and the hop count field set to 1 and 0 respectively, the destination and destination sequence number fields containing the address and the current sequence number of the sender and with the life time field set to ALLOWED_HELLO_LOSS · HELLO_INTERVAL (see appendix A.5). Each link

[3](1), p. 2

or network layer notification can be used to maintain the information on local connectivity.

Path setup

Establishing a route is initiated if a PU attempts communication with another PU to which there is no valid entry in the routing table. The routing table has the following entries for each route[4]: The originator (ORG) of a route request

destination	destination sequence number	repair flag	valid flag	valid destination number flag	hop count	next hop	life time	number of precursors	precursors

Figure 3.1: Fields for each entry of the routing table.

broadcasts a route request (RREQ) message. See appendix A.2 for the information contained in a RREQ.

PUs receiving a new RREQ can behave in two ways: In the first case the RREQ would be rebroadcasted as long as its layer 3 time-to-life (TTL) field is larger than 1 and the current receiver does not have a valid route to the destination. In the second case the receiving PU has a valid route to the destination and therefore responds by unicasting a RREP back to the ORG to which the (backward) path was established by the route of the RREQ. As the RREP travels back to the source of the route request the corresponding forward path is established. The following example shall explain how the needed information is collected during the path set up:

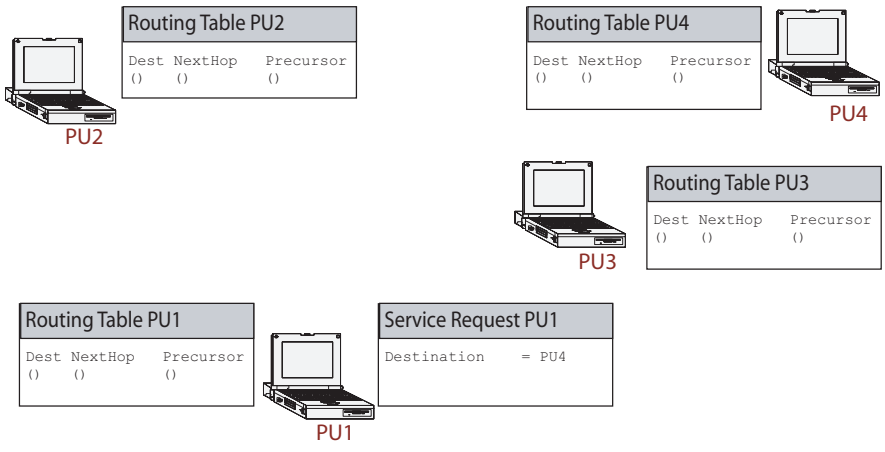

Figure 3.2: AODV path setup: Initial situation before service request.

In figure 3.2 the initial situation is shown. The routing table of every PU is empty. The higher layer of PU1 make a service request to layer 3 for PU4. A

[4]see appendix A.1 for further details

RREQ will be broadcasted, since a valid route to the requested destination is unknown.

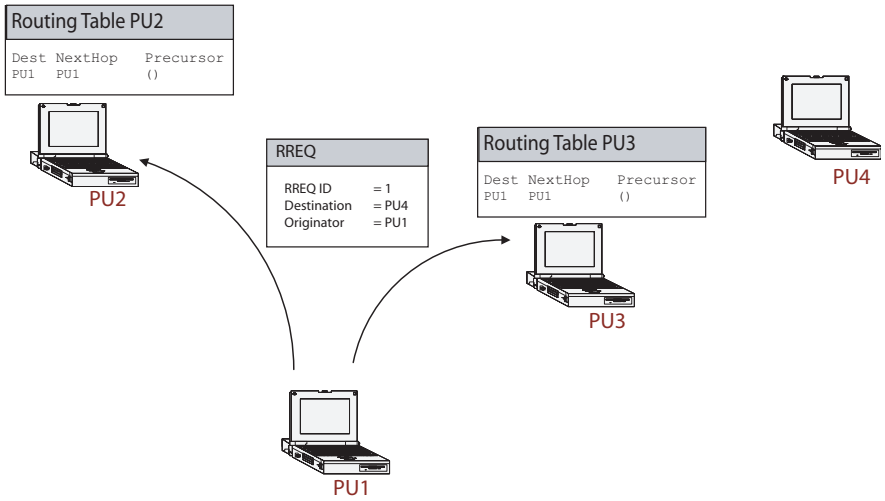

Figure 3.3: AODV path setup: Propagation of the route request (RREQ) (1).

Figure 3.3 shows the situation when the RREQ has been received by the adjacent PUs, namely PU2 and PU3. Both recipients update their routing table with the information from the RREQ, i.e. a route to the ORG of this service request is inserted which uses the PU indicate by the source field of the layer 3 header as next hop. In this case the address indicated by the layer 3 header source field and the address of the ORG are identical. The RREQ is again broadcasted, as non of the receivers has a valid route to the requested node.

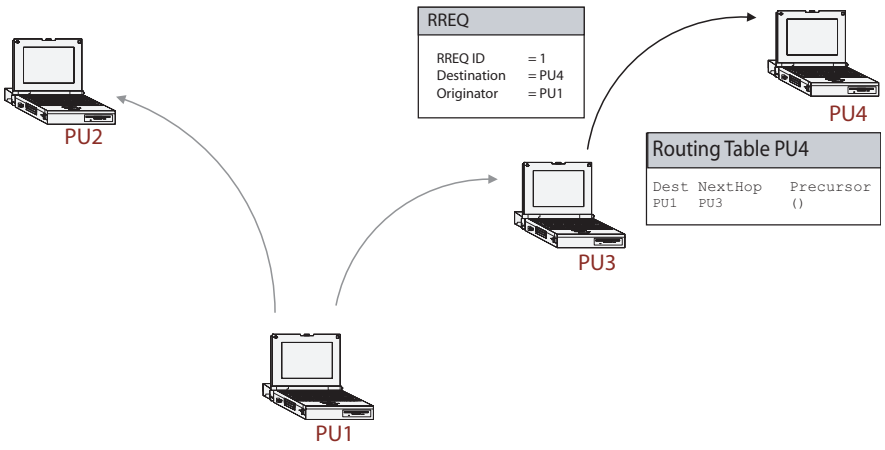

Figure 3.4: AODV path setup: Propagation of the route request (RREQ) (2).

After the PUs2 and 3 have finished broadcasting, PU1 receives the RREQ as well as PU4. PU1 discards the packets because it identifies the RREQ as the one that

it has just send itself. Figure 3.4 shows that as the RREQ is received by PU4 the backward path from the destination to the ORG has been established. Therefore the RREP of PU4 can be unicasted to PU1 with PU3 as intermediate hop.

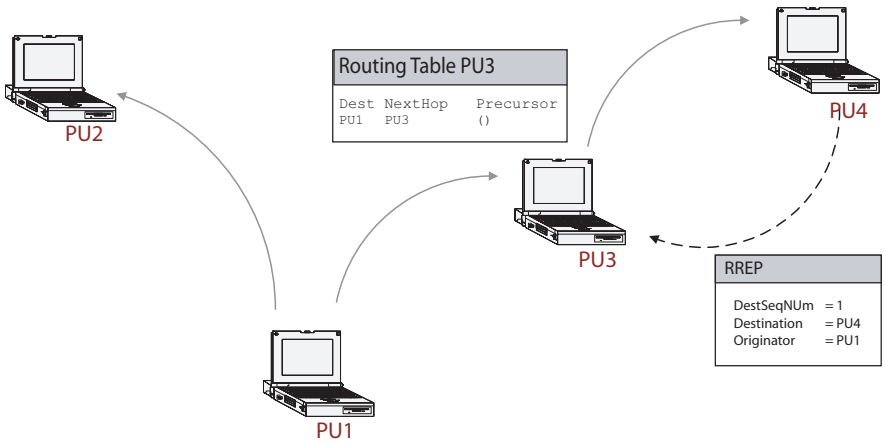

Figure 3.5: AODV path setup: Propagation of the route reply (RREP) (1).

When PU3 receives the RREP(see figure 3.5), it updates its already existing routing entry for the ORG and inserts the address of PU4 in the according precursor field. Further, PU4 will be inserted in the precursor field of the routing entry for PU1. Then the RREP is unicasted to PU1.

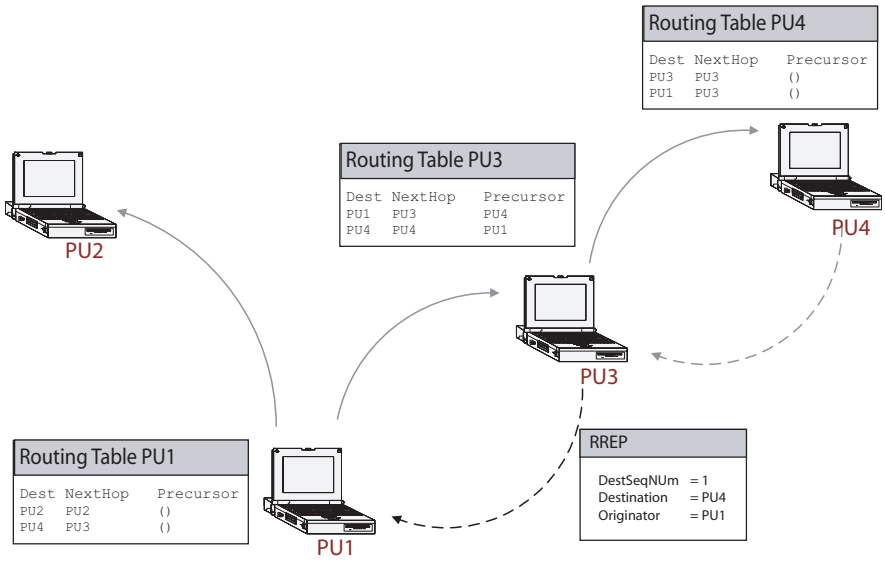

Figure 3.6: AODV path setup: Propagation of the route reply (RREP) (2).

Figure 3.6 shows the situation when the RREP has been received and processed by PU1. At this time, the forward path from the ORG to the requested destina-

tion using PU3 as intermediate hop has been established and the communication between them can begin.

Limiting the routing overhead

Limiting routing overhead is especially important for radio networks because of the limited bandwidth. AODV incorporates some features to limit the propagation and repeated processing of packets during route establishment. For instance, when broadcasting the first RREQ for a specific service request the TTL field will be set to a relatively small value thus allowing the RREQ to propagate only a few hops into the radio network. If the path setup fails in first place, subsequent RREQs will have larger values for the TTL field according to an expanding ring search.

Additionally, each RREQ is uniquely identified by the combination of the address and the sequence number of the ORG. Therefore a specific PU will process a RREQ only once and discard subsequent versions. Furthermore, AODV does not rely on periodic updates of routing information and the RREPs are unicasted back to the ORG of the route request. These features minimize the routing overhead introduced by AODV messages.

Handling link breaks and path maintenance

AODV uses so called RRER (Route Error) messages to inform the precursors of a route that the corresponding destination is no longer reachable using this route. With the example shown in figure 3.6, if PU3 has a route to PU4 and PU1 is using PU3 as next hop to reach PU4, PU1 is the precursor of PU3´s routing entry for PU4. Now, let us assume that PU4 moves out of range and is therefore no longer reachable by PU3. In this case PU1 would receive a unicasted RRER message from PU3 telling that PU4 is no longer reachable via PU3. Depending on the configuration, PU1 could decide to send a route request once again to determine a new path to the requested destination.

3.2 Simulating AODV with Matlab

The purpose of the Matlab© simulation is to determine if AODV can be used for routing in tactical nets and how important parameters of the algorithm have to be adapted.

Because routing algorithms are very complex and can hardly be investigated analytically, a simulation of AODV is attempted. There are several sophisticated network simulators available, for example *ns-2*. Matlab© will be used as platform for the simulation because the knowledge collected when implementing AODV, especially the UML diagrams, can be reused for a later C++-implementation. Additionally, for the purpose of this work it is sufficient to simulate aspects of Layer 3 and 2. Compared with *ns-2* which uses a layer 1 channel model as well,

this might lead to an accelerated processing of the simulation in comparison to *ns-2*.

The purpose of the Matlab© simulation is to determine if AODV can be used for routing in tactical nets and how parameters can be adapted to match the key characteristics of tactical nets.

3.2.1 Description of the model

The simulation uses an event-driven approach which means that there is a *Time Schedule* which list entries correspond to the tasks that shall be executed during simulation. Most simulators use this approach because processing time is decreased as only those time steps are simulated which really contribute to the simulation results. The *Time Schedule* can be altered, i.e. entries can be removed and added, during the simulation. An entry has the following fields:

- Time
- Activity ID
- Node ID
- Optional parameters

When interpreting one entry of the *Time Schedule* the simulated time is set to the time indicated by the entry and the task corresponding to Activity ID is executed by the `PU` specified by Node ID. Optional parameters are needed e.g. for a service request to determine the destination and the data amount to be send. The simulation consists of two separate parts: The movement of every node, i.e. `PU`, and the communication between the `PUs`.

At the beginning of the simulation the `PUs` are equally distributed on a rectangular area in which they can move. The `PUs` stay at their current position for the period of *pause_time* until they chose a random (every point of the rectangle has equal probability) aim within the rectangular area and a random velocity. When a `PU` reaches its new position it again waits for *pause_time* and chooses a new aim.

To account for the different velocities of persons and vehicles, the simulation uses three velocity groups which determine the mean of the gauss distributed velocity and the radius (action_radius) within which the next position can be chosen. At the beginning of the simulation it is randomly decided with equal probability to which velocity group a specific `PU` belongs (equal probability). An actual speed is randomly chosen from the normal distribution with the mean of the velocity group a particular `PU` belongs to and a deviation of mean/10. The velocity groups are:

- Mean group 1: 0,3 $\frac{m}{s}$

- Mean group 2: 3,3 $\frac{m}{s}$
- Mean group 3: 13,9 $\frac{m}{s}$

The communication between `PUs` includes random *service requests* to layer 3 to send a random amount of user data to a randomly selected `PU` (the destination is selected from the `PUs` with equal probability). Every 10 seconds there is a chance of 4 percent for a service request for each `PU`. However, the simulated layer 3 can be busy during certain periods of the simulation and therefore service requests might be rejected. This lowers the real service request probability.

It is assumed that there are two different types of user data which is reflected by the probability distribution of the data amount to be send for a specific service request: The first user data type is *e-mail with attachment*. With a probability of 0.2 a service request includes this data type and the data amount is chosen from the interval $N \cap [1\ 30]$ *kbyte* with equal probability. The second user data type is *short message*. A service request includes this kind of data with a probability of 0.8. In this case the data amount is chosen from the interval $N \cap [1\ 2]$ *kbyte* with equal probability.

Layer 3 of the simulation implements parts of the AODV algorithm and uses layer 2 to send data. Layer 2 provides the command `send_data(aDATA,iADDRESS)` and uses the function `layer2_finished_sending(bSUCCESS)` to inform layer 3 about the termination of a transmission. Layer 2 also implements a basic channel model which considers the ARQ functionality of RS-IRP. It calculates the real layer 2 data amount including repetitions. Therefore a layer 2 packet error rate is used to determine for every layer 2 packet independently if it has to be repeated. The layer 2 packet error rate is assumed to be 10^{-2} for the simulation.

3.2.2 Evaluation of the simulation and metrics

The simulation can be used to evaluate AODV regarding its use as routing protocol for RS-IRP. The simulation of AODV of this student research project is used to collect information about the following parameters:

HOP COUNT (HC) Fraction of routes that use optimal paths, one hop more than optimal and two hops more than optimal.

PACKET DELIVERY RATIO (PDR) Fraction of send user data that is really received by the destination.

BYTE OVERHEAD (BOH) Fraction of data that is caused by AODV messages.

LATENCY (LAT) Average time between the start of a service request and the end of the corresponding user data reception in the requested destination.

However, the presented simulation has some drawbacks that are mostly caused by the lack of time during implementation: The implementation of AODV comprises the handling of `RREQ`, `RREP` and `HELLO` messages. `RRER` messages and the route repair mechanism are not implemented. These features are used to inform `PUs` [5]that are likely to use a specific route of a link break and to reestablish broken links respectively. Further, it is more reasonable to measure the LAT as the time between the start of a service request and the time the first corresponding layer 2 packet containing user data arrives at the final destination. As this can not be added due to the lack of time, the average time for sending user data over one hop will be substracted from the measured LAT (see section 3.2.1 for the description of the data amount model):

$$LAT_{ofdm} = LAT_{ofdm,measured} - \frac{P_{sms} \cdot \overline{b}_{sms} + P_{e-mail} \cdot \overline{b}_{e-mail}}{D_{ofdm}} \quad (3.1)$$

$$LAT_{secom-v} = LAT_{secom-v,measured} - \frac{P_{sms} \cdot \overline{b}_{sms} + P_{e-mail} \cdot \overline{b}_{e-mail}}{D_{secom-v}} \quad (3.2)$$

(With $D_{secom-v} = 64\ \frac{kbit}{s}$, $D_{ofdm} = 9,6\ \frac{kbit}{s}$, $P_{sms} = 0,8$, $P_{e-mail} = 0,2$, $b_{sms} = 1,5\ kbyte$, $b_{e-mail} = 15\ kbyte$) Further, in contrast to other network simulators the presented simulation of AODV does not include message queues which results in a generally higher packet loss ratio.

3.3 Results

The metrics (see 3.2.2) were measured using the Matlab© simulation for different values of *route_timeouts* in order to investigate if AODV can be used for V/UHF communications in the considered tactical nets. Each value represents the mean calculated from 50 runs of the simulation and the error bars indicate the 95 % confidence interval of the mean. A list of the default parameters used for the simulation can be found in appendix A.5.

The *active_route_timeout* controls how long an established route will be treated as valid until it is exspected to be obsolete and invalid respectively. This parameter is important because an optimal value would decrease the average number of route request thus decreasing routing overhead. Because of the mentioned differences between tactical and ad-hoc nets, it is suggested that the *active_route_timeout* for the considered tactical nets can be increased to be larger than the proposed *active_route_timeout* for AODV [6] in networks with larger bandwidth.

It is assumed that the `PUs` of the simulated tactical networks have an **average *pause_time* of 15 minutes** which equals 900 s. This value is reasonable because

[5]so called precursors; see appendix A.1

[6]in (3), section 10, a value of 3000 ms for the *active_route_timeout* is proposed

in tactical situations time is needed, for example, to establish a stance. Simulations were run for both SECOM-V, with a **radio range of 20 kilometers** and a **data rate of 9.6** $\frac{kbit}{s}$, and for OFDM, with a **radio range of 10 kilometers** and a **data rate of 64** $\frac{kbit}{s}$. Further, each `PU` broadcasts a `HELLO` message once at the beginning of the simulation.

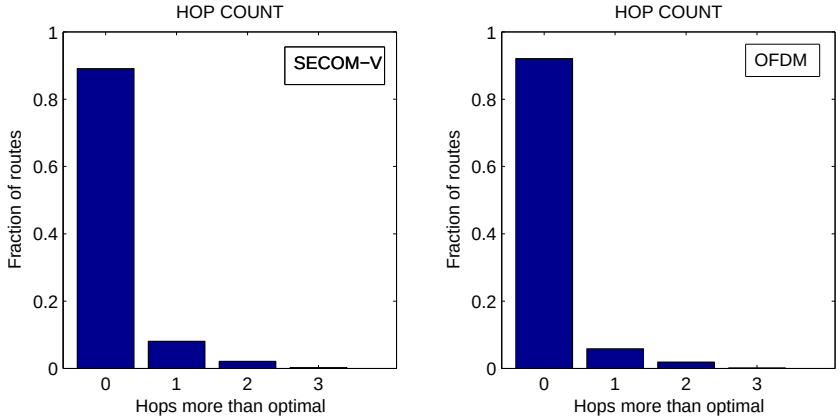

Figure 3.7: Mean fraction of the established route that are optimal, have one, two or three hop(s) more than optimal; average HC of simulations with: $active\_route\_timout \in [3\ 10\ 300\ 600\ 1200] \cdot s$, $pause\_time = 900s$, $D_{ofdm} = 64\ \frac{kbit}{s}$, $r_{ofdm} = 10\ km$, $D_{secom-v} = 9,6\ \frac{kbit}{s}$, $r_{secom-v} = 20km$.

AODV finds in most cases the optimal route for both SECOM-V and OFDM transmission modes (figure 3.7). A route can have more hops than optimal if a `PU` on the optimal path can not process or receive a `RREQ` or a `RREP`. This is because its layer 3 is busy or the channel is occupied by another `PU`. As no queuing of messages is implemented the layer 3 of a specific station can be busy, for instance, if it has just passed user data to layer 2.

Figure 3.8 shows that for increasing values of *active_route_timeout* both LAT and PDR decrease. The LAT decreases with larger values for *active_route_timeout* because less route requests are initiated as the previously established routes are longer valid and are more often reused for subsequent service requests. The larger the value for the *active_route_timeout* the more likely it is that the used route is already obsolete and transmissions using invalid routes will result in the loss of the corresponding user data. This fact is reflected by the PDR which decreases with larger values of *route_timeouts*. Therefore a compromise can be found that optimizes both LAT and PDR.

The ratio of SECOM-V and OFDM regarding LAT is $\frac{LAT_{scv}}{LAT_{ofdm}} = 1,3$ for all values of *route_timeouts*. This does not correspond to the ratio of data rates of OFDM and SECOM-V respectively which is $\frac{D_{ofdm}}{D_{secom-v}} = 6,7$. The reason why the higher data rate of OFDM has only a relative small impact on the LAT statistic is that OFDM has a smaller radio range as SECOM-V and therefore routes for

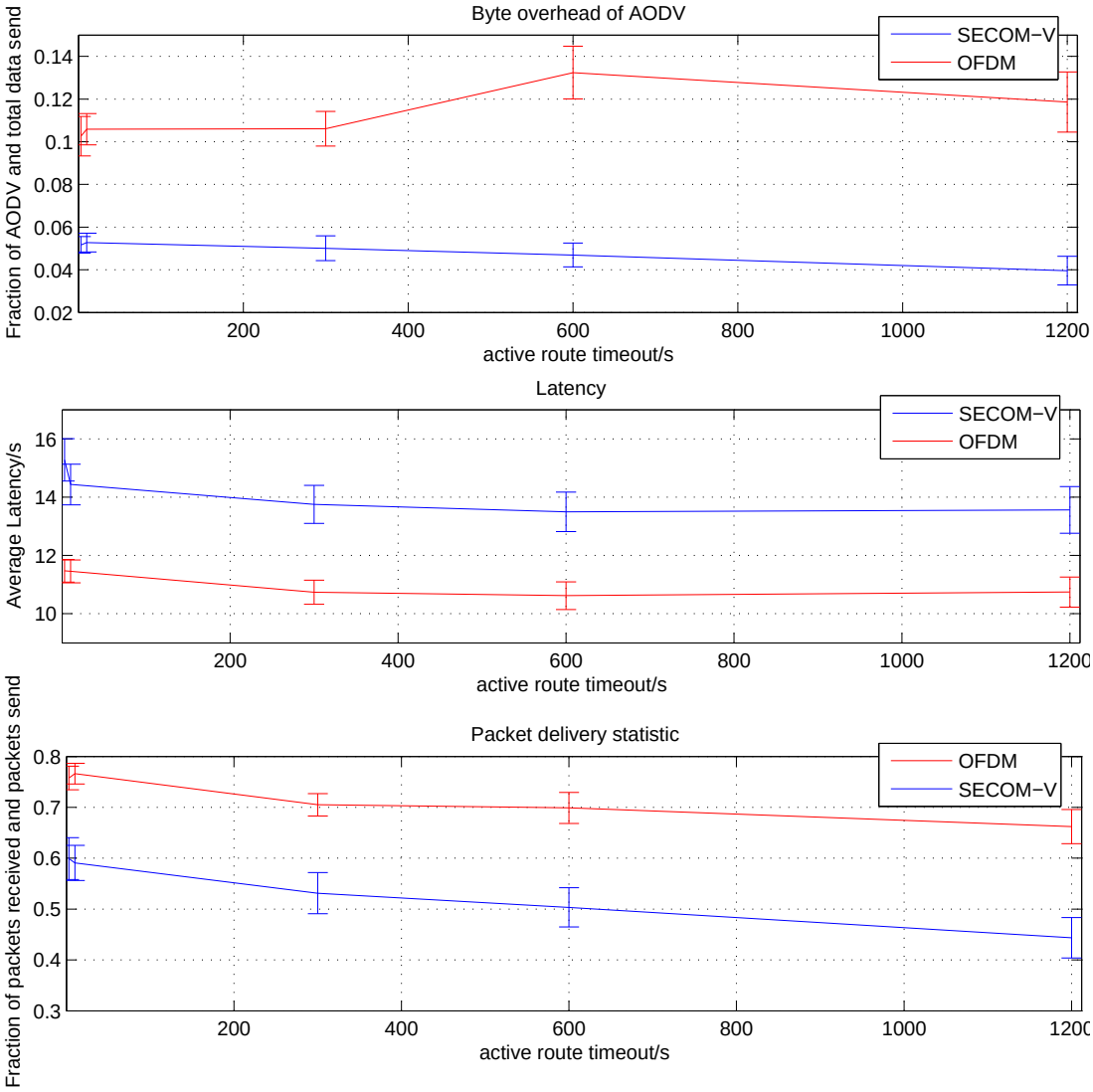

Figure 3.8: Results are based on simulation over 50 runs, and the error bars represent the 95 % confidence interval of the mean; $active\_route\_timout \in [3\ 10\ 300\ 600\ 1200] \cdot s$, $pause\_time = 900s$, $D_{ofdm} = 64\ \frac{kbit}{s}$, $r_{ofdm} = 10\ km$, $D_{secom-v} = 9,6\ \frac{kbit}{s}$, $r_{secom-v} = 20km$.

OFDM tend to have more hops as when using SECOM-V.

The gap between the PDR of OFDM and SECOM-V is also mainly caused by the different radio ranges. As the simulations for OFDM and SECOM-V use the same scenario regarding the rectangular area in which the `PUs` move, a larger number of `PUs` in SECOM-V nets is directly connected to each other than in tactical nets using OFDM. That is why collisions are more likely to occur for simulations for SECOM-V which results in a decreased PDR for this transmission mode. As mentioned in section 3.2.2 the PDR is also reduced as the simulation does not yet support AODV `RRER` messages and queuing of incoming packets.

The BO which is shown in the first graph of figure 3.8 decreases for SECOM-V for increasing values of *active_route_timeout*. This is the result of the before mentioned interrelationship between the *active_route_timeout* and the number of route requests. A full implementation of the AODV algorithm is expected to produce increasing values for BO for increasing values for *active_route_timeout* because in case that more and more obsolete routes are being used more and more link breaks would be discovered which would lead to the disemination of more `RRER` messages. The BO for OFDM increases for increasing values for *active_route_timeout* until *active_route_timeout* = 600 s. Then, the BO decreases for *active_route_timeout* ¿ 600 s. This behavior has to be further investigated as there is, at the moment, no explanation for it.

4 Summary and outlook

During this student research project the requirements for a radio based network layer regarding addressing and routing have been investigated. The requirements found were based on the project requirements of TacSys and the functionality provided by the Rohde & Schwarz tactical radio M3TR©.

The addresing concept need to reflect different, in a certain sense contradicting requirements in HF and in V/UHF networks. On one side HF supports global reception in joint military operation and thereby requests for an internationally registered unique addresing scheme that is supported y a given standard, STANAG 5066.

On the other side, the limited radio range but also the larger bandwidth given by the transmission characteristics in the V/UHF frequency bands allows real radio network operation requested by tactical networks. Operating such networks demands specific mission planning in which address plans are individually established by the operator.

In tactical networks full interoperations with alliances is not required. In contrast, customer rather prefer own non-standardized waveforms in tactical networks in order to prevent interception of their communication by other parties. M3TR© supports such non standard waveforms and the focus of the first part of this work focused on an appropriate addressing scheme.

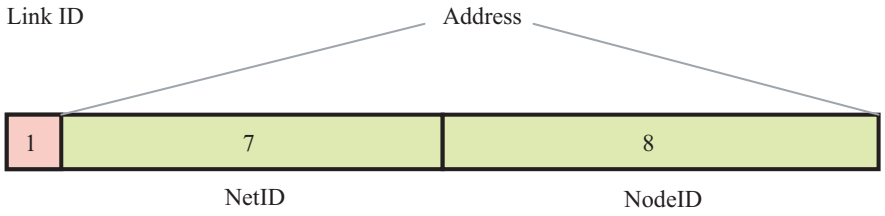

Figure 4.1: Network addresses for V/UHF communications in tactical radio networks of TacSys.

The network layer addressing scheme for TacSys (figure 4.1)has been optimized regarding the address length using the at the time available information. In addition the presented addressing scheme provides unicast, multicast and broadcast and incorparates radio remote control in the addressing process.

The ad-hoc routing protocol AODV was selected to be further considered as potential routing algorithm for V/UHF communication within the TacSys project. Using (3) as guide regarding the implementation of the algorithm a simulation

for Matlab© has been created to evaluate AODV with regards to the special requirements of tactical radio nets:

- Overhead introduced by routing messages shall be small in comparison to the available bandwidth.
- The routing algorithm shall be capable of extending the communication range in the V/UHF frequency bands by the use of intermediate hops.
- The routing algorithm shall not rely on periodical updates of routing information to support for radio silence.
- The routing algorithm shall consider the special conditions of tactical radio networks with regards to the characteristics of the V/UHF frequency bands.

It has been shown that AODV can be used as routing protocol for communications wihout relying on periodical updates of routing information. For a scenario that should apply to most real application of RS-IRP, AODV has proven to find optimal routes while introducing a relatively small routing protocol overhead. In this scenario, AODV uses a very small amount of the available bandwidth (4-5 percent for SECOM-V) and introduces a relatively small delay between service request and the actual receiption of user data in the final destination.

In order to further investigate the qualification of AODV as routing protocol for tactical radio networks, the Matlab© simulation has to be improved by reviewing the channel access model and by fully implementing AODV. Thereby it would be possible to set up a simulation environment which can be used to simulate specific application scenarios.

A AODV

A.1 Routing table

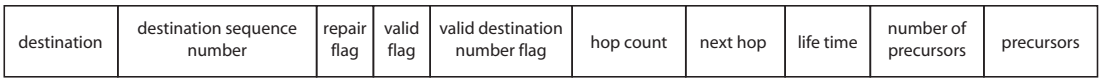

Figure A.1: Fields for each entry of the routing table.

Field	Describtion
destination	The address of the destination of this route.
destination sequence number	Self-explanatory.
repair flag	Repair flag; reserved for multicast.
valid flag	True if this route is valid.
valid destination number flag	If this entry includes a valid sequence number of the destination.
hop count	Length of the route in hops.
next hop	Address of the next intermediate `PU`.
life time	Indicates how long long this route can be used to forward packets.
number of precursor	Number of `PUs` that have used this route.
precursors	Addresses of `PUs` that use this route.

A.2 Route Request - RREQ

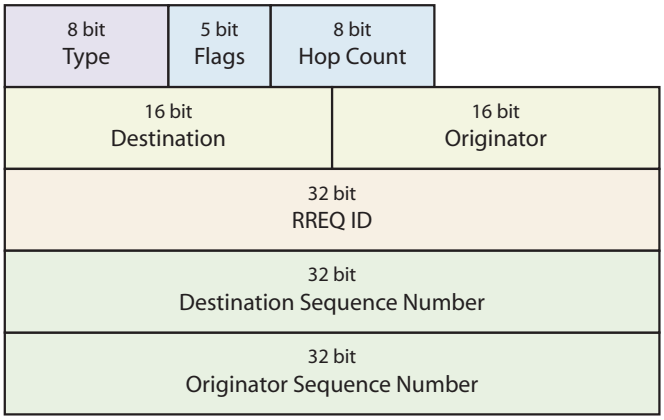

Figure A.2: Fields of the route request (RREQ) message of AODV.

Field	Describtion
Type	Type of AODV messages; 1 for `RREQ`
J flag	Join flag; reserved for multicast.
R flag	Repair flag; reserved for multicast.
G flag	Gratitous `RREP` flag; indicates whether a gratitous `RREP` shall be unicast to the `PU` specified in the Destination field.
D flag	Destination only flag; indicates only the Destination may respond to this `RREQ`.
U flag	Unknown Sequnce Number
Hop Count	Number of hops from the `ORG` to the `DEST`.
Destination	Address of the destination for which a route is desired.
Originator	Address of the originator which originated the route request.
RREQ ID	Number uniquely identifying the `RREQ` when taken in conjunction with the originating `PU` address.
Destination Sequence Number	The latest sequence number received in the past by the `ORG` for any route towards the `DEST`.
Originator Sequence Number	The current Sequence number of the `ORG`.

A.3 Route Reply - RREP

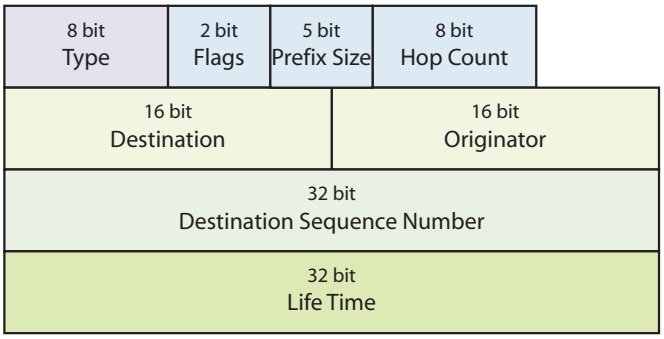

Figure A.3: Fields of the route request (RREP) message of AODV.

Field	Describtion
Type	Type of AODV messages; 2 for `RREP`
R flag	Repair flag; reserved for multicast.
A flag	Acknowledgement required.
Prefix Size	If non-zero, the the 5-bit prefix size specifies thet the indicated next hp may be used for any `PUs` with the same routing prefix as the requested station.
Hop Count	Number of hops from the `ORG` to the `DEST`.
Destination	Address of the destination for which a route is supplied.
Originator	Address of the originator which originated the route request.
Destination Sequence Number	The destination sequence number ascociated with this route.

A.4 Route Error - RERR

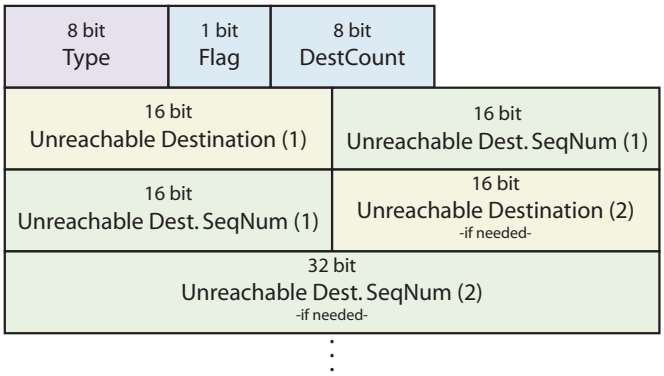

Figure A.4: Fields of the route request (RERR) message of AODV.

Field	Describtion
Type	Type of AODV messages; 3 for `RRER`
N flag	No delete flag.
DestCount	The number of unreachable destinations inlcuded in the `RRER`; must at least be 1.
Unreachable Destination(1)	Address of the destination that has become unreachable due to a link break.
Unreachable Dest. SeqNum(1)	The sequence number in the routing entry for the destination listed in the previous unreachable destination field. the route request.

A.5 Matlab©Simulation - parameters

```
%all data amounts in kbyte, all times in ms, all velocities in m/s
%all distances in m
t_end  = 5*3600 *1000;
num_stations  = 10;
area.x_length  = 60000;
area.y_length  = 40000;
speed.mean_speed_group1  = 0.3;
speed.mean_speed_group2  = 3.3;
speed.mean_speed_group3  = 13.9;
%meter
positioning.action_radius.group1 = speed.mean_speed_group1 * 1200;
positioning.action_radius.group2 = speed.mean_speed_group2 * 1200;
positioning.action_radius.group3 = speed.mean_speed_group3 * 1200;
positioning.pause_time  = 15*60000;
layer2_packet_length = 0.2;
packet_error_rate  = 10^-2;
packet_processing_time  = 10;
radio_delay  = 150;
packet_time_interval = ...
(layer2_packet_length*8)/(data_rate) + ...
2*packet_processing_time + 2*radio_delay;

CSMA_CD.retries  = 16;
CSMA_CD.slot_delay  = 1;
layer3_header.kbit_length  = 0.080;

AODV_params.RREQ_length  = 0.145;
AODV_params.RREP_length  = 0.119;
AODV_params.ACTIVE_ROUTE_TIMEOUT = 10*60*1000;
AODV_params.ALLOWED_HELLO_LOSS = 2;
AODV_params.NODE_TRAVERSAL_TIME = packet_processing_time + radio_delay;
AODV_params.HELLO_INTERVAL = 10*60*1000;
AODV_params.LOCAL_ADD_TTL = 2;
AODV_params.NET_DIAMETER = num_stations;
AODV_params.RERR_RATELIMIT = 10;
AODV_params.RREQ_RETRIES = 2;
AODV_params.RREQ_RATELIMIT = 10;
AODV_params.TIMEOUT_BUFFER = 2;
AODV_params.TTL_START = 1;
AODV_params.TTL_INCREMENT = 2;
AODV_params.TTL_THRESHOLD = 7;
```

```
AODV_params.NET_TRAVERSAL_TIME = ...
2*AODV_params.NODE_TRAVERSAL_TIME*AODV_params.NET_DIAMETER;
AODV_params.BLACKLIST_TIMEOUT = ...
AODV_params.RREQ_RETRIES * AODV_params.NET_TRAVERSAL_TIME;
K                                    = 5;
AODV_params.DELETE_PERIOD = ...
K * max (AODV_params.ACTIVE_ROUTE_TIMEOUT, AODV_params.HELLO_INTERVAL);
AODV_params.MAX_REPAIR_TTL = ...
0.3*AODV_params.NET_DIAMETER;
AODV_params.MY_ROUTE_TIMEOUT = ...
2*AODV_params.ACTIVE_ROUTE_TIMEOUT;
AODV_params.NEXT_HOP_WAIT = ...
AODV_params.NODE_TRAVERSAL_TIME+10;
AODV_params.PATH_DISCOVERY_TIME = ...
2*AODV_params.NET_TRAVERSAL_TIME;
AODV_params.RING_TRAVERSAL_TIME = ...
2*NODE_TRAVERSAL_TIME*(TTL_VALUE+TIMEOUT_BUFFER)
```

A.5.1 Layeer 3 Header

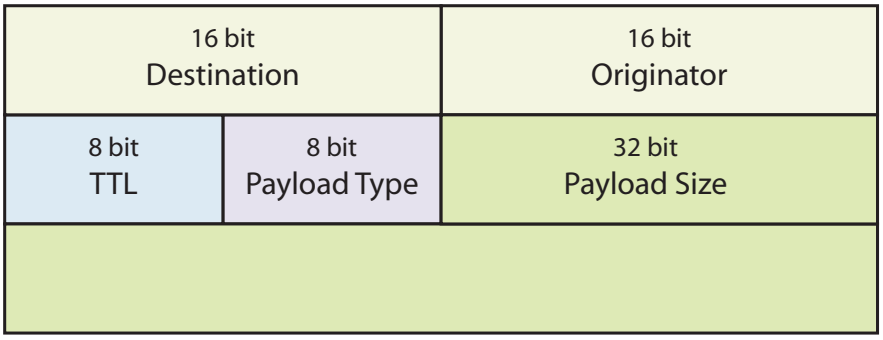

Figure A.5: Layer 3 header used for the Matlab© simulation.

Field	Describtion
Source	Originator address of this Layer 3 packet
Destination	Destination address of this Layer 3 packet
TTL	Time to life for this packet.
Payload Type	Type of paylaod; e.g. 1 one for AODV, 2 for user data.
Payload Size	Size of the payload in byte.

Abbreviations and Acronyms

BLOS	beyond-line-of-sight
LOS	line-of-sight
M3TR©	Multiband, Multirole, Multimode Tactical Radio
RS-IRP	Rohde & Schwarz-Interactive Radio Protocol
AODV	Ad-hoc On-demand Distance Vector routing
ASROR	Average Service Request Overhead Ratio
b	Data amount
BO	Byte Overhead; fraction of AODV data send and the totally send data
COMSEC	Communication Security
D	Data rate
HC	Hop Count
HF	High Frequency, i.e. 3 MHz to 30 MHz
ISO	International Organization for Standardization
JITC	Joint Interoperability Test Command
LAT	Latency
LSU	Link Setup
MANET	Mobile Ad-hoc Networks
MF	Median Frequency, i.e. 0.3 MHz to 3 MHz
ORG	Originator of a route request RREQ
OSI	Open Systems Interconnection
PDR	Packet Delivery Ratio; Fraction of user data that is received by its destinaion and the totally send user data
PU	Participating Unit in a radio net
r	Radio range
RERR	Route Error
RREP	Route Reply
RREQ	Route Request message
RREQ_RETRIES	Radio Request Retries
Stanag	Standardized NATO agreement
TacSys	Tactical System
TTL	Time-to-life
UHF	Ultra High Frequency, i.e. 0.3 GHz to 3 GHz
VHF	Very High Frequency, i.e. 30 MHz to 300 MHz

Bibliography

[1] Perkins, Charles E.; Royer, E. M.: *Ad-Hoc On-Demand Distance Vector Routing*. Techn. Rep., 1999.

[2] Perkins, Charles E.; Royer, E. M.: *Muticast ad hoc on-demand distance vector (MAODV)Routing*. IETF draft, July 2000.

[3] Perkins, Charles E.; Royer, E. M.: *Ad-Hoc On-Demand Distance Vector (AODV) Routing*. RFC 3561, 2003.

[4] Proakis, J. G.: *Digital Communications*. McGraw-Hill, New York, NY, USA, 2nd. ed., 1989.

[5] Schütz, M.: *Das große Handbuch der Kommunikationstechnik - Grundlagen, Geräte und Systeme*. Kriebel Verlag, 1991.

[6] Schumacher, A.: *Ad-Hoc On-Demand Distance Vector (AODV) Protocol*, May 2004. url-www.cs.helsinki.fi/kraatika/Courses/IPsem04s/slides/aodv.pdf.

[7] Tanenbaum, A. S.: *Computer Networks (Third Edition)*. Prentice Hall, Englewood Cliffs, NJ, 3rd. ed., 1988.