FFI RAPPORT

AD HOC NETWORKS USED IN EMERGENCY NETWORKS: The Trust Metric Routing Approach

WINJUM Eli, SPILLING Pål, KURE Øivind

FFI/RAPPORT-2005/04015

AD HOC NETWORKS USED IN EMERGENCY NETWORKS: The Trust Metric Routing Approach

WINJUM Eli, SPILLING Pål, KURE Øivind

FFI/RAPPORT-2005/04015

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER FFI/RAPPORT-2005/04015 **1a) PROJECT REFERENCE** 869/913	**2) SECURITY CLASSIFICATION** UNCLASSIFIED **2a) DECLASSIFICATION/DOWNGRADING SCHEDULE** -	**3) NUMBER OF PAGES** 61

4) TITLE
AD HOC NETWORKS USED IN EMERGENCY NETWORKS: The Trust Metric Routing Approach

5) NAMES OF AUTHOR(S) IN FULL (surname first)
WINJUM Eli, SPILLING Pål, KURE Øivind

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

7) INDEXING TERMS

IN ENGLISH:	**IN NORWEGIAN:**
a) Mobile wireless ad hoc networks	a)
b) Wireless networks	b)
c) Mobile networks	c)
d) MANET	d)
e) Routing	e)

THESAURUS REFERENCE:

8) ABSTRACT

Mobile wireless ad hoc networks have characteristics, which intuitively make them well suited for utilization in search and rescue operations. This report discusses and describes how mobile wireless ad hoc networks will strengthen the emergency network and reduce the impact of the shortcomings identified in the planned network. It is shown that mobile wireless ad hoc networks will represent extra connectivity, capacity and functionality. In order to make mobile wireless ad hoc networks even more applicable for search and rescue operations, the concept of Trust Metric Routing is proposed and described. The concept will improve connectivity considerably and lead to a significant throughput improvement within a large node density range. Aspects such as scalability and security are discussed.

9) DATE 2006-02-23	**AUTHORIZED BY** This page only Vidar S Andersen	**POSITION** Director

ISBN 82-464-0996-4

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

PREFACE

This report is part of the doctoral project of Eli Winjum. The project was carried out within the *Future Communication Systems* (FUCS) program at University Graduate Center at Kjeller (UniK) and was part of the *Ad hoc Technology in Catastrophe and Disaster Operations* at Thales Norway AS. The report describes and discusses benefits and implications of a potential utilization of mobile wireless ad hoc networks in rescue operations.

Ad hoc technology will play an important role in future tactical networks. Topics discussed and work reported in this report are relevant to the research conducted by the NbF GRID project. Therefore, the report is published and distributed as a FFI report of this project.

INNHOLD

Side

AD HOC NETWORKS USED IN EMERGENCY NETWORKS: The Trust Metric Routing Approach

1 INTRODUCTION

1.1 Background

The project *Ad hoc Technology in Catastrophe and Disaster Operations* forms the background for this report. The project is managed by Thales Norway AS and is supported by the Research Council of Norway, Applica, University Graduate Center at Kjeller (UniK) and Norwegian Defence Research Establishment (FFI). The major objective is to investigate the potential of utilizing mobile wireless ad hoc networks in search and rescue operations.

The communications network is a critical factor in emergency operations. The effectiveness of the operation depends on the network’s availability. The *Norwegian Public Safety Radio Network* will be deployed during the next five years and will be based on mature and well-proven technology. Long-range base stations will be connected to a fixed backbone. The network will also be capable of autonomous operation. Such operation, independent of base stations and fixed infrastructure, is a major difference between this network and other cellular technologies. The network will have nationwide coverage and is intended to serve the public safety and security services in their regular operations.

Mobile wireless ad hoc networks operate independently of a fixed or pre-planned infrastructure. The networks may be completely autonomous or may be linked to external networks through gateways. Any network node operates both as an end terminal and as a router. As an end terminal, the node runs user applications. As a router, the node discovers and maintains routes to other nodes. The routing capacity, which enables multi-hop communications, is one of the main differences between a mobile wireless ad hoc network and a plain relay-based solution like the one provided by the planned safety network. The nodes are mobile and can be connected dynamically in an arbitrary manner. This means that the network topology is constantly changing. Compared to fixed networks, mobile wireless ad hoc networks are more vulnerable to security attacks, since both passive and active attacks are easier to perform in a wireless and mobile environment. The dynamic network topology makes the detection of irregularities difficult. Due to the scarce bandwidth, power supply and processing capacity, traditional security solutions are often unfeasible. The lack of infrastructure, however, may be considered the main problem in design of security solutions. In spite of security challenges, mobile wireless ad hoc networks have become increasingly popular. So far, they have been associated mainly with military applications, but they will also serve an important role in search and rescue operations. Rescue operations are characterized by unpredictable and rapidly changing conditions. Mobile wireless ad hoc networks seem to have the capability of dynamical adaptation to current communication needs.

1.2 Objective and Scope

In conformance with the project objective, the purpose of this report is to show how mobile wireless ad hoc networks can supplement the planned emergency network:

- Describe the technology upon which the planned emergency network most likely will be based and analyze aspects regarding availability, connectivity, capacity, functionality and security in order to determine the benefits and implications of utilizing mobile wireless ad hoc networks. The purpose is to show that the new emergency network may be strengthened, if extended with mobile wireless ad hoc networks. Based on shortcomings identified in the emergency network, the incorporation of mobile wireless ad hoc technology is recommended
- Pinpoint and discuss areas where further work has to be done. An example is network connectivity: Mobile wireless ad hoc networks operate at relatively short transmission ranges and without base stations. The node density needed to avoid network partition is a critical factor. Special mechanisms must be added to ensure adequate connectivity if mobile wireless ad hoc networks are to be used
- Propose the concept of *Trust Metric Routing* in order to improve connectivity. The concept allows routing cooperation between different security domains while maintaining each domain's possibility to utilize routes that exclusively consist of domain-internal nodes. The concept provides for a possibility of utilizing foreign nodes as forwarders when desired destination nodes are not reachable otherwise. In rescue operations, this feature could be realized by utilizing the terminals of any actors present in the area. On the other hand, as operation goes on, the network may become crowded and the foreign nodes may no longer be included. Trust Metric Routing is described in a series of papers. This report aims at "putting the pieces together" and describing the concept in the setting of a mobile wireless ad hoc network incorporated in the Norwegian Public Safety Radio Network.

Mobile ad hoc networks are widely considered an important component of the fourth generation of wireless networks. Hence, the report indicates possible ways of strengthening and enhancing contemporary technology and functionality by deploying elements of future technology. The report does not give a technical description of a potential incorporation of mobile wireless ad hoc networks. The reasons are:

- Although the *Norwegian Public Safety Radio Network* most likely will be based on standards utilized by other European countries, the base technology is not yet determined. Further, these standards concentrate on the radio interfaces, whereas the underlying infrastructure is for implementation. Hence, major architectural decisions as circuit switching versus packet switching are not made. Circuit switching is the default mode. With regard to packet switching, fundamental services and protocols are so far not in compliance with industry standards
- The *Internet Protocol* (IP) suite has so far been essential within civil mobile wireless ad hoc networks. We know for sure that IP will play a major role in the new emergency network. Its actual role, however, is not determined.

Therefore, technical specifications for integrating mobile wireless ad hoc networks into the emergency network are left for further work. On the other hand, the choice of technology and protocols for the emergency network should reflect the benefits of such integration and ensure future interoperability.

1.3 Outline

The report is organized as follows: In chapter 2 operational and organizational aspects of a generic rescue operation scenario are described in order to identify the most important requirements for the emergency communications network and to give reasonable assumptions with regard to organizational and technical parameters. Chapter 3 describes and evaluates the technology upon which the planned emergency network in Norway most likely will be based.

The potential utilization of mobile wireless ad hoc networks is evaluated before we propose a network architecture, which extends the emergency communications network with ad hoc technology. Chapter 4 presents the concept of Trust Metric Routing and discusses its applicability. Simulation results regarding different aspects of routing cooperation are presented. Various methods to regulate the cooperation in order to deal with congestion are discussed.

Routing cooperation should not be at the expense of security, and chapter 5 discusses the security services needed to build and maintain a trustworthy network topology and to distinguish between trustworthy and untrustworthy routes. The proposed security scheme is evaluated with regard to resource consumption and compared to other security schemes proposed for the actual routing protocol. A few alternatives to Trust Metric Routing are outlined in chapter 6. Conclusions are given in chapter 7.

2 A RESCUE OPERATION SCENARIO

This chapter describes some operational and organizational aspects of a generic rescue operation scenario. The scenario description is a tool to identify the most important requirements to the emergency communications network. The description will be used as a justification for organizational and technical parameters. We only consider the aspects of the scenario that may have an impact on the communications network.

2.1 The Disaster

Rescue operations can never be fully planned. Important factors like where, when and extent are not known in advance. The disaster location may be an urban, suburban or rural area where public infrastructure exists. If the infrastructure is intact, the area may be reached by car. Electrical power and public communication networks will be accessible. A disaster may as well happen out of public infrastructure coverage, and the location reached only at foot, boat or helicopter. At sea, the disaster location may be a fixed installation as well as a ship. In the latter case, the location as such may move as the operation goes on. In case of for example forest fire or oil blow out/leakage, the disaster area may extend during the operations. Search operations may often cover several and wide areas at the same time. Even though the emergency services may be well prepared, trained and equipped to handle various disasters, there will be phases where the rescue operations will be subjected to improvisation.

2.2 The Rescue Organization

Actors involved in rescue operations may be employed by different cooperating organizations. The roles of the various organizations, teams and individuals are pre-planned, but it is impossible to pre-define a generic in-field organization in detail. For example, the first rescue teams to arrive at a disaster area may have to cope with scarce resources, which may influence the organization during the initial phase of the operations. Further, the location and severity of a specific disaster will influence the operation as well as the organization.

The organizations involved are primarily the Fire and Rescue Services, the Emergency Medical Services, the Police and, if needed, the Military. According to pre-defined procedures, the Police will establish an *Operational Management Group* as soon as possible. This group will coordinate all resources involved, no matter to which organization they belong. Further, a *Joint Coordinating Center* will be established outside the disaster area [44]. This center will be responsible for the over all resource management as well as for public information, and will have close connections to the Operational Management Group inside the area.

Inside the disaster area actors from the different organizations operate in collaborating teams. The Operational Management Group coordinates across organizations and manages the various rescue teams. Concerning professional matters, however, the teams are supervised by centers outside the area, for example by the emergency center at a hospital or by the control room at a Fire and Rescue Service. We consider the simplified organizational structure shown in Figure 2.1 to be generic. The fixed and pre-planned organization reflects the generic rescue operation, but the organization has to be flexible in order to adapt to the specific operation at hand. Reorganization of pre-planned teams and roles may be required. Teams may be combined

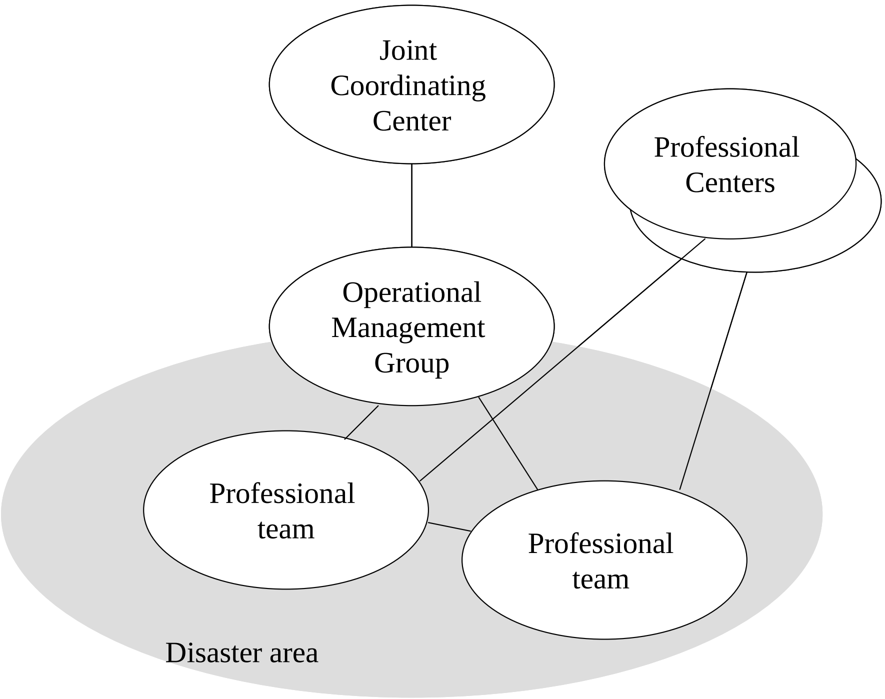

Figure 2.1 A generic rescue organization

or subdivided, and new teams may be established due to for example common operational mission or common location within the same geographical area. Teams may then overlap.

2.3 Other Actors

Only individuals belonging to the public rescue services are authorized to take part in rescue operations. Moreover, private rescue organizations may be involved. An example is the Red Cross, which sets up ad hoc rescue services and organizes search operations in areas that may not be covered by any infrastructure. Also, large companies may organize and train internal emergency services.

Especially, if the disaster is caused by an intentional action, there is a risk of hostile actors still being present. Actors like terrorists, hostile government agencies, criminals and hackers may have an interest in observing as well as of counteracting the rescue operation and may cooperate with allies outside the area.

Besides, there will be actors, which we call grey zone actors. Even though grey zone actors are not supposed to be hostile, their primary agenda may be different from taking part in the rescue operations. An example is mass media. In general, mass media enter disaster areas rapidly and may be present during the whole operation. The interests of the rescue organization and that of grey zone actors will sometimes converge and sometimes diverge. Depending on the disaster location, also spectators may be present.

2.4 Trust and Authentication

There is a mutual trust among the rescue organizations as well as among the individuals taking part in the operations. Trust is based on the individuals' membership in an organization and on operational roles, for example driver, surgeon or operations manager. Therefore, both an intra-organizational and an inter-organizational infrastructure for mutual authentication of memberships and roles must exist. Whereas organizational memberships are fixed and pre-defined, individuals may change roles dynamically.

Ideally, only individuals with authenticated membership in a rescue organization should take part in the operations. Even though systems for mutual authentication exist, the systems may be out of reach or suffer from other hindrances. In any case, the authentication process may take time. This means that legitimate members of the rescue organizations are formally regarded as untrusted until their memberships and roles are verified by the authentication system. Trust is obtained after a successful authentication process. The operations should not depend on the authentication system being available. Especially, in the initial phase of the operation, there should be a possibility for actors who are not yet authenticated, to take part immediately.

Also, there should be a possibility of making use of grey zone actors that are present in the area. Therefore, the communications system should be able to handle unauthenticated actors in a controlled and secure manner. Whereas legitimate actors will be authenticated and obtain trust sooner or later, grey zone actors will not. Nevertheless, their participation may still be useful.

A general, but informal trust is assumed to exist between the public rescue organizations and private emergency services that may have been involved in the first phase of the rescue operations. Even though objectives are similar, the mutual trust between the parties is supposed to be at a lower level, and it is not assumed that a formal means of mutual authentication is pre-established. If there is no authentication system to provide a mutual trust, actors from private emergency services will be considered untrusted during the whole operation. There may, however, be a need of their resources and cooperation. Trust between the rescue organizations and mass media is assumed to reflect their partly diverging missions.

2.5 Actor Distribution and Mobility

A detailed guideline for actor distribution and movements is impossible to specify. To a certain extent the location determines the way actors distribute throughout the area. Topology, vegetation, maritime conditions, tunnels and buildings may hinder an optimal distribution. The number of actors varies from incident to incident. Also within a particular operation the number varies. In the initial phase, there will be few, but the number may increase as operation goes on. Different phases will require different number of actors and different tasks to be solved. Therefore, the distribution throughout the area may change from phase to phase.

Nevertheless, there are some general patterns. Actor distribution will reflect the fact that rescue operations are group centric. It is a reasonable assumption that actors tend to form clusters rather than to scatter. For example, fire fighters may form one cluster, whereas a medical emergency team forms another one. In between, injured are moved away from dangerous spots and gathered for first aid and further transportation.

The location also determines the way actors arrive at the area. It is assumed that actors arrive mainly by cars at high speed, but boats and helicopters may also be utilized. Velocity may then range from zero to about 70 m/s. We assume that operations within a cluster will be on foot. With regard to distance and speed, mobility will therefore be limited. Actors move between clusters on foot or by vehicles at various speeds. In general, movements cannot be pre-planned. Even though movements may be coordinated in search operations, we do not assume that actors move in a coordinated manner.

2.6 Information Flow

The information flow will reflect the organizational structure. We distinguish between operational information and professional information. Operational information concerns the execution of the operations as such. This information is exchanged across organizational boundaries. In contrast, professional information is exchanged mainly among members of the same organization, for example medical data. In both cases communications with centers outside the disaster area is required. Communications with the outside, however, is not guaranteed and depends on the disaster’s location, severity and extent. The rescue operations may go on without external information exchange, but the quality and effectiveness may depend on communications with the outside. If access to external communications infrastructure is available, the capacity and quality may be reduced. Also hostile actors may disturb communications.

As a consequence of the potentially scarce communication resources, information exchange has to be prioritized according to its *importance*. Information will be transmitted as digital data, and it is not indifferent to whether the desired format is voice, text, picture or video stream, and information can also be classified according to its robustness to delay and loss. As a consequence of the potential presence of hostile actors and of the different levels of trust among actors within the disaster's vicinity, information has to be secured according to its *sensitivity*.

Classification according to importance has to be done dynamically as the operations proceed, whereas classification according to robustness and sensitivity may to a large extent be pre-defined. Classifications may depend on the roles of senders and receivers, information type and format.

2.7 Summary and Assumptions

Disasters may be categorized according to several parameters. Nevertheless, rescue operations cannot be pre-planned in detail. Operations have to be managed by a combination of general guidelines, pre-planned procedures and improvisations. Therefore rescue organizations have to be flexible and to allow reorganization according to the particular operation at hand.

Actors are employed by public rescue organizations and operate in overlapping teams. Teams may be organized across organizational boundaries, and may be combined and divided during the operations. Trust is based on authenticated relationships with a rescue organization and with operational and professional roles. Actors, which are not authenticated, are considered untrusted. Also actors, as mass media, will be present in the disaster's proximity.

The number of actors, their distribution and movements vary from incident to incident. Actors tend to cluster in geographically separated spots. Whereas speed varies throughout the disaster area, we assume that mobility is low within the clusters. Coordinated movements are not assumed.

The information flow will differ with regard to importance, format/media and sensitivity. Communications with the outside is desired, but not guaranteed. We assume, however, that voice communications are enabled locally within the disaster area.

The facets of a generic rescue operation scenario described in this chapter show that numerous parameters will be unknown in advance, and that a wide range of parameter values have to be taken into consideration. Therefore, an important characteristic of an emergency network should be flexibility.

3 EMERGENCY COMMUNICATIONS ARCHITECTURE

This chapter describes core requirements of emergency communication networks and the background for the planned emergency network in Norway. Some relevant base technologies are presented. Even though technology neutral, it is reason to believe that the specifications for the Norwegian network will be in conformance with the *Terrestrial Trunked Radio* (TETRA) standard. Therefore, we give an overview and discuss various aspects of TETRA-based networks in order to show their forces as well as their limitations. The purpose is to investigate how mobile wireless ad hoc technology might strengthen the emergency communications network. The potential utilization of mobile wireless ad hoc technology is then evaluated before we propose a schematic network architecture, which extends the emergency network with such networks.

3.1 Mission Critical Operational Needs

Since emergency operations involve different types of actors, there are different sets of network requirements. Requirements for public safety networks are described and specified by several international projects and standardization bodies, like TETRA Memorandum of Understanding (MoU) [43], *Mobility for Emergency and Safety Applications Project* (MESA) [29], *International Telecommunication Union* (ITU) [20], [19], *European Telecommunications Standards Institute* (ETSI) [13] and *Internet Engineering Task Force* (IETF) [21]. There seems, however, to be a broad international agreement on the basic requirements, which can be categorized as follows:

- Seamless radio coverage throughout the served area
- Network availability under exceptional conditions, including means of maintaining communications during infrastructure breakdown
- During major incidents and accidents the need for radio capacity increases. Capacity must be guaranteed to the rescue and law enforcement services
- Fast call set-up by instant connection and short response time
- Rescue operations are group-centric, and specialized functionality are needed to support group communications and dispatching. This includes dynamic management of communication groups, priority and security
- Voice quality allowing the listener to recognize the speaker, even under excessive background noise.

In order to meet the Schengen Convention, also international roaming and cross-border communications are needed.

3.2 The Norwegian Public Safety Radio Network

In Europe, separate service-specific networks based on analogue technology are now replaced by new, digital shared solutions. The process started in the early 1990s, and is pushed by the Schengen Convention, which mentions the necessity of establishing lines of communications among the countries to facilitate the cooperation between the police and custom authorities, particularly in border regions. The new emergency networks, are intended to have nationwide coverage by connecting long-range base stations to a fixed backbone. The networks are intended to serve the public safety and security services in their regular operations.

Up to now, Norwegian rescue services have been equipped with radio networks, which enable voice communications based on older technology. The networks are closed and do not interoperate across organizational boundaries. To compensate for weaknesses, wide use of *Global System for Mobile Communications* (GSM) is currently being made. Due to its large coverage also *Nordic Mobile Telephone* (NMT450) has been widely used. This system, however, was closed down at the end of 2004.

In 2004, after a process, which started in 1995, the Norwegian Parliament granted its consent that the Ministry of Justice and the Police during 2005 calls for tenders for establishing a shared digital radio communications system [30], [33]. The first rollout area is made up of six police districts in the Eastern part of Norway. According to the tentative time schedule, the

Norwegian Public Safety Radio Network will have nationwide coverage in 2009. The core users are the Police, Fire and Health services. Other users are organizations with public safety responsibility, for example the Defense, Civil Defense, energy supply services and voluntary aid organizations. Also vital services for society, such as traffic departments, harbor control services and security service companies with special responsibilities are potential users. Hence, the networks will not only serve acute rescue operations, but also serve vital needs of the society in case of catastrophes.

The core users have a need of approximately 37 000 vehicle mounted and hand held radio terminals as well as 280 fully equipped control rooms of different sizes. The number of base stations and switching nodes depends on the technology chosen, but initial studies based on TETRA have suggested 1 700 base stations. Regarding the infrastructure, it is emphasized that deployment into and re-use of existing public infrastructure will be of great significance to the cost. The aim is to use the existing infrastructure wherever possible and expedient. The amount of capacity guaranteed to rescue services is a matter of agreements with the network owners. The network will have interfaces towards, and be interoperable with, the public fixed telephone network, like the *Public Switched Telephone Network* (PSTN) and the *Integrated Services Digital Network* (ISDN), and cellular networks like GSM and the new railway safety network *GSM-Railway* (GSM-R). An overview of the network is shown in Figure 3.1 [33]. The high level architecture is in accordance with a TETRA-based solution. The radio network consists of

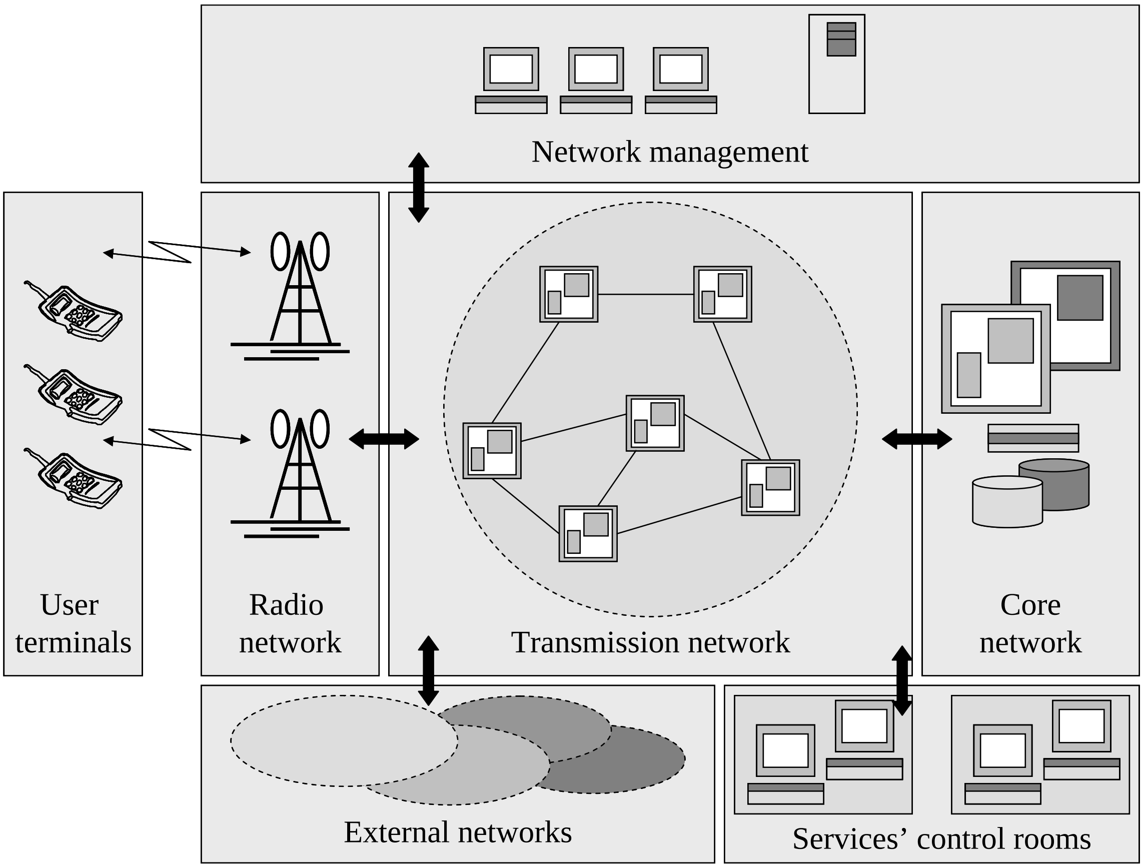

Figure 3.1 Norwegian Public Safety Radio Network

base stations, which are supposed to cover most of the populated areas as well as the main roads. Radio channels have low capacity. The core network consists of one or more switches, whereas the transmission network, which transports data between the core network and the radio network as well as external networks, consists of fixed connections. The network is supervised and maintained by a network management system, which may be centralized or distributed. More details are given in section 3.4.

The specifications shall be technology neutral. It is, however, pointed out that the commercial mobile telephone systems do not meet the altogether essential requirements for an emergency communications system.

3.3 Relevant Technologies

Two major purpose-built radio system technologies are used for public safety and security in Europe: TETRA [43] and TETRAPOL [46]. TETRA is an open standard, defined and supported by ETSI. The *European Commission* approves the standard. TETRAPOL is a descendant of TETRA-12, one of the proposals not chosen by ETSI. ITU, the *European Conference of Postal and Telecommunications Administrations* (CEPT) [12] and the European Commission have accepted the standard as a “de facto” standard. Within the Schengen cooperation, both TETRA and TETRAPOL are recommended. Both standards are specified to meet the requirements listed in section 3.1. The fact that TETRA was the recommended standard in the first instance has probably been a contributory reason why many European countries have chosen that technology. Efforts are made to enable communications between TETRA and TETRAPOL.

GSM enhanced with *Advanced Speech Call Items* (ASCI) has been a technology candidate. Also GSM upgrades like *General Packet Radio Service* (GPRS) and third generation networks like *Universal Mobile Telecommunications System* (UMTS) have been investigated [42], [45]. So far, no country has chosen GSM or UMTS as the basis technology for its national emergency network.

GSM-R is a variant of GSM and intended for private railway networks within Europe. The frequency band is different to public GSM. The network also offers additional voice functionality by the utilization of ASCI facilities like priority, pre-emption and group calling [45]. Railway safety networks are rolled out in several countries, and a GSM-R network is also planned for the Norwegian railway. The intention is to cover the entire railway network in 2007 [30].

3.4 Terrestrial Trunked Radio (TETRA)

This section describes important aspects of a TETRA-based emergency network. Unless otherwise stated, background information about TETRA and its applications is from papers, presentations and general information published at the official web sites of ETSI [14] and TETRA MoU [43] by December 2005.

3.4.1 Introduction

TETRA is a digital *Private Mobile Radio* (PMR) and *Public Access Mobile Radio* (PAMR) technology for police, ambulance and fire services, security services, utilities, military, public access, fleet management, transport services, closed user groups, factory site services and mining. TETRA is an open multi-vendor standard. In order to support the needs of emergency services throughout Europe, the standard has been developed over a number of years by the co-operation of manufacturers, users, operators and other experts. The standard builds upon the techniques of previous analogue trunked radio systems and the development of GSM during the 1980s. The work started in 1990 and the first standards were ready in 1995.

For emergency systems in Europe the frequency bands 380-383 MHz and 390-393 MHz have been allocated for use by harmonized digital land mobile systems. Additionally, whole or appropriate parts of the bands 383-385 MHz and 393-395 MHz can be utilized if required. For civil systems in Europe the frequency bands 410-430 MHz, 870-876 MHz / 915-921 MHz, 450-470 MHz, 385-390 MHz / 395-399 MHz, have been allocated for TETRA.

TETRA uses *Time Division Multiple Access* (TDMA) technology with 4 user channels on a radio carrier with bandwidth of 25 KHz. Both voice and data are supported. National and international roaming can be supported. In trunked mode of operation, TETRA provides a pooling of all radio channels, which are allocated on demand to individual users. In direct mode of operation, TETRA provides local communications independently of base stations and fixed infrastructure. Point-to-point and point-to-multipoint communications are supported both in trunked and direct mode.

3.4.2 The TETRA standards

The TETRA Project has produced a wide range of technical reports, technical specifications and standards. The vast majority concerns the radio interfaces, whereas important parts of the network, like the core network and the transmission network, are left for implementation. The following interfaces are covered, see Figure 3.1:

- *Air Interface* (AI), which is the interface between the base station and the user terminal
- *Direct Mode of Operation* (DMO) *Air Interface,* which is the interface between user terminals that operate independently of the base station
- *Peripheral Equipment Interface* (PEI), which is the air interface between the user terminal and a peripheral device, for example a computer
- *Inter-System Interface* (ISI), which is the interface between different TETRA systems
- *IP Inter-working Interface* (IPI), which is also an interface between different TETRA systems. The interface is based on *GPRS Tunneling Protocol* and supports roaming
- *External Network Gateway,* which is the interface between a TETRA system and an external communications system, like PSTN/ISDN or GSM/GPRS
- *Man Machine Interface* (MMI), which is the interface between the user terminal and the human user. The interface is not standardized
- *Remote Console Interface,* which is the interface between the network and a remote console, for example in a control room. The interface is not standardized
- *Network Management Interface,* which is the interface between the network and network management system. The interface is not standardized.

TETRA Release 2 (TETRA 2) is underway. The release provides general enhancements, in particular with regard to channel capacity.

3.4.3 Elements of the architecture of a TETRA-based network

Assuming that the network shown in Figure 3.1 will be realized as a TETRA-based network, we briefly describe some elements of the architecture:

The radio network consists of base stations and user terminals. As mentioned in subsection 3.4.1, there are two modes of operation: *Trunked Mode of Operation* (TMO), where communications are enabled via the base station, and *Direct Mode of Operation* (DMO), which handles out-of-coverage conditions. TMO services comprise speech, data, supplementary services, call control, mobility management, and security services. The data service offers circuit mode, packet mode comprising X.25 and *Internet Protocol* (IP), and the *Short Data Service* (SDS), which supports packets of various sizes. Both speech and data services support individual calls as well as group calls, including broadcast. Available services in DMO are speech (half duplex), data (circuit mode and SDS), some intrinsic services, addressing services and security services. There are four basic operational styles of DMO: The *Back-to-Back* enables terminal-to-terminal communications. The *DM Repeater* allows the DMO terminal coverage to be enlarged when needed. The *DM Gateway* relays between DMO and TMO and enables DMO terminals to communicate with the TMO system and vice versa. The *Dual Watch* offers periodic scanning of the other mode for incoming traffic.

As mentioned, four user channels are available for simultaneous usage. Depending on the selection of coding scheme, data rates from 2.4 to 7.2 Kbits/s are offered per time slot. Using all timeslots, available capacity ranges from 9.6 to 28.8 Kbits/s. DMO offers a maximum capacity of 7.2 Kbits/s.

TETRA 2 comprises two different technologies for high-speed data in the region from 30 to 400 Kbits/s: *TETRA Advanced Packet Service* (TAPS) and *TETRA Enhanced Data Service* (TEDS). TAPS is an overlay network based upon GPRS technology. TAPS aims at providing user data rates up to 470 Kbits/s (per carrier) and provides standard GPRS interfaces to external packet data networks. TEDS makes use of the existing *TETRA Release 1* (TETRA 1) standards to ensure backward compatibility. The objective of TEDS is to provide packet data at speeds approximately 10 times that available in TETRA 1. The high data rates come to the expense of range. The cell radius offered by TETRA 1 is around 5 km and the number of base stations required to cover for example Belgium (30 000 km^2) is approximately 380. Coverage analysis of TAPS shows that with a carrier bandwidth of 200 KHz, the cell radius offered at maximum data rate is 0.56 km. As a result the number of base stations needed to cover Belgium increases to more than 37 000. Coverage analysis of TEDS shows better characteristics. Nevertheless, with a carrier bandwidth of 50 KHz, a data rate of 200 Kbits/s reduces the cell area to 19% of the area covered by TETRA 1. At the same data rate TAPS would cover only 7%.

The core network consists of mainly *Switching Control Nodes* (SCNs). A typical conventional system consists of one centralized switching node with base stations connected. For larger networks, a hierarchy of switches may be used to reduce the cost of interconnections and to improve scalability. Figure 3.2A) [43] shows a conventional TETRA network. Components connected to the centralized switching node include the network management

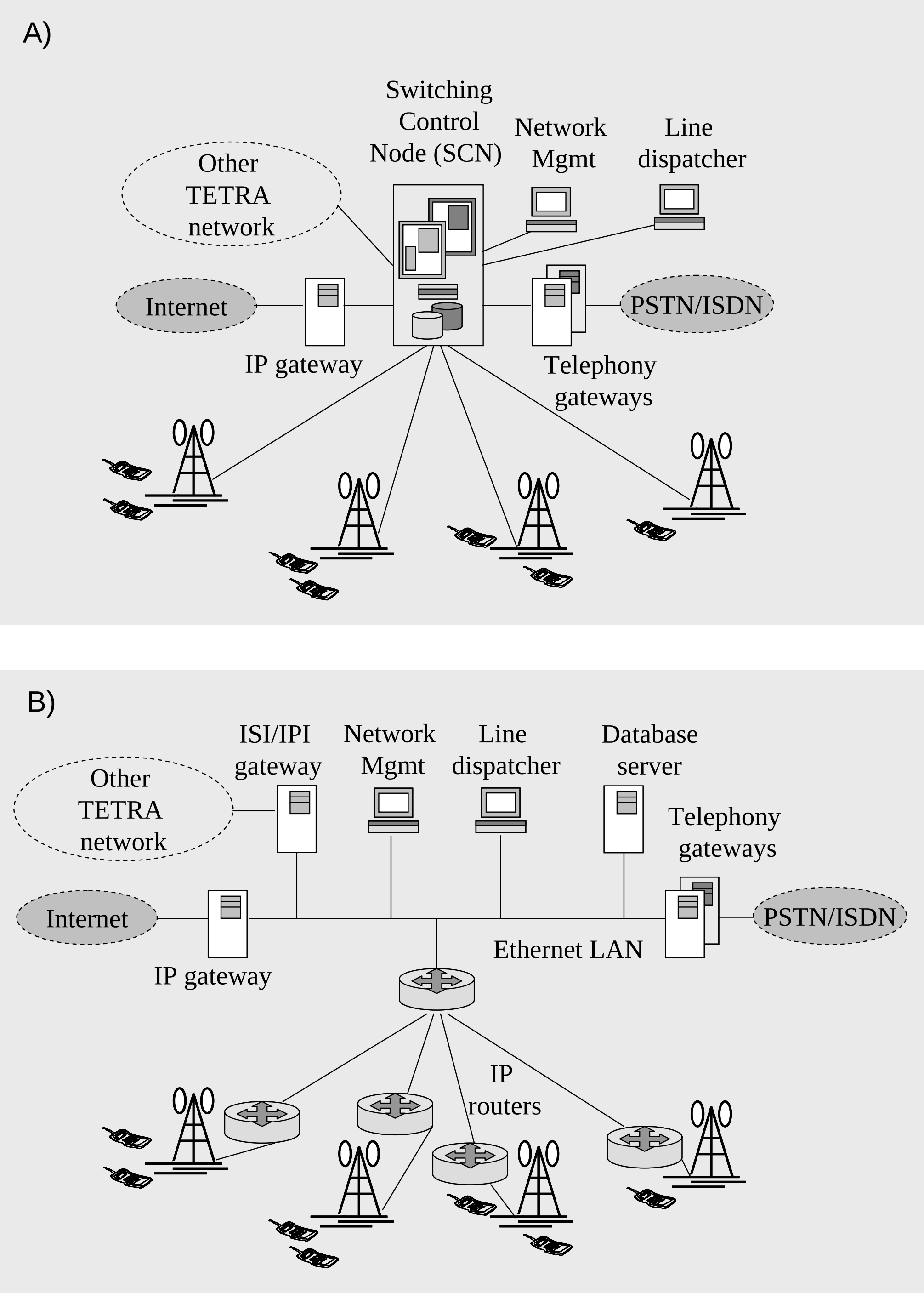

Figure 3.2 *A) Conventional TETRA network that supports IP-over-TETRA.*
B) TETRA-over-IP network.

system, other TETRA networks using ISI, external telephone networks and an IP gateway. Conventional TETRA networks support *IP-over-TETRA*. The IP gateway allows exchange of SDS and status messages between a TETRA terminal and an application running on a PC connected to the IP network. Also packet data is available on some conventional TETRA systems, allowing exchange of IP data between an application running on a PC connected to the

TETRA terminal and an application running on a server within the Internet. A variant of IP-over-TETRA is the use of the *Wireless Application Protocol* (WAP) on TETRA terminals.

TETRA-over-IP is often confused with *IP-over-TETRA* described above. A TETRA-over-IP network is shown in Figure 3.2B) [43]. This architecture is quite different from the conventional one. IP routers are utilized to interconnect the different infrastructure components. Routers replace the SCNs. Centralized switches are not necessary. During the call, a direct interconnection is established between the base stations installed on the different sites. Components connected to the *Local Area Network* (LAN) include the network management system, an ISI/IPI gateway, gateways to external telephone networks and an IP gateway. Since the IP protocol suite is used to interconnect all elements in a TETRA network, an existing IP backbone could be used to realize a resilient and flexible TETRA network. So far, TETRA-over-IP is not standardized. Current TETRA-over-IP solutions are based on proprietary technologies and are for example not compatible with *Voice-over-IP* (VoIP) industry standards. Each manufacturer has defined its own protocols for call establishment, transport of speech and database synchronization.

The transmission network is the TETRA backbone. In the conventional architecture shown in 3.2A), the transmission network connects the base stations to the switching nodes and interconnects switching nodes as well as different TETRA networks. The base stations are normally connected to the switching nodes via 64 Kbits/s bearers, which are sub-multiplexed with 8 Kbits/s channels. Given a TETRA-over-IP architecture as shown in Figure 3.2B), the transmission network interconnects the TETRA backbone routers. Backbone routers may as well be regarded as parts of the transmission network itself. Connections between routers are basically point-to-point links such as 2 Mbits/s E1 links or low speed synchronous V.35 links. Link speed ranges from 128 Kbits/s to 2 Mbits/s.

In TETRA terminology, the base stations, the core and transmission networks are called the TETRA *Switching and Management Infrastructure* (SwMI).

Network management may be internal or external. An internal management system caters for monitoring and control of a TETRA network whether single site or national in extent, whereas external management is applied to two or more TETRA networks connected by the ISI interface. The internal network management infrastructure is not standardized. The choice of architecture and protocols depends on the infrastructure details. The TETRA project has, however, defined an external network management scheme as a recommendation. So far the typical TETRA-based network is managed by a centralized management system.

3.4.4 Security in TETRA

Security is important in TETRA. The standard, however, does not contain a generic security policy. The standard offers several security management features, which may support different policy choices. References [36] and [37] give background information about TETRA security:

Authentication. To prove that a user/terminal and the network infrastructure/SwMI are who they claim to be, TETRA offers a service that provides mutual authentication. Authentication is based on proof of possessing a unique secret authentication key. The key is shared between a terminal and the SwMI and is unique for each terminal. Only legitimate terminals are allowed to enter the SwMI, and the terminals are allowed to use only the genuine SwMI. The authentication procedure involves a challenge-response mechanism. There are different ways of generating the key. The method depends on whether the user, the handset or both user and handset have to be identified. The key is supposed to be stored in a *Subscriber Identity Module* (SIM)/Smart Card at the terminal side and at the Authentication Center at the SwMI side. The authentication service is centralized and depends on access to the Authentication Center. Hence, the authentication key is not applicable in DMO. Successful authentication permits further security functions to be downloaded, for example encryption keys.

Confidentiality. The standard supports four different symmetric encryption algorithms for the air interface, *TETRA Encryption Algorithm 1:4* (TEA). TEA 2 is meant for European public safety organizations. There are also four types of keys for the air interface encryption: The first one is derived through the authentication procedure and is used to encrypt the link between the mobile station and the network on an individual basis. The second is a common key and may be utilized for messages that are directed to all stations within a certain area. The third one is a group key and is linked to a certain closed user group. The last key is a predetermined key, which can be used without prior authentication. Such keys may be used in DMO, where they may also provide for implicit authentication.

Key management is centralized. There are, however, options that enable decentralized management of authentication keys. The key management center distributes common keys and the group keys in accordance with an *Over The Air Rekeying* (OTAR) scheme. Terminals cannot receive new keys while in DMO. Security management features other than key management is also supported.

Disabling of terminals. A service, which disables stolen or lost terminals, is also provided. In DMO, the disabling feature is not available.

End-to-end security. There are possibilities of end-to-end encryption in order to protect user messages as well as control messages over an untrusted infrastructure. The symmetric *Advanced Encryption Standard* (AES) is the default algorithm. Likewise, there are possibilities of transferring authentication information between TETRA networks.

3.5 TETRA Provides a Minimum Solution

This section discusses some important aspects of a TETRA-based emergency network and shows that the network will represent only a minimum solution.

3.5.1 Availability and connectivity

An emergency communications network is supposed to be more reliable than its public commercial counterpart and thus to improve availability and guarantee capacity under exceptional conditions. In order to represent redundancy, the radio network as well as the backbone should be deployed independently of, and separated from, the public commercial communications infrastructure. As described in section 3.2, this infrastructure will be re-used wherever possible. This means that the Norwegian Public Safety Radio Network will not represent a *redundant* nationwide network. If the transmission network shown in Figure 3.1 is implemented as leased capacity in public commercial infrastructure, communications between a disaster area and the outside will rely on an intact public commercial infrastructure. Public infrastructure is vulnerable to local damage and local power breakdown. Moreover, the fixed and the cellular networks often share the same physical backbone. If also the TETRA base stations are co-located with existing communications infrastructure, the ability of external communications will rely on a single point of failure. Therefore, the planned emergency network has an essential vulnerability.

TETRA-over-IP networks will be more flexible and resilient than the conventional hierarchical and static TETRA networks. Any type of IP infrastructure can be utilized, whether it is the public Internet, a private intranet or a LAN using Ethernet. IETF has organized several working groups for treatment and security of emergency communications, for example the *Internet Emergency Preparedness* (IEPREP) group. The TETRA community, however, does not recommend utilizing the public Internet. Separate IP networks are recommended to ensure throughput and security. But even though the TETRA backbone routers are separated from the public Internet, the TETRA infrastructure still relays on public commercial communications infrastructure, at least at the physical layer.

Regardless of how the transmission network is implemented, communications *within* the disaster area should not depend on pre-established infrastructure being accessible. The ability to communicate independently of the pre-established infrastructure is crucial. The Norwegian Public Safety Radio Network is planned to cover close to 100% of the population. 10-20% of the area, however, will be out coverage. Rescue operations in areas that are permanently out of coverage require a capability of autonomous network operation. As described in subsection 3.4.3, DMO enables operation outside the coverage of the base station. DMO may also be utilized when access to the trunked infrastructure is not needed. Further, DMO may provide extra capacity when the trunked network is highly loaded. The capability to operate in an autonomous manner is a key differentiator between TETRA and other cellular technologies. The TETRA DMO functionality, however, is limited.

TETRA provides standardized gateways to external networks as PSTN, ISDN and GSM. Reference [30] states that cooperation between the Norwegian Public Safety Radio Network and the GSM-R network is required. In addition to economies of scale as regards the rollout, cooperation will provide coordinated coverage in certain train tunnels. Hence, there will be a need for gateways between TETRA and GSM-R. Frequencies used for the NMT450 (453-457 / 463-467 MHz) were recently subjected to auction. The holder of the technology neutral license is planning to deploy a *Code Division Multiple Access* (CDMA) 450 (CDMA2000) network [32]. Hence, there may also be a future need for gateways between TETRA and CDMA450. Since gateways are specified between the TETRA infrastructure and the external networks, external communications depend on this infrastructure being available. Hence, external networks can not be reached in DMO.

3.5.2 Capacity

The debate concerning TETRA/TETRAPOL versus public cellular networks as the base technology for emergency networks has highlighted functionality associated mainly with voice communications. Less attention has been paid to the capability of efficient data communications. Networks based on TETRA as well as on other cellular technologies, have low radio link capacity compared to for example wireless LANs (WLANs). TETRA 1 offers four timeslots, which enable a maximum of four simultaneous users. This means that only four calls can be set up at a time. The small number of time slots represents a severe limitation to the communications. Especially, in large operations the probability of idle time slot may be small. Due to the priority and pre-emption functionality, the probability of completing a regular low priority call may be small and lead to repeated call requests. The utilization of scarce resources may then become inefficient. The small number of time slots indicates that DMO functionality will be widely used for communications within the disaster area. In normal operation, however, DMO allows only one call at a time.

Given four simultaneous users, a maximum capacity of 7.2 Kbits/s is available per user. Therefore, not only the small number of time slots, but also the low data rate, represents severe restrictions to the communications. The actors' ability of exploiting important and useful resources will be limited. Not only the usage of resource demanding media as pictures and videos, will suffer. For example, communications with databases located outside the disaster area and remote surveillance of injured, will be difficult or impossible.

TETRA 2 will enhance existing data capabilities and enable more advanced applications. As described in subsection 3.4.3, the enhanced capacity comes to the cost of magnifying the number of base stations needed for TETRA 1. Likewise, the capacity of the transmission network has to be upgraded accordingly.

Delay caused by for example serialization and queuing in the IP routers has to be considered in an IP backbone. Typically, the links should be dimensioned for a load of 25%. Hence a TETRA-over-IP solution requires four times the minimum required bandwidth for a non-IP based synchronous interconnection. In addition, the IP packet overhead should be taken into consideration. To carry TETRA speech packets over an IP network, more than 50% of the packet size is used for IP routing and addressing.

3.5.3 Security

With regard to security the air interface between the mobile station and the network seems to be taken well care of by the TETRA standard. Since both the authentication service and the key management are centralized and depend on a pre-established communications infrastructure, the security services offered for the DMO are simple and limited. The DMO appears to be the weakest part of the radio network. With the general TMO air interface having a high level of security, the underlying fixed TETRA infrastructure may be an easy target for potential attacks. With few exceptions the underlying fixed network is not standardized but left for implementation.

3.5.4 Summary

Based on TETRA 1 the Norwegian Public Safety Radio Network will provide a nationwide emergency network, which satisfies mission critical operational needs. The network will not be redundant with regard to the transmission network, but will rely on commercial communications infrastructure. Besides, some areas will remain out of coverage. The ability to operate independently of a pre-established communications infrastructure is therefore required. TETRA

DMO provides a limited out-of-coverage functionality.

The small number of time slots restricts communications to a minimum. The small number of time slots indicates that even though limited, the DMO functionality will be widely used. A wide usage, however, will weaken the over all security, since the security services offered in DMO are limited compared to the general TMO air interface. The low data rates limit the communications to voice and the exchange of simple data formats. Therefore, a network based on TETRA 1 technology will represent a minimum solution for the Norwegian Public Safety Radio Network.

A TETRA-over-IP infrastructure will be more resilient and flexible than a conventional one. Nevertheless, an IP-based solution will not increase the network capacity. Even though IP-based solutions are the future trend within the TETRA community, work has to be done in order to meet the special requirements for mission critical applications, for example real-time voice transport.

Based on TETRA 2 the capability of data communications would be enhanced. On the other side, the cost of deploying the number of base stations required for equivalent coverage will be high. We therefore assume that a network based on TETRA 2 is an unrealistic option.

3.6 Utilization of Mobile Wireless Ad hoc Networks

This section discusses the potential utilization of mobile wireless ad hoc networks within the planned Norwegian Public Safety Radio Network as it is described in section 3.2 and 3.4. We propose and describe a schematic reference architecture, which incorporates ad hoc technology. Especially, with regard to the shortcomings discussed in section 3.5 mobile wireless ad hoc networks will strengthen the emergency network. On the other hand, in order to fulfill the requirements listed in section 3.1, further research is needed. Some research areas are discussed.

3.6.1 Schematic reference architecture

This subsection describes a possible architecture, which incorporates mobile wireless ad hoc networks into the generic network architecture presented in Figure 3.1. A mobile wireless ad hoc network operates independently of a pre-established infrastructure and is supposed to be self-configured. Base stations are not needed. Each node serves both as an end terminal and as a router. Routing protocols running in the nodes enable the exchange of topology information in order to calculate multi-hop routes. Given appropriate node density, end-to-end unicast communications between any pair of nodes is enabled. Multicast and broadcast are also options.

Intuitively, ad hoc networks will mainly serve as extensions to the radio network. A moderate option is then to utilize ad hoc technology at the border of base station coverage or as extra capacity for the exchange of specific types of information. Then the utilization of ad hoc networks is restricted. Even though this is a realistic alternative, we believe that the potential gain from integrating ad hoc networks will not be fully exploited. A radical option is to *replace* the user radios with ad hoc nodes. Then the utilization of the base station is restricted. The base station may serve as a gateway for communications with the outside and as a means of enhancing the coverage and connectivity of the ad hoc network in the disaster area. This alternative is infeasible since current technology for mobile wireless ad hoc networks is not able to meet the critical requirements regarding voice communications. Voice communications have to be *guaranteed* in the disaster area. Therefore, ad hoc nodes based on current technology should not replace the user radios.

A scenario with both TETRA-like handsets and mobile wireless ad hoc nodes are probably the most realistic short-term solution. An upcoming solution may be multi-band terminals with multiple IP interfaces. Multi-band facilities will enable the terminal to act as a TETRA radio, a GSM/UMTS terminal as well as a mobile wireless ad hoc node. Multiple IP interfaces enable the terminals to take part in different IP networks simultaneously, for example different ad hoc networks. The proposed reference architecture is shown in Figure 3.3.

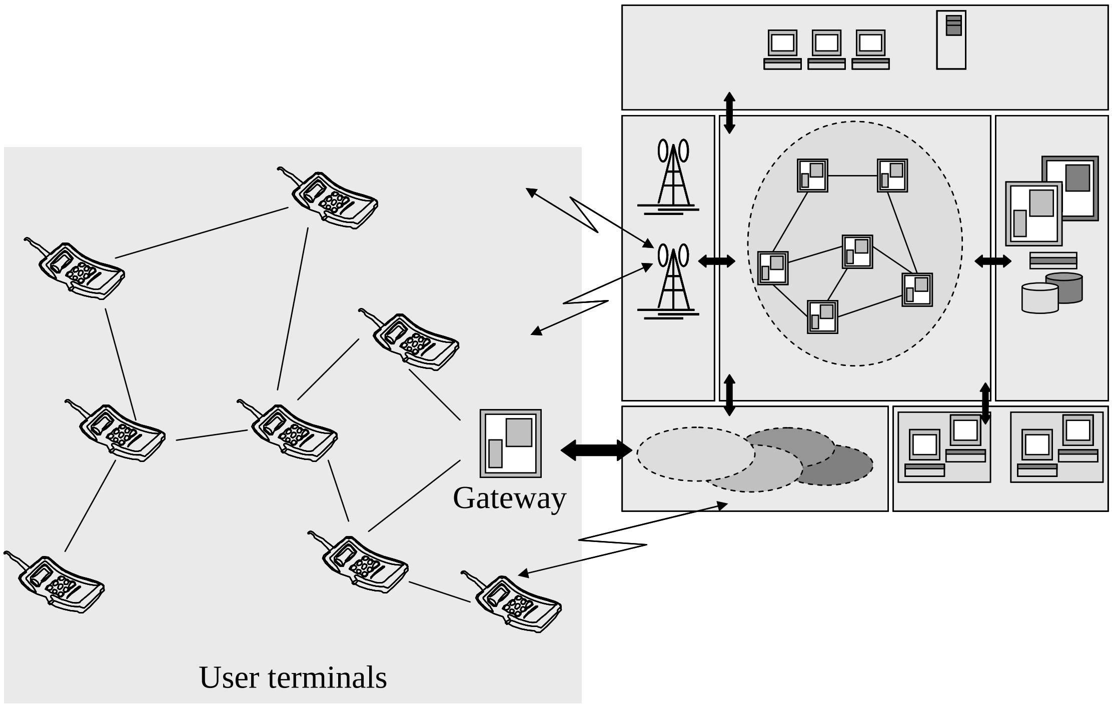

Figure 3.3 Emergency network extended with a mobile wireless ad hoc network

For simplicity we assume multi-band user terminals with multiple IP interfaces. Throughout this chapter the term *mobile wireless ad hoc network* is synonymous with *user terminals in ad hoc mode*. In ad hoc mode, user terminals will have a transmission range of 30-200 m and a nominal channel capacity greater than 2 Mbits/s. The link layer is based upon some IEEE 802.1x descendant technology, whereas the network layer is based on the IP protocol suite. Various types of routing protocols may be selected. Figure 3.3 indicates routes within the multi-hop ad hoc network as well as communications between user terminals and the TETRA base station. In order to enable seamless communications between a mobile wireless ad hoc network and a TETRA-over-IP infrastructure, an address policy, which involves the allocation and advertising of IP addresses, is required. A user terminal should be addressable within one or more ad hoc networks at the emergency site, within the private intranet of the particular rescue service and probably within the public Internet. In order to manage the initial phase of the operation, any legitimate node should be able to initiate an ad hoc IP network at the emergency site. Therefore, any node should be able to assign IP addresses, for example from a pre-planned address space.

External networks may represent additional redundancy, connectivity and capacity. Within the architecture shown in Figure 3.1, communications via external networks depend on access to the emergency infrastructure. In contrast, within the architecture shown in Figure 3.3, such communications may take place independently of the emergency infrastructure. This architecture makes direct connection to available public commercial networks a matter of policy. If a public cellular base station covers the disaster area, communications require only a valid SIM card. Communications with external IP networks, however, require one or more gateway nodes between the ad hoc network and the external networks. The gateways may be specialized nodes within the mobile wireless ad hoc network and at the same time they may serve as routers within external IP networks. We assume that gateway nodes are mounted in vehicles and consequently at hand in most operations. Connection to external networks, however, has to be arranged on site, either by rolling out cables or by mounting portable equipment for radio transmission. In order to exploit the additional connectivity and capacity offered by external networks, the address scheme should enable appropriate reachability/addressability. Solutions like multi-homing should be considered. A detailed policy and solution for the management of IP addresses depend on the underlying TETRA-over-IP infrastructure as well as on the alternative external infrastructure. IP version (v4/v6), security, available routing protocols and available mechanisms for the allocation and advertising of addresses are key factors. The address policy is related to the security policy and should especially be considered with regard to the choice of verifiable identities and authentication rules at the different communications layers.

Gateways should be equipped with a *Domain Name System* (DNS) and other Internet services. There are several options for external communications. Gateways at the disaster area should be able to handle several intranets in addition to the public Internet. Simple and good solutions might be based upon *Network Address Translation* (NAT) managed by gateway nodes. *Virtual Private Networks* (VPN) with *IP Security* (IP Sec) tunnels might be set up between the gateways and private intranet servers. Then, even though the public Internet is utilized as an alternative to the TETRA backbone, direct communications between an ad hoc terminal and the public Internet could be controlled and handled by the private intranet of the particular rescue service. The different intranets involved might also be interconnected through VPNs. Hence, the additional capacity and connectivity provided by external networks would be even more valuable.

Although mobile wireless ad hoc networks are especially well suited for integration in TETRA-over-IP architectures, we do not make particular assumptions regarding the implementation of the infrastructure shown in Figure 3.3.

3.6.2 Availability, connectivity and capacity

Even though a TETRA based network is able to operate in an anonymous manner, the DMO functionality is limited compared to a mobile wireless ad hoc network. With regard to out-of-coverage communications, ad hoc technology will represent additional and/or alternative connectivity and thus enhance robustness and user functionality. The routing capacity at the network communications layer, which enables multi-hop communications, is one of the main differences between a mobile wireless ad hoc network and a plain relay-based solution like TETRA DMO. In chapter 4, we investigate the node density needed to obtain connectivity to all nodes.

In case public commercial infrastructure is available in the disasters' vicinity, the ad hoc network would offer an alternative connection to external networks and thus increased redundancy to the emergency network as described in the previous subsection. The actors involved would then be able to exploit whatever communications infrastructure available in the area. Moreover, mobile wireless ad hoc networks may ease the communications with for example sensors used in observation of injured and robots used in fire fighting.

As described in subsections 3.4.3 and 3.5.2, TETRA allows four simultaneous users, whereas TETRA DMO may represent some extra capacity. In chapter 4, we will show that the utilization of mobile wireless ad hoc networks will increase the number of simultaneous users significantly. The re-use of frequency enables an increased number of simultaneous users, but also the number of simultaneous users located within a one-hop neighborhood will increase considerably.

A realistic nominal channel capacity in the mobile wireless ad hoc network will be greater than 2 Mbits/s. Even though throughput decreases as the number of hops increases, mobile wireless ad hoc networks will represent a significant improvement compared to 28.8 Kbits/s offered by TETRA 1. Hence, the mobile wireless ad hoc network may enable a wide range of applications, for example efficient exchange of pictures and videos. Further, the ad hoc network will reduce the load on base stations and contribute to a more efficient over all resource utilization.

3.6.3 Quality of Service (QoS), priority and pre-emption

Different types of traffic have different requirements in terms of predictable service, often expressed as requirements on bandwidth, timeliness, jitter (delay variance) and packet loss. As a consequence, the network must have the ability to classify and treat traffic differently. As network resources are limited, QoS also implies some sort of call or flow admission. When using the regular IP best-effort service, the delay, jitter and packet loss are not predictable in a scarce resource environment. Packets may be lost during transmission over a wireless link or discarded due to overload in the routers.

The best-effort service may be sufficient in most applications but may have a serious impact on the operation of some public safety applications. Within the TETRA community the call setup time and speech delay are important considerations. On the other hand, the dependency on instant call set up varies. Fire fighters and medical personnel may have to make decisions instantly, whereas coordinators may have longer time lags.

Two standard QoS models are developed for fixed IP networks: *Integrated Services* (IntServ) and *Differentiated Services* (DiffServ). IntServ uses the *Resource Reservation Protocol* (RSVP) to signal QoS requirements to the network elements in order to reserve resources along the route. In addition to the best-effort service, two service classes are defined:

One class provides bounds on end-to-end delay, whereas the other one provides guarantees on packet loss. Quality is guaranteed per flow.

To avoid scalability problems DiffServ treats traffic on an aggregate basis and only specifies per router treatment, or *Per-Hop Behavior* (PHB). Two styles of PHB are defined: One behavior focuses on delay (expedited forwarding), whereas the other one assures delivery (assured forwarding). Traffic is classified according to the PHBs and buffering and packet scheduling are only on a per class basis.

The actual QoS architecture to be used depends on the yet to be determined TETRA-over-IP-standard. Clearly, a QoS solution is needed within the TETRA-over-IP network as well as within the mobile wireless ad hoc networks. QoS in mobile wireless ad hoc networks is a relatively new research field, and the trend is towards developing lightweight alternatives to IntServ and DiffServ. Within IETF there are groups working on these subjects. Some approaches will be presented in subsection 4.6.6.

Priority and pre-emption are linked to the network’s ability to differentiate QoS. These requirements, however, are not emphasized in the current QoS architectures and will need to be researched and developed for ad hoc networks. Priority and pre-emption functionality has usually been associated with voice communication services like the “push to talk” express calls. The low capacity in TETRA-based networks, however, calls for strict priority and pre-emption regardless of medium/format. Whereas TETRA provides priority and pre-emption, this functionality has to be developed for mobile wireless ad hoc networks. Consistent priority policy has to be ensured throughout the networks. Priority and pre-emption policy may to a certain extent be pre-defined, but there is also a need to change the policy dynamically during the different phases of the rescue operations. Which information is the most important one, depends on current situation. Therefore, priority policy has to be managed dynamically.

3.6.4 Group communications

Since rescue operations are group centric, specialized functionality in group communications is one of the major network requirements, and one of the major facilities enabled by TETRA. As described in section 2.2, groups are pre-planned, but there is a need to reorganize as the operations go on. Hence, groups have to be established, combined, divided and dissolved dynamically. In a TETRA network, groups are managed in a centralized manner, for example by the services’ control rooms. Group management relies on communications via the trunked infrastructure and is not possible in DMO. Representing a “single point of failure”, centralized group management has a fundamental vulnerability.

Group management is an important research topic within mobile wireless ad hoc networks. Efficient distributed and dynamic solutions will make ad hoc technology even more suitable for emergency networks, especially when operated in an autonomous mode. Approaches to secure group management are presented and discussed in [58] and [28].

Multicast routing is a related and important research field. Due to the organizational structure, we assume that group communications are more important than one-to-one communications in rescue operations. Therefore, group communications call for efficient and interoperable multicast protocols in the emergency network as well as in the potential mobile wireless ad hoc extensions. An overview is given in [10]. The proposed approaches are classified into four categories based on how routes are created to the members of the group. The tree-based approach is a well-established concept in wired networks. A delivery tree is built and maintained. Examples of wireless variants are the *Ad Hoc Multicast Routing Protocol Utilizing Increasing ID Numbers* (AMRIS) and the *Multicast AODV* (MAODV) protocol, which is derived directly from the *Ad Hoc On Demand Distance Vector* (AODV) routing protocol. In contrast to the tree-based approach, the meshed-based schemes provide multiple paths between any source and receiver pair. The *On Demand Multicast Routing Protocol* (ODMRP) is an example. The stateless multicast approach tries to overcome the overhead required to maintain a delivery tree/mesh by including the list of destinations in the packet header. The last category is the hybrid approach, which combines the advantages of both the tree and mesh-based schemes. The *Ad Hoc Multicast Routing* (AMRoute) protocol is an example.

Group management is also related to security, which is discussed in the next subsection.

3.6.5 Security

Data exchanged between users and applications must be protected against violation of confidentiality and integrity. Attacks may be passive or active. A passive attack, such as eavesdropping, does not interrupt the communications and the operation, but may reveal valuable information. Active attacks, such as inserting false messages, modifying messages in transit or replaying old messages, may disrupt the network operations as well as the rescue operations. As described in section 2.4, there are several levels of trust between the actors involved in a rescue operation. The network should be able to reflect the different levels. The degrees of threats and risks depend on the type of disaster. Established and proven security solutions are resource consuming with regard to both computation and transmission. Due to limited capacity the emergency network should be flexible with regard to the level of protection. The network should be capable of resisting attacks in a hostile environment, but should also be able to utilize lightweight solutions when the possibility of attacks is supposed to be small.

The potential use of mobile wireless ad hoc networks introduces two new aspects to the radio network security. Whereas the air interface in TETRA is limited to one hop, the mobile wireless ad hoc network introduce *multi-hop*. This means that end-to-end protection has to be taken care of *within* the radio network. Further, the *network layer* is added to the communications. This means that the routing mechanism may be attacked in order to violate or to control the network itself or in order to serve an attack on user/application data. Therefore, *routing information* has to be secured in order to protect the network as such. Routing protocols in ad hoc networks are vulnerable to attacks. An adversary may manipulate the routing information by inserting false protocol messages into the network or by modifying messages in transfer in an unauthorized manner. Authentication and data integrity services are crucial to routing protocols utilized in rescue operations, and are also required in case the ad hoc network offers QoS and priority functionalities as described in subsection 3.6.3. By eavesdropping control messages an adversary may gather information for traffic analysis. Contrasting military operations, the risk of revealing such information is probably small in rescue operations. Therefore, we assume that encryption of routing messages is not required.

If mobile wireless ad hoc networks are to be integrated in a TETRA-based architecture, they should be subjected to the same security policy and interoperate with the standard security services and protocols. As mentioned in subsection 3.5.3, the security services offered in DMO are simple and limited. A potential mobile wireless ad hoc network capable of providing implicit authentication and encryption, which are based on preloaded symmetric group keys, is able to offer equivalent security without further research.

Security in mobile wireless ad hoc networks is a growing research field. A main objective is to develop secure lightweight mechanisms, algorithms and protocols in order to cope with the limited resources, especially the bandwidth constraints. Further, security services in ad hoc networks should be distributed and independent of pre-defined communications infrastructure. The research field may be subdivided into authentication, encryption, routing security, key management and group management.

3.6.6 Summary

We have proposed to strengthen the TETRA-based radio network by integrating mobile wireless ad hoc networks. Mobile wireless ad hoc networks will represent extra connectivity, capacity and functionality, especially when out of base station coverage. Therefore, ad hoc technology is first and foremost a realistic extension to the DMO functionality. The ad hoc technology will enhance the emergency network’s ability to operate independently of a pre-established communications infrastructure. Further, the ad hoc technology will increase the TETRA network capacity considerably. In both normal and autonomous operation, additional simultaneous users as well as larger data rates are enabled. Hence, new functionality and applications may be supported.

Ongoing research on QoS, priority, pre-emption and multicast/group management will enhance the ad hoc technology’s applicability in a TETRA-based emergency network. This research is not specific to the ad hoc technology. QoS, priority and pre-emption have to be developed in case a TETRA-over-IP infrastructure is chosen for the Norwegian Public Safety Radio Network. Future interoperation should be carefully considered such that the services can be offered throughout the network. With regard to security, the ad hoc technology could probably meet the requirements for TETRA DMO without extensive research. Further research will be necessary if the communications between any two mobile wireless ad hoc nodes is to be protected at the same level as the TETRA TMO air interface between a mobile station and its base station.

In order to make mobile wireless ad hoc networks even more applicable for emergency networks, we investigate aspects regarding connectivity, throughput, trust and security in depth in chapters 4 and 5.

4 TRUST METRIC ROUTING

4.1 Motivation

In chapter 3, we have shown that integration of mobile wireless ad hoc networks into the emergency network will lead to additional connectivity, capacity and functionality, especially when out of base station coverage. Since mobile wireless ad hoc networks operate at relatively short transmission ranges and without base stations, the node density needed to obtain connectivity to all nodes is a critical factor. Especially, in the initial phase of an operation nodes may be few and widespread. As described in section 2.5 the number of actors, their distribution and movements varies from incident to incident. Nevertheless, actors tend to cluster in geographically separated spots. Therefore, node density varies throughout the disaster area. If ad hoc networks are to be used in search and rescue operations, special mechanisms must be added to ensure adequate connectivity. A possible acceptable risk is to use third party nodes to strengthen the communications network at the emergency site. Also, there should be a possibility of immediate utilizing of legitimate nodes that are not yet authenticated. In order to improve connectivity, we propose the concept of *Trust Metric Routing* (TMR). TMR allows routing cooperation between different security domains while maintaining each domain's possibility to utilize routes that exclusively consist of domain-internal nodes. Hence, TMR provides for a possibility of utilizing foreign nodes as forwarders when desired destination nodes are not reachable otherwise. In rescue operations, this feature could be realized by utilizing the terminals of grey zone actors, which are present in the area, like mass media, spectators. Once the number of trusted nodes is sufficient, the third party nodes may no longer be included. As we will show, the needed node density is high to ensure connectivity. In addition, since the distribution of trusted nodes is dynamical and unpredictable, third party nodes may represent an advantage during the whole operations. On the other hand, as operation goes on, the network may become crowded, and congestion may be hard to avoid. A desired capability for ad hoc networks used in rescue and emergency operations should be the ability to formulate policies on whether and where to use third party nodes.

The rest of this chapter discusses the potential utilization of Trust Metric Routing in the network architecture described in section 3.6. After brief introductions to routing in general and TMR in particular possible applications of routing cooperation are presented. Routing cooperation according to TMR is simulated, and main results regarding cooperation gain are presented. Various parameters that may influence potential congestion are investigated. Main simulation results are presented, and various methods to regulate the cooperation in order to deal with congestion are discussed.

4.2 Routing in Mobile Wireless Ad Hoc Networks

In a mobile wireless ad hoc network the nodes operate as end terminals and at the same time as routers. Routing protocols running at each node, build a multi-hop network. The protocols can be optimized for different objectives. Two broad classes of protocols are reactive and proactive. The reactive protocols find a route on demand, representing a trade off between lower overhead at the potential cost of longer delay during a flow initiation. The proactive protocols exchange topology information in order to calculate and maintain routing tables in each node. Since flooding waste scarce bandwidth resources, such protocols need to address effective flooding schemes. Some proposed protocols try to utilize hierarchical routing, often with a combination of proactive and reactive. In addition, there are routing protocols based on geographical location of the different nodes. A review of proposed routing protocols can be found in [39]. So far there is no *standard* routing protocol. Different protocols are optimized for different network conditions, and current work within IETF indicates that one reactive and one proactive protocol will be standardized during the next few years. Based on experience regarding efficient flooding in ad hoc networks, current work also comprises a multicast forwarding protocol.

Proposed routing metrics are mainly based on selecting the shortest path between source and destination. Due to scarce resources in mobile wireless ad hoc networks, current research also focuses on the possibility of utilizing metrics, which reflects QoS requirements concerning bandwidth, delay and jitter. A routing policy may then regulate the route selections in order to optimize the utilization of network resources.

The choice of routing protocols for use in emergency networks has to consider some specific challenges. Since the network nodes are mainly handheld devices, the network topology directly reflects the distribution of actors. As described in section 2.5 the actor distribution as well as their movements are unpredictable, whereas speed ranges from zero to 70 m/s. The number of nodes, the node density and speed are parameters, which have major impact on the network throughput. No routing protocol is optimized for any network condition. In order to handle unpredictability and contradicting requirements, the ad hoc network should support a variety of routing protocols to ensure optimal operation for different network conditions. Interoperability with routing protocols utilized in the fixed emergency infrastructure may also be required. As mentioned in subsection 3.6.5, routing protocols in ad hoc networks are vulnerable to attacks, and it is crucial to secure the routing messages to protect the network. Most proposed routing protocols assume that all participating nodes are trusted. Nevertheless, security extensions are proposed to some of the schemes. Routing security is discussed in chapter 5.

4.2.1 The Optimized Link State Routing (OLSR) protocol

TMR operates in the setting of a proactive link state routing protocol. We have chosen the commonly used OLSR protocol as a basis for our work. The protocol is described and specified in [8]. The OLSR protocol is a proactive routing protocol proposed for mobile wireless ad hoc networks and is an optimization over classical link state protocols. The features of OLSR are representative of link state protocols. Each node selects Multipoint Relays (MPRs) from its set of one-hop neighbors such that all two-hop neighbors can be reached through at least one of them. Since only MPRs retransmit protocol messages, flooding of protocol traffic is minimized. Four message types are specified: Nodes broadcast their links to one-hop neighbors and their MPR selections through *Hello* messages. *Topology Change* (TC) messages disseminate topology information throughout the network. Only nodes, which are selected MPR by some other node, generate TC messages. The minimal set of link state information required is the set of links between the MPRs and their selectors. Routing tables are computed from the link state information exchanged through TC messages. *Multiple Interface Declaration* (MID) messages declare a list of interface addresses in case a node has more than one. *Host and Network Association* (HNA) messages declare non-OLSR interfaces. TC, MID and HNA messages are retransmitted in contrast to Hello messages. All message types utilize the same message header format. The message header stems from the message originator, whereas a packet header is attached to the message hop by hop.

4.3 The Concept of Trust Metric Routing

4.3.1 Concept overview

The concept of TMR is proposed and described in [50]. Within a *security domain* all nodes are subject to the same security policy and may share domain-internal keys and other security parameters. TMR enables routing collaboration between *different* security domains while maintaining explicit selection of forwarding policy. Cooperating security domains are integrated into a common routing domain, and may utilize each other's nodes as relays. At the same time, each domain has the possibility to calculate routes, which are composed of solely domain-internal nodes. These routes are considered trustworthy within the domain. Users may then choose between *trustworthy routes* and *ordinary routes*, which utilize foreign nodes. This choice may be based on the domain's policy with regard to security as well as to constraint-based routing. TMR operates in a proactive link state setting. The concept is shown in Figure 4.1. The figure shows two examples where the "white domain" has to depend on foreign nodes' willingness and capability of relaying information. Due to low node density, the white domain is not able to obtain full network connectivity without routing cooperation.

In order to identify the trusted nodes, the routing protocol must provide basic security services. As mentioned, we assume that confidentiality is not required for routing messages. With regard to the authentication, we assume that it is sufficient for a receiver to verify the message originators' membership of the security domain and to verify that the message is fresh and not modified in an unauthorized manner while in transit. We also assume a proper solution for key management. A simple security procedure, which aims at guaranteeing that only routes that meet defined security requirements are considered trustworthy within a security domain, is proposed in [50]. The procedure is based on basic authentication and data integrity services. The services are enhanced with replay protection in [48]. TMR requires each cooperating security domain to obtain only a valid shared key and a unique IP-address for each node. Security parameters regarding network layer is neither shared nor exchanged between security domains. The concept does not require any pre-defined parameters or pre-established infrastructure between the cooperating domains. Security aspects regarding TMR are discussed in chapter 5.

We have proposed some extensions to the protocol messages and modifications to the protocol procedures in order to enable TMR in OLSR. According to the standard protocol, each node selects MPRs from their set of one-hop neighbors such that all two-hop neighbors can be reached through at least one of them. When nodes from different security domains are integrated into one common routing domain, neighbor nodes belonging to any security domain might be selected. Foreign MPRs are needed in order to utilize foreign nodes. On the other hand, we do not want to reduce the domain-internal connectivity by excluding a domain-internal candidate node in advantage of a foreign one. Therefore, in TMR, a node selects its MPRs from the set of domain-internal neighbors, *if possible*. A foreign node is not selected unless it is the only node to provide reachability to a two-hop neighbor. Thus, a foreign node will never outperform a domain-internal node. A foreign MPR represents only *additional* MPR service compared to what would be the situation if the domain operated as one closed network. This modification enables the nodes to improve connectivity, but does not reduce their capability of computing trustworthy routes. The drawback is that this solution leads to more MPRs and consequently

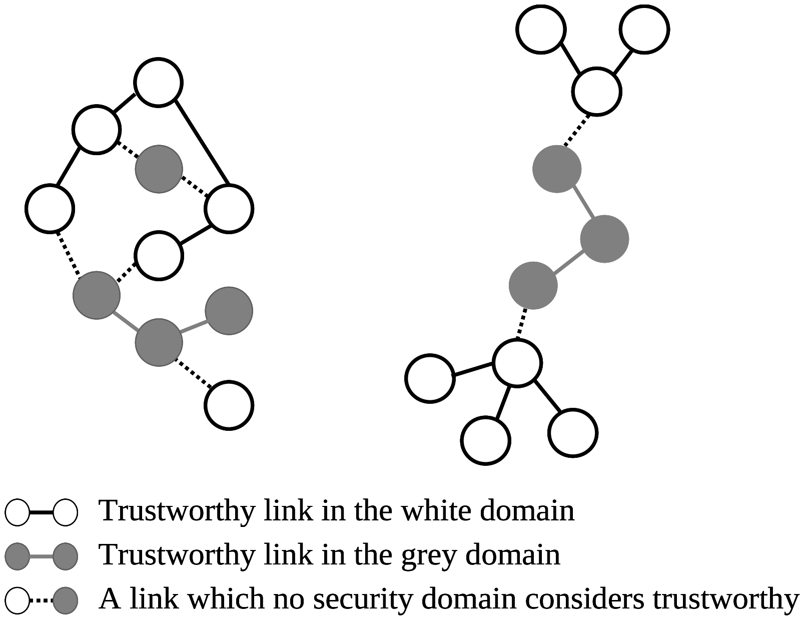
Trustworthy link in the white domain
Trustworthy link in the grey domain
A link which no security domain considers trustworthy

Figure 4.1 Networks where two different security domains cooperate in routing

increased control traffic.

Based on trust information nodes are able to calculate *two* routing tables. The first table is calculated according to the standard shortest path algorithm. Thus this table contains ordinary routes, which means routes to all nodes within reachability without regard to domain membership. The same algorithm calculates the second table, but trustworthiness is taken into consideration. The algorithm is applied exclusively to trustworthy links. Therefore, this table contains only trustworthy routes. Given both tables, the user may choose between two different routes to each destination. In case a trustworthy route is missing, the user may choose not to communicate with the desired destination node. Alternatively, a route utilizing foreign nodes may be selected. Details of the proposed extensions and modifications to the protocol are described in [50].

4.3.2 Related work

An idea related to TMR is the *Security-Aware ad hoc Routing* (SAR) [59]. SAR is a routing technique that incorporates security attributes as parameters into reactive route discovery in order to find a route with a quantifiable level of protection based on routing message properties like timeliness, authenticity, integrity and confidentiality. Network nodes may be grouped according to different trust levels. Each level shares secret keys for authentication and encryption. Whereas SAR operates within an organizational domain with a defined and obeyed trust hierarchy in order to provide flexible security choices, TMR operates within an area with *different* domains in order to enhance connectivity by integrating them into one common routing domain. SAR enables each trust level to discover suitable routes by encrypting the route request messages. Only nodes, which are able to read the control messages and to carry out the required protection level, take part in the discovery of a specific route. In contrast, the TMR technique requires each participating domain to obtain only a valid shared key for each node.

Our work is also related to ongoing research in node cooperation. Cooperation schemes detect and isolate misbehaving nodes, for example through “bad reputation” [6]. Another approach is to use credits to encourage cooperation [62]. Whereas these schemes aim to improve the behavior of single nodes, TMR enables and regulates the collaboration between different security domains that establish a common routing domain.

4.3.3 Applications of Trust Metric Routing

Our motivation is to enable utilization of foreign nodes as forwarders. In rescue operations, this feature could be realized by using the terminals of grey zone actors, which are present in the disaster area, like mass media and spectators. Even though the rescue organization as a whole may comprise several security domains at the user/application layer, we assume they establish *one common security domain* at the *network layer*. If grey zone nodes are utilized, these actors would not operate as a security domain, not even as a communications group. As individuals they may still provide the desired connectivity to the rescue organization.

The scenario, which involves grey zone actors, can be generalized into a scenario where two different security domains cooperate on an equal level and establish a common routing domain. In a rescue operation, this situation may occur when the public rescue organization cooperate with private rescue organizations like the Red Cross or in international operations. In general, TMR will be useful in operations where parties who do not fully trust each other, establish a common network. The generalized scenario is explored in section 4.4.

Efficient participation in a rescue operation should not depend on the authentication service being continuously available. TMR provides a possibility for legitimate actors who are yet not authenticated to take part in communications immediately

Communication groups within one single security domain can also use the concept. In rescue operations, the communications group is an essential entity, as described in section 2.2 and subsection 3.6.4. TMR is fully conformant to the group keys described in subsection 3.4.4, and would for example provide each group with the possibility to choose between routes that utilize all reachable nodes and routes that are restricted to nodes, which are verified members of the particular communications group. When TMR operates within a security domain, its built-in security will serve on top of the domain’s standard security services. This possibility may be useful in operations where security demands are especially high and in tactical operations. TMR can also support multiple levels of trust.

Conceptually, it is also possible to compose and classify routes according to the number of less trusted links. We do not believe this is of particular usefulness; the level of trust in a route should be the same whether it is composed of one or several links from less trustworthy partners. The risk will be the same.

A trust metric may also be used together with traditional QoS parameters in a multi metric routing scheme.

4.4 Cooperation Gain

In a rescue operation, actors are clustered in hot spots rather than spread evenly throughout the rescue area. Routing cooperation between two different security domains will be beneficial when node density is low. Therefore, we expect that routing cooperation will give the best benefit during the initial phase of the operations. The routing cooperation gradually becomes less advantageous as higher node density leads to congestion. This section identifies a node density range where routing cooperation between equal domains is beneficial. If cooperation is not wanted due to a change in trust between the parties or due to congestion, there should be a means of splitting the common routing domain. Relevant mechanisms will be discussed in section 4.6.

4.4.1 Related work

The optimum number of neighbors in a random stationary, slotted ALOHA network is studied in [24] and found to be approximately six. The throughput drops rapidly at lower number of neighbors, but is not so sensitive to an increase. The authors assume the network to be connected at an average degree of five. The result is reconsidered in [41], and optimal transmission is found to occur when the number of neighbors is nearly eight. In [55] the result is extended to that optimal asymptotic connectivity results when every node is connected to its nearest 5.1774 log n neighbors. Networks with mobile nodes are investigated and simulated in [38]. As the average speed increases, the optimum is found to shift to higher numbers of neighbors. Beyond the mobility/speed-dependent optimum, the throughput drops. The investigation concludes that a *global* optimum for varying node mobility does not exist.

4.4.2 Simulations results

Our results are specific to the modified OLSR protocol. We have identified a node density range where routing cooperation may be preferable. The cooperation gain is measured using the two parameters *connectivity* and *packet loss*. A network node's average number of routes and the average route length indicates the network connectivity. A high node density is needed to have connectivity to all nodes. The optimum level of cooperation occurs when the connectivity passes 95%, which means that a node in average has a route to 95% of the destinations. There is, however, a large node density range where routing cooperation may lead to a significant gain with regard to packet loss. Within this range the gain from increased connectivity is larger than the loss from increased congestion. Beyond the range the loss from increased congestion is larger than the gain from increased connectivity.

Figure 4.2 shows the upper and lower bounds on cooperation gain. A uniform traffic matrix is utilized, and packet loss is shown as the number of user packets correctly received in percent of the number of user packets sent. The left figure shows a set of reference values from a non-cooperation scenario. The network size varies from 8 to 24 nodes. The x-axis shows the corresponding average expected number of neighbors. Packets are lost mainly due to missing routes, and the figure shows that the loss decreases as node density and connectivity increases. The results from a cooperation scenario are shown to the right. Two identical domains establish a common routing domain, and the network size as well as the number of neighbors is doubled compared to the non-cooperation scenario. The lower bound on cooperation gain is obtained when both domain select only trustworthy routes for all packets. The results are roughly the same as in the non-cooperation scenario. Trustworthy routes are, however, utilized for *security* reasons, and we did not expect cooperation gain if only trustworthy routes were to be utilized. Since the results correspond roughly to the results from the non-cooperation scenario, the expected effect from extra MPR control traffic in the cooperation scenario seems to be minor. On the other hand, the extra MPRs represent added connectivity and may reduce bottlenecks and potential loss caused by congestion. The upper bound on cooperation gain is obtained when both domains select only ordinary routes that utilize all available nodes. The figure shows that routing cooperation according to TMR may lead to a significant gain. In our simulations, the optimum number of neighbors is 14. This value corresponds to the value at which 95% of the nodes are reachable, but the particular number is probably dependent of node mobility/speed. Beyond optimum packet loss grows due to general congestion. Nevertheless, routing cooperation is preferable until the expected number of neighbors reaches approximately 20.

Even though user traffic may be authenticated and encrypted, the utilization of foreign nodes as relays introduces vulnerability, which may not be tolerable to traffic with high security demands. Therefore, security policy may *demand* trustworthy routes for certain types of traffic. In order to benefit optimally from the increased connectivity, we propose to subject *additional* domain-internal traffic to a *best-effort trust routing* policy, which implies that trustworthy routes are selected *if available*. If a trustworthy route is missing, an ordinary one is selected. This solution combines the security demands for trustworthy routes with the cooperation gain obtainable from the utilization of foreign nodes. We have studied a case where 20% of the offered traffic is *bound* to trustworthy routes, while the additional traffic is routed according to the best-effort trust routing scheme. As expected the packet loss increases due to the restrictions on route selection. The gain is, however, still considerable compared to the non-cooperation scenario.

More results and simulation details are found in [51].

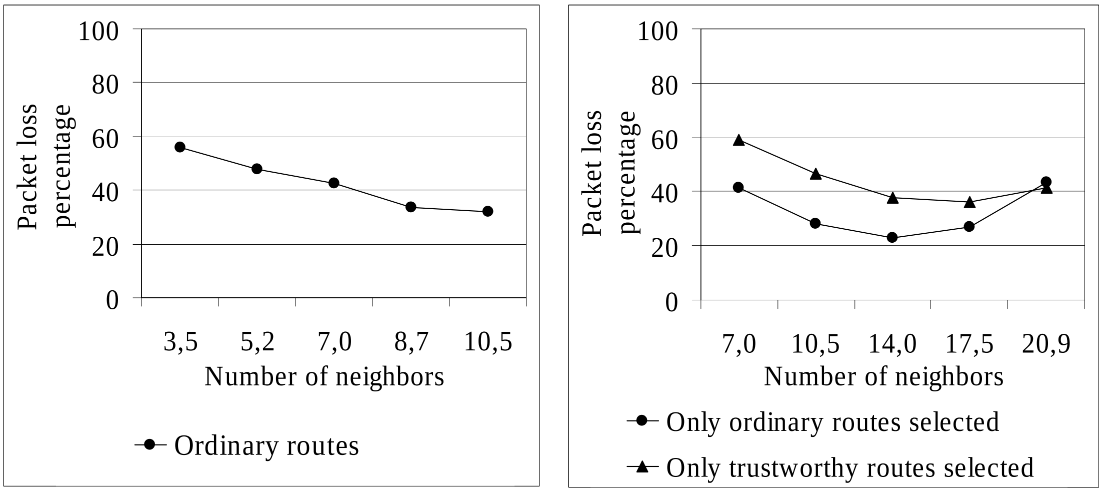

Figure 4.2 Packet loss in non-cooperation and cooperation scenarios

4.5 Adaptation to an Expanding Number of Network Nodes

So far we have shown that up to a certain limit network connectivity as well as network goodput (received packets/sent packets) will be improved by integrating nodes from different domains into one common routing domain. As described in chapter 2, the extent of a disaster is not known in advance, and the network must be able to adapt to an expanding number of network nodes and to an escalating traffic load. The unpredictable conditions under which a rescue operation takes place, calls for mechanisms, which enable such adaptations. Since node density may vary throughout the disaster area, the mechanisms should be distributed in order to enable local adaptation. In general, throughput suffers from low connectivity in networks where the node density is low, whereas high node density often means interference and congestion implying poor performance. In order to adapt to varying node density, routing cooperation has to be regulated. Efficient usage of ad hoc networks in search and rescue operations may depend on a combination of controlling load, number of nodes and transmission radius. We therefore investigate the potential of regulating the number of neighbor nodes when a network grows and the relationship between transmission radius, node density and packet loss for different traffic patterns. Previously, these factors have been analyzed independently and under not realistic traffic and routing conditions.

4.5.1 Related work

The results from [24], [41], [55] and [38], which were referred in subsection 4.4.1, assume that the network is saturated. In [60] it is found that *at lower offered load* there does not exist a transmit range that optimizes network throughput. Their simulations results show that in stationary as well as in networks with mobile nodes, the fraction of packets, which is correctly received, improves as the transmission radius increases.

Several routing protocols are compared in [5]. The delivery rate is investigated with regard to mobility and speed. Even though the number of sources varies, the offered traffic load is kept at a low level.

In all simulation scenarios referred above, the number of sources is less than the number of network nodes, which is fixed.

4.5.2 Simulations results

A comprehensive simulation-based analysis for the OLSR protocol and several traffic conditions is given in [52]. We assume a uniform traffic matrix and investigate how the fraction of correctly received packets is influenced when the number of neighbors is varied by altering the node density as well as when the number of neighbors is varied by adjusting the transmission radius. Under both sets of conditions we distinguish the impact of varying number of neighbors from the impact of varying traffic loads. We also study the packet loss and distinguish between packet loss caused by low connectivity and packet loss caused by general congestion. Our results are specific to the setting of the OLSR protocol and of RTS/CTS at the MAC layer.

Figure 4.3 shows our main results. Goodput is shown as the number of correctly received packets divided by the number of sent packets. In Figure 4.3A), the node density is a function of increasing number of nodes. The transmission radius is fixed at 250 m. The x-axis shows the number of network nodes. In Figure 4.3B), the node density is a function of increasing transmission radius. The number of network nodes is fixed at 40 nodes. The x-axis shows the transmission radius. In both figures, the corresponding expected average number of neighbors is shown in brackets at the x-axis. Reference [52] shows that in both cases the results confirm that 95% connectivity is obtained when the expected average number of neighbors reaches about 14, which corresponds to 32 network nodes in Figure 4.3A) and to a transmission radius between 200 and 250 m in Figure 4.3B).

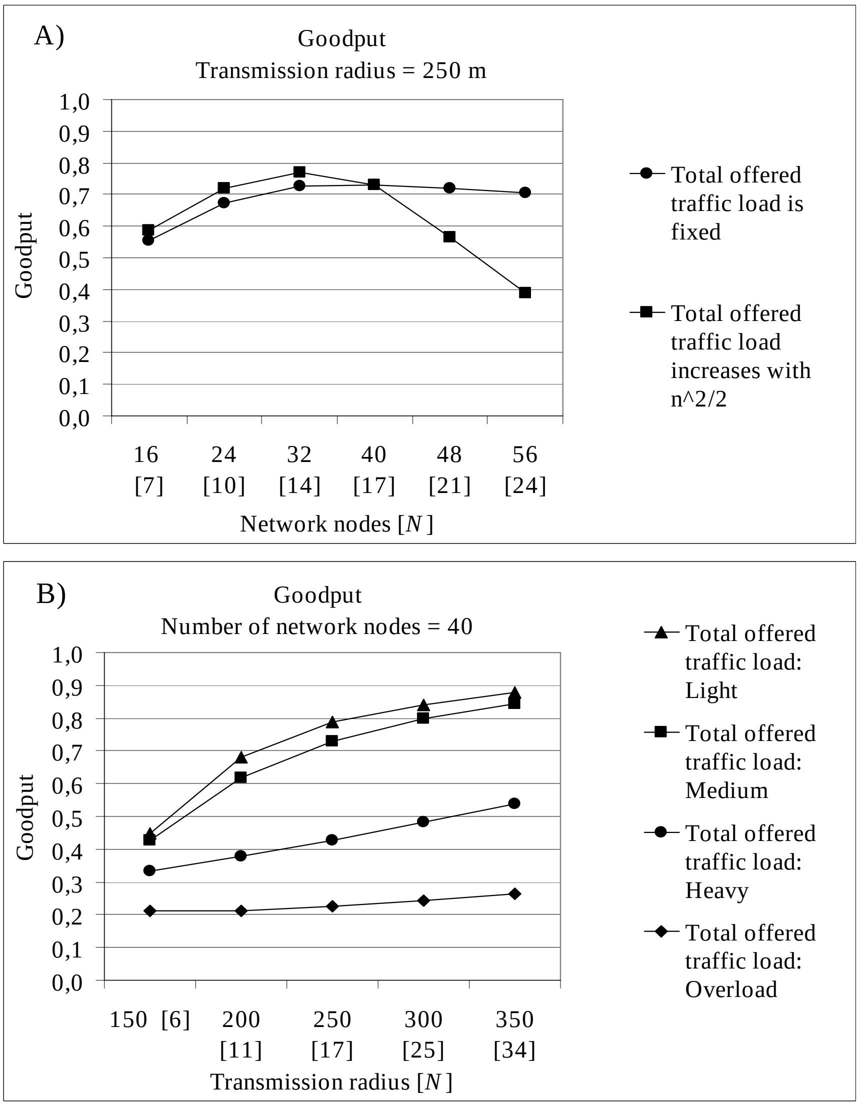

Figure 4.3 Goodput under different network conditions

Figure 4.3A) shows that when the increased number of neighbors is a result of increased number of network nodes, and as long as the network degree ensures a connectivity of about 95%, the goodput is barely influenced by the number of neighbor nodes at fixed traffic load. In contrast, when the offered traffic reflects the expanding number of network nodes, the goodput drops rapidly. In this case, the traffic load is similar to the one utilized in the TMR simulations results shown in Figure 4.2. The network copes well with an exponential traffic growth as long as the number of network nodes is kept moderate. The rapid goodput fall beyond the optimum is a result of heavy load, not a result of a larger number of competing neighbor nodes per se. The amount of offered traffic is a more important factor regarding goodput than the number of neighbor nodes.

Figure 4.3B) shows that as long as the network is not saturated, the fraction of correctly received packets improves when the increased number of neighbors is a result of a larger transmission radius. Beyond the point of 95% connectivity goodput *continues to increase* in spite of the increased number of neighbors. In the setting of RTS/CTS, the effect from reduced number of hops between source and destination seems to outperform the effect of increased number of competing nodes on a channel. This behavior is observed for different offered traffic loads. The improved fraction is most obvious for light traffic loads, but is also significant at heavy ones. The improvement evens out at overload. This result confirms previous results from the setting of a reactive protocol [60]. At a radius of 250 m the goodput ranges from 0.8 in the light loaded network to 0.25 in the overloaded one. This result confirms the trend from Figure 4.3A) regarding the impact of traffic load

More results and simulation details are found in [52].

4.6 Possible Regulation Mechanisms

As mentioned in section 4.4, there has to be means of splitting the common routing domain as well as means of regulating the cooperation in order to deal with congestion. If further cooperation is not wanted due to a change in trust between the parties or due to other security considerations, the cooperation has to be suspended immediately. In contrast, if further cooperation is wanted, there is a range of possible mechanisms, which could be utilized in order to adapt to an expanding number of nodes and to various node densities throughout the area. The results presented in section 4.5 indicate that mechanisms which regulate the traffic load may provide the most efficient way of adapting to an expanding number of network nodes and to escalating traffic load. In search and rescue operation, where traffic load is supposed to be proportional to the number of network nodes, such mechanisms will be crucial.

An expanding number of network nodes and escalating traffic load leads to congestion in any wireless network. Congestion may occur in any network, and has to be resolved. The small number of time slots and the low data rates available in networks based on TETRA 1 makes these networks susceptible to congestion. Hence, most of the techniques discussed in this section are relevant regardless of the utilization of mobile wireless ad hoc networks and regardless of the utilization of TMR. The techniques require further research in order to evaluate and compare their potential within the setting of TMR. Therefore, this section is also a listing of further work on the concept of TMR.

4.6.1 Splitting the network

We assume that there is a centralized decision to suspend the cooperation due to security considerations. A possible algorithm for removing from TMR cooperation is then to distribute a split message. When receiving a split message, the nodes immediately select only trustworthy routes for all domain-internal packets. Foreign routing messages as well as foreign user messages are dropped. The trustworthy routing table becomes the only one available. Eventually, all domain-internal packets in transit are taken care of by domain-internal nodes. In some cases, this may be sufficient. In other cases, the procedure must escalate and nodes may have to change to another and pre-defined frequency in order to avoid interference from the previous cooperating domain.

Drawbacks to this solution are that nodes, which are sporadically out of network range or nodes, whose reachability were dependent of foreign nodes, may miss the split message. Further, frequency change cannot be strictly synchronized in a mobile wireless ad hoc network, and a time overlap has to be allowed. Therefore, as long as a domain is involved in TMR cooperation, nodes have to listen to two frequencies.

Changing frequency is also a possible mechanism in order to deal with congestion. The algorithm outlined above may be utilized. Both connectivity and congestion, however, may vary throughout the area. One part of the network may suffer from high node density and congestion, whereas other parts may suffer from node scarcity and weak connectivity. A frequency change may solve the congestion problem, but at the same time leave the domain-internal nodes in several network partitions. A distributed decision algorithm might enable an overall wise decision. Distributed decision algorithms tend to be complex, and work has to be done to develop lightweight algorithms. Also, further research has to be done with regard to providing relevant decision parameters to the algorithms.

4.6.2 Separate gateways

Especially if routing cooperation is realized by utilizing the terminals of grey zone actors like mass media, the utilization of gateways will be a usable mechanism to regulate the traffic load. In this case, the foreign nodes do not establish a separate security domain but cooperate as individual nodes. It is reason to assume that they mainly communicate with actors outside the catastrophe area. Hence, their contribution to the total traffic load will be minor if access to external networks is not available. When access is available and foreign traffic load increases, this traffic could then be routed to separate gateways to public commercial infrastructure. Such gateways are in conformance with the architecture shown in Figure 3.3. Separate gateways could also be utilized in order to route local foreign traffic via external networks, and thus reduce load in the ad hoc network.

4.6.3 Adaptive transmission radius

In general, throughput suffers from low connectivity in networks where the node density is low, whereas high node density often means interference and congestion implying poor performance. An intuitive solution is then to control the number of neighbor nodes by regulating the transmission radius: In areas where node density is low, a larger transmission radius may strengthen the connectivity, while a smaller radius will reduce the number of competing nodes in crowded areas. The results from section 4.5 show that a reduction of the transmission radius will not lead to improved delivery rate. In contrast, *increasing* the radius in order to obtain fewer hops between source and destination would be better. This is a tradeoff between goodput and energy usage.

Our results confirm a previous result published in [60], which first and foremost investigates the optimum transmission radius with regard to energy consumption. It is found that at normal offered load there does not exist a transmit range that optimizes network throughput. Nevertheless, an optimum range exists such that energy efficiency is maximized. The optimal range is invariant to node mobility, and is much larger than the critical transmission range.

Our results also confirm results reported in [4] regarding the impact of the number of hops from source to destination. Their results show that when the power is sufficient to decrease the number of hops, the goodput increase slightly whereas the average delivery time decreases rapidly. Two schemes for power control are proposed. The power-aware routing schemes achieve the same performance as the classic algorithms while reducing the energy consumption. If performance degradation with regard to packet loss and delay is tolerated, considerable power gain is obtained.

Reference [11] reports that goodput decreases with increasing transmission radius. Whereas the effect from a reduced number of hops outperforms the effect of an increased number of neighbors in simulations mentioned above, these results show that the effect from the larger number of competing nodes dominates. A reason may be that the slotted aloha MAC layer are more prone to collisions than the MAC layers utilized in the other simulations. Also, the actual reduction of hops is not reported. As a consequence, and in contrast to the results mentioned above, optimum numbers of neighbors are reported. Two protocols that enable each node to dynamically adapt the connectivity range in order to achieve a near-optimal operating point are proposed. It is shown that the protocols reduce the packet loss caused by collisions.

In the schemes proposed in [11], all nodes utilize the same transmission range. Reference [35] suggests schemes in which each node adjusts the transmit power in response to topological changes. Based on locally available neighbor information, nodes lower their transmit power as the node density increases. Simulation results show that beyond the point of connectivity, throughput decreases as node density increases. Hence, the results reported in [11] are confirmed. Further, it is shown that topology control mechanisms reduce the packet loss and slightly improve the packet delay. Also in this work the actual reduction of the number of hops is not reported. It is also unclear how node density is varied.

As we can see, reported simulation results seem to differ with regard to the potential of reducing the number of neighbors by adjusting the transmission radius. Success with regard to improved goodput and delay seems to depend on whether the decreased power leads to an increased average number of hops from source to destination. The MAC layer’s ability to minimize collisions also seems to be an important factor. Nevertheless, the potential of reducing power consumption by power control mechanisms seem to be large, and should be an important mechanism to support the over all adaptation to an expanding number of nodes.

4.6.4 Connectivity-aware data rate adaptation

A connectivity-aware rate adaptation algorithm for multi-rate networks is proposed in [26]. The algorithm exploits the relation between transmission radius and data rate. A node compares its number of neighbors to a pre-supposed optimum number of neighbors and chooses its data rate accordingly. Simulation results obtained in a stationary network shows that choosing the optimum data rate has a significant impact on packet loss. To analyze the impact of data rate in a mobile environment, data rate could be included as a variable in the simulation scenario presented in section 4.5.

4.6.5 Control of queue utilization

Each node should operate near its maximum capacity. The optimum operating point is usually found well below saturation where queue utilization equals one. Reference [27] analyzes the optimum operating point under limited load in stationary one-hop IEEE 802.11-based networks. Traffic load is assumed to increase linearly with the number of nodes. It is found that the point of maximum throughput is at the saturation point only when the number of nodes is less than 10. At larger numbers of nodes it is shown that the saturation throughput degrades slower than the maximum throughput. The maximum throughput shifts to lower queue utilization with an increasing number of nodes and approaches an asymptotic value at large numbers. Queue utilization is sensitive to the packet arrival rate. In order to locate an optimum operating point, queue delay therefore has to be considered carefully. Significant benefits can be obtained through distributed control of queue utilization at each node. To our knowledge the effect of estimating the optimum operating point by controlling the queue utilization is not studied for mobile multi-hop networks. The technique may be a useful mechanism in the regulation of traffic load.

4.6.6 Quality of Service

As discussed in section 3.6, QoS is a desired and necessary capability in mobile wireless ad hoc networks. QoS implies that different types of traffic are handled according to their specific requirements and tolerance regarding timeliness and packet loss. In an emergency network, priority and pre-emption functionality is especially important. Providing QoS beyond the best-effort scheme is a challenge even in a fixed network where resource availability is more predictable. In mobile wireless ad hoc networks, resource availability is constantly changing, and hard QoS guarantees are not realistic. In contrast, soft guarantees allow the network to fall short of QoS requirements for certain time periods and up to permitted thresholds.

As mentioned in subsection 3.6.3 research is going on to establish comprehensive QoS solutions for mobile wireless ad hoc networks. Several models are proposed. INSIGNIA is a lightweight QoS model with per-flow granularity [25]. The model is especially suited for interoperation with IntServ in a cooperating fixed network. Bandwidth is the only QoS parameter. Two levels of service are offered in addition to the regular best-effort. The scalable, distributed and robust *Stateless Wireless Ad hoc Networks* (SWAN) scheme maintains a stateless model with no need to process complex signaling or to keep per-flow information [2], [21]. The model handles traffic on a per-class basis. Each node is able to treat traffic as real-time or as best-effort traffic. A rate control system is utilized. The system restricts best-effort traffic in order to provide the bandwidth required to support real-time traffic. The total rate should be below a certain threshold rate. A problem of SWAN is how to calculate the threshold rate. Both SWAN and INSIGNIA lack mechanisms for policy-driven QoS. *Flexible QoS Model for Mobile Ad-Hoc Networks* (FQMM) follows a hybrid approach by combining the per-flow granularity of

IntServ with the per-class granularity of DiffServ [54]. Hence, FQMM is able to classify the traffic into either granularity. When utilized in large networks, scalability is a problem of FQMM.

So far, the shortest path has been the implicit route selection criterion. QoS extensions are proposed to existing routing protocols, like the AODV, the OLSR and the *Destination Sequenced Distance Vector Routing* (DSDV) protocols [21]. The extensions enable other metrics, like minimum bandwidth or maximum delay. Also specific QoS routing protocols are proposed. Examples are the *Ad Hoc QoS On demand Routing* (AQOR) protocol, which provides signaling capabilities for resource reservation [56] and the *Core-Extracting Distributed Ad hoc Routing* (CEDAR) protocol, which selects routes that are highly likely to provide the requested bandwidth [21]. Multiple path routing is also a possible mechanism to satisfy required bandwidth and/or to provide back up paths. The capability of QoS makes traffic as a whole more robust to congestion. Hence, QoS is also a means of adapting to an expanding number of network nodes and increased traffic load. Improvement of QoS is a multi-layer problem, and research is going on at all communication layers.

4.6.7 Service level agreements

Service Level Agreement (SLA) and *Service Level Specification* (SLS) are elements from the QoS architecture in fixed networks. Reference [40] proposes to utilize SLA/SLS in QoS-enabled tactical networks. Possible and scalable implementations in an inter-domain setting are described. Further, call admission control is recommended. Likewise, in the setting of Trust Metric Routing SLAs and SLSs could be useful mechanisms to limit and control the traffic load. A SLA might regulate for example the amount of foreign traffic that should be forwarded by each domain. SLSs then detail the service levels provided, and should be negotiated dynamically according to network conditions. Solutions for the management of the SLSs will depend on the underlying QoS solution.

4.6.8 Adaptive service levels

Another possible way of adapting to increased traffic loads is to specify and pre-define minimum quality levels for transmission for different types of traffic, for example data rates. Likewise, algorithms that reduce the resource consumption to the minimum level should be specified for each type of traffic. Examples are “lossy” compression algorithms. In case of congestion, nodes may then automatically customize traffic to the available network resources. With pre-defined minimum requirements, information is sent only when potential quality degradation is meaningful. If the minimum service level cannot be offered, scarce resources are not spent on meaningless traffic. As soon as congestion is resolved, previous transmission quality is reestablished. In order to realize mechanisms that enable a controlled degradation of service level according to a pre-defined minimum for different types of traffic, further research has to be done. Means of distributing state information as well as guidelines and methods for analyzing such information have to be developed.

4.7 Summary

We have presented the concept of Trust Metric Routing and discussed the potential utilization within the context of the network architecture described in section 3.6. By integrating all available nodes into one common routing domain, TMR allows different security domains to utilize each other's nodes as forwarding nodes while maintaining each domain's possibility to select routes that exclusively consist of domain-internal nodes. Our simulation results show that TMR increases the connectivity and leads to a significant throughput improvement within a large node density range. Routing cooperation may be especially helpful in the initial phase of the rescue operations. Upper and lower bounds on cooperation gain are presented for a scenario where to identical security domains establish a common routing domain. The results also show that the utilization of mobile wireless ad hoc technology in the planned emergency network, will lead to a considerable improvement regarding the number of simultaneous users within the disaster area. On the other hand, routing cooperation implies an increased number of network nodes, which may result in congestion. Congestion is not specifically related to TMR, but has to be resolved in any network regardless of routing cooperation. Several mechanisms may be utilized to deal with escalating traffic load from an increasing number of network nodes. Our simulation results show that in order to maintain the goodput when network resources get scarce, transmission radius may be increased in order to reduce the average number of hops from source to destination. Mechanisms, which control the traffic load, however, would be the most efficient means of adaptation to an increasing number of nodes. A variety of possible mechanisms are presented. To analyze their applicability in the setting of Trust Metric Routing is left for further work.

5 SECURITY IN TRUST METRIC ROUTING

Routing cooperation should not be at the expense of security. Our work on security is based on two assumptions: First, participating security domains perform the standard routing protocol. All cooperating nodes are supposed to read and process any routing message. Therefore, network information has to be exchanged unencrypted throughout the network. Hence, a domain has the capability of computing routes to all nodes according to the protocol's standard metric, for example shortest path. Second, each participating domain is able to perform some essential security services. The scope of the services is the security domain itself. Thus, no security parameters are exchanged between security domains. TMR enables each domain to identify and protect the network information, which originates from nodes belonging to this domain. Further, each domain is able to compute routes solely based on this protected information. Based on the protected information, each domain is able to calculate routes, composed solely of nodes belonging to this domain. Such routes are referred as *trustworthy* within the particular domain. This chapter discusses the security services needed to build and maintain a trustworthy topology and to distinguish between trustworthy and untrustworthy routes in the context of TMR. The scheme is evaluated with regard to resource consumption and compared to other security schemes proposed for the OLSR protocol.

5.1 Related Work

General vulnerabilities, threats and security goals in ad hoc networks are reviewed in [7], [61] and [57]. Attacks on general routing information are described in [22]. Vulnerabilities in proactive routing are discussed, and countermeasures to a series of possible attacks are proposed in [18], [1], and [34]. Replay attacks are described and discussed in [3] and [31].

Security extensions to the OLSR protocol are proposed in [1] and [16]. The extensions comprise services for authentication, data integrity and replay protection. Security introduces extra overhead to the routing protocols. Overhead caused by the standard OLSR protocol is analyzed in [9] and [47].

The TMR technique requires each participating security domain to obtain a valid shared key for each node. This may be done in advance or dynamically in field. Some interesting approaches to dynamic key distribution are presented in [23] and [61], whereas a survey of relevant key management techniques is found in [17].

5.2 Authentication and Data Integrity

Nodes, which belong to the same security domain, must be able to authenticate each other, to verify data originators within the domain and to integrity-check exchanged information in order to calculate trustworthy routes. A trustworthy route is composed of trustworthy links. A link is regarded trustworthy when successful mutual authentication of the end points and an integrity check of the message content are performed. The link is then marked. When link information is disseminated throughout the network, message originators have to be authenticated and the messages have to be integrity-checked before the mark is adopted by the receivers and cleared for the calculation of the trustworthy routing table. Consequently, a trustworthy route is composed of nodes, which belong to the same security domain. Link information used in the calculation of a trustworthy route is integrity-checked and stems from nodes, which belong to the same security domain. To establish trustworthy routes, we identify two core security services:

First, we need a *data integrity service*. Unauthorized nodes shall not be able to manipulate network information without being detected, and the service shall be able to detect unauthorized or accidental changes done to routing messages. One-way hash functions may be used to realize the data integrity service. We assume that no messages are identical. Hence, the hash function produces an output, which is unique to the message.

Second, we need an a*uthentication service*. Unauthorized nodes shall not be able to inject false network information into the network without being detected, and the service shall be able to detect any routing message from unauthorized nodes, also if the unauthorized node poses as an authorized one. According to the definition of trustworthy links and routes, the authentication procedure must comprise the corroboration of a node's membership in a particular security domain. Identity and membership may be proved and verified *implicitly* through the *possession* of a shared secret value. The verification of such a possession then implies that the node belongs to a particular security domain, and that there is an authorized binding between the node and its identifier. The possession of the secret value may further imply that its IP-address is valid and assigned in an authorized manner. These implications are a matter of trust and agreement within the security domain. Nevertheless, we assume that these rules are easy to obey when there is a general and formal trust between the organizations, whose members establish a security domain, for example different rescue organizations. Hence, all nodes belonging to a security domain may share the same key. Further details about the services and the proposed security procedure are found in [50].

Authentication and data integrity services based on symmetric group keys are simple and fast compared to solutions based on asymmetric keys [15]. They are, however, more vulnerable if keys are lost or stolen. A standard TETRA group key could be utilized as the shared secret key in TMR. Even though key management in mobile wireless ad hoc networks should be dynamic and distributed, the TETRA key management features could be utilized by TMR. Then TMR would meet the security level required for the protection of the TETRA DMO, as discussed in subsection 3.6.5.

5.3 Replay Protection

Authentication and data integrity services aim to detect insertion of false messages and unauthorized modification of data in transfer. A possible way of tricking an authentication service is to replay recorded messages, which are already signed by a legitimate message originator. In order to detect such attacks, specific replay protection is needed in addition to authentication and integrity services. Mechanisms, which may enable a verification of the freshness of incoming messages, are often based on *timestamps* or *sequence numbers.* The received information is processed only if the timestamp/sequence number is within a specified interval. Reference [1] and [16] propose replay protection schemes based on clocks and external timestamp exchange protocols. In [48] we propose an alternative scheme based on extension of the existing message sequence number and on existing standard OLSR procedures.

Even without particular countermeasures, the OLSR protocol is rather robust to replay attacks, which intention is to manipulate the routing information. An attacker has to avoid that the replayed information is cancelled out by fresh messages from the message originator. Hence, in case of a Hello message, replay receivers have to be situated outside the range of the message originator, and in general the attack has to be targeted against at least one node, which corresponds to a link advertised in the replayed message. In case of other OLSR messages, the replay receivers have to be situated in another partition than the message originator. This attack, however, is harmless with regard to routing information.

We have shown that a scheme based on a simple message sequence number check may be sufficient, even though nodes are mobile and join and leave the network dynamically. We have identified a couple of scenarios where the scheme may fail. The shortcomings will be eliminated if nodes attach a receipt to each asymmetric link they announce in Hello messages. The receipt is the most recent Hello message sequence number received from the corresponding node.

Our replay protection scheme scales considerably better than the one presented in [1], which is based on global dissemination of local time information and requires large messages to be emitted at short intervals in order to support dynamic join and leave.

Further details are found in [48].

5.4 Performance Evaluation

As mentioned in section 5.1, two protection schemes are proposed for the OLSR protocol in addition to our proposals. All three schemes recommend a *signature* to provide authentication and data integrity. The schemes also include replay protection. Even though the schemes provide similar services, the designs differ. Hence, their impact on bandwidth consumption and delay diverge significantly. Due to the limited bandwidth, power and processing capacity in mobile wireless ad hoc networks, resource consumption should be an important aspect in security schemes. The proposed security schemes add extra overhead by increasing the average message size, introducing new message types and by including new procedures to the standard algorithms. In [49] we have analyzed the added bandwidth consumption and delay caused by these schemes. The schemes are specific for the OLSR protocol, but the mechanisms evaluated and compared, are relevant to the performance of link state routing in general.

Reference [1] proposes that each routing message should be signed by a separate corresponding signature message. Our analysis shows that the broadcast of two small messages has significantly higher bandwidth cost than the broadcast of a single one that is extended with a signature. Further, when the routing message and its corresponding signature message are sent independently, the receiver has to wait for a corresponding message. It is shown that the waiting time at least doubles the per-hop delay for TC messages.

In order to reduce bandwidth consumption, reference [16] proposes that forwarding nodes should aggregate routing messages into one packet, generate a signature message comprising the whole packet and send the signature message within this packet. This message aggregation technique is evaluated. In small networks, the probability of aggregating more than one TC message within a reasonable time period is small. In larger networks, the technique may reduce the bandwidth consumption. The analysis, however, shows that appropriate aggregation delays magnify the per-hop delay to an unacceptable level.

Two different timestamp exchange protocols proposed for replay protection have been evaluated. A protocol based on periodical and global distribution of local time information [1] scales poorly. In contrast, a protocol where neighbor nodes exchange local time information when needed [16], seems to perform well. This particular protocol, however, is bound to hop-by-hop authentication, which requires mutual trust between all network nodes. Message sequence numbers are also proposed as a basis for replay protection. Even though the particular message sequence number scheme evaluated extends the Hello messages noticeably, the scheme scales better than the alternative timestamp-based schemes. Results with regard to delay are shown in Figure 5.1A). We have calculated the fraction of a second the channel is occupied by the OLSR traffic. The timestamp exchange protocol proposed in [1] does not scale well, and make this scheme unfavorable. Also when the timestamp exchange protocol is not considered, the scheme scales poorer than the alternatives due to the doubled number of messages introduced by broadcasting separate signature messages. The message aggregation proposed in [16] scales well. An aggregation time of 0.5 seconds are utilized. Our scheme proposed in [50] and [48], produces a tolerable delay compared to the standard OLSR scheme.

The results presented in Figure 5.1A) represent a channel which is idle whenever a packet is to be sent, and can be regarded as the lower bound on the per-second delay caused by the transmission of OLSR messages. In Figure 5.1B) we calculate the average per-hop delay for a signed TC message when the probability of idle channel is 0.5. The delay caused by the message aggregation makes this technique infeasible. Simulation results indicate that a TC message in average is broadcast between two and three times [51]. Hence, the delay shown in Figure 5.1B) will be more than doubled, and may have severe impact on the nodes ability to maintain routing tables, which should reflect current network topology. Also the scheme proposed in [1] adds considerable delay. Our scheme adds about 12% to the standard OLSR delay. The figure also shows that given a fixed probability of idle channel, the network size does not influence the per-

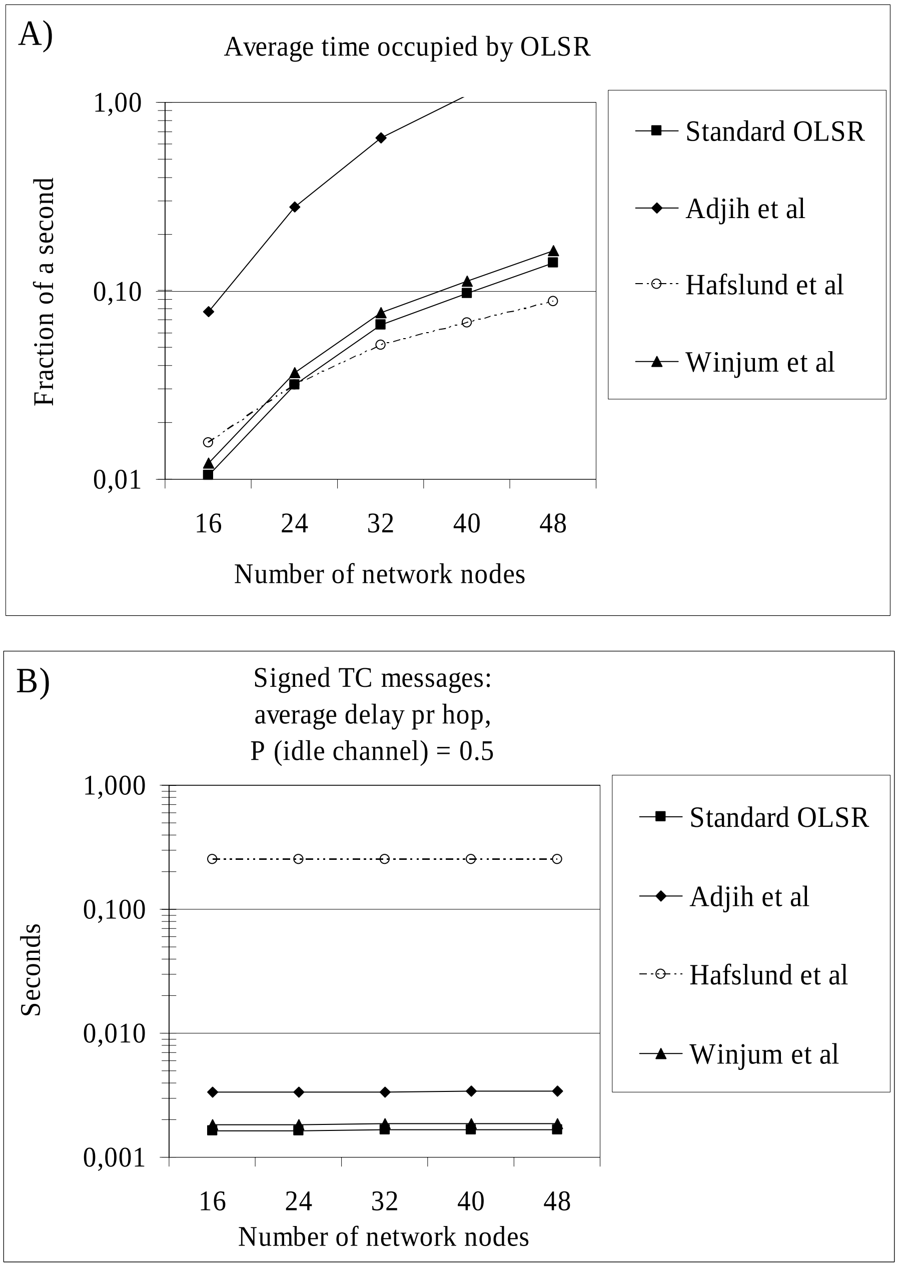

Figure 5.1 Delay

hop delay. The TC message size scales very well since the relative number of MPR selectors decreases with increasing network size

Of the schemes evaluated, our scheme, which is characterized by directly signed routing messages and message sequence numbers as the basic mechanism for replay protection, has better all over performance than the alternatives. More results and details regarding the analysis are found in [49].

5.5 Summary

We have discussed and proposed security services needed to build and maintain a trustworthy topology according to the concept of Trust Metric Routing. For authentication and data integrity services, we propose simple, fast and well-established mechanisms based on symmetric keys. For replay protection we have developed and proposed a new scheme based on sequence numbers. With consideration to performance, our security scheme is compared to two other proposals that provide security at an equal level. Our scheme seems to have better all over performance than the alternatives.

The scope of our security proposals is the routing protocol, which is not present in the TETRA radio network. Without further work, our protection scheme for the routing protocol and TMR offers security at the same level as the protection of the TETRA DMO. Even though out of scope, it should also be mentioned that protection at TETRA DMO level, which means authentication and encryption based on pre-defined shared symmetric keys, is easy to provide to user traffic within a mobile wireless ad hoc network.

6 POSSIBLE ALTERNATIVES TO TRUST METRIC ROUTING

The motivation for developing the concept of Trust Metric Routing is to improve connectivity in mobile wireless ad hoc networks when utilized in rescue operations. There are, however, a couple of alternative solutions. In this chapter we mention some alternatives in the setting of the reference architecture described in section 3.6.

6.1 Relay Nodes

Relay nodes may be deployed in areas with low node density. The relays may be regular network nodes, but their only function is to forward traffic. They may either be part of the routing scheme, or they may forward traffic “blindly” by broadcasting all received packets. Compared to routing cooperation according to TMR, the relay solution has the following main advantages: As the number of network nodes increases, the necessary number of relays will decrease. Besides, the relays will not offer added user traffic. Therefore, from the rescue organization’s point of view, less important foreign traffic will not waste scarce network resources. Disadvantages are: If relays are deployed in order to connect different clusters together in a static manner, as proposed in [53], they will easily become bottle necks. If not looked after, they may be stolen or replaced by intruders and thus represent a security risk. The solution is static, and the relay nodes may have to be moved around to serve different areas as operation goes on. Hence, the management of relays may waste human resources.

6.2 Gateway Nodes

If located within the range of a gateway node that provides access to an external network, ad hoc nodes may communicate via the external network. This solution is dependent on fixed infrastructure being available at several points within the disaster area, and is not an alternative if autonomous operation is needed.

7 CONCLUSIONS

Rescue operations cannot be pre-planned in detail, but have to be managed by a combination of general guidelines, pre-planned procedures and improvisations. Actors operate in overlapping teams, which may be organized across organizational boundaries, and may be combined and divided during the operations. Trust is based on authenticated relationships with a rescue organization and with operational and professional roles. The number of actors, their distribution and movements vary from incident to incident. The emergency communication networks should handle the variety, dynamics and unpredictability that describe the rescue operation scenario. Efficient and secure communications are crucial, within the disaster area as well as between the disaster area and the outside.

Based on TETRA-like technology the planned Norwegian Public Safety Radio Network will represent a nationwide emergency network that satisfies mission critical operational needs. The network, however, will be a minimum solution:

- The network will rely on commercial communications infrastructure
- The planned network provides a limited out-of-coverage functionality
- The small number of simultaneous users allowed in the network restricts communications to a minimum
- The low data rates restrict the communications to voice and the exchange of simple data formats.

The cost of building a redundant fixed network infrastructure and deploying the number of base stations required for efficient data communications will be high. Therefore, these options are not assumed to be realistic.

Mobile wireless ad hoc networks have characteristics, which intuitively make them well suited for utilization in search and rescue operations. The networks will reduce the impact of the shortcomings identified in the planned emergency network and will represent extra connectivity, capacity and functionality. Especially, the ad hoc technology will enhance the emergency network’s ability to operate independently of a pre-established communications infrastructure. Further, the ad hoc technology will increase the network capacity considerably. New functionality and applications may then be supported. Ongoing research on QoS, security and group management will enhance the ad hoc technology’s applicability in TETRA-based emergency networks. The research aims at developing efficient dynamic and distributed solutions in conformance with the rescue services’ need for communication networks that handle unpredictability and rapid-changing conditions. With regard to security, the ad hoc technology could probably meet the requirements for out-of-coverage communications without extensive research.

In order to make mobile wireless ad hoc networks even more applicable for rescue operations, we have investigated aspects concerning connectivity, throughput, trust and security in depth. In order to improve connectivity, we have proposed the concept of Trust Metric Routing. The potential utilization is discussed within the context of a schematic architecture, which extends the Norwegian Public Safety Radio Network with mobile wireless technology. Routing cooperation according to the proposed concept may be especially helpful in the initial phase of the rescue operations. By integrating all available nodes into one common routing domain, Trust Metric Routing allows different security domains to utilize each other’s nodes as forwarding nodes while maintaining each domain’s possibility to select routes that exclusively consist of domain-internal nodes. Such routes are called trustworthy routes. Trust Metric Routing enables the actors to exploit whatever communications resource available in the disaster area.

Routing cooperation implies an increased number of network nodes, which may result in congestion. Nevertheless, our simulation results show that Trust Metric Routing increases the connectivity and leads to a significant throughput improvement within a large node density range. Congestion is not specifically related to Trust Metric Routing, but has to be resolved in any network regardless of the utilization of mobile wireless ad hoc networks and regardless of the utilization of routing cooperation. Several mechanisms may be utilized to deal with escalating traffic load from an increasing number of network nodes. Mechanisms, which control the traffic load, however, would be the most efficient means of adaptation to an increasing number of nodes. A variety of possible mechanisms are presented. To analyze their applicability in the setting of Trust Metric Routing is left for further work.

Routing cooperation should not be at the expense of security. We propose and describe the security services needed to build and maintain a trustworthy topology according to the concept of Trust Metric Routing. Since Trust Metric Routing operates in the setting of link state routing, we have analyzed the performance of different security schemes proposed for the protection of the Optimized Link State Routing protocol. Our scheme seems to have better over all performance than the alternatives. Due to the limited bandwidth, power and processing capacity in mobile wireless ad hoc networks, resource consumption should be an important aspect in security schemes.

7.1 Required work

Mobile wireless ad hoc networks will strengthen the communications network at the emergency site. Nevertheless, as we have shown, work has to be done in several areas if the Norwegian Public Safety Radio Network is to be extended with mobile wireless ad hoc networks. The most important areas seem to be:

Configuration scheme. In order to enable seamless communications between a mobile wireless ad hoc network and the emergency network, a configuration scheme involving mechanisms and policy for the allocation and advertisement of IP addresses, is required. A configuration/address scheme is also required in order to exploit the extra capacity offered by available external networks. Solutions like multi-homing should be considered. Further, the scheme should comprise mechanisms for autoconfiguration. Such features are especially important in the initial phase of the operations.

Group management and multicast. Due to the group centric nature of the rescue operations, efficient distributed and dynamic solutions for group management should be developed. This is especially important in autonomous operation. Group communications are important in a rescue operations scenario. Therefore, efficient multicast routing protocols are essential. The group management schemes as well as the multicast protocols should interoperate with the corresponding solutions in the emergency network.

Quality of Service. As we have shown, resources are scarce within the emergency network as well as within potential ad hoc extensions. Also, in a mobile wireless ad hoc network links are unpredictable. Therefore, a comprehensive Quality of Service model, which comprises both the IP-based emergency network and the ad hoc extension, should be developed. The various proposals for QoS routing should be investigated. To meet the different quality requirements, priority and pre-emption will be important mechanisms.

Authentication. The concept of Trust Metric Routing focuses on routing security. Nevertheless, security is a multi-layer issue. Authentication may be regarded as the basic security service. A comprehensive authentication scheme should be developed for the network as a whole. The model should comprise the needs and requirements for verifiable identities and authentication at the various communication layers. Due to scarce bandwidth and other resources, efficient cross layer solutions should be investigated. This work is related to the address scheme mentioned above.

For all areas, the importance of interoperation between the emergency network and the ad hoc extensions should be stressed. Our reference architecture is just a starting point. The topics listed in this section are important building block within the final architecture.

ABBREVIATIONS

AES	Advanced Encryption Standard
AI	Air Interface
AMRIS	Ad Hoc Multicast Routing Protocol Utilizing Increasing ID Numbers
AODV	Ad Hoc On Demand Distance Vector
AQOR	Ad Hoc QoS On Demand Routing
ASCI	Advanced Speech Call Items
CDMA	Code Division Multiple Access
CEDAR	Core-Extracting Distributed Ad hoc Routing
CEPT	European Conference of Postal and Telecommunications Administrations
DiffServ	Differentiated Services
DMO	Direct Mode of Operation
DNS	Domain Name System
DSDV	Destination Sequenced Distance Vector Routing
E1	Standard interface for data exchange
ETSI	European Telecommunications Standards Institute
FFI	Norwegian Defence Research Establishment
FQMM	Flexible QoS Model for Mobile Ad-Hoc Networks
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSM-R	GSM-Railway
HNA	Host and Network Association
IEPREP	Internet Emergency Preparedness
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
IP Sec	IP Security
IPI	Internet Protocol Inter-working
ISDN	Integrated Services Digital Network
ISI	Inter-System Interface
ITU	International Telecommunication Union
ITU-T	ITU-Telecommunication Standardization Sector
LAN	Local Area Network
MAODV	Multicast AODV
MESA	Mobility for Emergency and Safety Applications
MID	Multiple Interface Declaration
MMI	Man Machine Interface
MoU	Memorandum of Understanding
MPR	Multipoint Relay

NAT	Network Address Translation
ODMRP	On Demand Multicast Routing Protocol
OLSR	Optimized Link State Routing
OTAR	Over The Air Rekeying
PAMR	Public Access Mobile Radio
PEI	Peripheral Equipment Interface
PHB	Per-Hop Behavior
PMR	Private Mobile Radio
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RSVP	Resource Reservation Protocol
SAR	Security-Aware ad hoc Routing
SCN	Switching Control Node
SDS	Short Data Service
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SLS	Service Level Specification
SWAN	Stateless Wireless Ad hoc Networks
SwMI	Switching and Management Infrastructure
TAPS	TETRA Advanced Packet Service
TC	Topology Change
TDMA	Time Division Multiple Access
TEA	TETRA Encryption Algorithm
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio
TETRA 1	TETRA Release 1
TETRA 2	TETRA Release 2
TMO	Trunked Mode of Operation
TMR	Trust Metric Routing
UMTS	Universal Mobile Telecommunication System
UniK	University Graduate Center at Kjeller
V.35	Standard interface for data exchange
VoIP	Voice-over-IP
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WLAN	Wireless LAN
X.25	ITU-T standard for packet-switched networks

REFERENCES

[1] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Mühlethaler, and D. Raffo. "Securing the OLSR protocol." Proceedings of the IFIP Med-Hoc-Net, Mahdia, Tunisia, 2003.

[2] G.-S. Ahn, A. T. Campbell, A. Veres, and L.-H. Sun. "SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks." Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE InfoCom), June, 2002.

[3] T. Aura. "Strategies against Replay Attacks." Proceedings of the IEEE Computer Security Foundations Workshop, Rockport, Massachusetts, June, 1997.

[4] P. Bergamo, D. Maniezzo, A. Giovanardi, G. Mazzini, and M. Zorzi. "Distributed Power Control for Power-aware Energy-efficient Routing in Ad Hoc Networks." Proceedings of the European Wireless, Florence, Italy, February, 2002.

[5] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols." Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98), Dallas, Texas, October, 1998.

[6] S. Buchegger, and J.-Y. Le Boudec. "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks)." Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Lausanne, June, 2002.

[7] Buttyán, and J.-P. Hubaux. "Report on a Working Session on Security in Wireless Ad Hoc Networks." *Mobile Computing and Communications Review*, vol. 6, no. 4, 2002.

[8] T. Clausen, and P. Jacquet. (2003). *RFC 3626: Optimized Link State Routing Protocol (OLSR).* Mobile Ad Hoc Networking Working Group of the IETF.

[9] T. H. Clausen, P. Jacquet, and L. Viennot. "Investigating the Impact of Partial Topology in Proactive MANET Routing Protocols." Proceedings of the Wireless Personal Multimedia Communications, November, 2002.

[10] C. de Morais Cordeiro, H. Gossain, and D. P. Agrawal. "Multicast over Wireless Mobile Ad Hoc Networks: Present and Future Directions." *IEEE Network*, January/February, 2003.

[11] T. A. ElBatt, S. V. Krishnamurthy, D. Connors, and S. Dao. "Power Management for Throughput Enhancement in Wireless Ad-Hoc Networks." Proceedings of the IEEE International Conference on Communications (ICC), New Orleans, Louisiana, June, 2000.

[12] European Conference of Postal and Telecommunications Administrations (CEPT). 2005. *http://www.cept.org/*

[13] European Telecommunications Standards Institute (ETSI). (2005). *http://www.etsi.org/*

[14] European Telecommunications Standards Institute (ETSI)/TETRA. (2005). *http://portal.etsi.org/radio/TETRA/tetra.asp*

[15] W. Freeman, and E. Miller. "An experimental Analysis of Cryptographic Overhead in Performance-Critical Systems." Proceedings of the IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecomm. Systems (MASCOTS), 1999.

[16] A. Hafslund, A. Tønnesen, R. B. Rotvik, J. Andersson, and Ø. Kure. "Secure Extension to the OLSR protocol." Proceedings of the OLSR Interop and Workshop, San Diego, California, 2004.

[17] A. M. Hegland, E. Winjum, S. F. Mjølsnes, Ø. Kure, and P. Spilling. (2005). *Key Management in ad hoc Networks, Survey and Evaluation* (Report Number 322). UniK.

[18] Y.-C. Hu, D. B. Johnson, and A. Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks." Proceedings of the IEEE Workshop on Mobile Computing Systems & Applications (WMCSA), New York, June, 2002.

[19] ITU-R. (2003). *Report M.2033 Radio communication Objectives and Requirements for Public Protection and Disaster Relief (PPDR)*. ITU.

[20] International Telecommunication Union (ITU). (2005). *http://www.itu.int/home/*

[21] Internet Engineering Task Force (IETF). (2005). *http://www.ietf.org/*

[22] M. Jakobsson, S. Wetzel, and B. Yener. "Stealth Attacks on Ad-Hoc Wireless Networks." Proceedings of the Vehicular Technology Conference, 2003.

[23] A. Khalili, J. Katz, and W. A. Arbaugh. "Toward Secure Key Distribution in Truly Ad-Hoc Networks." Proceedings of the IEEE Workshop on Security and Assurance in Ad Hoc Networks, in conjunction with the International Symposium on Applications and the Internet, Orlando, Florida, January, 2003.

[24] L. Kleinrock, and J. Silvester. "Optimum Transmission Radii for Packet Radio Networks or Why Six is a Magic Number." Proceedings of the IEEE National Telecommunication Conference, Alabama, 1978.

[25] S.-B. Lee, G.-S. Ahn, X. Zhang, and A. T. Campbell. "INSIGNIA: An IP-Based Quality of Service Framework for Mobile ad-Hoc Networks." *Journal on Parallel and Distributed Computing*, vol. 60, no. 4, pp. 374:406, April, 2000.

[26] F. Y. Li, E. Winjum, and P. Spilling. "Connectivity-aware Rate Adaptation for 802.11 Multirate Ad Hoc Networking." Proceedings of the 19th International Teletraffic Congress (ITC19), Beijing, China, August, 2005.

[27] Y. S. Liaw, A. Dadej, and A. Jayasuriya. "Performance Analysis of IEEE 802.11 DCF under Limited Load." Proceedings of the IEEE 11th Asia-Pacific Conference on Communications (APCC 2005), Perth, Australia, October, 2005.

[28] S. Mäki, T. Aura, and M. Hietalahti. "Robust Membership Management for Ad-hoc Groups." Proceedings of the Nordic Workshop on Security Protocols (NordSec), 2000.

[29] Mobility for Emergency and Safety Applications Project (MESA). (2005). *http://www.projectmesa.org/*

[30] Ministry of Justice and the Police, Norway. (2004). *Proposition No. 1 to the Storting - Supplement No. 3 (2004-2005)*. Ministry of Justice and the Police, Norway.

[31] S. Malladi, J. Alves-Foss, and R. B. Heckendorn. "On Preventing Replay Attacks on Security Protocols." Proceedings of the International Conference on Security and Management, 2002.

[32] Norwegian Post and Telecommunications Authority. (2005). *http://www.npt.no*

[33] Norwegian Public Safety Radio Network Project. (2005). *http://www.nodnett.no/*

[34] P. Papadimitratos, and Z. J. Haas. "Secure Link State Routing for Mobile Ad Hoc Networks." Proceedings of the International Symposium on Applications and the Internet, Orlando, 2003.

[35] R. Ramanathan, and R. Rosales-Hain. "Topology Control of Multihop Wireless Networks using Transmit Power Adjustment." Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE InfoCom), Tel Aviv, Israel, March, 2000.

[36] G. Roelofsen. (1998). *Security Issues for TETRA Networks*.

[37] G. Roelofsen. (2004). *TETRA security - An overview*. TETRA Memorandum of Understanding (MoU).

[38] E. M. Royer, P. M. Melliar-Smith, and L. E. Moser. "An Analysis of the Optimum Node Density for Ad hoc Mobile Networks." Proceedings of the IEEE International Conference on Communications, Helsinki, Finland, June, 2001.

[39] E. M. Royer, and C.-K. Toh. "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks." *IEEE Personal Communications*, pp. 46-55, April, 1999.

[40] I. Sorteberg, and Ø. Kure. "The Use of Service Level Agreements in Tactical Military Coalition Force Networks." *IEEE Communication Magazine*, vol. 43, no. 11, pp. 107:114, November, 2005.

[41] H. Takagi, and L. Kleinrock. "Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals." *IEEE Transactions on Communications*, vol. COM-32, no. 3, pp. 246:257, March, 1984.

[42] TETRA Memorandum of Understanding (MoU). (2004). *TETRA or GSM-ASCI network for Public Safety. Let the users decide*. TETRA MoU.

[43] TETRA Memorandum of Understanding (MoU). (2005). *http://www.tetramou.com/*

[44] TETRA project in Norway. (2002). *Proposed Norwegian National TETRA Network. Request for Information* (Report Number 02/5235). Ministry of Justice and the Police, Norway

[45] TETRA project in Norway. (2002). *The use of commercial Cellular Mobile Networks as a Solution for Public Safety Users in Norway*. Ministry of Justice and the Police, Norway

[46] TETRAPOL. (2005). *http://www.tetrapol.com/www/general/index.php*

[47] L. Viennot, P. Jacquet, and T. H. Clausen. "Analyzing Control Traffic Overhead in Mobile Ad-hoc Network Protocols versus Mobility and Data Traffic Activity." Proceedings of the IFIP Med-Hoc-Net, Italy, 2002.

[48] E. Winjum, A. M. Hegland, Ø. Kure, and P. Spilling. "Replay Attacks in Mobile Wireless Ad Hoc Networks: Protecting the OLSR protocol." Proceedings of the International Conference on Networking (ICN), Reunion Island, France, April, 2005.

[49] E. Winjum, A. M. Hegland, P. Spilling, and Ø. Kure. "A Performance Evaluation of Security Schemes Proposed for the OLSR Protocol." Proceedings of the IEEE Military Communications Conference (MILCOM), Atlantic City, New Jersey, October, 2005.

[50] E. Winjum, Ø. Kure, and P. Spilling. "Trust Metric Routing in Mobile Wireless Ad Hoc Networks." Proceedings of the World Wireless Congress, San Francisco, California, May, 2004.

[51] E. Winjum, P. Spilling, and Ø. Kure. "Trust Metric Routing to Regulate Routing Cooperation in Mobile Wireless Ad Hoc Networks." Proceedings of the European Wireless Conference, Nicosia, Cyprus, April, 2005.

[52] E. Winjum, P. Spilling, and Ø. Kure. "On Adaptation to an Expanding Number of Nodes." Proceedings of the IEEE International Workshop on Adaptive Wireless Networks (AWiN) in conjunction with IEEE Globecom, St. Louis, Missouri, November, 2005.

[53] Wireless Deployable Networks System (WIDENS) Project. (2005). *http://www.widens.org/*

[54] H. Xiao, W. K. G. Seah, A. Lo, and K. C. Chua. "A Flexible Quality of Service Model for Mobile Ad-Hoc Networks." Proceedings of the IEEE Vehicular Technology Conference (VTC), Tokyo, Japan, May, 2000.

[55] F. Xue, and P. R. Kumar. "The number of neighbors needed for connectivity of wireless networks." *Wireless Networks*, vol. 10, no. 2, pp. 748:767, March, 2004.

[56] Q. Xue, and A. Ganz. "Ad hoc QoS On-demand Routing (AQOR) in Mobile Ad hoc Networks." *Journal on Parallel and Distributed Computing*, vol. 63, no. 2, pp. 154-165, Februry, 2003.

[57] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. "Security in Mobile Ad Hoc Networks: Challenges and Solutions." *IEEE Wireless Communications*, no. February, pp. 38:47, 2004.

[58] Yasinsac, and J. A. Davis. "Modeling Protocols for Secure Group Communication in Ad Hoc Networks." Proceedings of the International Workshop on Security Protocols, Cambridge, UK, April, 2002.

[59] S. Yi, P. Naldurg, and R. Kravets. "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks." Proceedings of the World Multi-Conference on Systemics, Cybernetics and Informatics (SCI), 2002.

[60] W. H. Yuen, and C. W. Sung. "On Energy Efficiency and Network Connectivity of Mobile Ad Hoc Networks." Proceedings of the International Conference on Distributed Computing Systems (ICDCS), Providence, Rhode Island, May, 2003.

[61] L. Zhou, and Z. J. Haas. "Securing Ad Hoc Networks." *IEEE Network Magazine*, vol. 13, no. 6, Special Issue on Network Security, pp. 24-30, November/December, 1999.

[62] S. Zhong, J. Chen, and Y. R. Yang. "Sprite: A Simple Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks." Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE InfoCom), San Francisco, California, 2003.