FFI-rapport 2012/00294

Group communication in mobile military networks

Margrete Allern Brose and Mariann Hauge

Norwegian Defence Research Establishment (FFI)

13 February 2012

FFI-rapport 2012/00294

1175

P: ISBN 978-82-464-2072-1
E: ISBN 978-82-464-2073-8

Keywords

Nettverksbasert forsvar

Taktisk kommunikasjonsnettverk

Gruppekommunikasjon

Mobile ad hoc-nettverk

Ruting

Multicast

Approved by

Torunn Øvreås	Project Manager
Eli Winjum	Director of Research
Anders Eggen	Director

English summary

In both national and international tactical operations there is an increasing demand for electronic information that is wanted anytime, anywhere. This demand for information exchange is expected to increase even more in future operations. New ways of operating require information exchange between units that traditionally do not have much interaction. Multinational operations also require efficient information exchange between coalition partners. A large fraction of the traffic in mobile military networks will be intended for a group of recipients.

Due to the nature and constraints of military mobile ad hoc networks, it is therefore necessary to find the most efficient method for data distribution to groups. While there are many different ways to solve this, no single protocol will solve all situations efficiently. The goal of this work has therefore been to try to narrow down the range of protocols for group communication and see if there are certain types of protocols that are more relevant in a military setting.

To get a better understanding of the needs for group communication in a tactical setting, a series of vignettes were created. The vignettes were then used to identify the range of network parameters that might best define group communication in military networks. The groups of protocols were finally evaluated against these parameters.

The preliminary findings suggest that an efficient flooding-based protocol may be best suited for many group applications in mobile military network, while it may also be worthwhile to take a closer look at stateless and geographic protocols.

Sammendrag

I både nasjonale og internasjonale taktiske operasjoner er det et økende behov for deling av elektronisk informasjon hvor som helst, når som helst. Behovet for informasjonsutveksling er forventet å øke enda mer for fremtidige operasjoner. Nye måter å operere på krever informasjonsutveksling mellom enheter som tradisjonelt ikke har hatt særlig interaksjon. Multinasjonale operasjoner krever også effektiv informasjonsutveksling mellom koalisjonspartnere. Mye av denne kommunikasjonen vil være gruppekommunikasjon.

På grunn av egenskapene og begrensningene til mobile ad hoc-nettverk, så er det nødvendig å finne den mest effektive metoden for å distribuere data til grupper. Samtidig som det finnes mange måter å løse dette på, så vil ingen protokoll alene kunne løse alle situasjoner effektivt. Målet med dette arbeidet har derfor vært å prøve å snevre inn utvalget av protokoller, og se om det er visse typer protokoller som er mer relevante i en militær setting.

For å få en bedre forståelse av behovet for gruppekommunikasjon i en taktisk setting, så ble det definert en serie vignetter. Vignettene ble så brukt til å identifisere hvilke nettverksparametre som best definerer gruppekommunikasjon i militære nettverk. Til slutt ble de forskjellige protokollgruppene evaluert mot disse parametrene.

De foreløpige resultatene antyder at en effektiv floodingbasert protokoll kan være den type protokoll som vil være best egnet for mange gruppeapplikasjoner i mobile militære nettverk. Samtidig kan det og være verdt å se nærmere på tilstandsløse og geografisk baserte protokoller.

Contents

List of Tables

List of Figures

1 Introduction

As new applications and sensors are introduced to tactical operations, the capacity of the mobile communication infrastructure must also be increased. The wish for more information to single warfighters also enforces the need for more capacity in these networks. In radio communication there is a trade-off between data capacity, communication range and frequency use. It is not possible to get high capacity, long range and low frequency use all at the same time. Hence it is important that traffic transmitted on these networks use the network resources as efficiently as possible.

We envision that a large fraction of the traffic in mobile military networks will be intended for a group of recipients. Due to the nature and constraints of military mobile ad hoc networks, it is therefore necessary to find the most efficient method for data distribution to groups. There are many different ways to solve this, but no single protocol will solve all situations efficiently. The goal of this work has therefore been to try to narrow down the range of protocols for group communication and see if there are certain types of protocols that are more relevant in a military setting. In order to achieve this, the work was executed in several phases. In the first phase a series of military vignettes involving group communication was defined. This was done both to get a better understanding of the needs for group communication in a tactical setting and to have realistic situations to study the protocol types against. The vignette series is therefore a part of the results. In the next phase a survey of various group communication protocols was done. The final phase consisted of a high-level analysis of the groups of protocols against the vignettes.

2 Background

In both national and international tactical operations, there is an increasing demand for electronic information that is wanted anytime, anywhere. This demand for information exchange is expected to increase even more in future operations. New ways of operating require information exchange between units that traditionally do not have much interaction. Multinational operations also require efficient information exchange between coalition partners. These trends place tough requirements on the transport networks.

2.1 Mobile transport network

The network architecture for the Norwegian Armed Forces proposed in [34] is a network based on IP-family protocols, structured in a three-level network topology (see Figure 2.1).

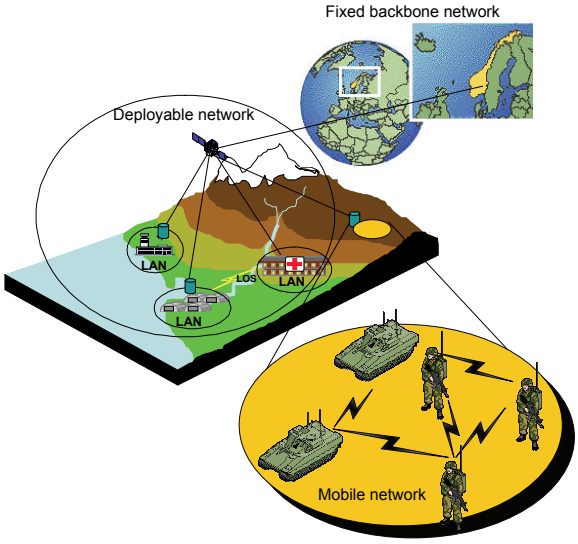

Figure 2.1 This figure illustrates the three-level network topology for the military network architecture

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

The mobile military network at the lowest layer in this figure is the focus of the work described in this report. This mobile network will be a type of Mobile Ad Hoc Network (MANET) [13]. A MANET is a multi-hop wireless data network. It is a self-configuring network of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily. The network's wireless topology may therefore change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or it may be connected to a backbone, the Internet, or another MANET. Each ad hoc node may initiate traffic, receive traffic, as well as forward traffic (operate as a relay).

Mobile ad hoc networks is an active research topic in both civilian and military research, but such networks are not in widespread use except for in military networks. A military MANET will often have some distinctive characteristics that are usually not found in MANETs studied in comparable civilian research. A civilian MANET usually consists of homogeneous links with fairly high bit rate (based on IEEE 802.11 type radios). A military MANET will usually have links with significantly lower bit rate and can consist of heterogeneous links. With heterogeneous links we mean links based on different transmission technologies (operation frequency, bandwidth, modulation etc.). This type of network faces a number of challenges, such as:

- lost links due to mobility
- route decisions, if presented with multiple paths via heterogeneous interfaces
- resource management of network resources that vary based on link channel conditions, traffic load due to mobility, etc.

As new application types are introduced to the mobile network, the network must provide better capacity (higher data rates). Ideally, every soldier in combat should be able to connect to the mobile network. Norwegian military procurement projects for combat equipment often state requirements for robust, high data rate, flexible mobile communication (e.g., Situational Awareness (SA-data) for the squad and distribution of a wide range of sensor data on all command levels). Designing a flexible, highly available, high capacity, tactical mobile network is a challenging task. Mobile military networks will in most cases offer a relatively (compared to civilian mobile networks) low data rate due to the operational requirements for long-range and robust communication. The frequency bands suitable for such communication links are also a limited resource. Mechanisms that can reduce the network resources required to distribute data in this mobile network, are therefore welcomed. In [24] the authors briefly discuss some of the challenges the designers of a military MANET face. One of the main topics in this discussion is efficient group communication. This is an area where optimal protocols and mechanisms may significantly reduce the network resource consumption. In this report we take a closer look at this research topic.

2.2 Transport of group traffic

A large fraction of the traffic in a military MANET is envisioned to be intended for a group of recipients (e.g., distribution of SA-data, push-to-talk voice service, and distribution of sensor data). Hence efficient data distribution to groups is important. The traffic flow in group communication can be divided into three different types; one-to-many, few-to-many and many-to-many. This classification focuses on the number of data sources to the group.

Group traffic may be transported using various mechanisms in the mobile transport network. One of which is unicast, where a point-to-point connection is established between each receiver and each source. Flooding-based mechanisms may also be used. With flooding, data from each source is flooded hop-by-hop to each node in the network (also nodes that are not part of the group). Finally, a variety of multicast protocols may be used to build a distribution tree that attempts to minimize the number of transmissions in the network for the data from the source(s) to reach all group members.

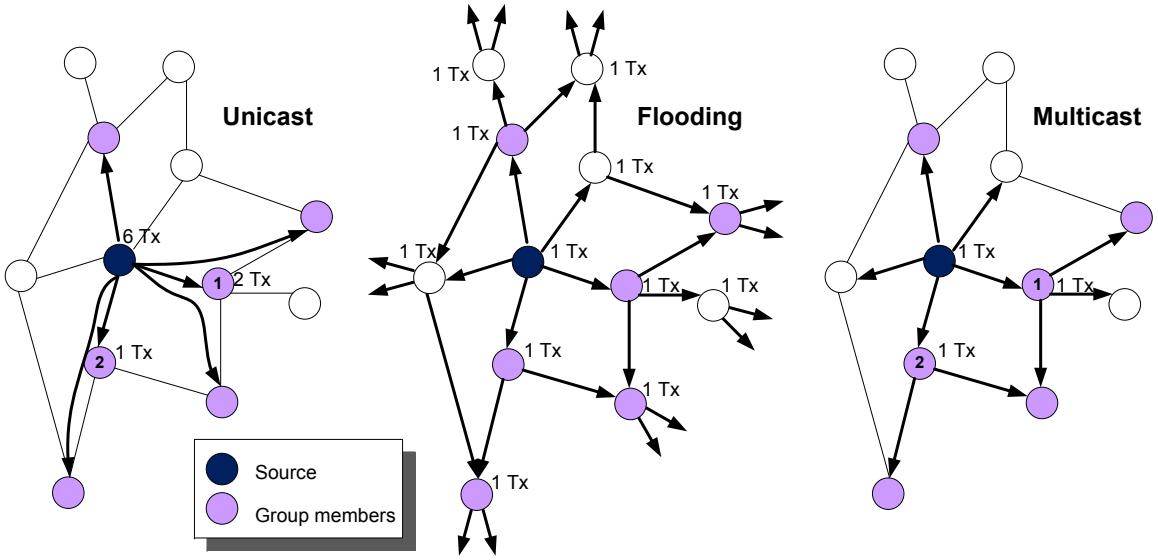

Figure 2.2 This figure illustrates three different network transport methods for group communication

Figure 2.2 shows the number of transmissions required in an example network to distribute a one-to-many scenario from the source to the shown multicast members, using the three different transport types. Note that this is a radio network; thus each transmission reaches all nodes that are within transmission range of the sending node. Two nodes that are within transmission range of each other have a link drawn between them. Unicast distribution to this particular group topology requires 6 + 2 + 1 = 9 transmissions (Tx) in the network. The basic flooding illustration requires the number of nodes (12) x 1 Tx = 12 transmissions. Note that many mechanisms exist to optimize the flooding process to reduce the number of transmissions required, e.g., [42]. We cover these mechanisms in Section 4.3. The last illustration shows transport with the use of a multicast tree that only requires three transmissions (the source and two relay-nodes) to distribute the group traffic to all members.

This example illustrates that efficient distribution of group traffic has the potential to significantly reduce the network load in a military MANET (compared to unicast and basic flooding). However, it is unfortunately impossible to find a MANET multicast protocol that is optimal (little overhead and high efficiency and throughput) for all possible situations (e.g., [39]). The efficiency of the protocols is influenced by the following key factors:

- node mobility
- network topology
- group size
- group-member density
- traffic characteristics

The reader should also be aware that the different distribution methods will perform differently when it comes to fairness and packet loss of the data-flows to the group. This will be discussed further in Section 5.

To get a better understanding of the types of protocols needed to most efficiently support group communication in military MANETs, it was necessary to identify a series of tactical operation vignettes where efficient group communication could be beneficial. In parallel with this we have performed a survey of the most interesting protocols for distribution of group traffic on the network layer of a MANET. The vignettes are used to elucidate the need for group communication and to identify a minimum set of protocol types (protocol mechanisms) that we think will be beneficial for most types of group communication applications in military MANETs.

Our focus in this report is on distribution of group communication inside the MANET. Clearly the mechanism chosen for this network segment must interact efficiently with the deployable military network, and the fixed backbone network to provide efficient end-to-end group services on network paths through any combination of these networks. This interconnection is beyond the scope of this initial work. The purpose of this work has been to identify protocol mechanisms for scalability, robustness, etc. Hence requirements for radio silence, security, reliability, differentiated QoS, etc., are also not treated in this report. These abilities will be reintroduced in future work.

2.3 Limitations of broadcast in a common IP-network platform

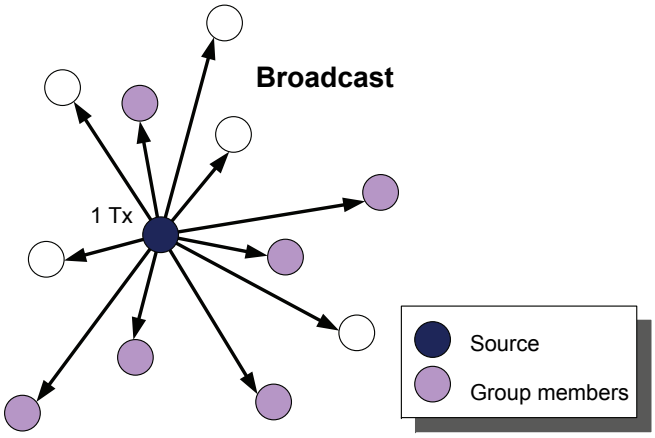

Figure 2.3 Broadcast in one-hop traditional CNR network

Traditionally, applications such as push-to-talk and exchange of SA-data have been distributed with broadcast on a one-hop Combat Net Radio (CNR) network (see Figure 2.3). This is a stovepipe type network where the applications and the radio are integrated, and visible at the network layer as one network node. The scope of the distribution has been limited by the range of the radio and by the frequency range allocated to the radios within transmission range. Two radios connected back-to-back could be utilized to extend the CNR network to multiple hops. When multicast is introduced instead of broadcast, this allows for more flexibility and dynamics in the distribution of group communication. Multicast allows for dynamic group size (number of receivers) and flexible scope (number of

network hops). Multicast is not yet in widespread use in Norwegian military mobile networks. One reason is that the CNR type network structure is still the prevailing architecture. Another reason is that most application types that provide group services do not (yet) support multicast. When the IP network model (where a common transport network is used to distribute all services on a platform) is introduced in the mobile military networks, the old CNR broadcast solution will not work[1], and a type of multicast routing must be supported to efficiently distribute group communication.

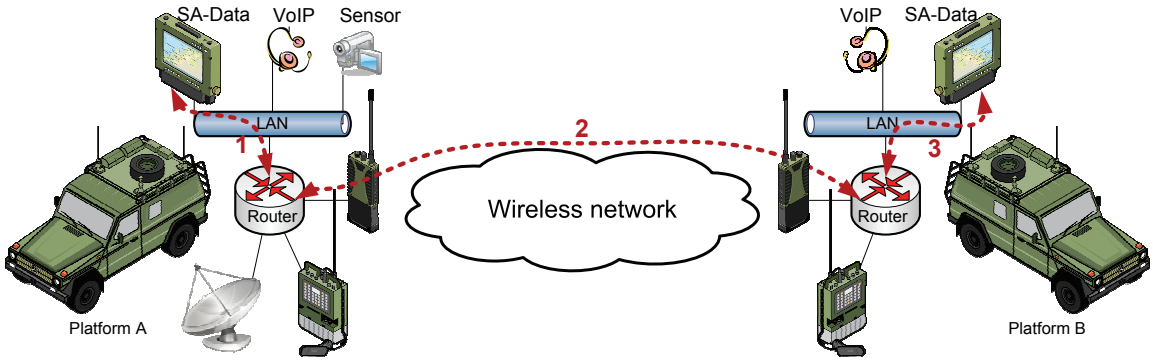

Figure 2.4 This figure shows that there is a minimum of 3 IP-layer network hops between a source on platform A and a receiver on platform B. A broadcast message from the source on platform A will only reach other clients on the LAN on platform A.

The reason why military applications and transport networks eventually must use a more sophisticated form for group communication than one-hop broadcast, can be explained with reference to Figure 2.4. This figure shows a flexible network structure on a platform. This can be any platform (e.g., ship, vehicle, aircraft and even a single warfighter). In this model the different applications and sensors on a platform are connected to the platform's Local Area Network (LAN). This LAN is connected to one or more platform router(s) that provide(s) access to the radio resources available on the platform. If one host connected to the LAN issues a broadcast message in this network, the broadcast message is distributed on the LAN, but does not go beyond the router and onto the wireless network. At the network layer in the protocol stack where the IP protocol runs, broadcast is a one-hop distribution method. In the scenario depicted in Figure 2.4 there is a minimum of 3 hops on the network layer between a source in vehicle A to a destination in vehicle B. To have a group message transmitted to different destinations in this type of network, either multiple unicast transmissions must be used, or there must be support for multicast.

3 Military vignettes

Given the fact that today's distribution of group traffic in most cases is predefined and not very flexible, we have spent some time predicting possible useful military vignettes for future group communication, given the flexible model of an IP-based military MANET and multicast routing.

[1]Proprietary solutions can be found for radios supporting efficient multi-hop flooding at layer two in the network protocol stack. However in this report we focus on standardized network mechanisms for basic network operation to ease the task of interoperability. For standardized IP networks, broadcast is a one-hop service at the network layer.

Hence most of the vignettes that we have created for this multicast study cannot be found in present tactical operations. We have described cases based on information exchange needs where using group communication would be favorable.

All our vignettes are given in the context of a tactical operation in the Army, but the traffic flow in these cases may easily be transferred to selected operations for the Navy, the Air Force, the Home Guard, and including elements from Non-Governmental Organizations (NGOs). In the vignettes we consider a national force, but the cases could also be applied to a coalition force.

Our context is a battalion-sized network. Figure 3.1 depicts a battalion with four companies/squadrons, each with four platoons, that each consists of four squads. In addition the figure contains supporting elements, such as logistics and artillery, and the brigade head quarters (HQ) and air support elements, that the battalion elements may need to communicate with. We have drawn the battalion network with different types of units to depict that this is a general battalion structure used as an example for the following vignettes and not a specialized battalion geared for a specific task. Most of the following scenario is relevant in situations where a battalion might be deployed.

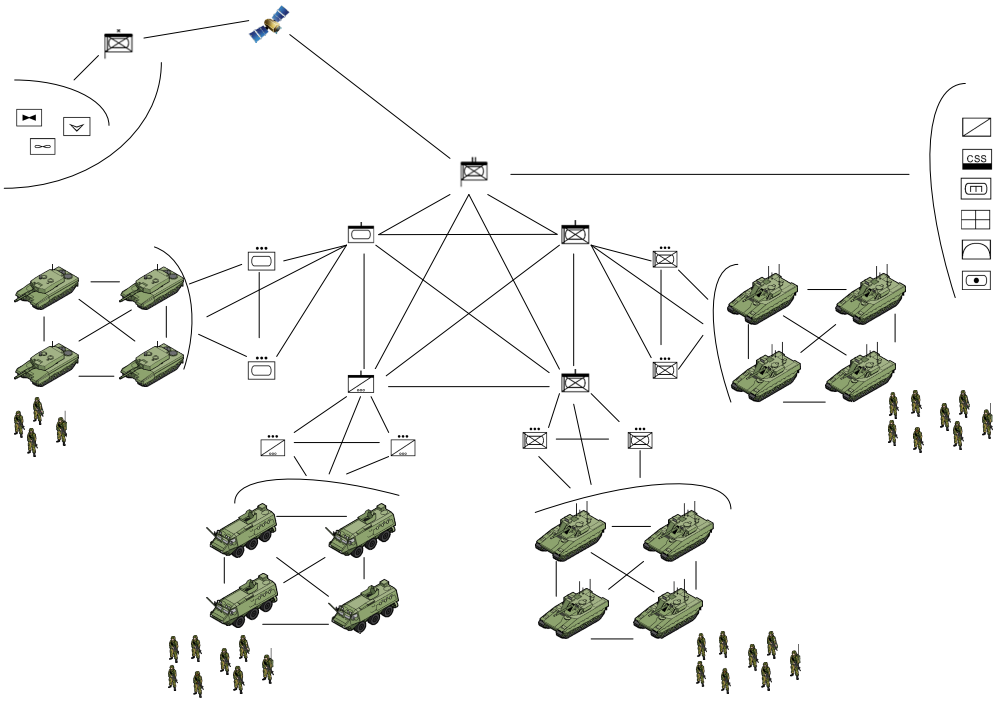

Figure 3.1 A battalion and supporting elements

In the following vignettes, which describe proposed information flows in this battalion network, we have focused on both planned and unplanned needs for information exchange from one-to-many or few/many-to-many. In all cases a variant of multicast may be an efficient data-distribution method.

We have based the vignettes on information exchange present in present-day networks and expanded this information flow with the added dynamics and flexibility available with multicast-type distribution.

For all vignettes we show the required information flow. In other words, the figures do not say anything about the actual network path used for data-packet distribution in the network. The vignettes describe information exchange needs, whereas it is the job of the network routing protocols (unicast, multicast) to find the best path for the wanted information exchange. One contribution of this report is to suggest the group communication protocol type(s) that would be best suited to find the optimal routes for distribution of the data that we see a need for in the vignettes.

3.1 Hierarchical communication

A typical information exchange requirement is information exchange through the traditional Command and Control (C2) structure, e.g., distribution of plans and orders downwards in the structure, and status reports upwards. The distribution of orders may be characterized as a one-to-many group, and the reports simple point-to-point communication, or a many-to-many group in the case where it is interesting to distribute the reports to leaders at different levels in the structure and/or to leaders of adjacent elements. Figure 3.2 depicts this type of hierarchical communication. These are also examples of planned communication.

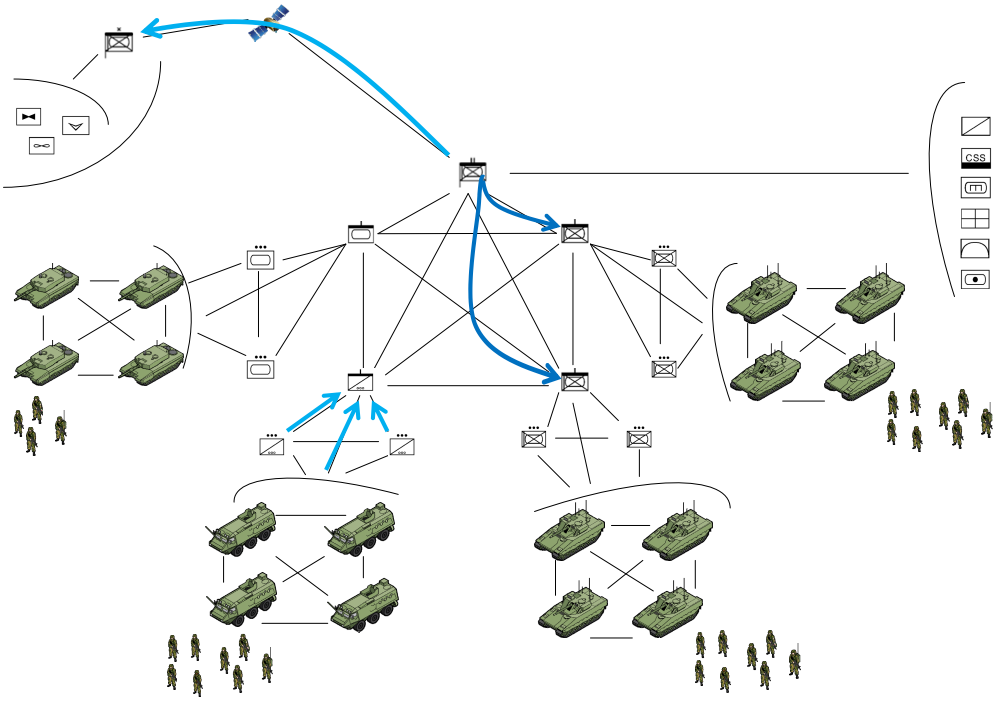

Figure 3.2 The figure shows hierarchical communication exemplifed with distribution of orders downwards in the structure and reports upwards in the structure

Push-to-talk Push-to-talk is the service that is most important in present-day tactical communication. Figure 3.3 shows two many-to-many type push-to-talk groups; one group representing a squad, and one group representing the vehicles in a platoon. The traditional push-to-talk cases can easily be handled with broadcast in present-day CNR networks. As these stovepipe networks are exchanged with the more flexible network model of a common IP-transport network for all services on a platform, some multicast service should be introduced to the network to support push-to-talk traffic.

A nice side effect of the introduction of multicast, is that the push-to-talk groups can also be expanded to include units in neighboring structures or leaders at higher levels in the command chain to allow these to listen to (or participate in) the communication during certain critical stages of an operation. This situation is represented with the example in Figure 3.4.

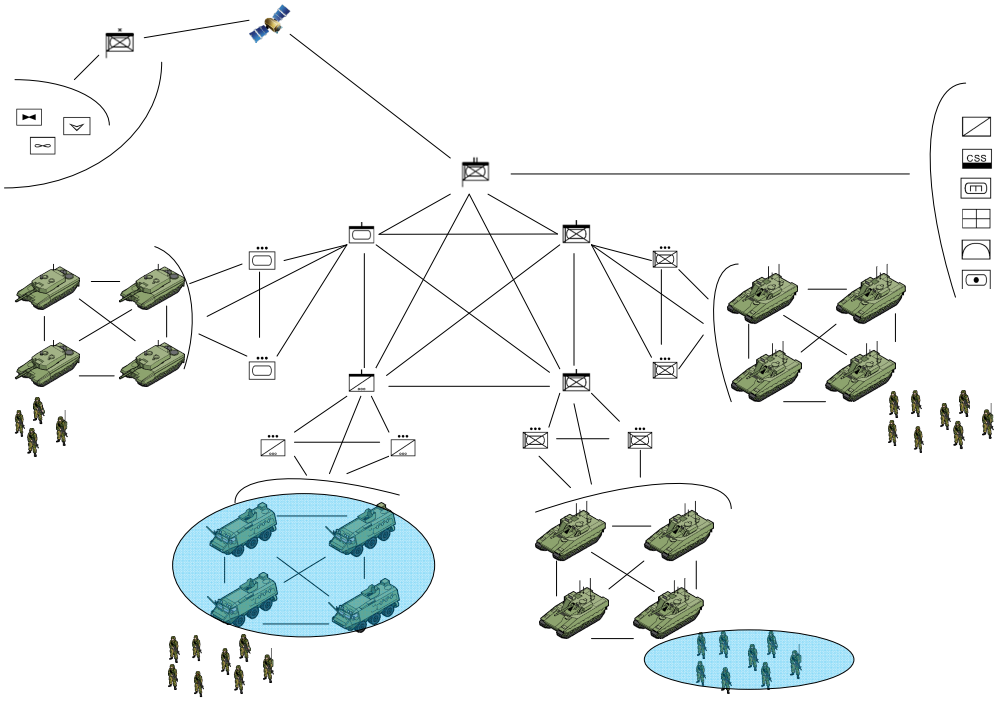

Figure 3.3 This figure shows two traditional push-to-talk groups

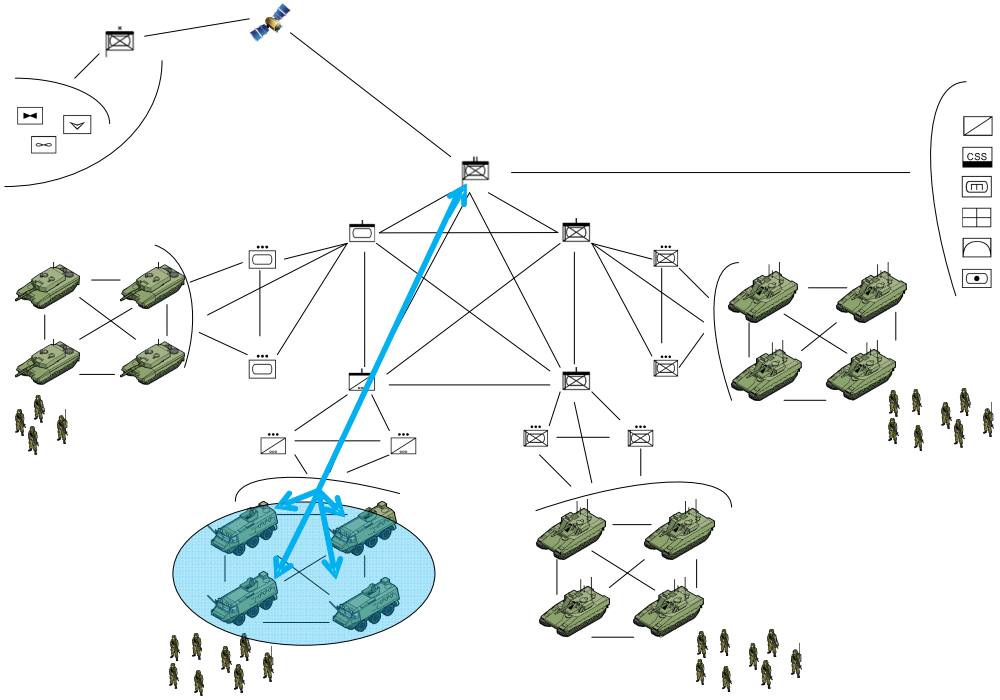

Figure 3.4 This figure shows a flexible push-to-talk group where elements outside the traditional CNR reach can join the conversation

3.2 Horizontal communication

There are other situations where communicating through the C2 structure is not the most efficient way of communicating. This type of information exchange may be described as horizontal communication, as the information does not flow via the C2 structure but rather across it, as depicted in Figure 3.5. For instance, there exists an operational need for friendly force tracking, that is, being provided with location information about other elements. Traditionally, distribution of friendly force tracking and observations has been provided with broadcast on a many-to-many group in a CNR network similar to traditional push-to-talk exemplified in Figure 3.3.

With the introduction of multicast these groups can be made more flexible to allow adjacent or remote elements in the group. It is vital for a military operation that elements know the position of other elements that they may affect with their actions, or possibly be affected by. This also includes the locations of external elements. The exchange of position information is an example of information that will be sent at regular intervals, and where the recipients may be predefined, or may join the exchange at a later stage.

The previous examples describe information exchange requirements where the communication for a large part may be planned in advance. When there is change in risk, it is crucial that those exposed can be alerted fast.

We will now present three vignettes which illustrate information exchange needs that arise from unplanned events. The first two involve two types of warning situations, and the third a situation where the need for medical evacuation occurs.

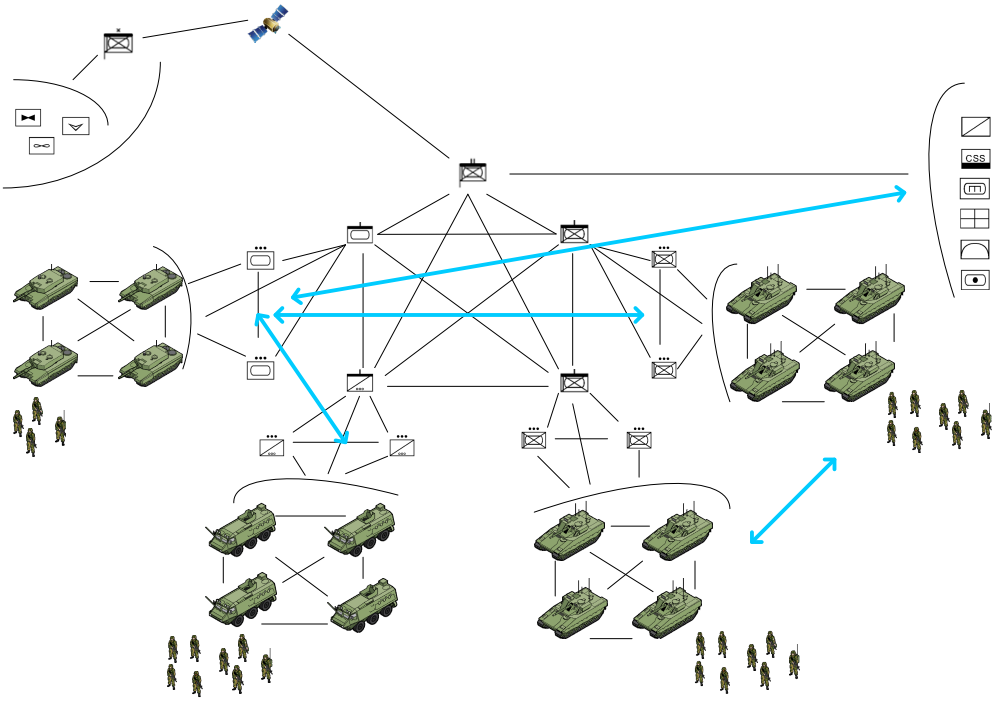

Figure 3.5 Horizontal communication exemplified with, e.g., distribution of friendly force tracking

Gas alarm This is a situation where a sensor that belongs to a squad detects a gas in the surroundings. It is therefore critical to distribute a warning immediately to all warfighters within a certain distance of this squad. This could be personell associated with a different company, support elements, or others. In addition to this horizontal distribution, information must be sent to inform the brigade HQ, and to logistics, so that an analysis and threat assessment can be done. These information exchange needs are described in Figure 3.6. This is an example of one-to-many group communication. It can also be a few-to-many situation if there are several detector sensors in the vicinity of the gas release.

When the analysis has been completed, information with the results needs to be sent back to the exposed parties, so they may take suitable action. Knowing which troops were in the area at the time of the alarm is not trivial, but in the future one may have some kind of battlespace history, which may include information on the whereabouts of the different units over a recent limited period of time. Another possibility is that units that are missing this information requests this from logistics. Finally, given that it was a gas, it will move and spread, depending on the weather conditions. There might also be elements that were in the area before the alarm, or that have entered the area afterwards. In which case there may be several others that need to be alerted too. The information could therefore be passed on to several companies, or even the whole battalion and supporting elements.

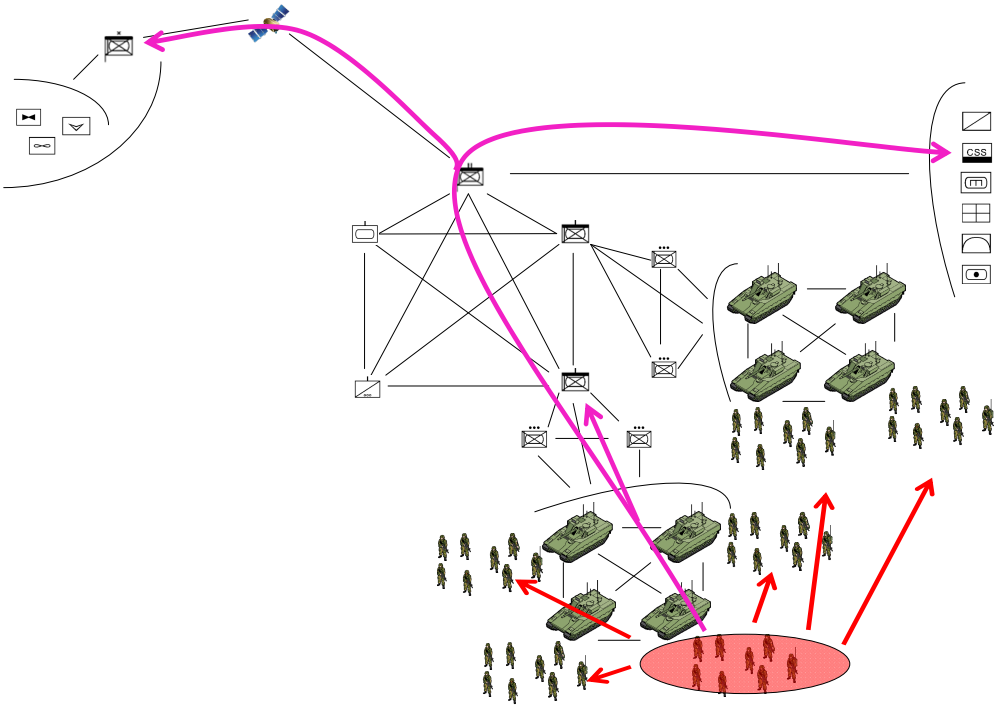

Figure 3.6 This figure shows a gas alarm scenario where all warfighters within a certain range of the gas release should receive an immediate gas warning. Sensor information is also distributed up the chain of command and to logistics for analysis

Hostile/Enemy artillery fire In the second warning situation, artillery makes an observation of an enemy artillery attack and of where the target area is. Apart from the standard notice to the brigade and reconnaissance, it would be desirable if those actually at risk are notified immediately, so they can take some action to be better prepared for the attack (Figure 3.7). This one-to-many group communication situation might involve both individual warfighters as well as complete units and sub-elements of adjacent units.

Medevac The last situation is a medical evacuation. A soldier has been wounded and needs to be brought out of the operation area. Since the brigade is in charge of the aerial elements, a request for a helicopter to assist the evacuation must be directed there. The brigade HQ will then give the order to send a helicopter. At the same time, the battalion HQ requests an ambulance from the medical service. The ambulance will pick up the wounded, and meet the helicopter at some location. In this situation it is critical that all the elements involved in the rescue operation (ie., the helicopter, the ambulance and the unit), have updated information on each others positions, the same situational awareness, including own and enemy units, and they will need to be able to communicate with each other (push-to-talk), exchanging information about their location and situation (Figure 3.8). This situation represents many-to-many communication.

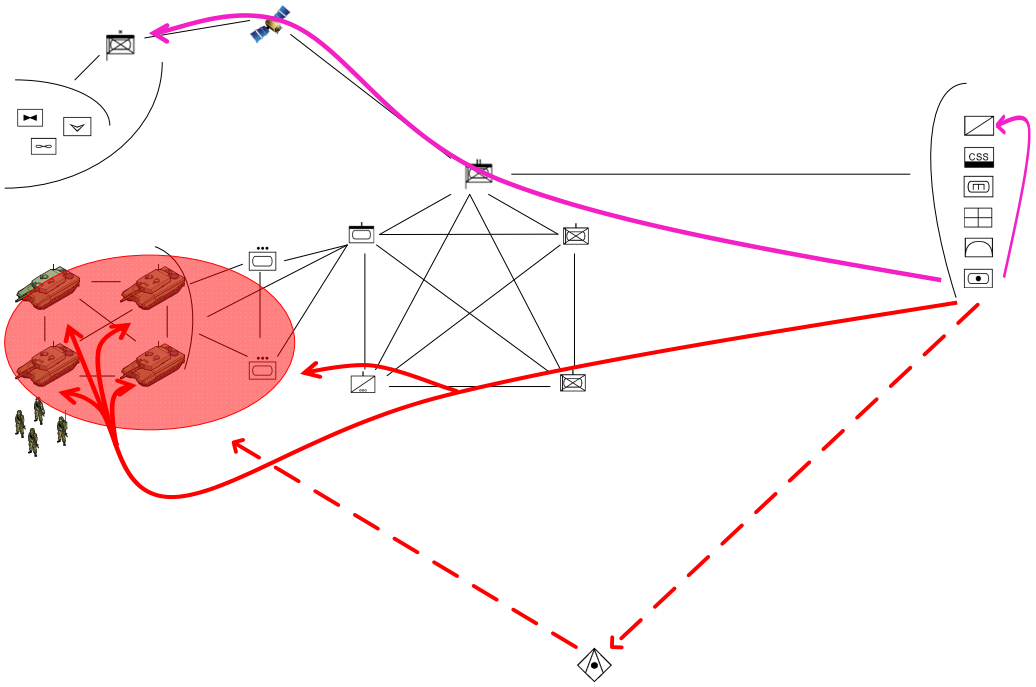

Figure 3.7 An enemy artillery observation where all friendly forces in the area of the calculated target area should be immediately alarmed

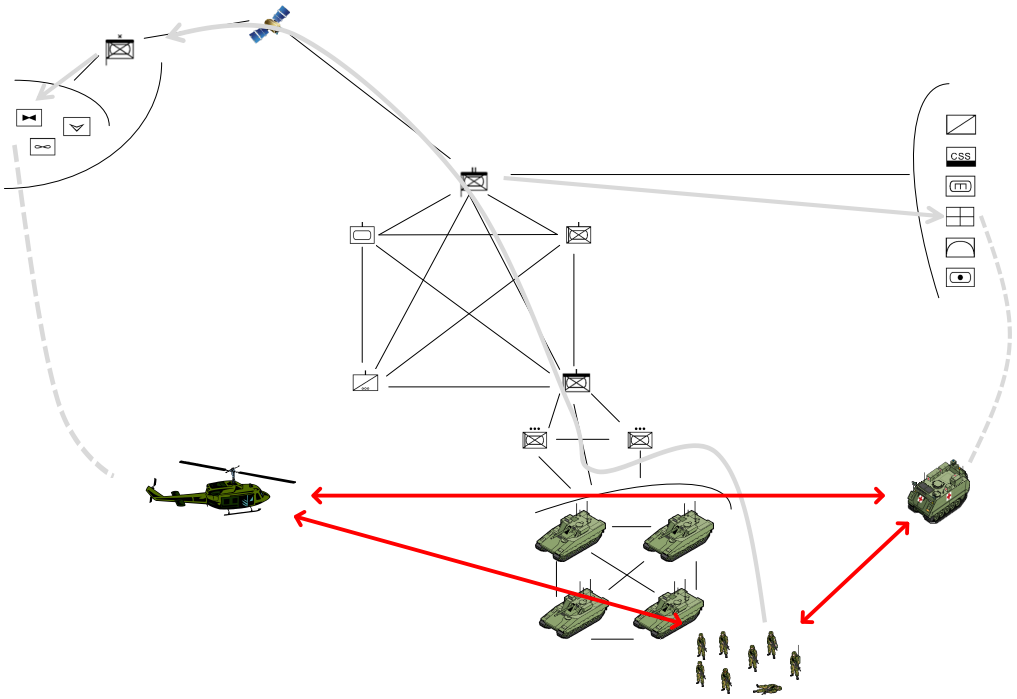

Figure 3.8 Different support elements need to have the same situational awareness as the warfighters that they are approaching for medical evacuation

4 Protocols

In this section we present a survey of group communication protocols for mobile ad hoc networks. The majority of the protocols we cover are multicast protocols, but we also include other protocol types for group communication (e.g., stateless protocols). The original wireline multicast protocols are based on a stringent multicast model. According to this model, a source may send data packets to a multicast group without being member of the group, and the source (and the group members) does not know the identity of the other members, nor the size of the group. This is the multicast model that defines the expectations applications will have to the multicast distribution mechanism. Military applications might have security requirements (or other requirements) that cannot be fulfilled by this definition, and where additional signaling will be needed to fulfill the military needs. However, the reader should be aware that most multicast protocols adhere to the given multicast definition. A few of the protocols presented in this report do however not fully follow this definition.

The multicast tree reorganization in MANETs is more frequent than in conventional wired networks, since the multicast protocols have to respond to network dynamics in addition to group dynamics. Consequently, multicast protocols designed for fixed networks do not support the dynamics of MANETs very well. For this reason a large number of multicast protocols have been suggested specifically for MANETs over the past years. Currently the IETF (Internet Engineering Task Force) has not agreed to any standard or experimental RFC (Request For Comments) for MANET multicast. A likely candidate to become an RFC is Simplified Multicast Forwarding (SMF) [43]. SMF is not a multicast protocol per se, it uses efficient flooding for multicast forwarding. This protocol will be covered in section 4.3.

All multicast protocols proposed by academia differ more or less in operation and/or which mechanisms they use to try to meet the challenges of mobile ad hoc networks. Each has its advantages and disadvantages, and since they are often tailored to specific scenarios, it has become evident that there will be no “one size fits all” protocol.

Multicast protocols can be categorized in a number of ways. The most common way is to distinguish between tree- and mesh-based protocols, and proactive and reactive routing mechanisms, but there are also other types of routing schemes, such as geographic routing. For the multicast surveys in [3] and [29], different, and somewhat more comprehensive, approaches for classifying MANET multicast routing protocols have been chosen. In [3], the multicast protocols are first divided into their layer of operation, and then classified with respect to maintenance approach, multicast topology, initialisation approach, and routing scheme. Junhai et al. [29] give a comprehensive taxonomy where the protocols are first classified into two main categories based on their primary routing selection principle, namely application dependent and independent protocols. Both categories are further divided into topology, initialisation and maintenance approach, and QoS, energy efficiency, reliable routing and network coding, respectively, which are also further classified. There are also surveys that address subgroups of these protocols, such as reliable protocols [51], and QoS-aware protocols [23] [44].

This report differs from the mentioned surveys in that it coveres a wider range of group communi-

cation protocols, and that the protocols are evaluated against situations representing group communication in mobile military networks. In this report we divide the protocols into the following main categories:

Stateless group communication In these protocols the addresses of the group members must be coded in the packet header. No multicast state and signaling is needed in the networks. These protocols rely on unicast routing for their operation. They do not fully adhere to the stringent IP multicast model.

Topological (mesh/tree) multicast protocols This category covers traditional multicast protocols that are derived from the classical IP multicast protocols for wireline networks. These protocols require multicast state and multicast signaling in the network. Most of these protocols adhere to the IP multicast model.

Flooding-based protocols These protocols distribute the data to all (not only the multicast members) users within the selected network scope. Flooding-based protocols employ different mechanisms to optimize the flooding process. A varying degree of state and signaling is required. These protocols are not multicast protocols per se since the data delivery is not limited to the members of the group, but most of them fulfill the requirements in the multicast definition.

Geographic protocols This category covers protocols that use a range of different mechanisms for data distribution, but common to all of them is that they route the group traffic based on the geographic position to the group members. Typically little or no network-state and network signaling are needed in these protocols. On the other hand, a location service is needed. Since these protocols require that the sender knows the position of the receivers, and they do not fulfill the multicast definition.

The next sections will give an introduction to the different categories of protocols and a brief outline of some of the protocols that belong to each category. An overview of the protocols can be found in Table 4.1, and a summary of typical simulation environments can be found in Appendix A.1.

4.1 Stateless protocols

Various scenarios may require different protocol solutions for optimal data distribution. One motivation for development of the stateless approach is the acknowledgment that the same routing strategy may not necessarily be suitable for varying group sizes. In stateless protocols the source keeps control of who the receivers are, and encodes these in the packet header. When an intermediate router discovers that several next-hop routers are needed to reach all the specified group members, the data-packet is replicated and the address field recalculated for each replication. Due to the header-overhead, these protocols are best suited for small groups, but they scale well for a large number of small groups since they do not require any state information in the routers. The

term session is often used instead of group, since a multicast group is often associated with a multicast address. In the stateless protocols the packets are addressed with the list of receivers and not with a multicast address. Stateless protocols rely on the underlying unicast routing protocol to make forwarding decisions along the path. Hence there is no need to maintain an additional multicast distribution structure. On the other hand, all routers between the sources and destinations must have support for stateless multicast routing for these protocols to work. The routers must also spend time on extra header processing. Another consideration is the type of traffic; the overhead per packet will quickly increase with the number of members, especially if the packets are small.

4.1.1 Xcast: Explicit Multicast

Xcast [5] is a stateless multicast scheme for small group multicast sessions. Each source node keeps track of the destinations it wishes to send packets to. When it wants to send a packet, it lists the address of all group members in the header. Each node along the way parses the header and partitions the destinations based on their next hop, and finally forward the packet to each of these next hops. The packet is converted to a unicast packet if at a point there is only one destination left. So in Figure 4.1 A sends a packet with destinations B, C, D to I_1. The packet is then forwarded from I_1 to I_2 with the same destination list. At I_2 one packet encoded with destination list B, C is sent to I_3, and one unicast packet is sent to I_4 with destination D. Packets sent to next hops must only contain destinations for which the receiving next hop is the correct next hop toward the destination, to avoid duplicate packets. In this protocol the source must have a list of all group members. In [5] it is assumed that the application that generates the group traffic will handle the signaling between group members and the source. Hence this signaling is out of scope for the Xcast protocol. Xcast is intended for fixed networks. It may however be applied to MANETs since it is assumed that the frequent topology changes in a MANET will be handled by the installed MANET unicast routing protocol.

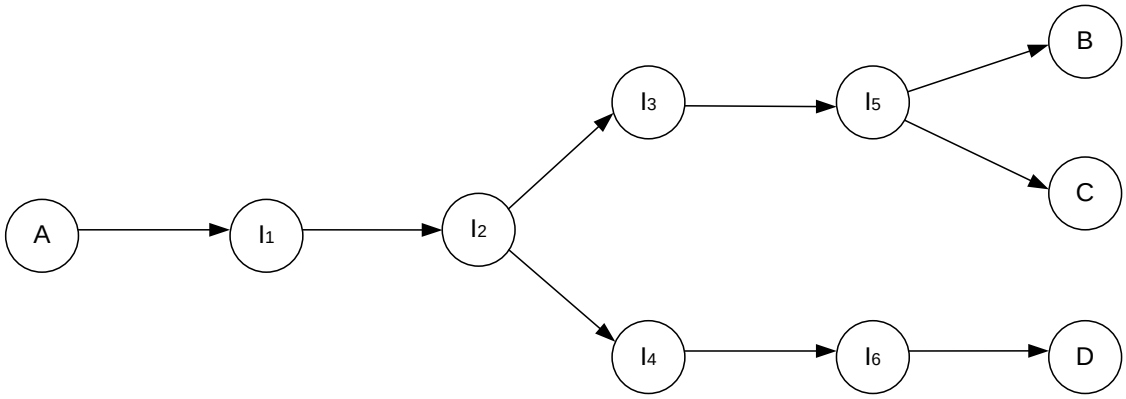

Figure 4.1 Xcast (from [5])

4.1.1.1 E^{2}M: Extended Explicit Multicast

E^{2}M [20] is a scheme for small group multicast which is built on top of Xcast. The goal is to support larger multicast groups. To achieve this, an Xcast Forwarder (XF) is introduced. As long as

the number of members in a session is small, the protocol works like Xcast. But when the number increases, a node may decide to become an XF for its down stream group members. The protocol uses the number of destination IDs in the received Xcast header and the corresponding number of next hop branches to make this decision. If a node N decides to be an XF it sends an XF_JOIN to the source including the list of destinations served by it, and a TTL, so that the source will know how many hops away the node is. If only one XF_JOIN is received, the source updates its eXplicitcast Forwarding Table (XFT), and from then on only includes node N in the extended packet header. In Figure 4.2 node N6 is chosen as the XF. To keep the source updated on the status of node Ns downstream neighbors, N periodically sends XF_JOINs including any such information. If more than one node with same next hop from the source sends an XF_JOIN, the source picks the node that is furthest away, or randomly if it is the same number of hops. E^2M does however support more than one XF per hop (hierarchical XFs). Different next hops will have different XFs. When an XF moves and, e.g., becomes part of a different path, as soon as the source learns this it gets the destination list from the XFT and includes this in the header, and removes the XF entry from the table.

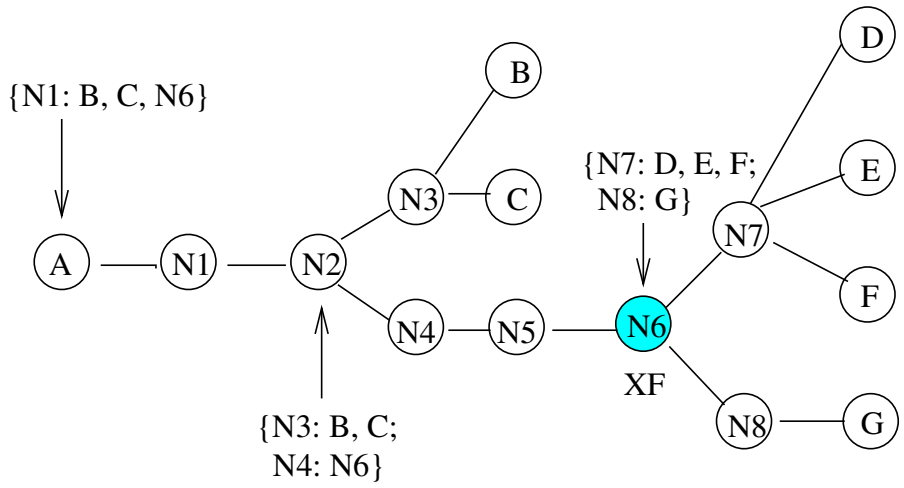

Figure 4.2 In this figure, node N6 is chosen as an Xcast Forwarder (XF) (from [20])

4.1.2 DDM: Differential Destination Multicast

DDM [28] is another protocol that uses stateless routing. It is unicast dependent, so it requires an underlying unicast protocol for unicast routing information, but it does not rely on a particular unicast routing protocol. In DDM the source controls the group memberships, and it encodes the destinations in the packet header. This is the stateless mode. DDM also has another mode: soft state. In the soft state mode next-hop information is cached, so that the protocol does not need to list all destinations in every packet header. When changes in routes or destinations occur, an upstream node needs to inform its next-hops regarding differences in the destination forwarding since the last packet. This state is only suitable if the number of groups is small, otherwise there would be too much state to cash. This mode is suited for applications which generate small data packets at a relatively high rate. The source acts as admission controller for the information it sends, and it

decides which JOINs it accepts, so it may dismiss a member if member control policy indicates that it should. No admission policies/security-related mechanisms are however addressed in [28]. When a node is interested in a multicast sessiob, it unicasts a JOIN to the source. If the JOIN is accepted, the source unicasts an ACK to the joiner. A node resends the JOIN if the node does not receive an ACK, using exponential back off. To refresh, the source periodically sets a poll flag in outgoing packets, and members then need to send a JOIN message to the source as a reply. Members may also send explicit leave messages to the source (max_leave_retry times to increase robustness).

4.2 Topological protocols

This section on topological protocols divides this large group of multicast protocols into two sub-groups; tree-based protocols and mesh-based protocols. The tree-based protocols aim to create a minimum distribution tree for the multicast group whereas the mesh-based protocols introduce some redundant links in the distribution trees to make the trees more robust with respect to topology changes.

4.2.1 Tree-based protocols

Tree-based protocols contain one path to each destination from a given source. With source specific trees, each source builds its own shortest path tree to reach its group members. When using a shared tree, one tree is shared by all sources with a single common root, a core-based tree (CBT) (or a rendezvous point tree). The multicast traffic travels from the source via the root and then down the tree, whilst for the source tree, the traffic travels directly to the receivers. In [32] the two approaches are compared in scenarios with multiple sources, and the authors conclude that while source specific trees can reduce network latency and possible congestion at the core, it requires the routers to make and maintain a large number of state entries. A shared tree reduces the number of entries, but having all group messages travelling via the core may then result in network latency and congestion at the core. An example of a protocol that makes use of source-based trees is the Adaptive Demand-Driven Distance-Vector Protocol (ADMR) [27], while the Multicast Ad Hoc On-Demand Distance-Vector Protocol (MAODV) [55] uses a shared tree.

4.2.1.1 ABAM: Associativity-based ad hoc multicast

ABAM [58] is an on-demand, tree-based, source-initiated multicast protocol. The tree is established primarily based on association stability. Association stability refers to spatial, temporal, connection and power stability of a node relative to its neighbors. A stable tree means less reconfiguration of the tree. Association stability results when the number of beacons received continuously from another node exceeds some predetermined value, taking into account signal strength and power life of neighboring nodes. The concept was introduced in the unicast protocol Associativity Based Routing (ABR) [57]. There are three phases in ABAM; Tree establishment, tree reconfiguration, and tree deletion. Since the protocol is source-initiated, a multicast session starts with the source broadcasting a query. Nodes receiving this query append their own address and information, like signal strength and power life, before rebroadcasting the query. Query messages are allowed to be forwarded more than once if the subsequent query promises a better quality route. Receivers collect

all messages for the groups they are interested in joining, and pick the most stable route back to the sender as their reply path. The source then uses the replies to compute the tree. It then sends out a setup message to the nodes in the tree, and these will from then on participate in multicast forwarding. Even if the protocol tries to compute as stable a tree as possible, there may still be need for some repairs due to node movement. ABAM has defined procedures for branch repair, subtree repair and full tree repair. If a receiver decides to leave the group, and if there are no other receivers on that branch, the tree will be pruned. If eventually all receivers leave the group, the tree is pruned incrementally. A source may also decide that it no longer wishes to be a sender and delete the tree. ABAM does not require an underlying unicast protocol, but it does require associativity information, and since this is implemented in ABR, ABR is used as underlying unicast protocol.

4.2.1.2 ADMR: Adaptive Demand-Driven Multicast Routing Protocol

ADMR [27] attempts to reduce non-on-demand components in the protocol. Multicast routing state is established dynamically, and only maintained for active groups and nodes situated between the senders and receivers. ADMR uses shortest-delay path to send multicast packets, which carry multicast forwarding state. This state is used by the forwarders to dynamically adapt to the sources' sending patterns to balance overhead and maintenance of routing state. ADMR supports both the traditional IP multicast service model and the source-specific service model. The protocol is tree-based, and rooted at the source. Only members of the tree forward packets, and only once per packet. Packets are not constrained to follow any particular branch or parent/child links during forwarding. The flood of a message constrained to the tree is referred to as a tree flood, and is similar to the forwarding group concept, used in, e.g., ODMRP, but is specific to each sender rather than the group; When a sender sends a multicast packet, it is flooded towards the receivers in the tree only. Each packet contains a sequence number, the hop count, the previous hop address, and the inter-packet time, which is the interval at which new packets should be expected from the sender. ADMR is designed to work independently of a unicast protocol, and may work with any or without one. If mobility is very high, a source may switch to flooding for a period.

4.2.1.3 AMRIS: Ad Hoc Multicast Routing protocol utilizing Increasing id-numberS

AMRIS [63] is an on-demand, shared-tree-based multicast protocol, which is designed to support multiple senders and receivers. AMRIS works independent of the underlying unicast routing protocol. A multicast session is initialized by the root, which is the node with the smallest ID (Sid). If there is a single sender, this node becomes the Sid. In cases where there is more than one sender, the Sid is elected among the senders. The other nodes then enter the initialization phase, and every node in the multicast session is dynamically assigned a session specific ID-number, which indicates its logical height in the tree. The number increases as the distance from the root increases, and this ordering is used to direct the multicast traffic. AMRIS maintains a *Neighbor-Status* table with existing neighbors and their IDs, and nodes use periodic beacons to signal their presence to neighboring nodes. Nodes that are not interested may still become part of the session when they are needed as intermediate nodes to forward traffic. AMRIS also has a *Branch Reconstruction* (BR) routine to deal with link breakages.

4.2.1.4 MAODV: Multicast AODV

MAODV [55] is a shared tree-based multicast protocol based on the Ad hoc On-Demand Distance Vector routing protocol (AODV) [54]. The group leader is responsible for initializing and maintaining the group sequence number, which is used to ensure freshness of routing information; Given multiple routes, a node will always choose the route with the largest sequence number. The number is periodically distributed to group members through broadcasted Group Hellos, which at the same time alerts other nodes of the existence of the group. A source node that wishes to join a group sends a route request (RREQ); either through unicast to the group leader if it knows the address due to having received group hello messages, or through a broadcast. Any node in the tree may respond to this request, and unicast a route reply (RREP) to the originator of the request. Nodes that are not members rebroadcast the RREQ. The source then unicasts a multicast activation (MACT) message to the next hop on the best route to activate that route. When link breaks occur, they are immediately repaired through RREQ, RREP and MACT messages. Similarly, if a node only wants to send a message to the group without joining, it sends a RREQ and any node on the tree may respond with a RREP. Nodes on the tree may leave the group only if they are leaf nodes.

4.2.1.5 MOLSR: Multicast OLSR

MOLSR [37] is a source-tree-based multicast protocol, which is an extension of the Optimized Link State Routing (OLSR) protocol [12]. It uses the topology knowledge of OLSR to build multicast trees. The trees provide the shortest route between a source and the multicast group members. All nodes in the network need not be multicast capable as long as those who are provide minimal connectivity between the sources and the group members. Sources periodically send a SOURCE_CLAIM message so that new members may join the tree, and each participant on the tree periodically sends a CONFIRM_PARENT message to its parent. When topology changes are detected the tree is updated. Nodes leave groups actively through sending a leave message, and by doing so they leave all trees associated with the group.

4.2.1.6 MZRP: Multicast Zone Routing Protocol

MZRP [65] is an extension of the Zone Routing Protocol (ZRP) [22]. It is a shared tree hybrid multicast protocol where multicast trees are created on demand whilst the multicast memberships for nodes are proactively maintained within their local routing zone. There are two types of nodes in a multicast tree: multicast forwarding nodes which forward packets and connect multicast members, and multicast group members. Multicast tree membership messages are broadcast within a node's local routing zone, so nodes keep track of groups and group members within their zone. If a node wants to join a multicast group, and it is already a forwarding node, it simply switches its status. If not, it sends a MRREQ; If it already has a route to any node on the tree, it sends a unicast MRREQ, if not, or if this fails, it sends a bordercast MRREQ via its bordercast tree. Reverse paths are established among the intermediate nodes. If all fails, the node becomes a group leader and starts broadcasting group leader messages to the whole network.

4.2.1.7 HiM-TORA: Hierarhical Multicast - Temporally-Ordered Routing Algorithm

HiM-TORA [50] is a hierarchical multicast routing protocol based on the unicast protocol TORA [53] and an autonomous clustering scheme. In this clustering scheme, the clusters are virtual nodes, and TORA is used to form a multicast tree consisting of these virtual nodes. Each virtual node is assigned a height with the source attaining the largest, and a decreasing height towards the leaf nodes. The spanning tree rooted at each cluster head is used to distribute the packets within each cluster. Clusters are classified into four categories; clusters that contain a source, clusters that contain a multicast member, clusters which multicast packets are forwarded via, and clusters in which no multicast packets are delivered to or from. The clusters hold a state which indicates the type of cluster. Each cluster is then regarded as an upper lever node in a hierarchical structure, and a multicast tree consisting of clusters that are related to the multicast session is formed. Nodes may change states due to movement, e.g., it may become necessary to elect a new cluster head. Also, if a node with cluster ID i finds itself surrounded by nodes with ID j, it switches ID to j. Each cluster is managed by a cluster head, which forms a spanning tree and collects information about the nodes. If a cluster is smaller than a threshold value L it merges with a neighboring cluster, and if it is larger than a threshold value U it splits into two clusters.

4.2.2 Mesh-based protocols

Mesh-based protocols are derived from tree-based protocols, but may provide more than one route for a packet to a destination. Because extra links are introduced in the multicast distribution tree, these protocols are more robust than the tree-based protocols with respect to topological changes. The disadvantages are more overhead due to redundant packet transmissions and also some extra control overhead.

4.2.2.1 CAMP: The Core-Assisted Mesh Protocol

In CAMP [19] a shared multicast mesh is defined for each group. The main goal of using meshes is to maintain connectivity with increasing mobility. Packets are forwarded along the reverse shortest path to the source, like in protocols based on source-based trees. CAMP assumes availability of routing information from a unicast protocol, and this protocol must provide correct distances to known destinations within a finite time. Join is receiver-initiated. CAMP uses cores to limit control traffic, and one or more cores can be defined for each mesh. Cores need not be part of the mesh. When a node wants to join, it sends a request towards a core. If no cores are reachable, it broadcasts the request in an expanding ring search. In the case where the node has neighbors that are duplex members of the group (i.e. will forward any multicast packet for the group) it can just announce its membership. Nodes that are directly attached to a multicast sender-only may join in simplex mode, which means that they only will act as relay for messages from this sender to the group, and not in the other direction. When there are no senders left attached to this node, it may leave again through advertising the change.

4.2.2.2 DCMP: Dynamic Core Based Multicast Routing Protocol

DCMP [15] is a source-initiated, on-demand multicast protocol which builds and maintains a shared mesh. This mesh is formed by a group of core-based trees. It is independent of any unicast protocol. The sources are classified into three categories; active, passive and core-active sources. The active sources flood join queries at regular intervals, while the core-active sources act as core for the passive sources, creating a shared mesh on behalf of these sources. The passive sources do not send join requests for creating the mesh, and they rely on the active sources to forward their data packets. Two parameters that decide the maximum number of passive sources supported by each core-active source and the maximum hop distance between a core-active source and a passive source are used to enhance the robustness of the mesh. When a source wants to send data it floods a join request which also indicates whether it can support more passive sources in order to avoid requests from nearby nodes that wish to change their status. Intermediate nodes store the ID number of the sending node and broadcast the packet if it is a non-duplicate request. The receiving node sends a reply packet along the reverse path. An intermediate node on the reverse path receiving the reply checks whether it is set as next node, and if so sets its status as forwarding node for this group. The intermediate node then builds a reply packet and broadcasts it. An active node may change its status to passive if the source sending the join request can support more passive nodes, the distance between the nodes is less than the maximum hop distance, and the node's ID is smaller than the sender's ID.

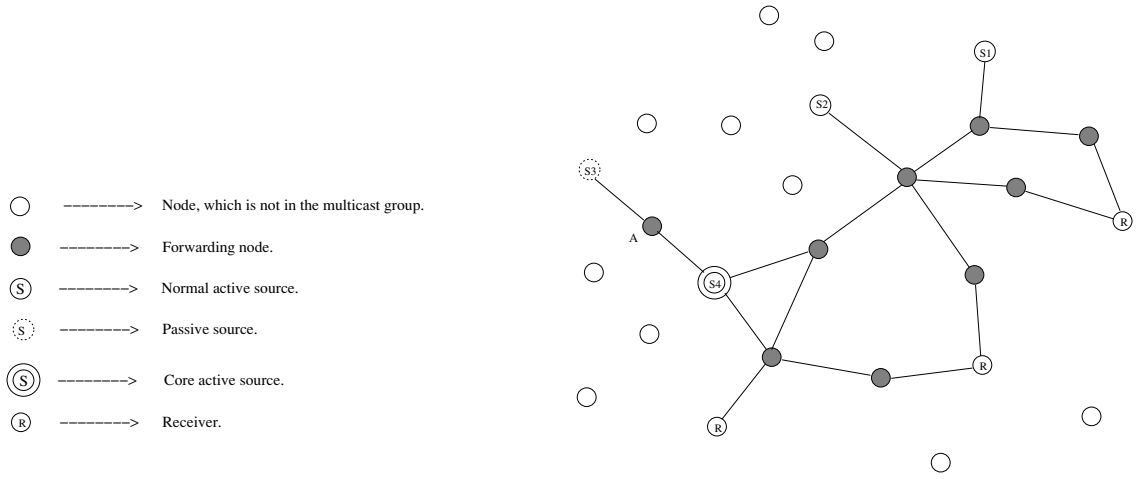

Figure 4.3 Mesh topology in DCMP (from [15])

4.2.2.3 ODMRP: On-Demand Multicast Routing Protocol

ODMRP [40] is a mesh-based, on-demand multicast protocol. Group memberships and routes are established and updated by the source reactively, with a request and reply phase. It is based on the forwarding group concept, that is, only a subset of nodes forwards the multicast packets via scoped flooding. ODMRP builds and maintains routes, and maintains group memberships on-demand. The protocol uses soft state so no explicit control packets need to be sent when a node wants to leave a group; If it is a source it stops sending Join Query packets, and if it is a receiver it does not send a Join Reply. ODMRP can coexist with any unicast routing protocol, and can also operate as a unicast

protocol, i.e., it does not require a separate unicast protocol. ODMRP initially used periodic join queries to maintain mesh structure when multicast sources have packets to send, but later developed passive clustering to avoid this for scalability in large networks with heavy loads. The protocol uses caching to detect duplicate packets. Routes are selected based on minimum delay, or on stability, when using mobility prediction. ODMRP is robust with respect to mobility, but produces a lot of control overhead. In evaluations of other protocols, ODMRP is often chosen as a protocol for comparison, and there also exists a lot of "improved ODMRP" protocols, a couple of which are described next. There are also hybrid protocols that use ideas from/parts of ODMRP, e.g. OPHMR, which will be described later.

ODMRP-MPR ODMRP-MPR [66] is a mesh-based on-demand multicast routing protocol based on ODMRP. The idea is to try to reduce the control overhead, obtain better scalability and resolve problems with unidirectional links through introducing Multipoint Relaying (MPR). The MPR-flooding is used in order to reduce the overhead incurred by the Join Query.

E-ODMRP: Enhanced ODMRP with Motion Adaptive Refresh ODMRP's robustness is owed to the periodic route refreshing, but if the refresh rate is too high this results in too much routing overhead, and if it is too low the protocol is unable to keep up with the topology changes. The idea behind E-ODMRP [49] is to let the refresh rate dynamically adapt to the environment.

4.2.2.4 PRIME: Protocol for Routing in Interest-defined Mesh Enclaves

PRIME [46] is an integrated framework for unicast and multicast routing in MANETs. The protocol is mesh-based, and the meshes are activated and deactivated based on whether there exists interest in destinations (unicast) and groups (multicast). The signaling overhead is mainly confined to these regions of interest. These enclaves are established reactively, and nodes proactively maintain routing information for destinations for which itself or other nodes in the region have interest. When a source becomes active, it piggybacks its first data packet in a Mesh Request (MR) packet, which is flooded. If a source sends more than one packet, a mesh spanning the active sources and the receivers is established. In the multicast case, the receivers elect a core for the group using mesh announcement (MA) packets. The elected core continues to send MAs periodically until there are no more active sources. Nodes use the information in the MAs to create neighborhood lists, and select one to three neighbors as next hops based on most recent (largest) sequence number and shortest distance to the destination. When the announcements stop, all routing information for the mesh is deleted. Nodes bundle MAs for different destinations/groups in order to reduce control traffic. This is done by waiting for a period when a routing event is detected, so that it is possible to aggregate other routing changes before transmitting the packet. The protocol allows for different delay periods depending on the urgency of the event.

4.2.2.5 OPHMR: Optimized Polymorphic Hybrid Multicast Routing Protocol

OPHMR [8] is a mesh-based, polymorphic multicast routing protocol that tries to combine the benefits of proactive and reactive behavior. It aims to maximize battery life, reduce communication delays, and improve deliverability, among other things. The backbone of OPHMR is based on ODMRP, which is responsible for its reactive behavior, and for the proactive behavior ZRP is used. In addition, OPHMR uses an optimized forwarding mechanism based on the MPR mechanism in OLSR; That is, only selected neighbors propagate control messages. The polymorphic algorithm is the main component of the protocol, and the polymorphic behavior is based on power levels and mobility; The nodes are in different behavioural modes depending on these factors; In Proactive Mode 1 (PM1) a node sends out periodic updates and uses received information to update its Neighbor Routing Table (NRT). Proactive Mode 2 (PM2) is similar to PM1 but periodic updates are sent at an interval longer than in PM1. In Reactive Mode (RM) periodic updates are sent and received updates are discarded. Finally, in Proactive Ready Mode (PRM) a node does not send updates but uses information received to update its NRT. The algorithm consists of two parts, the first, and main part, uses the node's power level to decide which mode to be in:

if $Power > Threshold1$ **then**
    if not in PM1, switch to PM1 and notify neighbors
else
    if $Power < Threshold2$ **then**
        if not in RM, switch to RM and notify neighbors
    else
        perform mobility routine

This is to make sure that the protocol only operates in its most proactive mode when power levels are high, and force it into reactive mode to save battery life when power levels are low. When the power level is between these two thresholds, it makes use of a mobility routine, which is the second part of the algorithm:

if $Mobility > MobilityThreshold$ **then**
    if $Power > Threshold2$ **then**
        if $Vicinity < VicinityThreshold$ **then**
            if not in PM2, switch to PM2 and notify neighbors
        else
            if not in PRM, switch to PRM and notify neighbors
else
    if not in RM, switch to RM and notify neighbors

In this part there are two considerations, the mobility level and the node density. When mobility is high, a proactive behavior is needed to keep up with the topology changes, but if the density is high, the proactive behavior may end up jamming the network. Therefore if the density is high, the node is set to be in PRM, and if not, in PM2. If a node wants to send a multicast message or join a multicast group, it sends a join request. Only nodes within that group may send join replies, and they need to update their multicast routing table. If the source or intermediate nodes have entries in

their neighbor table that belong to that group, they unicast the join request to those nodes. When the source node receives a join reply, it updates its multicast table and starts transmitting messages. The nodes also maintain a two-hop neighbor table and this is used to calculate the MPR information. Nodes broadcast their MPR information in the periodic updates. Only MPRs forward the updates.

4.3 Flooding-based protocols

Node mobility results in topology changes, and hence stale routes, so when the mobility is high, the cost of trying to maintain a multicast distribution structure quickly becomes very high. For such scenarios topology-based protocols become less suitable. The trade-offs between broadcast and multicast are studied in, e.g., [39], and [48] looks at flooding for reliable multicast with increasing mobility. The conclusion in [39] is that multicast is preferable in scenarios with low mobility and if less than 40% of the network nodes are members, while broadcast is preferable when mobility is high, and if more than 40% are members. The work in [39] has resulted in a hybrid multicast/broadcast protocol, which will be described in 4.3.3. In [48] the authors conclude that while flooding is a better alternative than traditional multicast with increasing mobility, even flooding is insufficient when mobility is very high, and points to more robust and persistent variations of flooding for better reliability. As shown in figure 2.2 flooding can result in a high number of network transmissions. Several mechanisms that aim to optimize the flooding process have been proposed. A basic flooding mechanism requires no network state information and no network signaling. As smart mechanisms are introduced, some state information and signaling are also needed to operate the flooding protocol. Optimized flooding protocols are also more vulnerable to mobility than the very robust basic flooding. In the following paragraph we summarize some of the mechanisms for optimized flooding.

Optimized flooding The simplest type of flooding is classical flooding (CF), where each node rebroadcasts each packet once. This requires duplicate packet detection (DPD), but there is, e.g., no dependence with respect to relay set algorithms[2] or neighborhood topology information. While CF is very robust with respect to delivery, with this type of forwarding there will often be a lot of redundancy, contention and collisions, especially in dense networks. This is referred to as the *broadcast storm problem* [47]. For these reasons, several methods for reducing the number of nodes that retransmit the packets have been developed. Some common methods of reducing the number of transmissions use neighbor knowledge. For instance, in Multipoint Relaying, a node has knowledge of its neighbors within a 2-hop radius. The node uses this knowledge to choose the set of 1-hop neighbors that cover its 2-hop neighbors most efficiently, as illustrated in Figure 4.4. The chosen nodes are called Multipoint Relays (MPRs). As mentioned in previous sections, there are also topology-based protocols that use MPRs to reduce the flooding of control traffic. Examples of use of MPRs are [42] and [10]. Another method, which is one of the schemes used in Simplified Multicast Forwarding (SMF), which will be described shortly, is E-CDS (Essential Connected Dominating Set).

[2]Cover set reduction techniques to optimize the flooding and relaying process

This scheme produces a common shared set of relay nodes for all nodes in the network. More details can be found in [41] which contains an evaluation of different CDS algorithms.

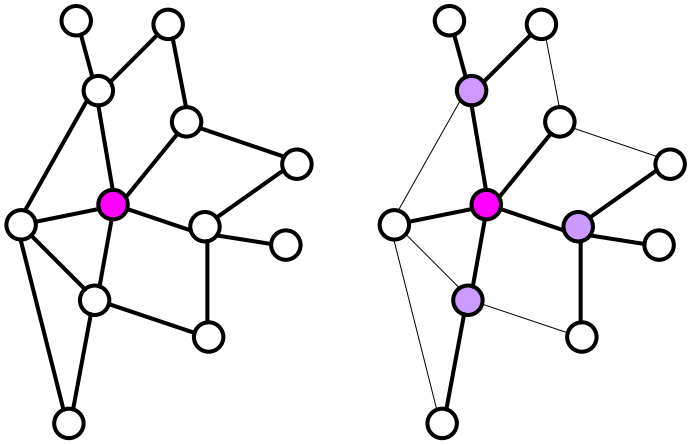

Figure 4.4 Reduced relay sets; The source's purple one-hop neighbors cover the source's two-hop neighbors.

There are also other mechanisms that can be used to optimize flooding. In [47], for instance, the authors suggest using probability to determine whether to retransmit or not. In the probabilistic scheme, a node will rebroadcast a packet with a predetermined probability. If the network is sparsely populated, the probability needs to be high, and if the network is densely populated, it needs to be low, so in this case some knowledge of the network topology is required. A different approach is a counter-based scheme, which uses a randomly chosen interval and the number of redundant packets received during that interval to decide whether to retransmit or not. It follows that in dense areas some nodes will not rebroadcast, and in sparsely populated areas all nodes may rebroadcast. Another approach described in [47] is a distance-based scheme, in which a node makes the decision of whether to rebroadcast or not based on the size of the additional area covered by a rebroadcast. The idea is to avoid rebroadcasting if this area is small, and it may, e.g., be based on distance from sending neighbor and redundant packets received. The method does not consider whether there actually are nodes in the area covered, only the size of the area. An overview of these and other methods can be found [62], which contains a survey of different broadcasting techniques as well as a study of a few protocols using different techniques. As already mentioned, CF is robust, but often results in too many redundant transmission. Reducing the number of relay nodes, on the other hand, will reduce the number of transmissions, but will at the same time make a protocol less robust. The evaluation of this trade-off, and choice of strategy, will depend on the specific scenario.

4.3.1 SMF: Simplified multicast forwarding

The motivation behind SMF [42] is to create a simple multicast service for a MANET type environment, and to provide an alternative multicast routing approach for small to moderate sized networks. The basic form of SMF uses classical flooding with duplicate detection. SMF also uses various known efficient flooding and relay set mechanisms to further reduce contention and congestion, e.g.

S-MPR, E-CDS [41]. The protocol has three styles of operation: Independent operation, where SMF performs its own relay set selection using information from an associated MANET Neighborhood Discovery Protocol (NHDP) process; operation with CDS-aware unicast routing protocol - a coexistent unicast routing protocol provides dynamic relay set state information based upon its own control plane CDS or neighborhood discovery information; and cross-layer operation, where SMF operates using neighborhood status and triggers from a cross-layer information base for dynamic relay set selection and maintenance (e.g., lower link layer).

Larsen et al. [38] analyze SMF with two of the forwarding mechanisms in the context of a tactical military network, and typical traffic in such a network, namely push-to-talk and Situational Awareness (SA)-data. The limitations of Source-based MPR (S-MPR) and Non-Source MPR (NS-MPR) is examined in this context, and the authors conclude that while S-MPR has problems with mobility, but is efficient in high load networks, NS-MPR is more robust, but creates congestion with higher loads. A combination of S-MPR and NS-MPR using a radio load metric is proposed, so that instead of deciding on the forwarding mechanism in advance, the two can be combined dynamically. The radio load metric is based on the medium time that all packets either received or transmitted occupies relative to the total time of measurement. When the radio load is low, the cost of using NS-MPR is low, and as the load increases it is better to switch to S-MPR. The radio load metric can be used to decide which algorithm to employ. The paper also suggests a preemptive switch to S-MPR for SA traffic when push-to-talk traffic is in the network, due to that the SA traffic was shown to affect the goodput of the push-to-talk traffic.

4.3.2 SMOLSR: Simple Multicast OLSR

SMOLSR [6] is a multicast protocol based on OLSR [12]. Unlike for MOLSR (section 4.2.1.5), no multicast tree is built. Data is flooded to the entire network using MPRs to reduce the number of retransmissions required to reach all nodes in the network. A packet is forwarded if and only if it is received for the first time and the node belongs to the senders MPR set. This is similar to SMF with MPR. According to the authors of [6] this protocol is suited for large, dense networks were traffic is random and sporadic between several, uniformly distributed nodes, rather than a small, specific group of nodes, where MOLSR is better suited.

4.3.3 Fireworks

Fireworks [39] is a two-tiered hybrid multicast/broadcast protocol that aims to combine the advantages of both routing strategies in order to be able to adapt better to a dynamic network. It creates and maintains a multicast backbone that connects pockets of broadcast distribution areas. A cohort is a densely populated area. One of the members is chosen as cohort leader. Cohort leaders establish a multicast tree that includes themselves and the source (the upper tier), and uses adaptive scope broadcasting to deliver messages to the other cohort members (lower tier) (see Figure 4.5). In the construction of this structure, a node that wants to join discovers the cohort and the cohort leader in the k-hop. If there is no cohort leader, there is a decision phase to elect leader. In the scenario that all the multicast group members are isolated, Fireworks is reduced to a pure multicast

scheme. The multicast source periodically sends out SOURCE-QUERY messages containing its *address* and *mcast-group*, which intermediate nodes forward once and set up the routing pointers back to the source. Cohort leaders that receive these broadcasts, unicast a reply back to the source via the route established when the intermediate nodes forwarded the SOURCE-QUERY message. The source then sends multicast packets to the cohort leaders via the tree constructed through coalescing the reverse paths. Within a cohort, the leader broadcasts these multicast packets. If the distance d to the member the furthest away from the cohort leader is smaller than k, the broadcast scope is reduced to d, in order to avoid unnecessary transmissions. Nodes that are cohort members periodically unicast CHILD messages to their leader to indicate their presence. If a cohort member wants to leave, it simply stops advertising that it is a CHILD to its cohort leader. A cohort leader similarly stops sending LEADER messages when it decides to leave. The cohort members will then either discover a new cohort with a leader, or invoke the discovery and election processes again. The multicast structure is maintained/refreshed through periodic exchanges of query-reply messages, initiated by the source.

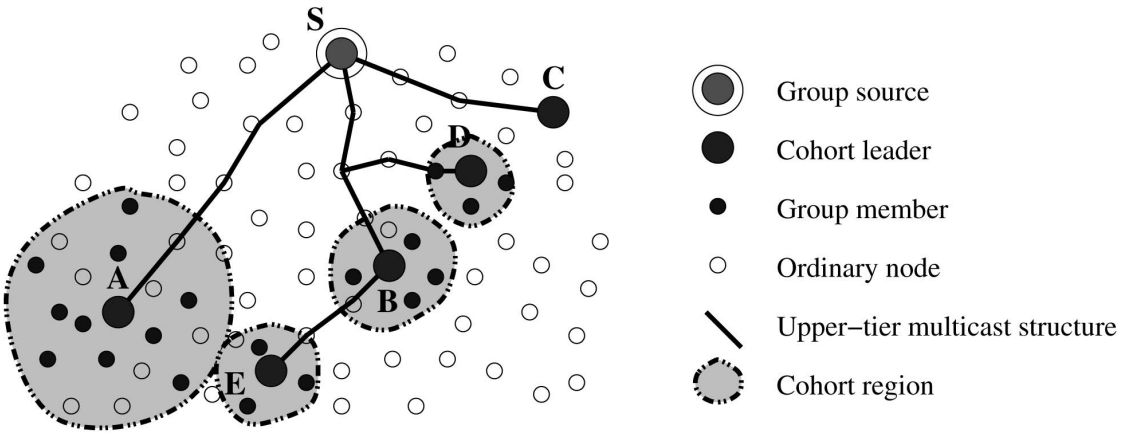

Figure 4.5 Fireworks structure (from [39])

4.4 Geographic protocols

As previously mentioned, there may be situations where there is a need to spread information to anyone residing within a particular geographic area, e.g., in the scenario with the gas alarm. In such situations variations of multicast schemes such as position-based multicast, or flooding-based multicast, called geocast, may be a good choice. In geocast, messages are delivered using flooding to an implicitly defined group referred to as the geocast region. The simplest approach is flooding with duplicate detection. To limit the flooding, a forwarding zone is defined, and all nodes residing outside this zone will drop the messages. Position-based multicast schemes comes in different forms, some use local information only to make forwarding decisions, others have some structure with explicit group memberships. Most geograghic protocols assume GPS, while some handle that the occasional node is unaware of its position through some recovery strategy.

4.4.1 RSGM: Robust and Scalable Geographic Multicast Protocol for Mobile Ad Hoc Networks

RSGM [64] is a zone-based routing scheme using position information. It assumes that all participating nodes have knowledge of their position. The zones are defined as geographic squares. The scheme consists of a two-tier membership management and forwarding structure. A zone structure based on position information is built at the lower tier. If a zone at this tier has members, a zone leader is elected on-demand. Zone memberships are explicit. The leader manages the group memberships and collects the positions of the members in its zone. The zone memberships are then reported to the sources by the zone leader at the upper tier. Packets from the sources are forwarded to the group members through the zone leader. The source only needs to keep track of the zones. The zone leader notifies the source when a zone no longer has members. Control messages are aggregated to reduce overhead, e.g., a zone leader hears a report message from a downstream neighbor, and aggregates this report with its own report before it is sent towards the source. The forwarding thus follows a tree-structure without there being a need to maintain such a structure. For each hop geographic greedy forwarding is used [30]. When next-hops have been decided, the packet is unicast by the source over each hop together with a list of destination zones that must be reached through that hop. Intermediate nodes that do not belong to a zone in the list forward in a similar manner. If a zone leader receives a packet destined for its zone, it replaces the zone ID in the packet destination list with a list of the zone members, and if a group member that is not the leader received the message it replaces the zone ID with its zone leader. The message is then forwarded using the same strategy.

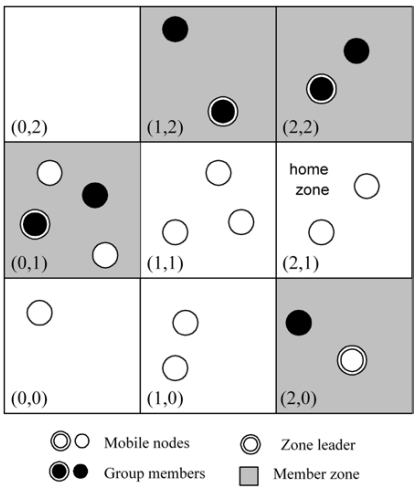

Figure 4.6 The zone structure (from [64])

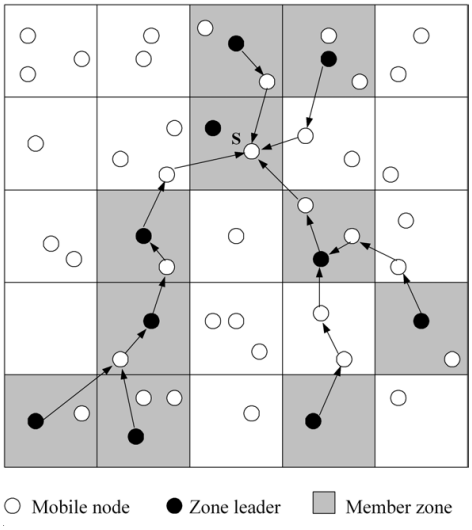

Figure 4.7 The aggregation of report messages (from [64])

4.4.2 SPBM: Scalable Position-Based Multicast

SPBM [59] uses geographic position of nodes. It bases the forwarding decision on whether or not there are group members located in a given direction. The protocol allows for hierarchical aggregation of membership information, and for this purpose the network is divided into a quadtree (see Figure 4.8).

The membership update mechanism aims to provide each node in the ad-hoc network with an aggregated view of the position of group members. For this purpose, each node maintains a global member table containing entries for the three neighboring squares for each level from level 0 up to level (L - 1). In addition, each node has a local member table for nodes located in the same level-0 square. Each entry in the global member table consists of the square's identifier and the aggregated membership information for all nodes in that square. A node indicates its group membership status by broadcasting announce messages within its level-0 square (i.e., to its direct neighbors). Update messages are then used to provide all nodes that are located in a level-1 square with the aggregated membership information for the four level-0 squares contained in the level-1 square. This is done by periodically selecting one node in each level-0 square. The same process is used for higher levels.

The protocol does not require maintenance of a distribution structure, nor does it use flooding. This forwarding scheme is a generalization of position-based unicast routing; A forwarding node selects one of its neighbors as next hop such that the packet makes progress towards the destination. In the case that a node does not have such a neighbor, even if there may exist a route to the destination, a recovery strategy is used. The most important characteristic of position-based routing is that forwarding decisions are based on local knowledge only; there is no need for a global route. This makes this type of protocols regarded as scalable and robust with respect to topological changes.

If a forwarding node does not find a next hop that yields geographic progress, a recovery strategy is employed. For this, SPBM uses a distributed planarization of the network graph in combination with the right hand rule. The algorithm first planarizes the surrounding network graph. The node then determines the angles between the lines drawn from the node to each of the neighbors, and the line drawn from the node to the destination. The packet is sent to the neighbor which position makes the smallest angle. This destination is marked as a *recovery destination*, and the current position is stored in the packet to indicate where the recovery mechanism started. The next hop checks if it is closer than the recovery starting point, if not, the recovery step is repeated, else, the protocol returns to the normal forwarding procedure.

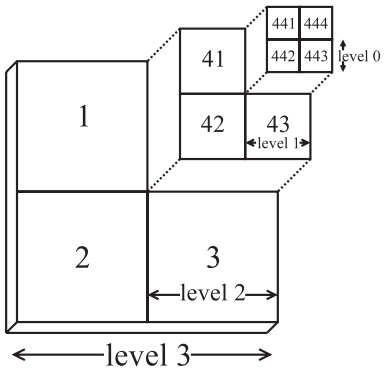

Figure 4.8 The network as a quadtree [59]

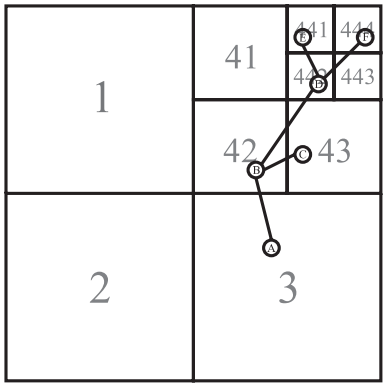

Figure 4.9 Forwarding on the quadtree [59]

4.4.3 Flooding-based geocast

In [33] three geocast protocols are proposed which attempt to utilize physical location to reduce overhead. A geocast message is delivered to the set of nodes within a specified geographical area. The geocast group is implicitly defined as the set of nodes within the specified area. The specified area is referred to as the geocast region, and the set of nodes in the geocast region forms the geocast group. If a node is inside the geocast region it is automatically a member of the corresponding geocast group. To determine group memberships, each node is required to know its own physical location. The forwarding zone is defined as a rectangular shape, which is the smallest that contains both the source and the geocast region, and may be identical to the geocast region, or larger. The first scheme uses a static forwarding zone. The forwarding zone (the coordinates of the four corners) is set by the source node and not modified along the way (see Figure 4.10).

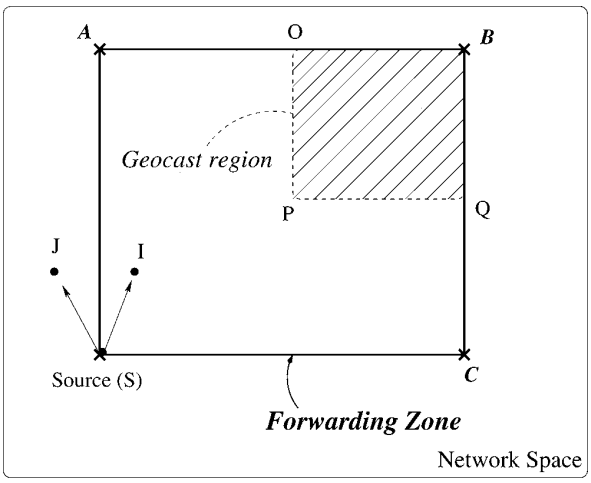

Figure 4.10 Forwarding zone and geocast region for static zone scheme with source outside geocast region (from [33])

The second protocol is an adaptive scheme in which intermediate nodes redefine the forwarding zone in the same manner as the source, and the goal is to reduce the forwarding zone along the way and thereby reduce overhead. Depending on the topology this may work, or it could result in none of the geocast group members receiving the packets. To avoid the latter, the scheme is modified with one-hop-flooding, which works as follows: if a node's forwarding zone contains at least one one-hop neighbor, it forwards the packet containing the adapted forwarding zone to its neighbors, if not, the node performs one-hop flooding with the forwarding zone set to the whole network so that every neighbor will consider itself a member of the node's forwarding zone.

The third protocol is the adaptive distance scheme. In this scheme the source node includes 1) the geocast region, 2) the location of the geometrical centre of the geocast region, and 3) the coordinates of the source. Upon receiving a packet, a node first checks if it is in the geocast region, if so it accepts the packet. If the source's distance to the geometrical centre is larger than or equal to the distance from the receiving node to the geometrical centre, the receiving node forwards the packet and replaces the source coordinates with its own. If not, the receiving node checks if the source is within the geocast region, and if it is, the packet is forwarded, otherwise it is dropped. Like the adaptive zone scheme without the one-hop-flooding, there is no guarantee that the packet will reach the geocast members.

4.4.4 Geoflood

Geoflood [1] is an optimized flooding protocol where the protocol tries to deliver a multicast packet to all nodes in the network with less overhead than a basic flooding protocol. A range of optimized flooding protocols are discussed in Section 4.3. Geoflood is described here since it requires knowledge of its own geographic position to carry out the optimization. The nodes each define a Cartesian plane with their own location as the origin, and use the four quadrants (NE, NW, SE, SW) to decide whether to forward a packet or not. Each message contains a location field which is updated at each forwarding node. The forwarding decision is based on these steps 1) if a node receives a packet it has forwarded before, the packet is dropped; 2) when a node receives a packet for the first time it notes the quadrant the message was received from and waits for time t, and if the packet arrives from all four quadrants before the time t has passed, the packet is dropped, otherwise it is forwarded after time t has passed. If a node is unaware of its location it will forward a packet it receives immediately with an empty location field, and a location-aware node that receives such a message will not assign the message to any quadrant. Nodes that are the furthest away from the sender should have the smallest waiting time t, while nodes close to the sender should wait the longest. The algorithm assumes that nodes are able to discern their own location, but does not require that they know the location of their neighbors. Although this is not strictly required for *all* nodes to know their location, the bandwidth overhead savings increase with the number of location-aware nodes.

4.4.5 GMZRP: Geography-aided Multicast Zone Routing Protocol in Mobile Ad Hoc Networks

GMZRP [9] is a hybrid multicast protocol which aims to combine the advantages of topological and geographical routing, and is inspired by the unicast protocol ZRP [22]. GMZRP extends the route discovery procedure in ZRP to a multicast tree discovery procedure and also optimizes the flooding of the multicast route request (MRREQ), and aggregate the resulting route replies (RREP). GMZRP optimizes the flooding process by partitioning the network into small zones, and it guarantees that each geographical zone is queried only once. The protocol operates on-demand and utilizes geographic partitioning to reduce route discovery overhead. GMZRP maintains a multicast forwarding tree at two levels; the sequential geographic zones the tree spans, and the sequential nodes the tree spans hop-by-hop. While circles overlap, the zones are hexagons inside circles, so that there is coverage without overlapping zones. Each zone has unique ID, and six neighboring zones.

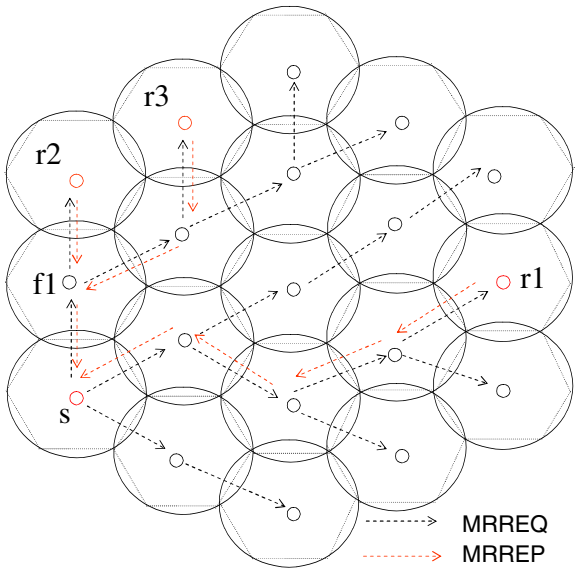

Figure 4.11 This figure shows an example of flooding of MRREQ and the corresponding RREP (from [9])

GMZRP is independent of geographic unicast protocols, and can work over any such protocol. Figure 4.11 shows the propagation of a multicast route request from a source s to a multicast group G={r1, r2, r3} and the reverse multicast route reply. The MRREQ packets reach all the three receivers along the shortest paths determined by the proposed strategy. Once a receiver receives a MRREQ packet, it replies a MRREP packet back to the source along the reverse route, which is also the shortest path. Since both r2 and r3 will receive MRREQ packets forwarded from the zone of f1, these will generate the same MRREP packets. To reduce overhead, f1 then only forwards one MRREP packet to the source.

4.5 Summary

This section has given an overview of a number of different protocols that aim to solve group communication in mobile ad hoc networks. These protocols may be divided into topological, stateless, flooding-based and geographic protocols. It is clear that no single protocol will solve all situations efficiently, but a particular type of protocol may be better suited for a certain class of scenarios. In the next section we therefore categorize our vignettes according to some key factors, and see how well the different classes of protocols may be suited for these cases. The goal is not to single out one particular protocol, but to try to narrow down the range of protocols to those that may be suitable in a mobile military network. Table 4.1 shows an overview of the protocols presented in this section. The table includes type of protocol, level of overhead incurred, dependence on underlying unicast protocol, and the main motivation behind the protocol design.

Table 4.1 Protocol overview

Protocols				
Protocol	**Type**	**Control overhead**[1]	**Unicast dependence**	**Motivation**
ABAM: Assiciativity-based ad hoc mulicast	source-tree	high	no	use association stability to try to create a more stable tree
ADMR: Adaptive Demand-Driven Multicast Routing Protocol	source-tree	high	no	minimize proactive components to reduce overhead
AMRIS: Ad Hoc Multicast Routing protocol utilizing Increasing id-numberS	shared-tree	high	no	use ordering of session-specific member ids to direct the multicast flow
CAMP: The Core-Assisted Mesh Protocol	mesh	high	yes	uses cores to limit control traffic
DCMP: Dynamic Core Based Multicast Protocol	mesh	high	no	reduce overhead through classifying sources as active or passive
DDM: Differential Destination Multicast	stateless/soft state	low	yes	soft state mode - cash next-hop info to reduce header size
E^2M: Extended Explicit Multicast	stateless	low	yes	extend xcast to support larger groups
E-ODMRP: Enhanced ODMRP with Motion Adaptive Refresh	mesh	high	no	reduce overhead through dynamic adaption of refresh rate
Fireworks	source-tree/flooding	high/low	no	adapt to network dynamics, exploiting the trade-offs between broadcast and multicast
Flooding-based geocast	geographic	low	no	utilize physical location information to decrease overhead of geocast delivery
Geoflood	geographic	low	no	reduce bandwidth overhead through limiting broadcasts
GMZRP: Geography-aided Multicast Zone Routing Protocol in MANETs	geographic/source-tree	high	no	utilize geographic partition to reduce route discovery overhead
HiM-TORA: Hierarhical Multicast - Temporally-Ordered Routing Algorithm	source-tree	high	yes[2]	use autonomous clustering to realize reliable packet delivery
MAODV: Multicast Ad hoc On-Demand Distance Vector routing algorithm	shared-tree	high	yes[2]	extend AODV with multicast capability
MOLSR: Multicast Optimized Link State Routing	source-tree	high	yes[2]	use OLSR topology information to build multicast trees
MZRP: Multicast Zone Routing Protocol	shared-tree	high	yes[2]	scale to large numbers of senders and groups
ODMRP: On-Demand Multicast Routing Protocol	mesh	high	no	only subset of nodes forward via scoped flooding
ODMRP-MPR: ODMRP with Multipoint Relays	mesh	high	no	reduce control overhead using MPR-technique from OLSR
OPHMR: Optimized Polymorphic Hybrid Multicast Routing Protocol	mesh	high	no	improve various metrics through exploiting reactive/proactive benefits using power, mobility and vicinity density awareness
PRIME: Protocol for Routing in Interest-defined Mesh Enclaves	mesh	high	no	reduce overhead through confining signaling to active regions of interest
RSGM: Robust and Scalable Geographic Multicast Protocol for MANETs	geographic	low	no	scale for larger group/network, robust forwarding wrt topology changes
SMF: Simplified Multicast Forwarding	flooding-based	low	no	provide a simple multicast forwarding mechanism using efficient flooding
SMOLSR: Simple Multicast Optimized Link State Routing	flooding-based	low	yes[2]	uses flooding via MPR
SPBM: Scalable Position-Based Multicast	geographic	low	no	scalability, robust forwarding wrt topology changes
XCAST: Explicit Multicast	stateless	low	yes	support a large number of small multicast sessions

[1] As it is difficult to quantify the level of overhead more specifically, we decided to distinguish between those that generate little overhead and those that may produce a lot more overhead, as this is the most important distinction.

[2] Extends/based on unicast, or uses information from unicast protocol

5 Discussion

The previous section outlined a wide variety of protocols that each has a different approach to solving group communication. Protocols designed for group communication in mobile ad hoc networks have for the most part been evaluated using network simulators. Very few run actual real life experiments, and most evaluations only cover a few protocols. There are also multiple issues with how simulations to evaluate protocols in such networks are performed. In effect, the type of scenario used bears very little resemblance to a military scenario (or any other real life scenario). The question was then how to evaluate the suitability of the various protocols, which is why we decided to define a series of vignettes that would give us both a better understanding of the tactical needs and some requirement characteristics to study the protocols in relation to. Section 3 describes a typical network situation, with vignettes illustrating information exchange needs where using group communication would be favorable. Our focus has been to look at the protocols' operation for distribution against the type of network we have and the information exchange needs that exist. First we will give a brief account of some of the issues with regards to simulations; a discussion then follows where we look at the properties of the different types of protocols against key factors in the vignettes.

5.1 Evaluating protocols/simulation issues

Using network simulators has a lot of advantages. It is less costly than experiments, it is possible to run simulations with similar conditions several times, and to change one variable at a time. The problem is that the conditions most often used do not have much resemblance to what the realistic conditions might be. A common simulation scenario typically involves nodes that move according to a random mobility model and with a uniform traffic pattern. Although using mobility models that attempt to model real life behavior, e.g., [39], is becoming more popular, most use the Random waypoint (RWP) model [7]. Studies, e.g., [25] [26], have shown that the choice of mobility model has a great impact on the performance of a protocol. This has also been shown to be the case for traffic models. Simulations are often run with constant bit rate (CBR) traffic flows, which is traffic generated according to a deterministic rate, and where packets are of constant size. Karpinski et al. [31] show that the relative performance of protocols can be inverted when changing from a simplistic traffic model such as CBR to using real traffic.

How a protocol behaves during a simulation, or in a controlled indoor environment, may also differ from its behavior in an uncontrolled outdoor environment. For instance, in an outdoor environment there may be obstacles in the terrain that prevents two nodes from communicating even if they are within a distance where they normally would be able to communicate. Gray et al. [21] addressed this issue and found that the performance in packet delivery ratio yielded opposite results when switching from indoors to outdoors.

A survey concerning the use of simulations to evaluate MANET protocols [35] also points out several shortcomings relating to issues such as the simulation setup, execution, and output analysis. Table A.1 shows an overview of the simulation environments used in relation to the protocols in the

survey part of this report. There is still no "benchmark scenario" in use, so no two simulations are the same. For instance, some of the protocols have only been evaluated using one source, and with a fixed group size, while for other protocols it has been taken into account that varying these may affect the results. Hence it is difficult to compare the different results.

Another issue with respect to previous research is that a lot of it has been done in civilian settings with typically much higher bit rates than what is usually the case in a military setting, where bandwidth may be scarce and fluctuating. For these reasons, there is no proper basis for comparing all the different protocols. We therefore needed to take a different approach to evaluating the various protocols, which resulted in creating a series of vignettes and extracting some key factors. In the next section we look at the properties of the different types of protocols against these factors.

5.2 Evaluation of protocols in relation to the vignettes

In Section 3 we presented the vignettes we have created for this study. The purpose of creating these vignettes was twofold: To get a better understanding of the need for group communication in mobile military networks, and to identify the range of network parameters that might best define group communication in military networks. The latter gives us something to use to evaluate the surveyed protocols. The vignettes represent a more realistic environment than most of the discussed simulation scenarios, while at the same time limiting the infinitely large choice of network parameters (i.e., network topologies, mobility models, traffic load, etc.) to a smaller number.

In our study of the efficiency of the protocol types, the goal has not been to decide on a particular protocol, but rather to try to narrow down the range of protocols, and see if there are certain types of protocols that are more relevant in a military setting. In order to do so, we have looked at the properties of the different types of protocols, against key factors in the vignettes. The efficiency of the protocols is influenced by factors such as node mobility, network topology, group size, group-member density, and traffic characteristics. We define the performance of the protocols in terms of fairness and goodput. With goodput we mean the percentage of received packets relative to transmitted packet for a flow. With fairness we mean that all group members should have almost equal goodput.

In the vignette series described in Section 3 there is always a possibility of high mobility, due to moving vehicles, although there will also sometimes be groups of vehicles moving together, and hence not necessarily always high relative mobility between all of the nodes. The group size varies in the different vignettes, from potentially large, ie., several companies, to small groups, such as in the Medevac situation (Figure 3.8). The node density also varies; in the Medevac situation the density is initially sparse, whereas the vignette with friendly force tracking (Figure 3.5) represents a network where the group member density is high. The different vignettes also represent a wide variety of traffic patterns, from regular position updates, via push-to-talk, that may have preplanned group memberships or not, to sudden alerts. When it comes to the number of sources, there is a range of situations from a single source, to every member of the group being sources. The key factors of the vignettes are summarized in Table 5.1

	Group density	Group size	# of sources	Max mobility	Packet size	Traffic load	Geography important?
Friendly force tracking	dense	large	many (all)	high	small	low	yes
MEDEVAC	sparse/dense	small	several (all)	high	small-medium	low	yes
Gas alarm	dense	potentially large	1-few	high	small-medium	low	yes
Artillery	dense	variable	1	high	small	low	yes
Push-to-talk	sparse/dense	small	1-few (all)	high	small	high	yes
Plans/orders	sparse/dense	small-medium	1	high	large	high	no

Table 5.1 Key factors in the military vignettes

Mobility In our study of the various protocol groups against the vignettes, we start with a look at the protocols robustness to mobility. More precisely we study the protocols robustness to changes in the network topology. We call this section for mobility since most network topology changes come as a result of node mobility. However, topology changes might also come in stationary situation due to varying channel conditions, and some group mobility might not result in any topological changes. A group communication protocol is robust to mobility if it is able to provide high goodput and good fairness in networks with a lot of topology changes.

As we can see from Table 5.1 mobility may be high for all vignettes. If we recall from the previous section, the various protocol types are optimized for different levels of mobility. For instance, the minimum distribution tree of a tree-based protocol makes it vulnerable to high mobility. For tree-based protocols it therefore becomes costly and difficult to build and maintain multicast trees that have high goodput for these cases. Mesh-based protocols try to improve the performance during high mobility through introducing redundant links in the distribution trees to make the trees more robust. The level of redundancy in these protocols determine the protocols robustness.

The extent to which a stateless protocol handles mobility, depends on how well the underlying unicast protocol handles mobility. The level can therefore not be assumed to be very high.

With geographic protocols, since decisions are made en route hop-by-hop, the protocols are in some respect robust to mobility. On the other hand, mobility also means that the recipients' location may become outdated. As such, position-based protocols may not be such good choice. Flooding-based geographic protocols may perform better, as the goal of these protocols is to reach a geographic region, but the destination nodes may still have moved away from the target area.

Flooding-based protocols are in general the most robust with respect to mobility. It must however also be noted that as smart mechanisms are introduced to make the flooding more efficient, these protocols become more vulnerable to mobility. The choices of mechanism used to implement efficient flooding will therefore be of importance.

Multicast member density If we look at Table 5.1, we see that in our vignettes we have networks where the groups are either large and dense, or we have small groups that may be sparse or dense.

Stateless protocols are designed for small groups, that may be sparsely distributed in the network, and may hence be suitable in cases such at the Medevac situation. Flooding-based protocols do well in networks where the group member density is high, while they incur too many redundant transmissions when the group member density is sparse. Protocols based on flooding may therefore be suitable in the situation with friendly force tracking. Topological protocols are very efficient both for dense and sparse networks, as long as the traffic load is high relative to the signaling overhead and the mobility is low. These protocols are expensive for small, sparse groups. This is even more true for mesh-based protocols, than for tree-based. Geographic protocols will work better with dense groups. Figure 5.1 shows a summary of the above factors in relation to the various protocol types.

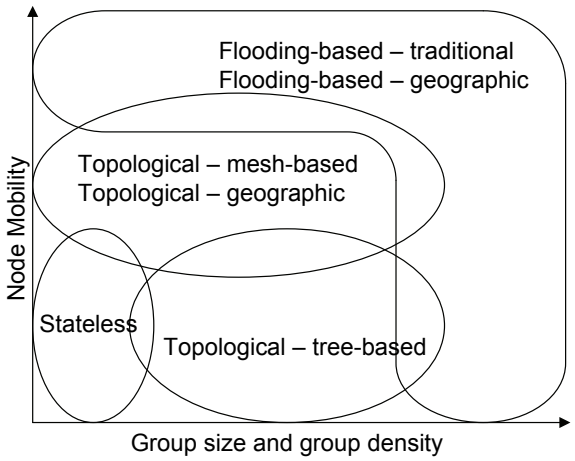

Figure 5.1 Protocols vs. mobility and group size and density

Packet size and traffic load When it comes to packet size, this varies in our vignettes, but the packets will often be small in mobile military networks. In particular, we therefore need to consider stateless protocols. As mentioned in Section 4.1 the overhead associated with stateless protocols is the size of the list of group recipients in the header of the multicast data-packet. The overhead for these protocols is therefore high for small data packets. In the Medevac and Push-to-talk vignettes (Figures 3.8 and 3.4, where the stateless approach may seem as a good choice, the packet size will in general be small. Therefore, even though these are protocols suited for small groups, they may still not be such a good choice after all. In [28] the stateless protocol also has a soft state mode where the destinations do not have to be listed in every single packet, and may therefore be suitable for applications that generate small packets at a high rate, such as voice over IP.

The other protocol groups are not directly influenced by packet size, but one needs to consider the traffic load. If the traffic load is low, maintaining a multicast distribution tree becomes expensive. The traffic load is in most of our vignettes low, apart from push-to-talk and distribution of plans and orders. Although the load will be a function of the number of sources, we consider it to be low in the friendly force tracking situation; in addition to very small packets, the update intervals will be relatively long, and there will likely be aggregation of messages. Plans/orders generate the heaviest

load, but these are also not distributed very often.

Importance of location In several of the situations we find that geographic position is important, either explicitly or due to proximity. For instance, in a case such as the artillery attack (Figure 3.7), information needs to be sent to troops in a certain geographic area, but not in proximity relative to the source. In the vignette with the gas alarm, the troops' proximity relative to the node that discovers the gas matters. Geographic protocols allow multicast groups to be defined based on their geographic position. Multicast scope can be defined as an area on a map. This functionality is not available in any of the other group protocols discussed in the report. Some variation of a geographic protocol may therefore be suited for situations where geography matters. The advantage of geographic protocols is that they can adapt to changes en route and are hence robust to rapid topological changes (mobility). A problem with geographic protocols is that there is a risk of reaching a dead-end (local minimum). There exist different strategies to work around this, but there is still no guarantee that the packet will reach the destination. As already mentioned, mobility also means that the recipients' location may become outdated. In the case of proximity, another option is a flooding-based protocol. Also, if we have friendly force tracking, position could be translated to address, and as such sent to relevant destinations, if this information is relatively fresh.

Overhead There are different types of overhead associated with group communication protocols, e.g., overhead from signaling traffic needed to maintain the multicast distribution tree, and overhead due to redundant transmission of the multicast data. This overhead incurs an extra load on the transport network, and must be much lower than the gain available with group communication compared with unicast distribution.

While tree-based protocols, which build a minimum spanning tree for multicast distribution, are the most bandwidth efficient, this also makes them very vulnerable to topology changes. The extra robustness of the mesh-based protocols relative to tree-based protocols on the other hand also means more overhead due to redundant packet transmissions and also extra control overhead. Both groups of topological protocols require a lot of state information to be maintained.

Stateless protocols use the underlying unicast information, so since there is no need to maintain an additional multicast distribution structure, no extra signaling for the sake of multicast has to occur. The overhead associated with these protocols is the size of the list of recipients in the header of each multicast data-packet.

A basic flooding mechanism requires no network state information and no network signaling, but may result in a high number of redundant network transmissions. This overhead is largest for sparse multicast member densities. As smart mechanisms are introduced to make the flooding protocol more efficient (reduce the overhead due to redundant packet transmissions), some state information and signaling are also needed to operate the flooding protocol, in the form of local (one-hop) signaling to identify a subset of a node's neighbors to do multicast forwarding. Often this local signaling can be shared with the underlying unicast routing protocol (e.g, OLSR's S-MPR and OSPF's CDS

[43]). Optimized flooding is hence not suited for sparse multicast groups, but is very efficient for dense multicast groups.

Geographic protocols in general require no extra control overhead, as there is no route discovery or maintenance, only use of neighborhood knowledge. The control overhead for geographic protocols is mainly related to management. In a military setting, knowing each others positions is something that will already be in place, and as such it may be regarded as not part of the protocol overhead alone. Some overhead may incur for geographic protocols if they, for instance, encounter a local minimum, and need to execute a recovery strategy, which, e.g., could make use of flooding, or discovery of an alternative route cannot be made in time. In such cases the goodput for geographic protocols will temporarily be reduced.

6 Concluding remarks

While there may be a need for more than one solution to meet the needs for group communication in a tactical setting, there are certain types of protocols that seem the better fits. As has also been concluded by others [61], we find that an efficient flooding-based protocol may be best suited for many group applications in mobile military networks. Flooding-based protocols are able to support high goodput and fairness in networks with high mobility, incur little control overhead, and are suitable for large, dense networks. Hence, as a minimum requirement, such multicast support should be available in radios and routers in a mobile tactical network. The main drawback with these protocols is the overhead resulting from redundant packet transmissions. The choice of mechanisms to implement efficient flooding should be studied further.

We also believe it to be worthwhile to take a closer look at stateless protocols for small groups. For small, sparsely populated groups, unicast is the only sensible option to stateless multicast. For these multicast groups, stateless protocols are able to reduce network resource consumption almost for free. The drawback is that stateless protocols often will give lower goodput and fairness compared with unicast in networks where there is a high probability for bit errors. The question is whether or not the gain available with stateless multicast is high enough to justify lower goodput and less fairness.

While geographic protocols are a less mature group of protocols (e.g., problems related to local minimum), we think they deserve more research focus. We find that these protocols (particularly the flooding-based) may lend themselves to military applications, as they have advantages such as little overhead and the ability to react to topology changes en route.

Topological protocols represent high signaling overhead and low robustness to mobility. For these reasons, topological protocols are the least suitable in this type of environment. Note that these protocols might be suitable in adjacent networks of other types (e.g., deployable and backbone network as illustrated in Figure 2.1), however these network types are not in scope of this discussion.

Finally, we think hybrid multicast protocols that combine stateless multicast, or some topological variant, with an efficient flooding-based protocol (maybe geographic), may be useful in a military

setting. In several situations it might be that information needs to travel some distance from the source until it reaches the destination area where almost all of the members of the multicast group are. Both the artillery vignette and stage two of the gas alarm vignette represent situations where this is the case. A hybrid protocol might also do well in our scenarios for future work where we want to study issues associated with end-to-end multicast through several network types (e.g., deployable and mobile).

7 Future work

To follow up on the preliminary conclusions, we need to do a more detailed analysis. This would involve studying a selection of protocols, including performing simulations, using realistic models for mobility and traffic patterns. As mentioned in Section 2, there are also several other issues that need to be addressed; such as that the MANET segment must interact efficiently with the deployable military network, and the fixed backbone network to provide efficient end-to-end group services on network paths through any combination of these networks. There are also other requirements, such as security and reliability. In the following we give some more background on a few of these issues that we need to look at in the further work in this area.

7.1 Evaluating protocols further

In order to get more concrete results, we need to do a more detailed analysis of a selection of protocols. It is also clear that this will have to involve simulations. In relation to the simulation issues listed at the beginning of Section 5, the goal should be to use models that have a closer resemblance to real life scenarios, in order to produce more realistic simulation results. As already mentioned, there has been work done regarding more realistic mobility models. It might therefore be possible to find models that could apply to a military setting in which there will be clustering and some degree of group mobility (e.g., a squad, or a platoon). The Hierarchical Group Mobility model (HGM) [18] is, for instance, designed specifically for a military MANET, and thus attempts to reflect the properties of a military operation; hierarchical command structure, purpose of action, and strong planning. Other models can be found in [2], which gives a survey of mobility models for performance analysis in tactical mobile networks. It includes models with different dependencies (spatial and temporal) and restrictions (geographic). In a tactical setting, depending on the application, there will be various traffic patterns, from regular SA-data to bursty VoIP traffic. Creating a realistic traffic model is not trivial: While synthetic traffic models may provide patterns that are far from realistic traffic patterns, they have parameters that may be altered without affecting other parameters, while traffic traces need to be used without significant alteration if they are to provided the desired realism [31]. Karpinski et al. [31] discuss how to incorporate trace data into synthetic models, and how to investigate which aspects of real traces may be altered without detrimentally affecting the resulting performance metrics. There are of course many other factors that will influence the outcome of real life tests compared to running simulations, since it is hard to simulate the real world and to predict what might occur during, e.g., a military exercise or operation. However, realistic traffic models and mobility models are two important parameter settings in a good simultion model.

7.2 Multicast in heterogeneous networks

In this survey we have studied group communication protocols for homogeneous MANETs. Mobile military networks often consist of radio links with different characteristics (e.g., bit rate, transmission range, delay, etc.), hence the transport network for the multicast traffic may have heterogeneous links. Protocols optimized for homogeneous networks does not necessarily work well for heterogeneous networks. We would like to study this topic further. We have already started a study of a flooding protocol on a very heterogeneous network and have proposed to use a delay-component in the flooding process to avoid overloading a long-range low bit rate network segment with flooding data from links with shorter transmission delay. This delay mechanism is described in [45]. We have not yet done an analysis of the performance of the flooding protocol with the proposed delay functionality, this will therefore also be part of future work for multicast in heterogeneous networks.

7.3 Interconnecting MANET multicast with multicast in adjacent networks

As pointed out in, e.g., [14], multicast research has mainly been performed on isolated uniform networks. Hence there is not much experience with multicast distribution to groups that span several adjacent networks where the networks run different multicast protocols. Some work has been done to provide the glue between an optimized flooding mechanisms in the MANET and a topological protocol in the backbone [14]. This paper also provides solutions for forwarding of multicast membership information from clients in the MANET to multicast routers in the backbone. RFC 4605 [17] provides mechanisms for forwarding of group membership information. However, this solution distributes the information on a optimized spanning tree and is therefore not robust to high network mobility. Landmark et al. [36] propose mechanisms that enable optimized flooding mechanisms to identify duplicate packets from different multicast gateways.

The vignettes presented in Section 3 show situations where the multicast group may have members in several radio networks, or in both the deployed network and the mobile network. For these reasons it is important to have efficient solutions for interoperability of multicast protocols in adjacent networks. This is also on our list for topics that require future work.

7.4 Quality of Service

Differentiated Quality of Service (QoS) for group traffic is also a necessity. In order to achieve a somewhat predictable behavior from a MANET, the network must support QoS mechanisms such as priority, preemption, traffic management, Service-Level Agreements (SLA) and admission control. Group traffic as well as point-to-point traffic must be treated with the same QoS policy. Group traffic and point-to-point traffic will in many cases require different solutions to implement the same QoS mechanisms. For example bandwidth estimates and resource reservation is very complicated for group traffic since it is difficult to estimate the impact one transmission link in the multicast distribution tree has on a neighboring link. Fairness in the distribution of group traffic is also more difficult in a network with differentiated QoS since it will happen frequently that traffic cannot be sent to all members in a group due to lack of QoS guarantees on the path to some of the members in the group. Preemption is another QoS parameter than must be discussed. In the case where the

network cannot support the traffic to a multicast group and something must be preempted, there is a choice of preempting the link to one of the group members and allow the traffic to flow the the remaining group members, or terminate the complete multicast flow. It is clear that more work is needed on QoS multicast. A survey on state of the art for QoS multicast can be found in [16]. This paper also summarizes some of the open issues concerning QoS multicast.

7.5 Reliable multicast protocols

For many military applications reliability will be an important requirement. At the same time MANETs are prone to packet losses, which makes designing reliable protocols difficult. In addition, e.g., retransmitting data also increases the network load which in turn may lead to more packet losses. There have been attempts, though, and some of the approaches have been surveyed in [51] and [60], which also use two different classification schemes. In [60] the protocols are classified into deterministic and probabilistic protocols. While probabilistic protocols only guarantee delivery within a certain probability, nodes in deterministic protocols will only accept a packet that is received by all.

Ouyang et al. [51] classify protocols according to recovery mechanisms; Automatic Retransmission Request (ARQ)-based, Forward Error Correction (FEC)-based, and gossip-based. In ARQ-based protocols lost packets are retransmitted until they are recovered at all the receivers. ARQ-based protocols are thus the same as the previously mentioned deterministic protocols. FEC-based protocols include redundant data in each packet before retransmitting; If the original data consists of k packets, the k packets are encoded into n packets, where $n > k$. The property of the encoder is such that if any k of the n packets are received, the source data can be reconstructed. In gossip-based protocols recently received packets are retransmitted in a peer-to-peer manner from a group member to a subset of the group members. The message also contains information about missing packets. Gossip-based protocols only achieve high delivery ratio with high probability, they do not guarantee reliable delivery for all packets.

7.6 Security

In a group communication setting there are several important security considerations in regards to the situations described in this document. One being group dynamics: In some cases the members are known in advance, while other times nodes will need to join a new group, and there will be cases where new groups will need to be formed. In addition, members will on occasion disappear, due to mobility, radio silence etc., and one needs to be able to handle these reappearing. Another issue is anonymity. This may have to do with anonymity amongst members, or anonymity towards non-members. For instance, it is undesirable to be identified as a critical node. Other times, such as in an alert scenario, there may be special forces nearby which need to be alerted, while they at the same time should be able to operate undetected. Security is rarely addressed in the papers describing the various protocols, while it is sometimes pointed out that it is an important issue, but is usually labeled “future work”. If security is addressed, it is usually in supplementary work, such as in [4], where a multicast protocol is used as a basis and role-based access control features are

incorporated to achieve control of access to the multicast groups, and the information exchanged within the groups. The SMF and Xcast drafts do contain some security considerations. For example for SMF, possible denial of service attacks and mitigation strategies are addressed. With regards to Xcast, there also exists an Internet Draft describing general issues relating to securing Xcast traffic [52], such as memberhip management and key management. When considering security and threats in general, it is important to evaluate what the real threats are, what are the capabilities of the adversaries, etc. In this setting availability, for instance, is very important, while information may be short-lived, so that it may not always impose danger if an adversary may overhear a conversation. More on security and threat modelling for ad hoc networks in general can be found in [56] and [11].

References

[1] J. Arango, M. Degermark, A. Efrat, and S. Pink. An Efficient Flooding Algorithm for Mobile Ad-Hoc Networks. In *Proceedings of the 2nd Workshop on Modeling and Optimization in Mobile Ad Hoc and Wireless Networks (WiOpt)*. IEEE, 2003.

[2] N. Aschenbruck, E. Gerhards-Padilla, and P. Martini. A Survey on mobility models for performance in tactical mobile networks. *Journal of Telecommunications and Information Technology*, 2/2008, 2008.

[3] O. Badarneh and M. Kadoch. Multicast Routing Protocols in Mobile Ad Hoc Networks: A Comparative Survey and Taxonomy. *EURASIP Journal on Wireless Communication and Networking*, 2009.

[4] E. E. Barka and Y. Gadallah. A Role-based Protocol for Secure Multicast Communications in Mobile Ad Hoc Networks. In *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference (IWCMC)*. ACM, 2010.

[5] R. Boivie, N. Feldman, Y. Imai, W. Livens, and D. Ooms. Explicit Multicast (Xcast) Concepts and Options. RFC 5058 (Experimental), November 2007.

[6] L. Bouraoui, P. Jacquet, A. Laouiti, M. Parent, and L. Viennot. Ad hoc communications between intelligent vehicles. In *Fifth International Conference on ITS Telecommunications ITST*, 2005.

[7] 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. In *Proceedings International Conference on Mobile Computing and Networking (MobiCom)*. ACM, 1998.

[8] L. Chen, A. B. Mnaouer, and C. H. Foh. An Optomized Polymorphic Hybrid Multicast Routing Protocol (OPHMR) for Ad Hoc Networks. In *Proceedings IEEE International Conference on Communications (ICC)*. IEEE, 2006.

[9] H. Cheng, J. Cao, and X. Fan. GMZRP: Geography-aided Multicast Zone Routing Protocol in Mobile Ad Hoc Networks. *Mobile Networks and Applications*, 2009(7):165–177, 2009.

[10] S. Y. Cho and C. Adjih. Optimized Multicast based on Multipoint Relaying. In *Proceedings of the First International Conference on Wireless Internet (WICON)*. IEEE, 2005.

[11] J. Clark, J. Murdoch, J. A. McDermid, S. Sen, H. R. Chivers, O. Worthington, and P. Rohatgi. Threat Modelling for Mobile Ad Hoc and Sensor Networks. In *Annual Conference of ITA (ACITA) 2007*. ITACS, 2007.

[12] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental), October 2003.

[13] S. Corson and J. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501 (Informational), January 1999.

[14] C. Danilov. MANET Multicast with Multiple Gateways. In *Proceedings Military Communications Conference (MILCOM)*. IEEE, 2008.

[15] S. K. Das, B. S. Manoj, and C. S. R. Murthy. A Dynamic Core Based Multicast Routing Protocol for Ad hoc Wireless Networks. In *Proceedings International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. ACM, 2002.

[16] V. T. M. Do, L. Landmark, and Ø. Kure. A Survey of QoS Multicast in Ad Hoc Networks. *Future Internet*, 2(3):388–416, 2010.

[17] B. Fenner, H. He, B. Haberman, and H. Sandick. Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying"). RFC 4605 (Proposed Standard), August 2006.

[18] A. Fongen, M. Gjellerud, and E. Winjum. A Military Mobility Model for MANET Research. In *IASTED PDCN'09*, Innbruck, Austria, February 2009. IASTED/ACTA Press.

[19] J.J. Garcia-Luna-Aceves. The Core-Assisted Mesh Protocol. *Journal on selected areas in communications*, 17(8), 1999.

[20] H. Gossain, C. Cordeiro, K. Anand, and D. P. Agrawal. E^2M: A Scalable Explicit Multicast Protocol for MANETs. In *Proceedings IEEE International Conference on Communications (ICC)*. IEEE, 2004.

[21] R. S. Gray, D. Kotz, C. Newport, N. Dubrovsky, A. Fiske, J. Liu, C. Masone, S. McGrath, and Y. Yuan. Outdoor Experimental Comparison of Four Ad Hoc Routing Algorithms. In *Proceedings International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*. ACM, 2004.

[22] Z. J. Haas, M. R. Pearlman, and P. Samar. The Zone Routing Protocol (ZRP) for Ad Hoc Networks (work in progress). Internet Draft, Internet Engineering Task Force. (draft-ietf-manet-zone-zrp-04.txt), July 2002.

[23] A.-H. A. Hashim, M. M. Qabajeh, O. Khalifa, and L. Qabajeh. Review of Multicast QoS Routing Protocols for Mobile Ad Hoc Networks. *IJCSNS International Journal of Computer Science and Network Security*, 8(12), 2008.

[24] M. Hauge and S. Haavik. Intelligent Tactical IP Router. FFI-Rapport 2009/01708, Norwegian Defence Research Establishment, 2009.

[25] A. P. Jardosh, E. M. Belding-Royer, K. C. Almeroth, and S. Suri. Real-world environment models for mobile network evaluation. *IEEE Journal on Selected Areas in Communications, special issue on Wireless Ad hoc Networks*, 2005.

[26] G. Jayakumar and G. Ganapathi. Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols. Journal of Computer Systems, Networks, Communications. Hindawi Publishing Corporation, 2008.

[27] J. G. Jetcheva and D. B. Johnson. Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks. In *Proceedings International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. ACM, 2001.

[28] L. Ji and M. S. Corson. Explicit Multicasting for Multicast Ad Hoc Networks. *Mobile Networks and Applications*, 8:535–549, 2003.

[29] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu. A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks. *IEEE Comminucations Surveys and Tutorials*, 11(1), 2009.

[30] B. Karp and H. T. Kung. Greedy perimeter stateless routing for wireless networks. In *Proceedings International Conference on Mobile Computing and Networking (MobiCom)*, pages 243–254. ACM/IEEE, 2000.

[31] S. Karpinski, E. M. Belding, and K. C. Almeroth. Wireless Traffic: The Failure of CBR Modeling. In *Proceedings Broadnets*. IEEE, 2007.

[32] S.-C. Kim and K. Shin. A Performance Analysis of MANET Multicast Routing Algorithms with Multiple Sources. In *Proceedings of Fifth International Conference on Software Engineering Research, Management and Applications*. IEEE, 2007.

[33] Y.-B. Ko and N. H. Vaidya. Flooding-Based Geocasting Protocols for Mobile Ad Hoc Networks. *Mobile Networks and Applications*, 7:471–480, 2002.

[34] Ø. Kure and I. Sorteberg. Network Architecture for Network Centric Warfare Operations. FFI-rapport 2004/01561, Norwegian Defence Research Establishment, 2004.

[35] S. Kurowski, T. Camp, and M. Colagrosso. MANET Simulation Studies: The Incredibles. *Mobile Computing and Communications Review*, 9(4), 2005.

[36] L. Landmark, Y. Lacharite, and L. Lamont. Multicast Forwarding Using Multiple Gateways and Hash for Duplicate Packet Detection in a Tactical MANET. In *Proceedings Military Communications Conference (MILCOM)*. IEEE, 2007.

[37] A. Laouiti, P. Jacquet, P. Minet, L. Viennot, T. Clausen, and C. Adjih. Multicast Optimized Link State Routing. Rapport de Recherche 4721, Institut National de Recherche en Informatoque et en Automatique (INRIA, 2003.

[38] E. Larsen, L. Landmark, V. Pham, Ø. Kure, and P. E. Engelstad. Optimized Group Communication for Tactical Military Networks. In *Proceedings Military Communications Conference (MILCOM)*. IEEE, 2010.

[39] L. K. Law, S. V. Krishnamurthy, and M. Faloutsos. Understanding and exploiting the tradeoffs between broadcasting and multicasting in mobile ad hoc networks. *Mobile Computing, IEEE Transactions on*, 6(3):264 –279, march 2007.

[40] S.-J. Lee, W. Su, and M. Gerla. On-demand multicast routing protocol in multihop wireless mobile networks. *Mobile Networks and Applications*, 7(6), 2002.

[41] J. Macker, I. Downard, J. Dean, and B. Adamson. Evaluation of Distributed Cover Set Algorithms in Mobile Ad hoc Networks for Simplified Multicast Forwarding. *ACM SIGMOBILE Mobile Computing and Communications Review*, 11(3), 2007.

[42] J. P. Macker, J. Dean, and W. Chao. Simplified Multicast Forwarding in Mobile Ad hoc Networks. In *Proceedings Military Communications Conference (MILCOM)*. IEEE, 2004.

[43] J. Macker (ed.). Simplified Multicast Forwarding (work in progress). Internet Draft, Internet Engineering Task Force. (draft-ietf-manet-smf-12.txt, July 11, 2011.

[44] M. Masoudifar. A review and performance comparison of QoS multicast routing protocols for MANETs. In *Ad Hoc Networks*, volume 7, pages 1150–1155. Elsevier, 2009.

[45] K. Mathiassen and M. Hauge. Design of a delay functionality for multicast packets - an extension to "Simplified Multicast Forwarding". FFI-Notat 2009/01984, Norwegian Defence Research Establishment, 2009.

[46] R. Menchaca-Mendez and J.J. Garcia-Luna-Aceves. An Interest-Driven Approach to Integrated Unicast and Multicast Routing in MANETs. In *Proceedings of the 16th IEEE International Conference on Network Protocols (ICNP)*. IEEE, 2008.

[47] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu. The Broadcast Storm Problem in a Mobile Ad Hoc Network. In *Proceedings International Conference on Mobile Computing and Networking (MobiCom)*. ACM, 1999.

[48] K. Obraczka, K. Viswanath, and G. Tsudik. Flooding for Reliable Multicast in Multihop Ad Hoc Networks. *Wireless Networks*, 7:627–634, 2001.

[49] S. Y. Oh, J.-S. Park, and M. Gerla. E-ODMRP: Enhanced ODMRP with Motion Adaptive Refresh. *Journal of Parallel and Distributed Computing*, 68(8), 2008.

[50] T. Ohta, T. Kawaguchi, and Y. Kakuda. A New Multicast Routing Protocol Based on Autonomous Clustering in Ad Hoc Networks. In *Proceedings Autonomous Decentralized Systems (ISADS)*, pages 297–305. IEEE, 2005.

[51] B. Ouyang, X. Hong, and Y. Yi. A Comparison of Reliable Multicast Protocols for Mobile Ad Hoc Networks. In *Proceedings SoutheastCon*. IEEE, 2005.

[52] O. Paridaens, D. Ooms, and B. Sales. Security Framework for Explicit Multicast. Internet Draft, Internet Engineering Task Force. (draft-paridaens-xcast-sec-framework-02.txt), June 2002.

[53] V. D. Park and M. S. Corson. A highly adaptive distributed routing algoritm for mobile wireless networks. In *Proceedings IEEE INFOCOM '97*, pages 1405–1413. IEEE, 1997.

[54] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003.

[55] E. M. Royer and C. E. Perkins. Multicast Ad hoc On-Demand Distance Vector (MAODV) Routing (work in progress). Internet Draft, Internet Engineering Task Force. (draft-ietf-manet-maodv-00.txt), 15 July 2000.

[56] D. Spiewak, T. Engel, and V. Fusenig. Unmasking threats in mobile ad-hoc networks settings. *WSEAS Transactions on Communicastions*, 6:104–110, 2007.

[57] C.-K. Toh. Associativity-Based Routing Protocol for Ad Hoc Mobile Networks. *Wireless Personal Communications Journal: Special Issue on Mobile Networking and Computing Systems*, 4(2):103–139, 1997.

[58] C-K. Toh, G. Guichal, and S. Bunchua. ABAM: On-Demand Associativity-Based Multicast Routing for Ad Hoc Mobile Networks. In *Proceedings 52nd Vehicular Technology Conference (VTC)*, volume 3, pages 987–993. IEEE, 2000.

[59] M. Transier, H. Füßler, J. Widmer, M. Mauve, and W. Effelsberg. A hierarchical approach to position-based multicast for mobile ad-hoc networks. *Wireless Networks*, 13(4):447–460, 2007.

[60] E. Vollset and P. Ezhilchelvan. A Survey of Reliable Broadcast Protocols for Mobile Ad-hoc Networks. CS-TR 792, School of Computing Science, Newcastle University, 2009.

[61] J. Weston (ed.). Interoperable Networks for Secure Communications. INSC Phase 2: Task 3 (Mobility) Final Report, INSC-II/Task3/DU/003, July 2006.

[62] B. Williams and T. Camp. Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks. In *Proceedings International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. ACM, 2002.

[63] C. W. Wu and Y. C. Tay. AMRIS: A Multicast Protocol for Ad hoc Wireless Networks. In *Proceedings Military Communications Conference (MILCOM)*. IEEE, 1999.

[64] X. Xiang, Z. Zhou, and X. Wang. Robust and Scalable Geographic Multicast Protocol for Mobile Ad Hoc Networks. In *Proceedings 26th Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2007)*. IEEE, 2007.

[65] X. Zhang and L. Jacob. MZRP: An Extension of the Zone Routing Protocol for Multicasting in MANETs. *Journal of Information Science and Engineering*, 20(3):535–551, 2004.

[66] Y. Zhao, L. Xu, and M. Shi. On-Demand Multicast Routing Protocol with Multipoint Relay (ODMRP-MPR) in Mobile Ad-Hoc Network. In *Proceedings International Conference on Communication Technology (ICCT)*. IEEE, 2003.

Abbreviations

ABAM	Associativity-based ad hoc multicast
ADMR	Adaptive Demand-Driven Multicast Routing Protocol
AMRIS	Ad Hoc Multicast Routing protocol utilizing Increasing id-numberS
AODV	Ad Hoc On-demand Distance Vector
C2	Command and Control
CAMP	Core-Assisted Mesh Protocol
CBR	Constant bit rate
CDS	Connected Dominating Set
CF	Classical Flooding
CNR	Combat Net Radio
DCMP	Dynamic Core-based Multicast Routing Protocol
DDM	Differential Destination Multicast
DPD	Duplicate packet detection
E^2M	Extended Explicit Multicast
GMZRP	Geography-aided Mulitcast Zone Routing protocol
HF	High frequency
HGM	Hierarchical Group Mobility model
HiM-TORA	Hierarchical Multicast Temporally-Ordered Routing Algorithm
HQ	Headquarters
IETF	Internet Engineering Task Force
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LARDAR	Location-Aware Routing Protocol with Dynamic Adaption of the Request zone
LAN	Local Area Network
MANET	Mobile Ad Hoc Network
MAODV	Multicast AODV
MOLSR	Multicast OLSR
MPR	Multipoint relay
MZRP	Multicast Zone Routing Protocol
NGO	Non-governmental organisation
ODMRP	On-demand multicast routing protocol
OLSR	Optimized Link State Routing
OPHMR	Optimized Polymorphic Hybrid Multicast Routing
PRIME	Protocol for Routing in Interest-defined Mesh Enclaves
QoS	Quality of Service
RFC	Request for Comments
RSGM	Robust and Scalable Geographic Multicast
RWP	Random Waypoint
SA	Situational Awareness

SATCOM	Satellite Communication
SLA	Service-Level Agreement
SMF	Simplified Multicast Forwarding
SMOLSR	Simple Multicast OLSR
SPBM	Scalable Position-Based Multicast
VHF	Very high frequency
Xcast	Explicit multicast

Appendix A Typical simulation environments

Table A.1 Typical simulation environments

Protocol	Simulator	Mobility model	Duration (s)	Area (m x m)	#nodes	#sources	Group size	Speed (m/s)	Transmission range	Bit rate	Traffic model	Metrics
ABAM	GloMoSim	RWP	180	175 x 175	40	1	4	0-5	50	2Mbits/s	CBR, 500 bytes, 1 pkt/s	data throughput, control overhead, number of hops, end-to-end delay
ADMR	ns-2	RWP	900	1500 x 300	50	1(3)	5-30	0-20	250	2 Mbits/s	CBR, 64 bytes, 4 pkt/s	packet delivery ratio, normalized packet overhead, forwarding efficiency, delivery latency
AMRIS	PARSEC	Brownian	200	1000x1000	100	1	25-100	1-20	150	2 Mbits/s	100 bytes, 10 pkts/s	packet delivery ratio, routing overhead, end-to-end delay
CAMP	CPT	"random"	350	-	32	1-2	32	0/30m/s	-	1 Mbit/s	4/2+2pkts/s	percentage of missed packets, average packet delay, total control packets
DCMP	GloMoSim	RWP	200	1000x1000	50	0-20	5,20	0-20	250	2 Mbits/s	CBR, 512b, 10 pkt/s	packet delivery ratio, control overhead/packet delivered data packets/packet delivered
DDM	ns-2	RWP	900	1000x1000	50	1-10	2-50	0-20	250	2 Mbits/s	CBR, 512 bytes, 4 pkt/s	packet delivery ratio, sent/delivered, routing overhead
E^2M	ns-2	"random"	500	1000x1000	75	1	40	2-10	250	-	CBR, 512 bytes, 2 pkt/s	average xcast header size, control forwards per packet packet delivery ratio
E-ODMRP	ns-2	RWP	900	1200x800	100	1-6	20	1-20(50)	-	-	CBR, 512 bytes, 4 pkt/s	packet delivery ratio, packet overhead, byte overhead, total control packets transmitted, average route refresh interval
Fireworks	ns-2	RWP/RPGM	50-300	1250x1250	100	1-4	10-90	5-15	250	2 Mbits/s	512 bytes, 2-8 pkt/s	packet delivery ratio, forwarding overhead vs. #sources, packet delivery ratio vs. cluster radius, normalized total overhead vs. degree of clustering
Flooding-based geocast	ns-2	"random"	500-1000	1000x1000	10-30-50	1		5-20	250	2 Mbits/s	1-2 pkt/s	Accuracy of geocast delivery, overhead of geocast delivery
Geoflood	ns	"random"		1000x1000	(density)			0-20	250	2 Mbits/s		Overhead, coverage, latency
GMZRP	GloMoSim	RWP	100	1250x1250	100	1	15-75	0-20	250	-	CBR, 128 bytes, 5pkt/s	packet delivery ratio, normalized packet overhead, average path length
HiM-TORA	ns-2	RWP	300	2000x2000	150	1(5)	10	1-20	250	-	CBR, 512 bytes, 4 pkt/s	number of control packets, number of delivered packets delivery efficiency
MZRP	ns-2	RWP	200	1000 x 1000	50	1-15	1-25	1-20	250	2Mbits/s	CBR, 64 bytes, 2pkt/s	packet delivery ratio, normalized routing overhead, packets transmitted/packet delivered, route discovery delay
ODMRP	GloMoSim	"random"	600	1000x1000	50	1-20	5-40	0-20	250	2Mbits/s	CBR, 512 bytes, 1-50pkt/s	packet delivery ratio, packets transmitted/packets delivered, control bytes transmitted/data bytes delivered, all packets transmitted/data packets delivered
ODMRP-MPR	ns-2	"random"	400	1200x1200 x	50	1-20	1-20	0-2	150-350	2 Mbits/s	CBR, 512 bytes	Packet delivery ratio, data packet transmitted/delivered, control overhead, control+data packets transmitted/data packet delivered
OPHMR	GloMoSim	RWP	1000	2000x2000	50-500	10	40	0-60	225	2 Mbits/s	CBR, 512 bytes, 1-70 pkt/s	power conservation, packet delivery ratio, end-to-end delay
PRIME	QualNet	RWP/GM	150	1800x1800	100	1-24	20	0-20		2 Mbits/s	MCBR, 256bytes, 10 pkts/s	packet delivery ratio, generalized group delivery ratio end-to-end delay, total overhead
RSGM	GloMoSim	RWP	500	2400 x 2400	400	1	100	1-40	250	-	CBR, 512 bytes, 16 pkt/s	packet delivery ratio, normalized control overhead, average path length, joining delay
SMF	ns-2	Random walk	600	710x710(?)	25	1/4	25	1-20	250	2Mbits/s	CBR, 256bytes	percentage of goodput
SPBM	ns-2	RWP	180	$(350-2800)^2$	$100/km^2$	1-15	5-25	0-15	250	2 Mbits/s	64 bytes, 1pkt/s	packet delivery ratio, overhead - total bytes at MAC layer, end-to-end delay