FFI-RAPPORT

18/00936

A Flexible and Dynamic Method for Efficient Group Communication in Mobile Military Networks

Lars Landmark
Mariann Hauge

A Flexible and Dynamic Method for Efficient Group Communication in Mobile Military Networks

Lars Landmark
Mariann Hauge

Norwegian Defence Research Establishment (FFI) 13 November 2018

Keywords

Nettverksbasert forsvar
Taktisk kommunikasjon
Samband

FFI-rapport
FFI-RAPPORT 18/00936

Prosjektnummer
136702

ISBN
P: 978-82-464-3066-9
E: 978-82-464-3067-6

Approved by
Jan Erik Voldhaug, *Research Manager*
Tor-Odd Høydal, *Director of Research*

The document is electronically approved and therefore has no handwritten signature.

Summary

Group communication will be one of several important services that should be available in the networks for the tactical edge also in the near future. Group communication is used in situations when information is meant for several receivers forming a group within a predefined network area. We expect that the need for efficient support for group communication will increase with the introduction of more sensors, autonomous systems and more information sharing in future common operations. Within the project Tactical C4IS for the land domain (P8043), different concepts for a future mobile communications infrastructure are studied. It will most likely be necessary with a new and/or upgraded network architecture that includes efficient group communication when the chosen concept is realized.

In this report, we propose a possible future network architecture and study how some important group communication services (e.g., push-to-talk voice and situation awareness) can be efficiently supported. The network architecture makes use of high-capacity radios with the purpose of increasing data capacity at the mobile tactical edge. In order to maintain distance over radio networks where high-capacity radios are used, it will be necessary to forward the traffic via relays (multihop). Intermediate nodes must therefore forward group information in order to reach the respective receivers. The purpose of the study is to propose a solution to support group communication that is robust and at the same time requires as little as possible of the network resources to provide the services.

The Simplified Multicast Forwarding protocol (SMF) enables robust data distribution and is a candidate for distributing the exemplified services in future military high-capacity radio networks. The disadvantage of this protocol is that it distributes the information to the entire radio network even in situations where the receivers are located in a smaller area of the network. In this report, we therefore describe several methods to limit the forwarding of group traffic when the SMF protocol is used, taking into account topology change caused by for instance mobility. We further propose to combine one of these methods with another type of protocol, Explicit Multi-unicast (Xcast). This proposal can provide robust support for group communication in challenging terrain with the goal of reduced network resource consumption compared with the use of standard SMF. One advantage is the ability to do traffic management of group traffic and thereby reduce the load on the network. Furthermore, the method can be improved to also support group communication across several radio networks in heterogeneous mobile networks. We expect such heterogeneous mobile networks to become more prevalent in the future.

This report proposes a design of how to tailor the dissemination of group information in a robust manner when SMF is used. It is necessary to evaluate the method with simulation and/or network emulation to study the proposal in more detail. The report is mainly written for network designers addressing group communication in mobile radio networks.

Sammendrag

Gruppekommunikasjon vil være en av flere viktige tjenester i fremtidens taktiske ledelses-systemer. Med gruppekommunikasjon mener vi informasjon som er ment for en begrenset mottakergruppe innenfor et forhåndsdefinert nettverksområde. Vi forventer at behovet for gruppekommunikasjon vil øke i fremtiden grunnet innføring av flere sensorer, autonome systemer og mer utstrakt deling av data for bedre felles situasjonsforståelse. Prosjektet *Taktisk ledelsessystem for landdomenet* (P8043) har studert forskjellige konsepter for en mobil kommunikasjonsinfrastruktur hvor brukerfunksjonalitet understøttes av en fremtidsrettet tjenesteinfrastruktur. Det vil sannsynligvis være nødvendig med en ny og/eller oppdatert nettverksarkitektur med god støtte for gruppekommunikasjon for å realisere konseptet som blir valgt.

I denne rapporten har vi laget et design for hvordan noen viktige taktiske gruppe-kommunikasjonstjenester (for eksempel push-to-talk tale og situasjonsforståelse) kan støttes i en mulig fremtidig nettverksarkitektur. Nettverksarkitekturen gjør bruk av høykapasitetsradioer med den hensikt å øke datakapasiteten i mobile taktiske kommunikasjonsnettverk. For å opprettholde forbindelse over avstand i radionettverk hvor høykapasitetsradioer er brukt, vil det være behov for å sende trafikken via relé (multihop). Informasjon som er ment for en gruppe av mottakere, må derfor videresendes av mellomliggende noder for å nå frem til alle. Målet med studien er å finne effektive løsninger for å sende denne typen informasjon på en robust måte som samtidig bruker minst mulig datakapasitet.

Protokollen Simplified Multicast Forwarding (SMF) muliggjør robust distribusjon av data og er trolig en kandidat i fremtidige høykapasitets radionettverk. En ulempe med denne protokollen er at den i utgangspunktet sprer informasjon ut til hele radionettverket, også i situasjoner der mottakerne befinner seg innenfor et begrenset område. Rapporten beskriver derfor flere metoder for å avgrense spredningen av gruppekommunikasjon når SMF er brukt, samtidig som vi tar høyde for endringer i nettverket i form av for eksempel node mobilitet. Vi forslår videre å kombinere en av disse metodene med en annen type protokoll, Explicit Multi-unicast (Xcast). Forslaget gir mange muligheter. Det kan gi robust støtte for gruppekommunikasjon i utfordrende terreng, samtidig som den er forventet å redusere ressursbruken sammenlignet med standard SMF. Gevinsten er trafikkstyring av gruppekommunikasjon og dermed redusert ressursbruk. Forslaget kan også enkelt videreutvikles til å støtte gruppekommunikasjon over flere radio-nettverk i et heterogent nettverk. Vi forventer at heterogene nettverk vil bli mer utbredt i fremtiden.

Rapporten gir et skrivebordsdesign for hvordan avgrense spredning av gruppeinformasjon ved bruk av SMF. Det vil være nødvendig å evaluere løsningen i simulator og/eller emulert testbed. Rapporten er hovedsakelig skrevet for nettverksdesignere som er interessert i gruppe-kommunikasjon i mobile radionettverk.

Content

1 Introduction

There is an ongoing activity to renew C4IS (Command, Control, Communications, and Computers Information System) for the land based forces of the Norwegian Armed Forces (P8043). A new, or updated network, architecture is likely required to implement the chosen concept. The work to renew the C4IS is not finished, but many factors indicate that future military operations will need higher network capacity, and will have more traffic meant for one or more groups of receivers. We expect that a large share of the traffic in the lower military echelons is traffic meant for a group, e.g., data to provide friendly force tracking and push-to-talk voice. In this report, we call this communication for group communication and the traffic for group traffic.

Future military networks will likely have sensors deployed, and some of these will be used at the tactical edge enforcing a need for higher capacities in some segments of the radio networks. Autonomous systems consisting of multiple autonomous platforms, such as Unmanned Ground Vehicle (UGV), Unmanned Sea Vehicle (USV) and Unmanned Aerial Vehicle (UAV) will require robust and safe communication to take advantages of being able to cooperate in order to reach a common goal. More focus on joint operations may also require more information to flow in and between units or among groups for improved network robustness and situations awareness. This dictates a need to deploy radios with sufficient data rates for future requirements, and network functionalities addressing group communications.

Radio capacity in terms of available data rate is often an inverse function of the transmission range. Radios with high data rate usually operate in higher frequency bands (e.g., UHF) since there are not enough frequencies available at lower frequency bands to allocate the wide bandwidth (e.g., 1.25MHz) that is needed for higher data rate communication. One consequence, given an acceptable transmission power budget, is a shorter transmission range compared with lower frequency networks and often, variable channel conditions during mobility in all other terrains than flat topology with little vegetation. Therefore, group communication to a unit (e.g., company, platoon) can typically not be sufficiently supported with a one-hop radio-broadcast. Mobile ad hoc network (MANET) techniques or some other technologies are needed to automatically choose relays to forward the traffic multiple hops to reach all nodes in the unit (see section 3.2 for an explanation of 1-hop radio-broadcast versus multihop).

Earlier work at FFI [1, 2] has pointed out that there is no “one size fits all” protocol to support efficient group communication in mobile military network. (These protocols are usually referred to as multicast in the literature). Since building and maintaining multicast distribution trees is costly and more error prone in mobile wireless environments, these references conclude, that an efficient flooding protocol like Simplified Multicast Forwarding (SMF) [3] is a candidate to support group communication in many military scenarios. The main reasons listed in [2,3] are its robustness to high mobility and efficiency in scenarios where group members are located in close proximity of each other, which is also often the case in military group communication scenarios.

In our work we have assumed one likely future network architecture (see chapter 2), and study how existing important services can be efficiently supported in the new architecture. We use land based forces as the example in this report. More specifically, we discuss methods for delivering traffic (e.g., friendly force tracking or push-to-talk voice communication) to and within a co-located group that represents a small part of the entire radio network where high data rate network radios are extensively used (e.g. we want to serve a company-sized group in a battalion-size network). We further take mobility and other network disturbance into account, and propose a robust method for group communication. The proposed method is based on SMF, which is a likely candidate to be used in future radio networks for supporting communication to a group. The SMF flooding technique is used as baseline and works by flooding the data-packets to the whole network. Clearly, if the network e.g., covers a battalion and the data is meant for one company of the battalion, it is not resource efficient to flood the data to the entire battalion. Therefore, in this report we discuss and propose improvements to efficient flooding techniques that can limit the flooding of a packet to a smaller segment of the network and at the same time be robust to changing topologies due to for instance mobility and signal noise.

The report is organized in the following way; in chapter 2 we describe the network architecture and military scenario that is assumed for the discussion. In chapter 3 we describe different methods for group communication, the relevant protocols for this discussion. In chapter 4, the techniques for scoping SMF are proposed and discussed. In chapter 5, we discuss the support for flexible group communication in a heterogeneous mobile military network. Related work is covered in chapter 6. Finally, chapter 7 gives concluding remarks.

2 Network architecture and military scenario

As more high data rate radios are introduced in the area of operation, it is debated how the network architecture should look like. How large should the network be in order to best deal with the tradeoff between efficient end-to-end connections in a larger network, efficient use of the large (e.g., 1.25MHz or 5MHz) frequency bands required by these radios, and available network capacity to the warfighter? In this report, we study an architecture that is described in the following, which we believe is a plausible architecture for the future military tactical networks.

We make two assumptions that define the architecture for the following discussion. 1) We assume that high data rate radios are deployed extensively. 2) We assume that one radio network is deployed to cover a large unit (e.g., battalion-size), on one frequency band (see Figure 2.1 for an example). Potential advantages with this architecture are efficient end-to-end connections throughout the network and a need for fewer frequency bands compared with a situation with smaller networks. Next, we assume that the multicast protocol that is most likely

to be available in a high data rate military MANET radio is based on an efficient flooding protocol (e.g., SMF) due to its robustness and simplicity.

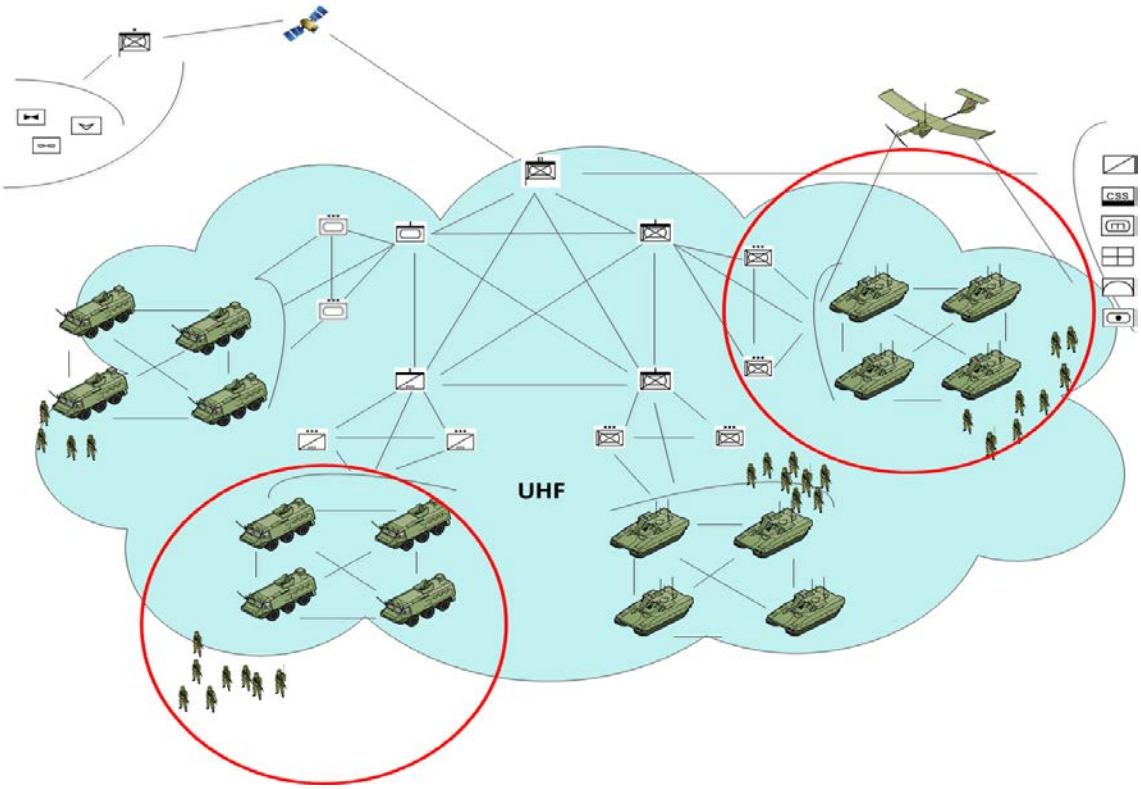


Figure 2.1 This figure shows a high data rate radio network spanning a battalion. Two example target groups for group communication are shown, a company group and a platoon group.

We believe that this network architecture differs from the architecture typically used by the Norwegian Armed Forces today. High data rate radios require multiple hops to reach the complete network, and the choice to have one network covering a whole battalion removes the network boarders that are typically used to define the information domain (multicast group) for group traffic to smaller units today. The one-hop broadcast domain that covers the group of choice is not present anymore.

It is important that the new network architecture can continue to support traditional important services for the lower military echelons in an efficient manner. For example, it should be possible to provide friendly force tracking and push-to-talk to smaller network segments than the entire network (e.g., a company or platoon). In the example battalion network illustrated in Figure 2.1, the data must traverse multiple radio hops to cover the whole battalion, either with ground based communication or in combination with elevated radios (see [4] for more information about advantages and disadvantages with elevated nodes for group communication). Given that the group that should receive data from a certain application is smaller than the battalion, the traffic flow should be controlled such that it reaches the members of the group only, and does not flood the whole network.

3 Group communication

Methods for group communication are often implemented by multicast protocols and referred to as multicast in the network literature. Support for group communication can be implemented on different layers in the OSI stack, and can be exemplified as application-, overlay- and IP-multicast. In this report, we focus on IP-multicast and use the term multicast when we refer to multicast protocols as the technique used to forward the data and the term group communication when we consider the information that needs efficient support for group traffic.

In this chapter, we give necessary background information for the discussion in chapter 4. First, we introduce the two basic modes for group information exchange named push and pull. Next, we introduce group communication and multicast forwarding. Further, we introduce the two multicast protocols that our proposal and discussion is based on. The two protocols are Simplified Multicast Forwarding (SMF) and Explicit Multi-unicast (Xcast).

3.1 Group communication modes

Group communication services can be divided in two different modes; push and pull.

Pull mode: The pull mode presents the cases where the group members ask to be part of a multicast group that provides a specific service (e.g., friendly force tracking in a company) by explicitly joining a multicast group. This can be done on demand with dynamic signaling, or the group members for the service can be pre-defined. With this mode, the receiver controls if it wants to be part of the group and receive the information associated with the group. The sender cannot reach a receiver that has not sent a join message to show interest for the group. This mode is the mode supported by the classical multicast design originally proposed by Deering [5].

Push mode: In push mode, the traffic is pushed to a specific group of receivers. This mode is controlled by the source. The information is pushed to every node in the network and a receiver that is not interested in the traffic can choose to ignore the traffic (but still keep receiving traffic from the source) or stop the traffic by issuing a prune messages. In case a prune message is sent, a multicast distribution tree is being built and only interested receivers will receive group traffic.

For efficient ad-hoc targeted delivery of data content, the push mode is interesting. This mode can also be interesting for military scenarios where it is beneficial to push traffic to a specific group defined either by geographical position or by the military organization. Figure 3.1 shows one example of a gas alarm pushed to affected warfighters. More examples of this kind can be found in [1].

Military group communications services will, to a larger degree than seen in civilian networks, require a combination of both push and pull. Pull is advantageous in settings where the user is interested in receiving some specific data. Push, on the other hand, is beneficial in situations

where e.g. an alarm must be sent to a specific group that was not preplanned to be interested in this information. Hence, pull is beneficial for preplanned traffic, whereas push is needed for delivering alarms, alerts, and orders etc. to an ad-hoc group.

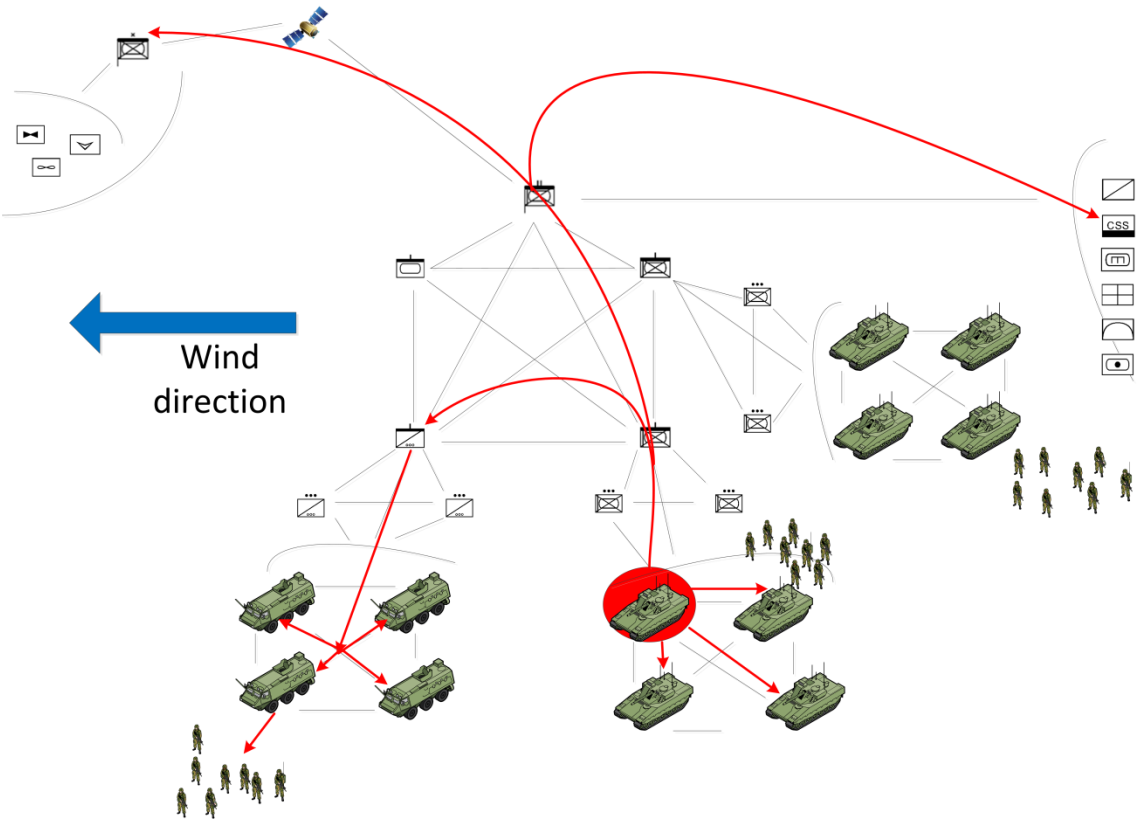


Figure 3.1 *The figure shows a scenario where a gas is detected in the highlighted vehicle; next, a gas alarm is pushed to an analysis unit, the HQ and the expected affected area given input such as wind direction.*

The main difference between pull and push is based on who initiates the traffic. For pull, one or more nodes in the network must request the data (join the group) before the traffic is being sent to the requested receivers. For push, the source itself starts sending data to the group without the group/receivers first asking for it.

3.2 Methods for group information exchange

A range of different transport techniques at the different OSI layers can support group communication for mobile wireless networks. The following figures (Figure 3.2. and Figure 3.3) illustrate the main difference between one-hop radio-broadcast, unicast flooding and multicast. It is important to note, that there is no superior multicast method/protocol for all scenarios, but the different methods have their advantages and disadvantages depending on environments such

as mobility, group size, member density etc. One interesting technique, as an example that operates on the MAC layer (not illustrated here), is named cooperative broadcast [6]. It is based on TDMA, and aims to synchronize transmissions in order improve the signal to noise (S/N) at the receiver.

Figure 3.2 shows traditional one-hop radio-broadcast that is commonplace in the Norwegian Armed Forces today. When broadcast is used for group communication, all units that are inside radio coverage of the sender receive the information, and units that are outside of radio coverage do not. For radios with long range, this method can cover a large group. For radios with short and very variable range, this method is in most cases insufficient.

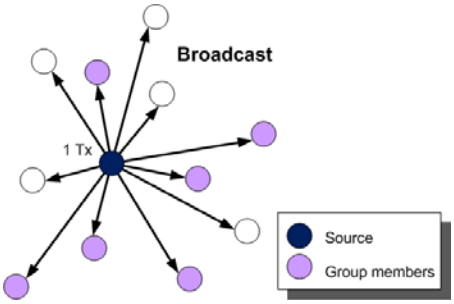


Figure 3.2 An illustration of one-hop broadcast used as the technique for group communication to a group inside the communication range of the source. This technique does not reach possible group members outside the radio coverage of the source.

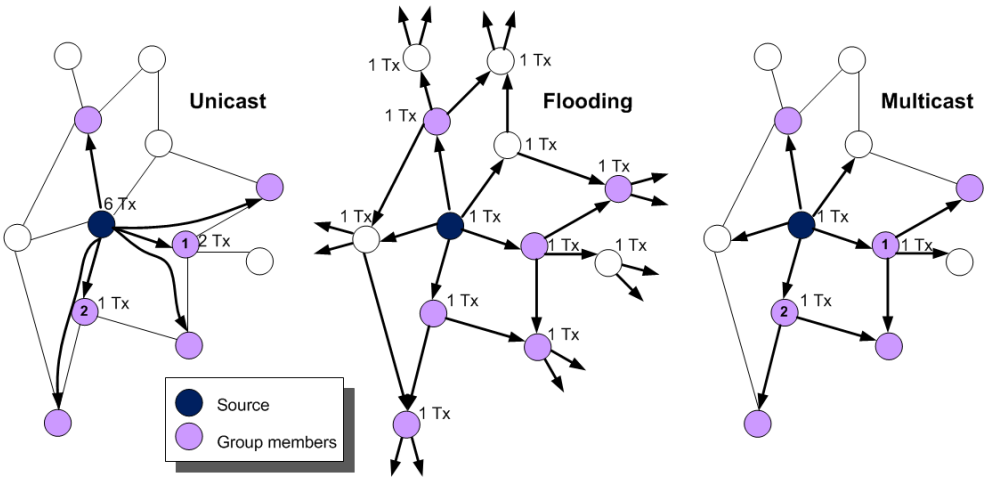


Figure 3.3 An illustration of three different techniques (unicast, flooding, multicast) for group communication and how much network resources each of these require to forward traffic to a multicast group. Note, flooding protocols are often also called multicast (i.e. Simplified Multicast Forwarding (SMF))

Figure 3.3 shows different methods used when members of the group are outside of the broadcast range of a radio. When unicast is used, multiple point-to-point connections are setup

between the source and each of the group members. With flooding, each radio rebroadcasts all new incoming packets. In this manner, a packet is flooded to all radios in the network. Optimizations exist to reduce some of the redundant transmissions with the flooding technique. With traditional multicast, a common distribution tree is established to reach out to the receivers.

The multicast architecture consists of two main building blocks; a multicast group management protocol and a multicast routing protocol. The group management protocol runs in the local area network (LAN) and is responsible of keeping track of the multicast receivers within the local LAN. The multicast routing protocol is used in the core network, and is responsible for building the multicast forwarding tree between routers. Hence, the multicast routing protocol is typically used within an autonomous system to connect gateways to local networks or LANs. The group management protocol runs within the local network keeping track of the actual receivers. Internet Group Management Protocol (IGMP) [7] support group management in the LAN for IPv4 while Multicast Listener Discovery (MLD) [8] is used for IPv6. We will not describe IGMP/MLD in this work, but it is assumed implemented in the end hosts. Multicast routing protocols in mobile radio networks have received much attention during the last decades and many protocols have been proposed [1, 9]. Some of these protocols attempt to build a minimum multicast spanning tree in order to minimize required network resources, whereas others introduce some mesh connections to increase the robustness.

The methods in Figure 3.3 differ in the number of transmissions needed to provide a data packet to the group, and the communication robustness. The figure illustrates a one-to-many scenario, with one source and many receivers. Note, in this figure the network consists of radios and not wired links; thus each transmission reaches all nodes, in case of no errors, that are within transmission range of the transmitting 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. Many mechanisms exist to optimize the flooding process to reduce the required transmissions. The last illustration(Figure 3.3” Multicast”) shows transport with the use of a minimum multicast spanning tree that only requires three transmissions (the source and two relay-nodes) to distribute the group traffic to all members.

When it comes to robustness versus resource efficiency, unicast, multicast and flooding have their own advantages and disadvantages. The performance depends on, but is not limited to, the multicast member density, packet symbol rate on the link (packet modulation), the mobility (rate of link breaks) and the link error rate. Link error rate is the rate of errors experienced over a radio link due to channel variations caused by, for instance, interference, mobility and jamming.

Unicast is most robust in situations with error prone links, since it often uses retransmissions Automatic Repeat-Request (ARQ) in situation of lost packets on the MAC layer. On the other hand, if the packet is lost when e.g. mobility has led to a broken link, ARQ on the MAC layer

might not help, but rather consume resources as packets are retransmitted without the next hop being within transmission range. Furthermore, unicast is in most situations, less resource efficient than broadcast since the broadcast domain of wireless communication is not exploited. That is, it is not recognized that a packet only needs to be transmitted once when there are several receivers within the sender's transmission range (e.g., three copies of the packet are sent between the source and node 1 in Figure 3.3 for unicast, but only one packet is sent for broadcast/multicast). For sparse multicast member densities, this does not matter much, and unicast can be a good solution.

Classical IP multicast solutions are very resource efficient in terms of transmitted packets as they aim to build a minimum spanning tree to reach all receivers. Some overhead (signaling traffic) is necessary to build and maintain the spanning tree for the multicast group. This is a less robust technique because of few redundant packet transmissions and no use of ARQ on the MAC layer, thus it is very vulnerable to packet loss due to mobility or error prone link/channels. In order to improve the performance of error prone networks, redundant (mesh) connections are introduced in some protocol proposals. The added redundancy, in mesh, improves the connectivity among group members, and we achieve better resilience against topology changes at the cost of more redundant packet transmissions. For more information about types and characteristics of MANET IP multicast protocols see e.g., [1].

Flooding protocols can be optimized in different manners (e.g., for robustness or for efficiency). These protocols are robust to packet loss both due to error prone links and due to broken links because of redundant packet transmissions. A lost packet from one neighbor might be received from another neighbor transmitting the same packet. A common goal of these protocols is to flood the data to the whole network. For dense member densities, these protocols can often show a good tradeoff between robustness and resource efficiency. They have gained popularity in military networks due to the low signaling cost and high robustness of the optimized flooding techniques as they often have a high density of multicast receivers. The added cost for improved robustness and low signaling overhead is more redundant traffic leading to less residual network capacity for other traffic types.

3.3 Simplified Multicast Forwarding

Simplified Multicast Forwarding (SMF) is an experimental RFC [3], and supports push services natively; any group traffic that is delivered to the network will be flooded by SMF to the whole network without the need for multicast memberships. It is a well-known, and tested, optimized flooding protocol, and thus one of the candidates for group communication support in modern mobile high data rate military radios. The motivation behind SMF is to provide robust multicast support in mobile wireless networks with a high density of multicast receivers (all or most of the users are interested in the group traffic). In such networks, building and maintaining a connected multicast forwarding tree is challenging due to high dynamics.

SMF utilizes two important building blocks; Duplicate Packet Detection (DPD) and reduced relay set. DPD is needed in multi-access wireless networks where the same packet can be

received from more than one neighbor. The duplicated packet must be detected and not retransmitted. Reduced relay set is used to reduce the number of forwarders in the network. SMF aims to flood the group traffic, using a reduced relay set, to the whole network. Thus, SMF does not need to maintain information about multicast group members, nor build a forwarding tree.

SMF is not tied to a specific routing algorithm, but can use various known efficient relay set mechanisms to improve the resource efficiency of the protocol. The idea behind the relay sets is to identify the minimum number of neighbors that must forward a packet in order to reach all two-hop neighbors (form a connected dominated set CDS). Classic Flooding (CF) is defined as the simplest case of SMF where DPD is performed but no reduced relay set is used. The latter is a very robust but less resource efficient solution. A more efficient solution, at the cost of robustness, is to calculate a minimum relay set. Many algorithms are proposed to calculate relay sets, which yield different tradeoffs between redundant packet transmissions (robustness) and resource efficiency. Some of the algorithms are described as appendixes in [3]. The performance of the selected relay set is depended on mobility, node density and traffic load. High mobility calls for a larger set of multicast relays, while high traffic load calls for a reduced set. The most optimal would be to change the relay set depending on the military scenario, as investigated in [10] with respect to traffic load and mobility.

Clearly SMF, as is, is not efficient when the multicast receivers are a small subgroup of the whole network. Hence, we are in this report addressing the problem of limiting the range of SMF's flooding to cover a group that is co-located in a section of the entire radio network while preserving SMF's robustness.

3.4 Explicit Multi-unicast(Xcast)

Explicit Multi-unicast (Xcast) [11] is used in combination with SMF for one of the proposals in this report. Xcast uses the unicast routing protocol to forward group traffic. Consequently, Xcast does not need to build or maintain a multicast tree. Xcast is motivated for small multicast groups in contrast to traditional multicast groups identified by a multicast address. Xcast does not make use of a multicast address, but the source keeps track of the receivers and encodes the identifier of the receivers in a list in the packet header. The unicast routing table is used to route the packets. 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. When there is only one destination left, the Xcast packet can be converted into a normal unicast packet, which can be unicasted along the remainder of the route. This is called X2U (Xcast to Unicast). Due to the header-overhead, these protocols are best suited for small groups. On the other hand, they scale well for a large numbers of small groups since they neither require any state information in the routers, nor signaling to build distribution trees, but rely only on unicast routing. There is no need to maintain a multicast distribution tree, instead the routers must 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 (e.g., voice samples).

Xcast does not differentiate between push and pull mode. In both cases, the multicast source must know all the receivers of the data (to be able to code the list of receivers in the packet header). In pull mode, the multicast source starts with an empty list that is being filled as different nodes join the group, while in push mode, the multicast source needs to acquire the list of receivers from somewhere else. One example can be a soldier sending a gas alarm. Based on the alarm and weather information the affected (geographic) areas are identified resulting in an alarm being sent towards the personnel within the expected gas exposure area(s).

4 Limiting the Forwarding of Simplified Multicast Forwarding to a Defined SMF-Scope

In this chapter, we motivate and describe several methods to adapt and/or modify SMF to efficiently provide group communication for a group where the group members are assumed to be in close proximity of each other and where the group is assumed to be a subset of the nodes covered by the whole network. Hence, we describe and discuss added functionality to SMF that limits the flooding of SMF to only cover the interested receivers of the group traffic. We also propose a method that uses the modified SMF in conjunction with Explicit Multi-unicast (e.g. Xcast) to improve the flexibility of the multicast solution.

4.1 SMF-Scope and multicast groups

We need a method to limit the flooding of SMF to a segment of the network (e.g. a company, platoon etc.). The methods must be able to control the range of SMF, i.e. to set a SMF-Scope for the flooding of SMF. The interested receivers of a group communication service makes up a multicast group. Classic SMF does not pay attention to the multicast group; instead, it floods the multicast group information to the whole network, i.e. implicitly reaching all the group members. When we in this report want to stop SMF from covering the entire network, we must introduce some notion of group membership to SMF in order to constrain the flooding to stop when all group members are covered. We do this by introducing the SMF-Scope to SMF. The reason why SMF was chosen as the multicast protocol in the first place was based on the assumption that the interested multicast receivers are in near proximity of each other, and that there is a high multicast member density in the network segment. Thus, we assume that this expectation also holds for the groups that represent a small segment of the network. This situation is likely for many military scenarios (e.g. friendly force tracking or push-to-talk internal to military units). For the remainder of the report we use the term SMF-Scope to describe the portion of the network that SMF floods the group traffic.

For military scenarios, the following multicast groups are suitable for SMF when SMF-Scope is used to limit the dissemination of group traffic. A SMF-Scope can be defined by:

Organizational multicast groups: We call multicast groups that mirror the military organization for organizational groups. These groups represent all members of a specific part of a military organization e.g., all units in a specific squad, or units in a specific mission.

Geographic multicast groups: With geographic groups the nodes' locations decide if they are part of the multicast group or not. A defined area on a map defines the group, and all nodes positioned inside the defined area make up the group. A geographic multicast protocol e.g. [12] inherently supports geographic multicast groups.

Geographic groups is not commonly used in military networks but it is interesting in order to provide new services such as pushing alarm messages (e.g., gas and artillery alarms) to a geographic area. Geographic groups and organizational groups can be used both for push and pull services.

The focus of the discussion in this report is on using SMF with a defined SMF-Scope to support forwarding of group traffic to organizational groups. We choose this type of groups since these are expected to be used extensively in military operations today, and should be supported efficiently also in a new network architecture as exemplified in the scenario used for this report (chapter 2). The main reasons for introducing an SMF-Scope to the SMF-protocol are to preserve radio resources, thus do not disturb network nodes that are not interested in the group traffic. Network resources are scarce in mobile military networks and, hence resource efficient data dissemination methods must be addressed. Limiting the scope of traffic dissemination is also a security achievement since this reduces the number of data exposed nodes.

For the remainder of the report, the following is the case: We want to ensure efficient and robust delivery of group traffic to the group members of an organizational group e.g. a company in a battalion as shown in Figure 2.1. The figure shows a high data rate radio network spanning a battalion. Two example groups are shown; a company group and a platoon group. However, in challenging terrain for radio propagation, it might be necessary to use nodes that are not part of the group to be able to reach all members of the group as illustrated in Figure 4.1.

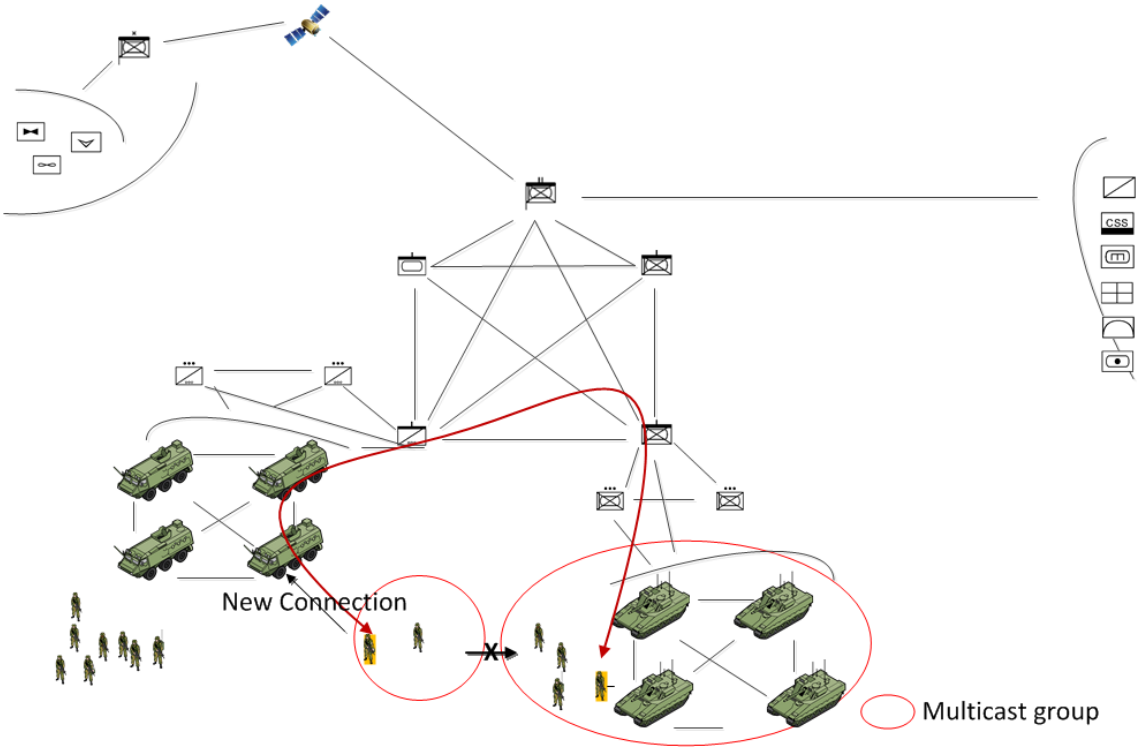


Figure 4.1 Forwarding traffic to group members by way of other nodes in the battalion.

In the following, we address the following problems:

1. Techniques to constrain the flooding of SMF to a defined SMF-Scope.

2. For each technique a discussion on how to set the optimal SMF-Scope in order to get the best tradeoff between robustness and resource utilization. The target is to have the whole multicast group covered by the SMF-Scope.

3. Describing a more flexible multicast solution where SMF-Scopes are used in conjunction with Xcast. In this situation, a subset of the multicast group is covered by one or several SFM-Scopes and these (as well as other lone members) are connected with Xcast.

4.2 Techniques for SMF-Scoping

4.2.1 TTL to set the SMF-Scope

A straightforward method to set the scope of SMF to a smaller size than the complete network, is to set a limit on time to live (TTL) for the IP packet in the network. All routers in an IP network decrement the TTL by one when they forward the packet, thus if the source decides to set the TTL=3, the packet will traverse at most 3 hops in the network. This is an easy but not very efficient solution. The main reason is the difficulties to set the best TTL value. The number

of hops required to reach all members in the multicast group will differentiate in different terrain (e.g., flat, urban, forest, mountains), different operations (e.g. convoy, combat) and even different channel conditions. Furthermore, the source can be on the edge of the network that represents the group, or in the center. This makes it very difficult to predict the correct TTL to make sure that all multicast members are covered by the SMF-Scope while at the same time limiting the flooding to a minimum. This method is best suited in cases where the source is located in the center of the group. The advantage with this solution is that it only requires permission to set the TTL value of the traffic flow. There is no need for modification of the SMF-protocol. Another advantage is that the source decides the TTL and thus the forwarding nodes do not need to have any knowledge about the group members or the SMF-Scope.

This method can be improved with some added information. For the multicast groups that we consider here, we have said that a military unit is identical to the group e.g., the group represents all the members of a platoon. Thus if the node knows its organizational association it also knows that it is part of the multicast group. Given that each source node 1) knows its organizational association and 2) also knows the IP addresses of the other members of its group (military unit), then the node can look at the unicast forwarding table, to get a better understanding of the network topology and use this to help set the TTL limit. If the metric of the routing protocol is hop count, the routing table can be used directly to find the network span of the group. If some other metric is used, then it might be necessary to access the topology database of the unicast routing protocol to find the necessary information to set TTL.

Based on the routing table, the hop count or the distance to the furthest node in the multicast group plus a guard value for added robustness can be used directly to set the TTL. This improvement ensures that the whole group is covered by the SMF-Scope, but unnecessary traffic is likely to flow in the network (e.g., the amount of unnecessary traffic depends on the source location in the network; whether the source is situated in the middle of the network versus at the edge of the network topology of the group). The advantage with this method compared with the previous basic TTL method is to support the possibility to automatically change the TTL in response to topology changes. This technique is robust and can support delivery of group traffic to the multicast group as long as the unicast routing protocol is able to keep up with the topology changes. Most router platforms provide methods to read the forwarding table, thus this can easily be done by a modified SMF protocol. If the hop count is not available in the forwarding table, the method needs access to the unicast routing protocol process.

4.2.2 Administrative SMF-Scope with aid of TTL

Another technique is to combine TTL limit with administrative scoping [13] as used in the Internet. For more information about administrative scope, see also appendix A. Also with this method, it is assumed that each node knows its organizational association. With this technique, the multicast source sends the group traffic with a preconfigured static TTL. Each forwarding node that is part of the multicast group will not decrement the TTL. Consequently, as long as the packet is being forwarded by members of the organizational multicast group, the TTL is not

being decremented. The TTL decreases first when it is being forwarded by a node that is not part of the group, and stops when TTL=0.

This method is robust for some mobility patterns and challenging terrain/channel but not to partitioning of the multicast group where the network distance between group members exceeds the set TTL. As for the plain TTL technique, this method requires permission to set the TTL, and must have the ability to not alter the TTL value of the traffic flow. Hence, SMF must be modified to not decrement the TTL value for each SMF packet within the SMF-Scope.

4.2.3 Administrative SMF-Scope with aid of MultiPoint relays (MPR)

It is also possible to combine SMF forwarding rules with mechanisms similar to administrative scoping. Each SMF relay decides if it should forward the group traffic or not. The forwarding decision is based on local information about the nearby presence of other nodes that are part of the group. It is again assumed that each node 1) knows its organizational-association and 2) also knows or acquires the IP address of the other members of the multicast group.

A standard SMF with the optimization technique of choice can be used. For the following description we assume the Multi Point Relays (MPR) algorithm of OLSR [14] as the optimization technique. The MPR algorithm selects the minimum set of one-hop neighbors to reach all two-hop neighbors. The MPR method is also the commonly used method by SMF to choose multicast forwarders.

In our example, we assume that SMF is running in the entire battalion and that an MPR set is selected for each network node. In administrative multicast scoping, an edge router is responsible of either forwarding or discarding the group traffic. In our example, all MPRs take a similar role as the edge routers; the MPRs have to decide to forward the group traffic or not. That is, the MPRs located on the edge of a multicast group will typically decide to drop group traffic packets, while MPRs located closer to the center of the group forward the packets.

The MPRs must decide to reject or forward the group traffic. The decision depends on whether the multicast solution should be optimized for robustness or for resource efficiency. All MPRs know their 1-hop neighbors and 2-hop neighbors (this is needed to elect the MPRs in the first place). An MPR forwards group traffic according to the SMF rules. In addition to the SMF rules, each MPR investigates whether itself and/or a 1-hop neighbor and/or a 2-hop neighbor are a member of the multicast group.

If the goal is to optimize for resource efficiency and not allow the group traffic to be forwarded by any non-group member, then the forwarding rule is; the MPR forwards traffic only if the MPR itself is member of the multicast group as shown in Figure 4.2

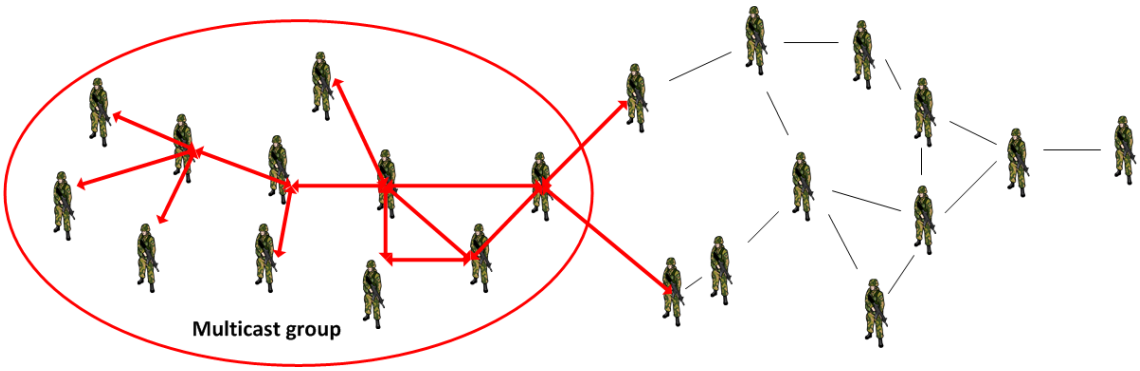


Figure 4.2 Group traffic (red arrows) forwarded only by MPRs that are member of the multicast group

This method is preferable in situations when the multicast members keep a tight formation and the terrain allow for good radio coverage among the SMF-Scope forwarders.

If the goal is to have more robustness in challenging topologies, then it is often required to use nodes that are not part of the group as relays in order to keep the group connected. In such situation, the forwarding rule can be; the MPRs forward traffic if either the MPR itself is a multicast member or a 1-hop or 2-hop neighbor node is a multicast member. For this case, the group traffic will radiate up to three hops away from a multicast member before it is being stopped as illustrated in Figure 4.3.

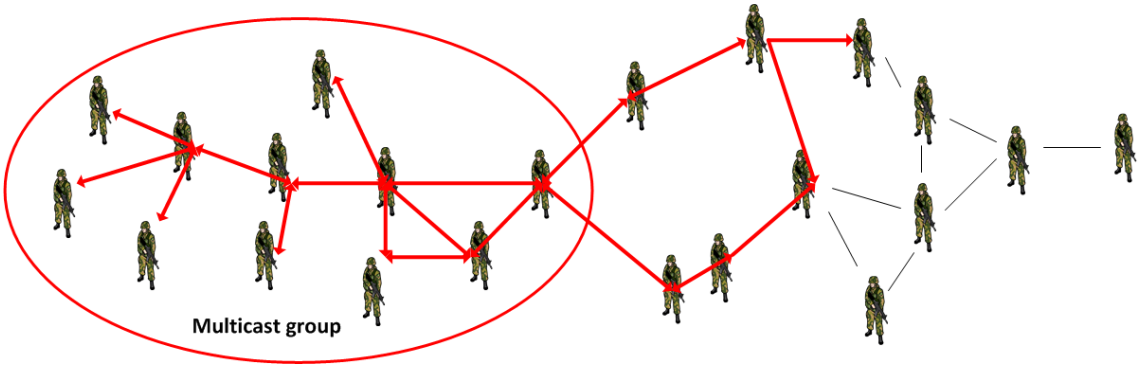


Figure 4.3 Group traffic (red arrows) forwarded as long as an MPR sees a multicast member among its one-hop or two-hop neighbors.

This method is very robust and is able to connect multicast members that can be up to 5 hops apart as illustrated in Figure 4.4. However, this comes at the cost of potentially flooding the traffic to many non-member nodes.

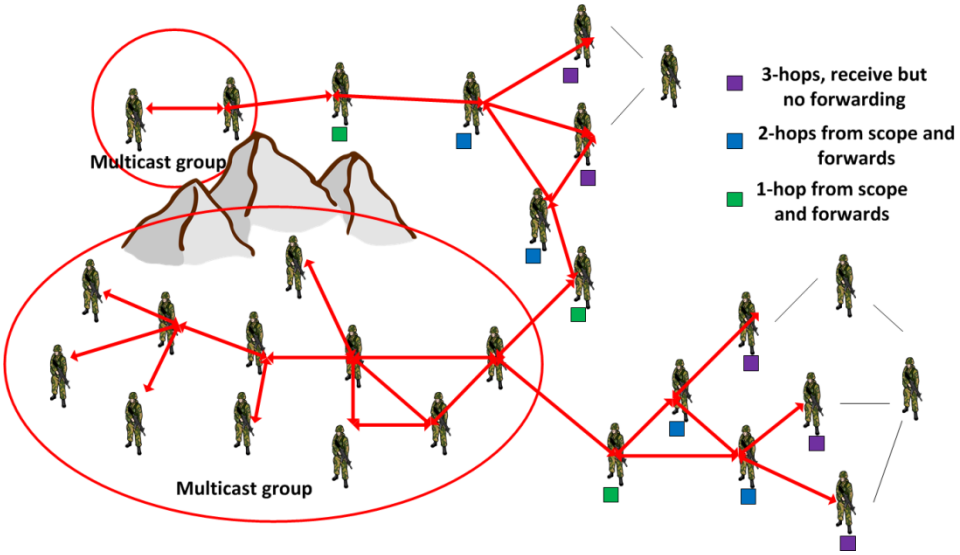


Figure 4.4 A fragmented multicast group is connected when MPRs forward group traffic in case of multicast members being within 2-hops from each other.

Several different configurations for robustness can be supported simultaneously with this MPR method. The requirement is that all MPRs keep state information about the multicast members of the different groups. This membership information can be statically configured, or the 1-hop and 2-hop neighbors can signal their group memberships as part of the 2-hop topology information signaling. Furthermore, the method can dynamically adapt to the size and topology of the multicast group. The benefit of this technique is that it can be tailored to be either very resource efficient or fairly robust to mobility and challenging topologies. Standard SMF must be modified to support this technique, but there is no need for information from other protocols that can be difficult to access.

4.3 Tailored SMF in conjunction with Explicit Multi-unicast(Xcast)

The presented methods, to tailor the SFM-Scope, vary regarding flexibility, dynamics and robustness. In challenging topologies or in situations where the topology of the group members will change much during the operation (the group needs to split up and/or mingle with other units) the SMF-Scope must be set very large to ensure that the whole multicast group is covered by the SMF flooding. This is not very efficient and better methods to provide delivery to the whole multicast group is required to preserve resources.

We propose one method that allows the multicast group to be served by several smaller SMF-Scopes and where the SMF-Scopes are interconnected with added forwarding logic. The forwarding logic must ensure robust traffic delivery to the complete group. The role of SMF-Scope leaders is proposed. These leaders assist in the interconnection of multiple SMF-Scopes. The proposed method shares many similarities to MANET protocols build on clusters such as Hierarchical OLSR [15].

The SMF-Scope leader can be statically configured or dynamically elected by the highest IP address (or similar methods). It is assumed that the multicast group is fully connected when the operation starts. The node that is chosen as the first SMF-Scope leader becomes the designated SMF-Scope leader. The SMF-Scope leader announces itself to the SMF-Scope and if it sees another announcement with a higher IP address, then it will remain silent and remove itself as leader.

SMF-Scope leaders are responsible for disseminating heartbeat messages to the SMF-Scope members to keep track of SMF-Scope connectivity. The heartbeat messages must have the same range as the flooding of the group traffic. The choice of method for heartbeat dissemination (the SMF-Scope of the dissemination) could be different for different military scenarios and operation types. It might also be beneficial to change methods during an ongoing operation. One plausible implementation is to use “Administrative SMF-Scope with aid of TTL” as described in section 4.2.2 for the heartbeat messages. If a group member does not receive the expected heartbeat for a predefined timeout period, then it is assumed that the group member is outside the range of the SMF-Scope. The nodes will in response to the timeout issue a scope leader heartbeat message in order to establish a second, SMF-Scope. The node with the highest IP address will become the SMF-Scope leader for the new SMF-Scope segment. In this manner several SMF-Scopes can be established to support an organizational multicast group that must spread out for some reason.

The new SMF-Scope leader of the partitioned multicast group segment must establish connection with the designated SMF-Scope leader. One method can be to use the unicast routing table. The designated SMF-Scope leader has the function of being a meeting point during the establishment of the connection between SMF-Scope leaders as shown in Figure 4.5. The forwarding logic works like this: The SMF-Scope leader of each SMF-Scope forwards all traffic generated by all multicast sources within its SMF-Scope, via unicast, to the designated SMF-Scope leader. The designated SMF-Scope leader keeps state of all SMF-Scope leaders of the multicast group. Due to its role of being the meeting point, it receives all group traffic, and further uses Xcast (that address the SMF-Scope leaders) for efficient forwarding of the group traffic to all SMF-Scopes that make up the support for the multicast group. Each SMF-Scope leader is further responsible for forwarding the group traffic received via Xcast within its SMF-Scope, (using one of the described SMF-Scope techniques).

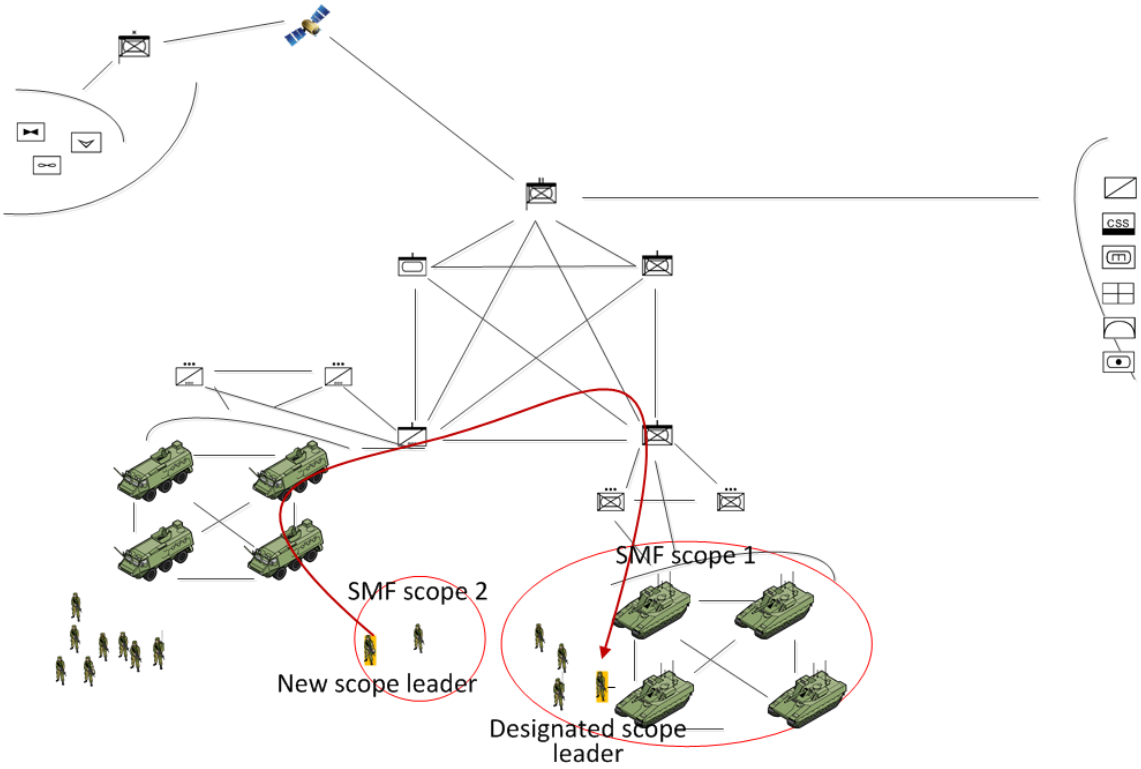


Figure 4.5 A new SMF-Scope segment elects a new leader and connects back to the designated SMF-Scope leader.

In case all/most members of the multicast group are sources and receivers of the traffic (e.g., friendly force tracking), this method would require traffic being sent from all SMF-Scope leaders to the designated SMF-Scope leader for further distribution. The method shares many similarities with a shared multicast tree with a common Rendezvous Point (RP) as used by PIM-SM [16]. The method uses unnecessary resources as traffic is sent to one distribution point and further multicasted from this point. Additionally, the designated SMF-Scope leader is a single point of failure.

A second method, optimized for a traffic pattern with multicast sources in all SMF-Scope segments, is to establish a network between the SMF-Scope leaders. The SMF-Scope leaders must in this case build an overlay network between them. In order to establish the overlay network, the SMF-Scope leaders must discover each other. This can be done by asking the designated SMF-Scope leader for the list of SMF-Scope leaders. Each SMF-Scope leader can then use Xcast to address all the other SMF-Scope leaders for the multicast directly. An alternative to asking the designated SMF-Scope leader for the list of SMF-Scope leaders is to flood a discovery message to the whole network, requesting information of the other SMF-Scope leaders. The latter method removes the single point of failure of the designated SMF-Scope leader and is therefore more robust at the cost of added overhead.

The method discussed in this section supports forwarding of group traffic to a multicast group where the topology can change from a close formation to a split or spread formation and where it is assumed that a physical connection is available between the SMF-Scope segments. If the network is physically partitioned, it is not possible to connect the network segments until the topology change to a fully connected network. The technique is able to support a dynamic group topology at the cost of the added overhead to establish and maintain the overlay network between the SMF-Scope leaders.

The technique requires changes to the SMF protocol as well as support for Explicit Multi-unicast e.g., Xcast in all nodes. The protocol to establish and maintain the SMF-Scope leader infrastructure must also be designed. The proposal must be further studied with simulations to verify its performance versus overhead.

The method shares many similarities with Mobile IP [17]. Each SMF-Scope leader can be seen as a mobile node; the mobile node/SMF-Scope leader has moved from its home network. The designated SMF-Scope leader can be seen as a home agent keeping track of the mobile node. With this analogy the method proposed in this section can be implemented by use of existing software and functionality, by reusing the techniques of mobile IP. Some modification is, however, required. The common implementation of Mobile IP is for Local Area Network (LANs) and assumes proxying of the address resolution protocol (ARP). In our proposal, the home agent must operate on IP addresses instead of MAC addresses. Mobile IP, and how it can be used to support the method given in this section, is briefly described in appendix A2.

5 Support for flexible group communication in a heterogeneous mobile military network

5.1 Flexible group communication

The method described in section 4.3 can be extended to support a wider range of group types. One example is where external sources and receivers are not part of the organizational group that made up the original multicast group, can also join the group. In military operations, there are situations when it is beneficial for an external source to send data to a specific military unit. Examples are alarms and orders. It is also of interest to allow external nodes to join the multicast group in order to receive information from a military unit. One example can be a MEDEVAC team that wants to subscribe to friendly force tracking from the company with the wounded soldier. These external multicast members can be quite far away, geographically, from the rest of the group.

For the following we assume that the existence of the relevant multicast group and the designated SMF-Scope leader is known beforehand. Alternatively, in a situation where the multicast group is not preconfigured, and where the external nodes are not aware of the multicast group, it is assumed that the designated SMF-Scope leaders announce themselves along with the multicast group to an assigned network registry.

In situations where external sources want to send traffic to a specific multicast group, the external sources can unicast the information to the designated SMF-Scope leader. In case only the designated SMF-Scope leader is targeted by the external source, the designated SMF-Scope leader is responsible of distributing the information in his SMF-Scope and to the potentially remaining SMF-Scope leaders. Figure 5.1 shows two sources that send group traffic to the designated SMF-Scope leader.

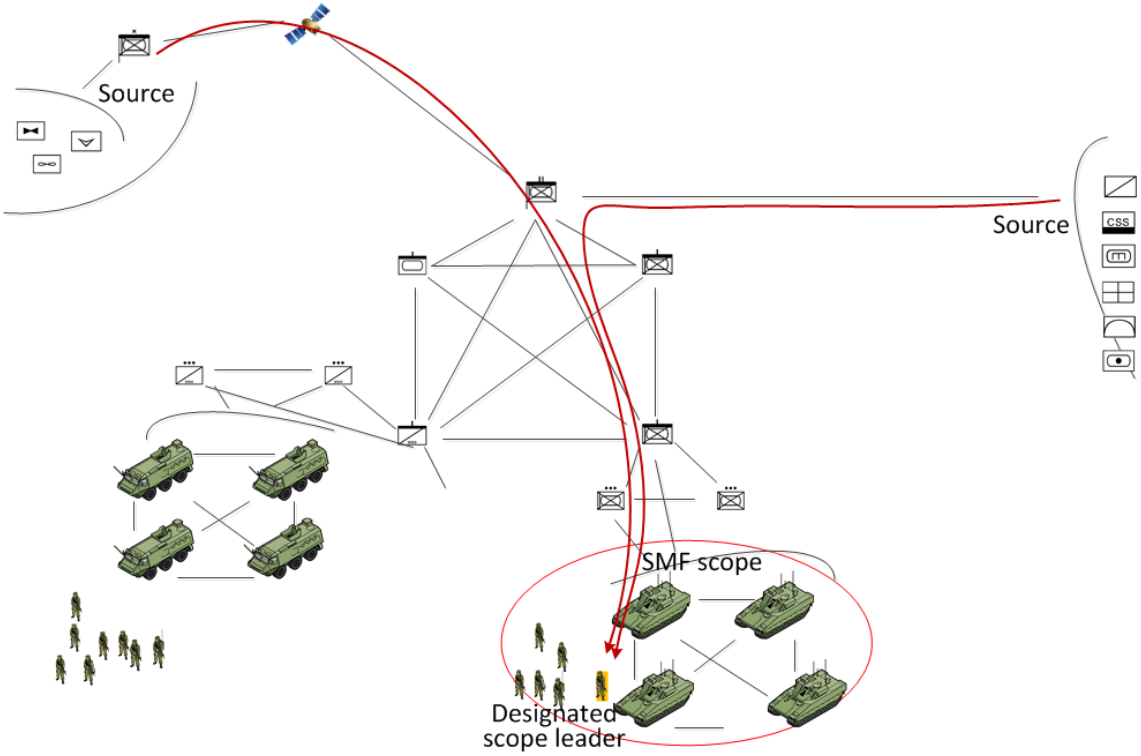


Figure 5.1 External sources send group traffic to the designated SMF-Scope leader.

An alternative method, in case of multiple SMF-Scope leaders, is for the external source to join the overlay network for the SMF-Scope leaders and use Xcast to send its group traffic to all SMF-Scope leaders of the multicast group directly in the same manner as traffic is disseminated between SMF-Scope leaders. The information about the SMF-Scope leaders can be acquired by requesting the information from the SMF-Scope leaders' overlay network. Figure 5.2 shows an external source sending directly to the SMF-Scope leaders.

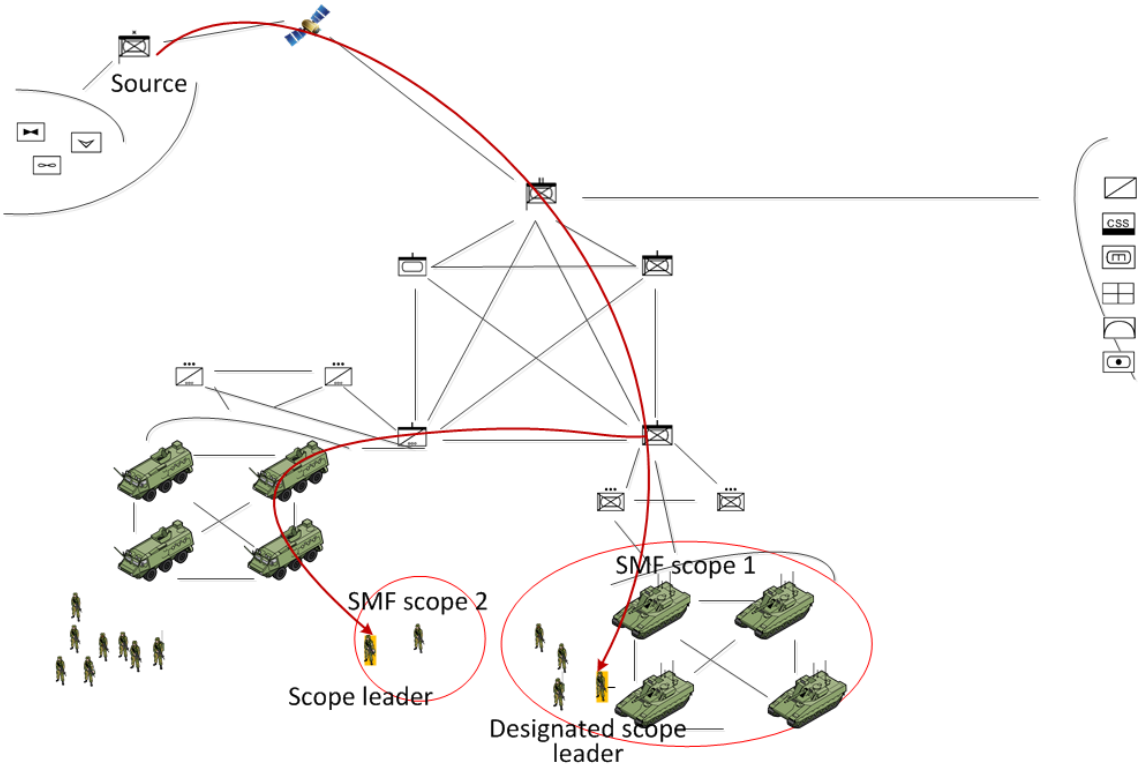


Figure 5.2 An external source sends group traffic to a multicast group represented by two SMF-Scope leaders connected by Explicit Multi-unicast(Xcast). The source knows the address of each SMF-Scope leader.

A similar procedure can be used for external receivers. An external node that wants information from the multicast group can send a join towards the designated SMF-Scope leader. The designated SMF-Scope leader treats the external receiver(s) in a similar manner as other SMF-Scope leaders and includes the external receiver(s) in the Explicit Multi-unicast messages that forward the group traffic of the group. Alternatively, the external receivers can join the Xcast group of SMF-Scope leaders.

The scenario described (scoped SMF in conjunction with Xcast) is one that could potentially be served similarly well with a traditional mesh-based multicast protocol. It must be further studied how the SMF and Xcast solution performs compared with such protocol (e.g., On-Demand Multicast Routing Protocol (ODMRP) [18]).

5.2 Group communication over heterogeneous mobile military radio-networks

The method described in the section 4.3 can also be used to provide support for group communication across a heterogeneous mobile military network. The external multicast members mentioned above might sometimes be connected to another radio network that cannot be reached by the SMF protocol in the battalion radio network example in Figure 2.1. Another example is a connected coalition network where each partner provides friendly force tracking

distributed with SMF in their national radio networks. There is a need to share the friendly force tracking between the partners. For both of these situations Xcast can be used to connect the multicast members in different networks. Xcast relies on unicast routing to forward the traffic. Thus, if unicast routes are available in the heterogeneous network, the Xcast service to connect the designated SMF-Scope leaders of each SMF-Scope and external receiver/sources can be made available. In a heterogeneous mobile network, it will seldom be advantageous to flood the whole network to request information about the multicast group. Hence, some assigned network registry or preconfigured information should be available to the designated SMF-Scope leader. How this is done is out of scope for this report.

6 Related work

There exist a few proposals for multicast scoping. From civilian networks, multicast scoping has been used with the help of Administratively Scoped IP Multicast [13] and Time To Live (TTL). The main idea behind scoped TTL is to assign a TTL value to an IP packet depending on the network scope of this multicast packet. In Administrative Scoped multicast each network edge router is given a control functionality to be responsible to either forward or discard multicast packets. Military networks share many similarities to these civilian applications. The network is typically built hierarchically and groups are often clearly defined. As an example, a military group could be a platoon, company or battalion. The group participants within these groups are typically operating in close proximity and might reuse civilian technology for multicast forwarding based on TTL and/or administrative scoped domains. We have used similar techniques in a few of the proposals discussed in this report.

In [19], Yi et al. extended the Landmark Ad hoc Routing (LANMAR) protocol [20] with multicast routing with the name Multicast-enabled Landmark Ad Hoc Routing (M-LANMAR). M-LANMAR is a two-tier multicast protocol and inherits the benefits of a hierarchical multicast protocol. It unicasts group traffic to the team leader at tier one, where tier one can consist of elevated nodes. The unicast packets are further flooded by the team leader within the team at tier two or ground nodes. With some modification the tier two groups could be organized to cover a similar multicast group as the ones supported by an SMF-Scope. Results show that M-LANMAR provides efficient and reliable multicast compared with the application of a “flat” multicast exemplified by On-Demand Multicast Routing Protocol (ODMRP) [18] that does not exploit team coordinated motion.

In [23], the authors describe an elastic multicast design based on SMF. The main idea in this work was to use a larger relay set for multicast forwarding in areas where the network are affected by frequent topology changes, while using a reduced topology set in more stable network areas. In a more recent work, this protocol is extended [21]. In [21], the authors added several functionalities where one of the contributions was to regulate the multicast rate.

Basically, it works by rate limiting multicast flows unless instructed otherwise. That is, multicast flows are flooded according to the design in [23], but multicast flows with high data rate are throttled by a token bucket. All multicast flows are disseminated by SMF, but the available per hop rate is based on having a downstream receiver or not. A node interested in a specific multicast flow sends an EM-ACK upstream informing the upstream node to not throttle the multicast flow. Consequently, network portions having multicast receivers will not throttle the group traffic while portions not having receivers will rate limit the group traffic. This method does not directly solve the problem of limiting the flooding to a specific SMF-Scope, but is able to reduce the traffic (throttle) to SMF nodes that are not interested in traffic for a specific group.

In [4] the authors focused on group communication and elevated nodes using SMF. Standard SMF was used as a baseline and compared with methods that utilize an elevated node with added functionality for robustness. The work analyzed the effect of an elevated network node and its impact on the dissemination of multicast packets using SMF. An elevated node has a larger footprint than ground nodes and is therefore often preferred as a relay node for multicast. However, one consequence of the large footprint is a reduction of the preferred redundancy of multicast forwarding in SMF. Two problems were addressed in the paper; the first problem was to improve the probability of reaching the elevated node with multicast traffic while at the same time reduce the redundant transmissions. Unicast was selected as the best forwarding method from the multicast source to the elevated node. The source encapsulates the multicast traffic and sends it to the elevated node. The elevated node decapsulates the multicast packet and forwards it using SMF. However, unicast is not very robust against mobility. Multicast traffic was therefore buffered at the source before it was encapsulated and sent up to the elevated node. The source waits for a copy of the buffered multicast packet to arrive from the elevated network node via the SMF distribution until a timer expires. If the timer expires, the source itself sends the buffered data as multicast using plain SMF. Using the buffer will help in situations where the unicast path up to the elevated network node or the multicast path from the elevated network node is disrupted. A UAV as a network element can in many situations be used to reach out to a specific co-located group. Two parameters need to be addressed to fully utilize the UAV as multicast relay to cover a specific co-located group. The combination of UAV altitude and antenna needs to be further investigated.

7 Conclusion

In this report, we have exemplified a possible architecture for high data rate radios that might be one of several future architectures used by the military forces. We want to be able to provide the traditional group communication services of friendly force tracking and push-to-talk voice in an efficient manner to smaller groups than the whole network in the chosen network architecture. We have based the solutions on Simplified Multicast Forwarding (SMF) due to its simple

protocol design (no multicast tree is built or maintained) and its robustness. A multicast group at the tactical edge is often identical to a military unit (e.g., a company or a platoon). This type of group, presents the target group for the methods proposed and discussed in this report.

We have described three different methods that can be used to constrain the flooding of SMF to cover the multicast group but not flood the whole network. One method "TTL to set the SMF-Scope" only requires access to set the TTL of the group traffic; it does not require any changes to the protocols. This method might be possible to use with many existing military radios. The method is very basic and is not able to adapt to varying group topologies. The two other proposals are able to adapt somewhat to changing topologies and can be tailored for different levels of robustness. These require some simple changes to the SMF protocol.

When one SMF-Scope is used to serve all the multicast group members, it is important to set the SMF-Scope large enough to ensure that the whole multicast group is covered. We have also proposed a more flexible method that allows the multicast group to be served by several small SMF-Scopes by using Explicit Multi-unicast (e.g., Xcast) to connect the different SMF-Scopes. This method can also support group traffic to a multicast group that includes external sources and receivers that are not part of the military unit and that can be located far away from the unit. The method inherits mechanisms typically present in cluster protocols to build a network of SMF-Scope leaders to keep the SMF-Scopes connected, as well as being the connection between the SMF-Scopes and external sources and/or receiver. This opens for more flexible group communication services than seen today. The proposed method can also overcome limitations seen by other multicast protocols in a heterogeneous network environment.

This report describes the design, but does not provide quantitative evaluations. Hence, more work is needed to simulate and/or emulate the solutions to see how well the protocols perform in a typical military mobile network.

References

[1] M. A. Brose and M. Hauge, "Group communication in mobile military networks," FFI Rapport 2012/00294, 2012.

[2] M. Hauge, M. A. Brose, and O. I. Bentstuen, "Group communication in tactical networks: A discussion," in proceedings *MCC*, St. Malo, France, pp. 1-8, 2013.

[3] J. Macker(ed.). "Simplified Multicast Forwarding", IETF, *RFC6621 (Experimental)*. May, 2012. Available: http://www.ietf.org.

[4] L. Landmark, E. Larsen, A. Fongen, and Ø. Kure, "Improving simplified multicast forwarding using an elevated relay node," in proceedings *MoWNeT*, Avignon, France, pp. 1-6, 2017.

[5] S. E. Deering and D. R. Cheriton, "Multicast routing in datagram internetworks and extended LANs," *ACM Trans. Comput. Syst.*, vol. 8, no. 2, pp. 85-110, 1990.

[6] J. Grönkvist, A. Komulainen, U. Sterner, and U. Uppman, "Dynamic scheduling for cooperative broadcasting in tactical ad hoc networks," in proceedings *IEEE MILCOM*, Baltimore, MD, USA, pp. 1034-1040, 2016.

[7] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan. "Internet Group Management Protocol, Version 3", IETF, *RFC3376*. October, 2002. Available: http://www.ietf.org.

[8] R. Vida (Ed) and L. Costa (Ed). "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", IETF, *RFC4604*. June, 2004. Available: http://www.ietf.org.

[9] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile Ad-Hoc networks," *Commun. Surveys Tuts*, vol. 11, no. 1, pp. 78-91, 2009.

[10] E. Larsen, L. Landmark, V. Pham, Ø. Kure, and P. E. Engelstad, "Optimized group communication for tactical military networks," in proceedings *IEEE MILCOM*, pp. 1905-1911, 2010.

[11] R. Boivie, N. Feldman, Y. Imai, W. Livens, and D. Ooms. "Explicit Multicast (Xcast) Concepts and Options", IETF, *RFC5058 (Experimental)*. Nov. 2007. Available: http://www.ietf.org.

[12] Y.-B. Ko and N. H. Vaidya, "Flooding-Based Geocasting Protocols for Mobile Ad Hoc Networks," *Mobile Netw Appl*, vol. 7, no. 6, pp. 471-480, 2002.

[13] D. Meyer. "Administratively Scoped IP Multicast", IETF, *RFC2365*. July 1998. Available: http://www.ietf.org.

[14] T. Clausen, C. Dearlove, P. Jacquet, and U. Herberg. "The Optimized Link State Routing Protocol Version 2", IETF, *RFC7181*. Apr. 2014. Available: http://www.ietf.org.

[15] G. Ying, L. Lamont, and L. Villasenor, "Hierarchical OLSR - a scalable proactive routing protocol for heterogeneous ad hoc networks," in proceedings *IEEE WiMob*, pp. 17-23 Vol. 3, Aug. 2005.

[16] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, R. Parekh, Z. Zhang, and L. Zheng. "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", IETF, *RFC7761*. March, 2016. Available: http://www.ietf.org.

[17] C. Perkins (Ed.). "IP Mobility Support for IPv4, Revised", IETF, *RFC5944*. Nov. 2010. Available: http://www.ietf.org.

[18] S.-J. Lee, W. Su, and M. Gerla, "On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks," *Mob. Netw. Appl.*, vol. 7, no. 6, pp. 441-453, 2002.

[19] Y. Yi, M. Gerla, and K. Obraczka, "Scalable team multicast in wireless ad hoc networks exploiting coordinated motion," *Ad Hoc Networks*, vol. 2, no. 2, pp. 171-184, 2004.

[20] P. Guangyu, M. Geria, and H. Xiaoyan, "LANMAR: landmark routing for large scale wireless ad hoc networks with group mobility," in proceedings *ACM MobiHoc*, pp. 11-18, 2000.
[21] B. Adamson, J. P. Macker, and J. W. Weston, "Elastic multicast: Design extensions and experimentation results," in proceedings *IEEE MILCOM*, Baltimore, MD, USA, pp. 581-586, 2017.
[22] R. Hinden and S. Deering. "IP Version 6 Addressing Architecture", IETF, *RFC4291*. Feb. 2006. Available: http://www.ietf.org.
[23] C. Danilov, T. R. Henderson, O. Brewer, J. H. Kim, J. Macker, B. Adamson, "Elastic Multicast for Tactical Communications", IEEE Military Communications (MILCOM) Conference, pp. 1-6, Oct 2012.

A Appendix

A.1 Administrative scoping address scheme in IPv4 and IPV6

In this section, we describe the support of multicast scope within IPv4 [13] and IPv6 [22] and show how addresses are allocated for this purpose by the different IP versions. Both versions support multicast scoping, but differ in their multicast scope features.

IPv4 and IPv6 both support multicast scoping. In IPv4, the administrative scope is defined in RFC2365. One of the key properties of administrative scope in RFC2365 is:

"The key properties of administratively scoped IP multicast are that (i). Packets addressed to administratively scoped multicast addresses do not cross configured administrative boundaries, and (ii). Administratively scoped multicast addresses are locally assigned, and hence are not required to be unique across administrative boundaries."

As defined, administrative scope in IPv4 cannot be used across administrative domains. Hence, a boundary router will not forward packets matching an interface's boundary definition in either direction. The address range allocated for administrative scope in IPv4 is defined to be the range 239.0.0.0 to 239.255.255.255.

IPv6 defines multicast addresses differently from IPv4. From RFC4291:

"An IPv6 multicast address is an identifier for a group of interfaces (typically on different nodes). An interface may belong to any number of multicast groups. Multicast addresses have the following format:

```
|   8    |  4 |  4 |                   112 bits                   |
+------ -+----+----+----------------------------------------------+
|11111111|flgs|scop|                   group ID                   |
+--------+----+----+----------------------------------------------+
```

"

The scope value is a 4-bit multicast scope value used to limit the scope of the multicast group. For instance scope value 4 indicates Admin-local scope and is defined as:

"Admin-Local scope is the smallest scope that must be administratively configured, i.e., not automatically derived from physical connectivity or other, non-multicast-related configuration."

Scope value 8 indicates Organization-Local scope defined as:

"Organization-Local scope is intended to span multiple sites belonging to a single organization."

The flag field sets the flag for the specific multicast address. As for RFC 2373 there is only one flag defined; the Transient (T) flag. The flag field is only being used by the low order bit. If 0 is

set, it means that this address is permanently assigned and well known, while 1 indicates that it is a transient address. IPv6 provides a 112 bits group ID that is unique within its scope.

A.2 Mobile IP

Mobile-IP [17] is a well-known method used for connecting mobile nodes moving outside of their home address range or network boundary. Many implementations exist, and Mobile IP is a building block that can be used in our setting. The main problem that Mobile-IP tries to solve is to allow a mobile node to move from one network to another and still be reachable with the IP address of its home network. Mobile-IP uses a home agent responsible of setting up the connection from the current connection point of the mobile node to the node that is trying to reach the mobile node via its home address.

Multicast forwarding is supported in Mobile-IP. For multicast pull-mode, a mobile node can join a multicast group by one of two methods; either connecting directly to a multicast router in the visited network if one exists, or send a join message to the home-agent located in the home network. In our case, the mobile node would need to send a join to the home agent in the home network. Upon receiving multicast traffic, the mobile node can disseminate multicast traffic by using a similar method as the one selected for multicast dissemination in the home network, for instance by using the same method as exemplified in section 4.2.2. Hence, the Mobile-IP method can be reused, more or less as is, for connecting separate SMF-Scopes. In our setting, the mobile node will be the new scope leader, while the home agent is the designated scope leader.

Simulations must be done to compare the performance and overhead of the different methods.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

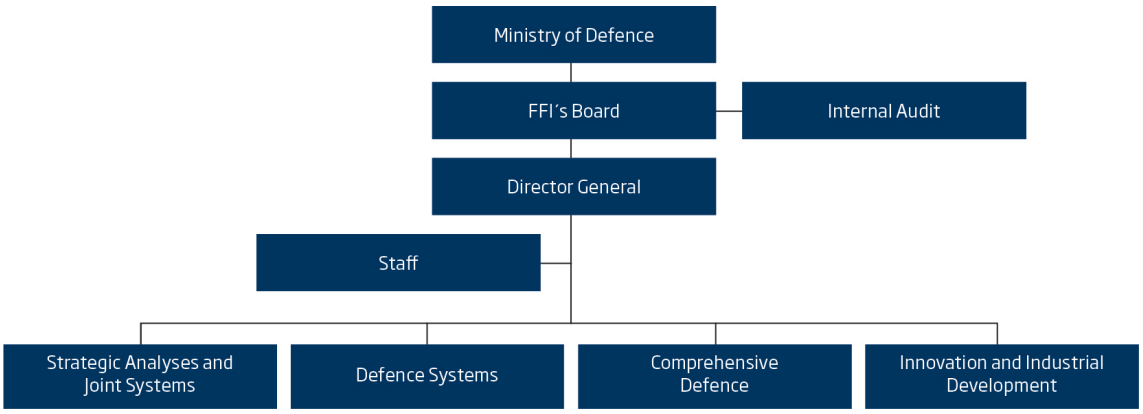
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment