www.czasopisma.pan.pl PAN www.journals.pan.pl
INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2014, VOL. 60, NO. 1, PP. 7–13
Manuscript received January 13, 2014; revised March, 2014. DOI: 10.2478/eletel-2014-0001

Selected Issues of QoS Provision in Heterogenous Military Networks

Mariann Hauge, Lars Landmark, Piotr Łubkowski, Marek Amanowicz, and Krzysztof Maślanka

***Abstract*—Tactical ad-hoc networks are evolving today towards complex heterogeneous networks in terms of architecture, protocols and security. Due to the difference in network resources and reliability, end-to-end quality of service provisioning becomes very challenging. If we also take into account communication issues such as unpredictable connectivity, preferential forwarding for special traffic classes, intermittency due to node or communication link failure, the problem is further aggravated.**

In this article, we examine the major challenges that must be solved in order to provide efficient QoS provisioning in the heterogeneous network. Finally we describe QoS-aware mechanisms for inter-domain and intra-domain heterogeneous networks, also including real-time services provision in highly mobile environments.

***Keywords*—E2E QoS, connectivity, routing, heterogenous networks**

I. Introduction

In recent years there has been a growing desire to always be connected, and to provide network access to individual warfighters. To accommodate this need, networks with different characteristics (e.g., transmission technologies, protocols, policies, etc.) must be connected. The consequence is that the resulting network is very heterogeneous, and that heterogeneous networks eventually will become the norm for military tactical mobile networks as it is for strategic networks and in the Internet. The heterogeneous networks (HN) may include both wired and wireless components. Also, heterogeneous networks may be composed of two or more internally homogeneous networks. At a higher level, heterogeneity may refer to different network policies as well as trust and security management. In tactical military networks the potentially relatively large variation in available network resources and the potentially very low data rates, imply that it is challenging to solve efficient end-to-end (E2E) quality of service (QoS) provisioning in these networks.

The importance of providing end-to-end QoS over heterogeneous networks is widely discussed in the literature, in particular if applied to the IP world. Reference [1] states that "... the network operators are willing to open up their network resources to innovative new service providers, which include mechanisms for supporting end-to-end QoS guarantees (across multiple domains), and for the flexible and dynamic creation of new services".

M. Hauge and L. Landmark are with the Norwegian Defence Research Establishment (FFI), Kjeller, Norway.

P. Łubkowski, M. Amanowicz and K. Maślanka are with the Faculty of Electronics, Military University of Technology, Warsaw, Poland (e-mail: piotr.lubkowski@wat.edu.pl).

It will become the norm that medium- to large-scale wireless tactical networks are heterogeneous. They will incorporate sub networks with significant diversity in terms of latency, data-rate, robustness, traffic load, and so forth. To provide a reliable network for different operation types and in varying terrains, a tactical mobile network infrastructure must consist of a variety of wireless network types, e.g., long-range communication for reach-back connections and a higher bandwidth network for local communication. It is important to be able to combine different radio systems in an operation to provide an efficient and robust network, and in order to improve information flow between coalition partners. A common heterogeneous network gives the operator a single entry point to all network resources, both national equipment and equipment owned by the coalition partners participating in the mission. Such network of networks will be better utilized, and multiple transmission technologies and routing paths will improve communication reliability by providing alternative routing paths during e.g. jamming attempts.

In this network, the resources will vary and efforts to minimize the signaling traffic in low capacity networks must be taken. The traffic load can often overtake the capacity of the heterogeneous network. It is therefore crucial to support end-to-end QoS and prioritization of operation critical traffic. It is also important to use the network resources in an optimal manner for the mission and thus make sure that only traffic that has a high chance of reaching the destination is admitted into the network. It is also crucial that the QoS solutions in these single domain (or collection of small domains) networks must interact very efficiently with the inter-domain QoS architecture. Furthermore, it is necessary to develop an auto configuration mechanism to support inter-domain routing protocols in case of changes in the deployable networks' topology.

Nevertheless, the provision of end-to-end QoS (both intra-domain and inter-domain) while maintaining the required level of service availability, when different types of mobility is also taken into account, is still an open issue.

The remaining part of the paper is organized as follows: Section II point to related work. Section III discusses important QoS challenges in the military HN. The results of work relating to the provision of intra-domain network connectivity are described in section IV. In section V we explain the mechanisms for inter-domain E2E QoS support introduced in the routing and signaling protocols. Section VI suggests interaction between the inter-domain and the intra-domain solutions, and in the final section we present the summary and way ahead.

II. Related Work

Provision of E2E QoS is an important challenge in the area of HN. Many QoS-enabled architectures and protocols have been proposed to solve the problem of end-to-end quality of real-time audio/video and high quality data services. The AQUILA project [2] suggested distributed QoS middleware for the single domain homogeneous IP network. One of the achievements of the project was leveraging the concept of traffic classes, redirection from IntServ to DiffServ architecture and use of BB (Bandwidth Broker). In the EuQoS project [3] a heterogeneous scenario with five different technologies of access networks was considered. The Classes of Service (CoS) proposed were based on the DiffServ concept with the number of CoSs limited to six and four in the access and core network respectively. The signaling layer proposed by the EuQoS project was built using an augmented SIP protocol called EQ-SIP [3]. The QBone project [4] conducted research in the field of QoS provisioning for the global IP network i.e. multi-domain scenario. The architecture proposed by QBone team was built on DiffServ architecture with Bandwidth Broker. For the inter-domain communication the SIBBS (Simple Interdomain Bandwidth Broker Signaling) protocol was proposed [4].

The proposed architectures of the referenced EU projects are more or less based on the DiffServ IP model. As far as this model is concerned four alternatives are taken into account: no control (where only a basic priority mechanism is applied), static trunks, DiffServ-PCN (Pre Congestion Notification) [5], and BB, not available in the market for now but a great potential for QoS management. In the presented solutions emphasis is put on traffic management, bandwidth optimization, Call Admission Control (CAC), QoS signaling protocols and network planning. The presence of QoS signaling protocols, as RSVP-TE [6], is essential. Mapping the QoS requirements over the different private technologies is a topic for QoS management. The same concept applies if CAC is considered. If there are no signaling schemes to manage resources dynamically, the Service Level Specification (SLS) support is left to the experience of network operators at network planning level.

The mentioned QoS architectures are all designed with the focus of E2E QoS support in cellular mobile networks and in fixed networks with several network service providers. However, military tactical networks differ from the typical heterogeneous networks found in civilian infrastructure due to their features such as frequent topology changes, mobility of users and service providers, common use of wireless links, multi-hop wireless paths, relatively low data rates, large variation in maximum available data rate, and limited processing and power capacity of network nodes. The trust relation between network partners is also different in a coalition than between commercial network providers, and the Service Level Agreements (SLAs) can have a different role (not a contractual agreement of quality and cost, but more an approximate agreement of willingness to make resources available). The traffic pattern in the different networks can also be quite different.

In the work we present in this article, we have had these differences in mind in the design of the mechanisms, and by suggesting an interaction between a Multi Topology (MT) routing protocol used in the mobile tactical environment and the QoS provisioning framework running in the tactical backbone.

The MT routing protocol is an intra-domain QoS routing protocol. QoS-routing aims to find a route which provides the required service quality for a specific traffic type. This can be done using routing metrics based on parameters like delay, data rate, signal to noise ratio, route stability, etc. These protocols must be combined with a resource manager and a traffic classifier (e.g., DiffServ-like classification) to support QoS in the network. Two survey papers [7], [8] give a comprehensive overview of many of the available QoS-routing proposals.

However, most of the QoS-routing schemes are reactive routing protocols. We believe proactive protocols will be necessary in tactical MANETs to reduce the routing response time and increase the predictability of the network availability. We also think it is beneficial in a very heterogeneous environment to store several routes with different characteristics to support separate QoS requirements. The MT supported QoS architecture [9] that we utilize in this article is a simple but powerful scheme with a proactive routing protocol that maintains multiple topologies in the routing domain and consequently provides multiple paths from source to destination. Each topology/path is associated with a single or multiple QoS-class(es).

III. QoS Challenges in Heterogeneous Networks

The QoS models discussed so far work out the problem of E2E QoS provisioning with an overlay network covering the different networks traversed from source to destination. In a military tactical network, one or several of these networks might be a very heterogeneous MANET where mobility can lead to reduction and/or renegotiation of QoS parameters. A Demand Assigned Multiple Access (DAMA) SatCom connection represents a similar situation. QoS mechanisms that can adapt to the rapid changes of the QoS characteristics of the E2E path traversing a heterogeneous network domain also needs to be addressed. QoS routing and admission control are among the parameters that are to be discussed here.

In deployed and mobile military networks the resources are limited and can vary much over time (e.g., due to hostile activity or changes in channel propagation conditions). Conceptually, the QoS architecture should consist of admission control, resource monitoring and management, and the ability to preempt flows when the network is congested. This implies another challenge that needs to be emphasized. It is connected with the problem of QoS policy definition and implementation and could be solved by using priority, admission control as well as preemption.

Furthermore, as not all flows are admitted and some flows have to be preempted there is a fairness problem. In homogeneous MANET type networks; short distance flows (in number of hops) use typically more resources than flows

over longer paths. A tradeoff exists between high network utilization and fairness. A similar situation will also exist in heterogeneous networks.

It should be noted, also, that provision of end-to-end QoS cannot be realized without routing based on valid resource information and resource management and with connected security mechanisms.

Taking this into consideration, the following QoS challenges should be taken into account:

- signaling: In a multi-domain network, it is imperative to install and manage QoS in each domain. The need is to transfer QoS requirements among network portions implementing their own technologies and protocols. This requirement has also been emphasized e.g. by the NATO Science and Technology Organization (STO) working group on Protected Core Networking (PCN) [10]. The signaling protocol used to signal the requirements should be designed to rapidly cope with changes in the network topology, and thus end-to-end QoS conditions. In order to increase the robustness of the different connections in the network, the protocol must:
  - release resources reserved for a specific traffic-flow if the flow disappears for a certain period of time and
  - provide alternative routes to the destination in case of node failure or congestion in the network. Therefore signaling across all domains on the data-path is needed.
- cross-layer QoS mapping: The data network is composed of functional layers where each layer must cooperate to support end-to-end QoS provision. The overall perceived service quality depends on the QoS achieved at each layer of the network. The QoS requirements at the application layer should be classified into a set of QoS classes with their corresponding application layer metrics. The QoS requirements must flow vertically across the layers and need to be received, understood and satisfied by all layers in the network stack. Therefore a vertical mapping of QoS metrics is critical. If the different layers do not cooperate to support a QoS requirement, but instead choose their best support for the required QoS independent of each other, there is a risk that the layers can in the worst case, select to use mechanisms that undermine each other. Cross-layer mechanisms can be used both to improve QoS support internal in a homogeneous networks, but also to provide relevant QoS/resource information between networks in a heterogeneous network. In the latter case it is imperative that the different networks have a common understanding of what the information made available by the cross-layer functionality, means.
- QoS routing: Military HN (MHN), are very dynamic in their nature due to the use of mobile nodes and radio resources. The time-varying low-capacity resources of the MANET, which is very often a basic part of a military heterogeneous network, make maintaining accurate routing information very difficult.
  - intra-domain routing: The network layer maintains the end-to-end path whereas the MAC layer is in charge of access to the medium for the next hop on the path. The path selection and the channel access must aim to support the same QoS requirement for the data packet. Link quality and channel traffic-load known at the MAC layer should be made available to the routing layer and topology information from the routing layer can be useful for the MAC layer. It is also beneficial to maintain multiple paths/topologies with different QoS characteristics in the network.
  - inter-domain routing: The border routers must be able to automatically reconfigure their routing daemons in order to support end-to-end QoS over deployable networks composed of multiple autonomous systems that can move relative to each other. They can organize more than one link to other ASs. Moreover, each domain can be partitioned or merge. The autonomous system border router (ASBR), equipped with BGP functionality, should be responsible for appropriate traffic routing and routing policy and reacts automatically to changes that occurs in AS.

Some of challenging issues mentioned above are discussed in the next part of the article.

IV. Providing Connectivity and QoS over Single-domain Heterogeneous Networks

The QoS architecture in military tactical networks must consist of a set of mechanisms and solutions for the mobile tactical edge and a set of mechanisms and solutions for the deployed backbone and its connections to the strategic network. The mechanisms must interact very well.

In this section we describe a possible architecture for providing connectivity and differentiated QoS support in heterogeneous mobile tactical networks. The purpose of this solution is to exploit the existence of parallel paths in the network to support differentiated QoS. It is assumed that the heterogeneous network might consist of radios based on different transmission technologies (capacity, range, delay, etc.). The purpose of the design is to find the path that traverses the group of transmission technologies that best suits the requirement of a traffic class. In the current phase this solutions supports multiple networks organized in a single domain, but it can also be extended to support multiple domains.

The suggested solution defines multiple routing topologies in the network in order to support different QoS-classes. These topologies are then used to ensure that data packets are only forwarded on topologies with sufficient capabilities to support the requirements of the dataflow. We combine Multi-Topology (MT) routing (e.g., [11], [12]) and traditional DiffServ-like [13], [14] mechanisms to utilize all available transmission means in the tactical network and increase the robustness of the network.

A traditional link state routing protocol maintains one routing table with one entry for “the best route” to all destinations

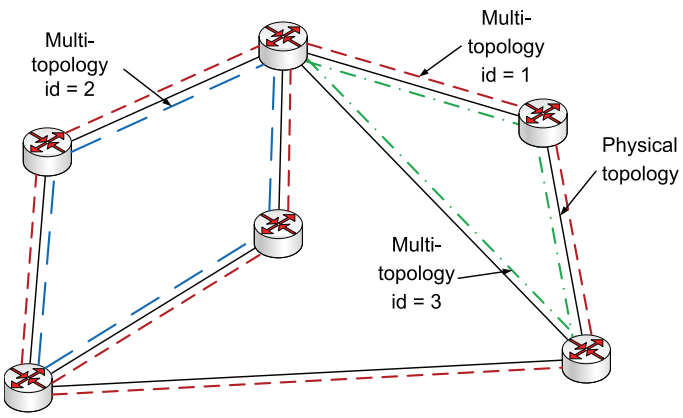

Fig. 1. This figure shows a network with three different topologies.

TABLE I
THE USE OF THE RADIO NETWORKS IN THE TOPOLOGIES

Radio Type	Low data-rate topology	High data-rate topology	Low delay topology
Nation 1 SatCom	X	-	-
Nation 1 UHF Network1	X	X	X
Nation 1 VHF Network	X	-	X
Nation 1 UHF Network2	X	X	X
Nation 2 UHF Network	X	X	X

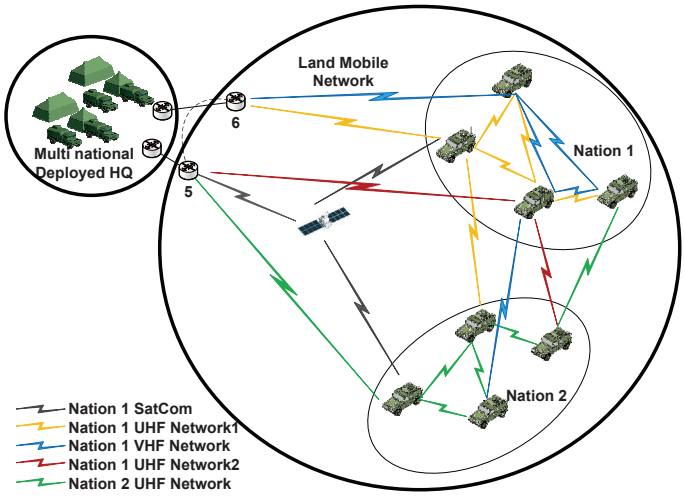

Fig. 2. A very heterogeneous mobile network.

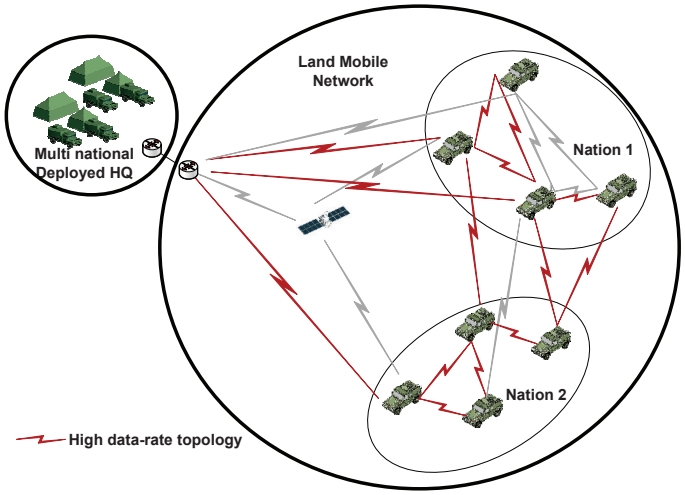

Fig. 3. The links that participates in the high data-rate topology.

in a network domain (or several of the best routes for load balancing purposes). The best route is calculated based on the chosen metric (e.g., shortest path first (SPF) or lowest cost, where the cost parameter can be established based on any set of link parameters).

A Multi-Topology routing (MT-routing) protocol maintains several topologies within the network domain at the cost of a few extra bytes in the routing packets. Each topology spans a subset of the physical topology. The shortest path first calculation (other metrics can be used if available) is performed for each topology to discover the best routes within the topology. The cost of one link can be set different for the different topologies. Only the links belonging to the actual topology are included in the calculation. The results of the SPF calculation are stored in one forwarding table for each topology. In Fig. 1 we present a network where three topologies are defined on the physical topology. A number of topologies can be defined on a single physical link. All the physical links in the domain must be part of the default topology. The default topology is used for routing traffic and ensures that routing information reaches the complete network domain.

During network configuration, topologies can be tailored to represent many different purposes. We use the topologies in order to support QoS. In the MT supported QoS architecture, we configure and maintain several network topologies that each spans a subset of the physical topology. The topologies are configured to represent a certain QoS characteristics of the network, and the topology will then only contain paths that support the specified QoS characteristic. Each topology has its own forwarding table that is used to forward data packets classified as belonging to that specific topology. The Type of Service (TOS) field in the IP packet can be used to supply the tag for the choice of topology and forwarding table. If a destination address is not available in the forwarding table associated with the QoS-class, then no path exists in the network where the specific QoS-class is allowed to be transported. Thus the flow should not be admitted to the network. Traffic that cannot be supported is stopped at the network edge. Hence, MT will only admit supported traffic, and all other traffic is early discarded without draining valuable resources.

Figure 2 gives an example of a heterogeneous mobile coalition network that consists of several radio networks. Table I shows how three different QoS topologies can be

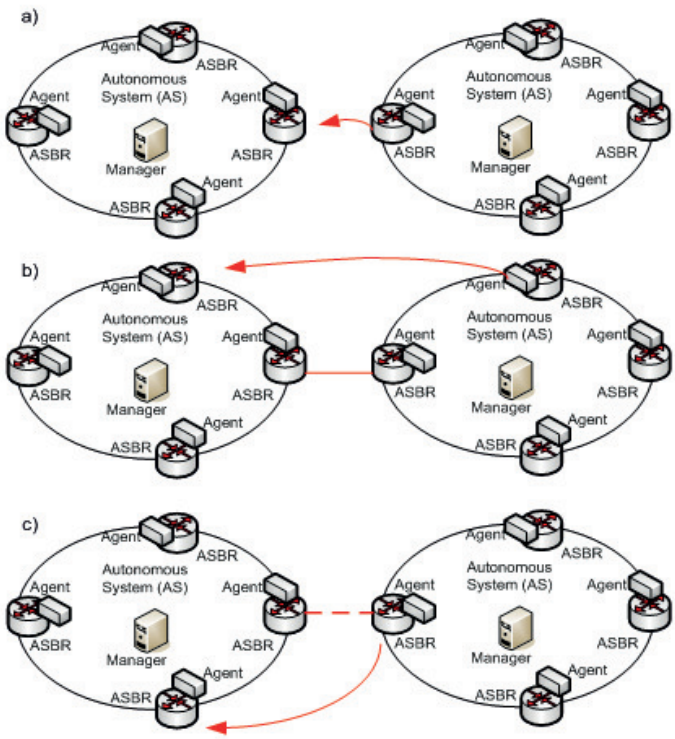

Fig. 4. Typical AS mobility scenarios.

configured in this network. Figure 3 further visualizes the high data-rate topology.

This MT supported QoS architecture has been studied in the Coalition Network for Secure Information Sharing (CoNSIS) project [15]. The examples given above are taken from that study. More information about the use of this design in CoNSIS can be found in [9].

We see the use of multiple topologies paired with a DiffServ-like architecture as a simple but powerful tool to dynamically block traffic at the source for flows that cannot be supported by the current network topology, and thereby improve the QoS and available capacity for admitted traffic.

The architecture also allows traffic tagged with different QoS classes to be routed on separate paths through the heterogeneous network. This allows optimal choice of the routing path for a QoS class, at the same time preserving the robustness and resource efficiency present with a common heterogeneous transport network. This mechanism can also enforce some load balancing in the network.

The protocol can run directly on the different radios, it can be implemented as an overlay network or it can interact with the routing protocols in the different sub networks by importing routing information from these networks into one or more topologies. Currently, the MT-protocol build topologies based on static predefined link characteristics. The benefit of it is that this value is always a correct "typical value". If there is no route to the destination in the chosen forwarding table, then it is certain that the traffic flow cannot be sustained. On the other hand, if a route is available, it is not certain that this route has enough capacity available to sustain the traffic. In future work we want to investigate if dynamic parameters representing the real time resource situation for the links can be incorporated efficiently with the MT-routing protocol to better support the resource management mechanism. Alternatively, additional resource management mechanisms based on e.g., polling techniques [16] can be combined with the MT-supported QoS architecture to incorporate dynamic changes in e.g., channel quality and traffic load to further improve the scheme for admission control purposes. The resource mechanism must be executed for all defined topologies.

V. Providing E2E QoS over Multi-domain Heterogeneous Networks

In order to support connectivity over multiple autonomous systems in tactical heterogeneous networks, the border routers have to be able to automatically reconfigure their routing table.

We have assumed that each autonomous system has its own traffic management policy, handled by a central manager implemented in the selected server. The manager is able to manage the border routers (ASBRs) via the agents located in the managed routers. It is assumed that the IP address of the manager is known by each agent, and then active agents can be registered in the manager.

Let us assume three basic autonomous system mobility scenarios depicted in Fig. 4 The ASBR with BGP has to detect its exterior neighbor routers during new ASes attachment (Fig. 4a), during attachment of additional ASBR (Fig. 4b) or changing previous point of attachment (Fig. 4c). This behavior is possible due to the exterior link detection procedure described below. We called the scheme presented below "BGP-based routing configuration management protocol" (BGP-CMP).

The agent located in the router must inform its manager that a new AS has been attached. After the link detection process, the peer agents communicate with each other in order to transfer information about the AS numbers (ASN) allocated to their ASs, and information about the IP addresses of the neighboring managers. Afterwards, each agent transfers this information to its home manager. Based on this information, the managers select the main manager, which is responsible for global address allocation to the common link between the ASes. The main manager selects the addresses from its address pool and informs its agent. The agent receiving the message with the new addresses informs its peering agent from the new AS, and the neighboring (slave) manager. Now, both managers can start the ASBR configuration procedure.

The AS can also move to a new position which enforces a need for ASBR reconfiguration (Fig. 4c). The agent located in the ASBR has to detect that the neighboring router is not accessible and inform the manager about this event in order to reconfigure the ASBR.

Each ASBR agent in the autonomous system is responsible for detection of the attached router in the neighboring AS. Our proposal is based on typical solutions for such problems and uses Neighbor Discovery (ND) frames sent periodically

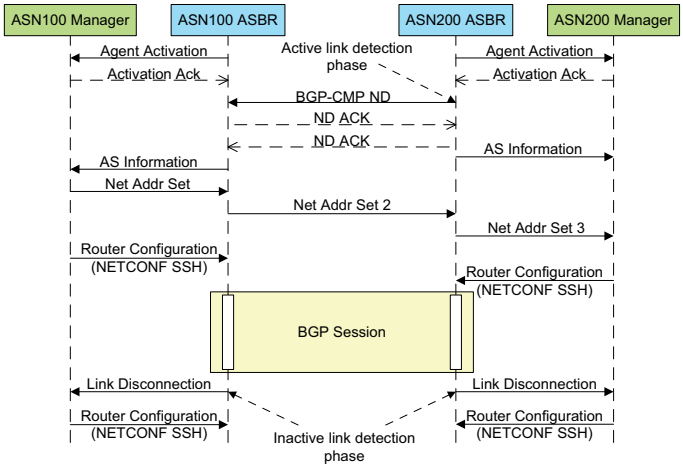

Fig. 5. Flow diagram of BGP-CMP messages.

on the exterior router interfaces. In the case of IPv6 protocol stack, ND frames are sent to the multicast group for all link-local nodes and in the case of IPv4 to the link-local broadcast address. The ND messages are next used by the other router on the link for extracting the sender's link-local address and the ASN. It is now possible to send the *ND Acknowledged* message to the adjacent router in order to inform the router that sent the ND about the new connection and the manager's address. After the ASBR agents get to know each other's ASBR exterior interface link-local addresses, they can send information about the new connection to their managers. The ND ACK messages also contain information about all other ASs in which the BGP-CMP aware architecture is implemented. This allows managers to detect and solve the problems of domain ASN duplication as well as to start the partitioning and merging procedure. In the case of the same ASN configuration in both connected systems, the AS manager which knows about more BGP-CMP aware ASs will be selected as the manager of the newly connected systems.

The flow diagram of the BGP-based routing configuration management mechanisms is presented in Fig. 5. The diagram presents a set of message flows in the case of a new connection between two ASes. After the link detection phase is completed, the ASBR agents exchange information about their managers' addresses using ND ACK messages. This address is then sent via the message called *AS Information to the AS managers*. Based on the information about the neighboring ASN and a comparison of this to its own ASN, each manager selects the master manager as the manager with the lowest ASN (ASN100 in our case).

Then, the ASN100 manager sends the message *Net Addr Set* to its agent, informing the agent about the network global IP address selected on the exterior link configuration. This information is then resent via the message *Net Addr Set 2* to the neighboring agent's link-local address, and finally via the message *Net Addr Set 3* to the ASN200 manager. After this message sequence is completed, both managers start the configuration of their ASBRs (addresses and peering) using NETCONF SSH session [17]. NETCONF is an XML-based protocol used to perform management functions, mainly targeted at provisioning, but capable of monitoring certain configuration and operational state information. Because configuration data is sensitive information, security issues must be addressed. If SSH is used, only the users that are allowed to login to the system will be allowed to access NETCONF.

If the exterior link disconnection is detected by the border routers, each ASBR sends the message *Link Disconnection* to the managers. After this message sequence, both managers start the reconfiguration of their ASBRs (clearing the addresses and peering).

In the case ASBR loses the connection with the manager, a new manager activation procedure starts. If a newly connected router is not activated, a *ND acknowledged* message is sent with the not active flag set. This starts the procedure of ASBR configuration to set the router as one of our AS border routers. In order to support the QoS provision ASBR cooperates with the modified SIP protocol described in [18] which enables resource reservation for the supported service types.

VI. Interaction Between Intra- and Inter-domain QoS Mechanisms

There exist many proposals for QoS mechanisms within networks and between networks. In this paper we have described one intra-domain method that establish forwarding tables according to link technology or QoS metric and further map traffic to the respective forwarding table and we have described one inter-domain proposal for establishing an end-to-end QoS signaling framework.

In order to make the best use of the relatively scarce network resources in a tactical military network, it is beneficial to allow for efficient information flow between the intra-domain QoS mechanisms and the inter-domain mechanisms. When intra-domain QoS information is available, this information will in most cases be more accurate and fresh than information gathered by an inter-domain overlay mechanism. The challenge is how we convey our QoS parameters between the inter- and intra-domain QoS protocol, and how to utilize the information.

A basic mechanism for interaction between the MT-supported QoS architecture described in section IV and a distributed Bandwidth Broker (BB) is described in [19]. An improved version of this interaction can be used for interaction with the mechanisms described in section V. We are currently enhancing the functionality in the MT-layer Service Access Point (SAP) to support the following functionality: A prerequisite is that a set of QoS classes is defined for the mission, which is interpreted in the same way for all ASes and all network layers in the network. In this situation the QoS agent in the boarder router can query the intra-domain MT-mechanism for the present QoS support available on the route to a single destination, or to a network segment. The MT-mechanisms will respond with the list of QoS classes currently available on the path(s) to the queried destination. This information can be relayed to the Policy manager of the AS and further signaled to other ASes for use by the BB.

An alternative approach also worth investigating is to reflect MT routing information up to the inter-domain QoS protocol that further collect MT information from the other AS and calculate a MT route table for inter domain routing and finally provide this to the BB. This information can be used as a coarse admission control functionality supported by a reactive end-to-end solution provided by the BB that make the actual resource reservations given positive answer for resource availability from the MT-mechanisms.

A third solution could be to use ideas from pathlet routing [20]. Each autonomous network collects QoS information for the paths between their own network gateways (boarder routers). These paths are announced with the source and destination gateway and QoS metric. This information is further disseminated to all BBs. The information can then be used for ordinary route calculation or for source routing. In source routing each source calculates its own route towards the destination based on its own requirements and policy, and each intermediate router forwards the traffic complying with the source based routing path and the local traffic policy.

We will consider these solutions in our future work.

VII. Summary and Way Ahead

This paper describes an intra- and inter-domain framework for integrated heterogeneous networks. Support for QoS, and high mobility management are one of its most important features. Although both presented solutions provide a specified level of QoS, further joint work will be carried out in order to ensure interaction between the MT and ASBR solutions. This work will look for ways to use the information provided by the MT-routing protocol in the ASBR to improve E2E QoS.

References

[1] S. Giordano, S. Salsano, S. Van den Berghe, G. Ventre, and D. Giannakopoulos, "Advanced QoS Provisioning in IP Networks: The European Premium IP Projects," *IEEE Communications Magazine*, vol. 41, no. 1, pp. 30–37, January 2003.

[2] AQUILA – Adaptive Resource Control for QoS Using an IP-based Layered Architecture, Project Number: IST-1999-10077, http://www-st.inf.tu-dresden.de/aquila/.

[3] EuQoS – End-to-end Quality of Service support over heterogeneous networks, http://www.euqos.eu.

[4] QBone Architecture, http://qos.internet2.edu/wg/documents-informational/draft-i2-qbone-arch-1.0/.

[5] P. Eardley (ed.), "Pre-Congestion Notification (PCN) Architecture," *RFC5559*, June 2009.

[6] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," *RFC3209*, December 2001.

[7] L. Hanzo-II and R. Tafazolli, "A survey of QoS routing solutions for mobile as hoc networks," *Comparative Oriental Manuscript Studies COMST*, vol. 9, no. 2, pp. 50–70, 2007.

[8] R. Asokan, "A review of Quality of Service (QoS) routing protocols for mobile Ad hoc networks," in *International Conference on Wireless Communication and Sensor Computing (ICWCSC)*, Chennai, India, 2010.

[9] M. Hauge, J. Andersson, M. A. Brose, and J. Sander, "Multi-Topology Routing for QoS Support in the CoNSIS Convoy MANET," in *Meaning, Context & Cognition (MCC)*, Gdańsk, Poland, October 2012.

[10] "RTO-TR-IST-069 Requirements for a Protected Core Networking (PCN) Interoperability Specification (ISpec)," July 2012, AC/323(IST-069)TP/424, Final Report, (NATO UNCLASSIFIED).

[11] S. Mirtorabi and A. Roy, "Multi-topology routing in OSPFv3 (MT-OSPFv3)," July 2007, draft-ietf-ospf-mt-ospfv3-03.txt (work in progress).

[12] P. Psenak, S. Mirtorabi, A. Roy, L. Nguyen, and P. Pillay-Esnault, "Multi-topology (MT) routing in OSPF," *RFC4915*, June 2007.

[13] S. Blake *et al.*, "An architecture for differentiated services," *RFC2475*, 1998.

[14] D. Grossman, "New terminology and clarifications for diffserv," *RFC3260*, 2002.

[15] A. Eggen *et al.*, "Coalition Networks for Secure Information Sharing (CoNSIS)," *to be published at MILCOM 2013 (invited paper)*, November 2013, San Diego, CA, USA.

[16] A. Mohammad, O. Brewer, and A. Ayyagari, "Bandwidth estimation for network quality of service management," in *Military Communications Conference (MILCOM)*, Orlando, FL, USA, 2007.

[17] M. Wasserman and T. Goddard, "Using the NETCONF Configuration Protocol over Secure Shell (SSH)," 2006, draft-ietf-netconf-ssh-06.txt.

[18] P. Lubkowski and D. Duda, "Implementation, Validation, and Practical Verification of SIP QoS-Aware Application for The Federated Tactical Systems," in *Military CIS Conference MCC'2010*, Wrocław, Poland, 2010.

[19] F. T. Johnsen, T. Hafsoe, M. Hauge, and O. Kolbu, "Cross-layer Quality of Service based admission control for web services," in *HeterWMN*, Houston, TX, USA, December 2011, pp. 315–320.

[20] P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, "Pathlet routing," in *ACM SIGCOMM*, Barcelona, Spain, August 2009, pp. 111–122.