Responsible Source Multicasting

Mihály Orosz and Gábor Hosszú PhD

Department of Electron Devices, Budapest University of Technology and Economics,
Magyar tudósok körútja 2, Building Q, section B, 3rd floor
Budapest, H-1117, Hungary
{hosszu, mihi}@nimrud.eet.bme.hu

Abstract. There is no effective method to support IP level Internet wide multisource multicast sessions, that can be easily used from almost every ISP There are several protocols implementing the necessary functionality, but the penetration of them is really low recently. The most obvious work all-round is using SSM – Source Specific Multicasting, in which, the IP multicast session is identified by the multicast group address and the source's unicast IP address. SSM allows using all the SSM address range for every source IP addresses and limits the address allocation problem inside the host of the source; however, its significant drawback is that the SSM has no native support to create multicast sessions with more than one source; it uses separate source specific distribution trees for every single source therefore it needs more resources on the router side. The alternative solution for supporting multisource multicast session is the ASM – Any Source Multicasting. However, its significant drawback is the lack of Internet wide dynamic address allocation. To address the recent problems of the Internet wide multisource multicast session a novel IP multicast service model, the Responsible Source Multicasting - RSM is introduced in this paper. RSM uses shared distribution trees like ASM; however, builds a reverse path tree towards an appropriate well-known unicast IP address like SSM. The paper demonstrates that this novel multicast routing protocol handles Internet wide multisource multicast sessions. The paper also shortly presents the DAMA – Dynamic Address Allocation of Multicast Addresses protocol for dynamic multicast IP address allocation, which works in a strong collaboration with the RSM.

Keywords: IP multicast, Routing, ASM, SSM, Multicast, dynamic address allocation mechanism

1 Introduction

This paper describes RSM, a new IP level multicasting service model. This service model consists of two components; a Dynamic Address Allocation of Multicast Addresses (DAMA) session management protocol and the Responsible Source Multicast (RSM) routing protocol [1]. The RSM routing protocol can be implemented as an extension to the most commonly used Sparse-Mode Protocol Independent Multicast (PIM-SM) protocol [3]. Although RSM routing may use the underlying

unicast routing to provide reverse-path information for multicast tree building, it is not dependent on any particular unicast routing protocol.

To highlight the problem needs to be addressed if Internet wide sessions are needed, we compare the unicast and multicast sessions from service registration to data exchange aspects [2]. Most of the unicast services on the Internet are registered in the Domain Name System (DNS). This service directory is based on the unicast address of the host offering the service. In order to join to a service running on a server only the unicast IP address of the server is required by the underlying IP subsystem. The routing is done automatically using the unicast IP addresses. However, there is no commonly used (operating system supported) service registration mechanism for global multisource multicast services that provides the necessary information for the multicast routing protocol as well.

In order to examine more deeply the possible solution of the global multicast address allocation, we should consider separately the two main groups of the multicast service model, namely the Source-Specific Multicast (SSM) [4] and the Any-Source Multicast (ASM) [5].

2 Multicast routing background

The problem behind the Internet-wide penetration of ASM infrastructure is the lack of simple, useful dynamic address allocation mechanism, that lets the short range of multicast IP addresses available for the applications. Beside some solutions are developed recent years, the problem is still unresolved Internet-wide [16]. The well-known solutions can be divided into two groups. One uses real dynamic address allocation (dynamic allocation group), the other tries to avoid dynamic allocation (limited or static allocation group).

Dynamic Allocation Group. Most important representatives of the dynamic allocation group are PIM-SM/MBGP/MSDP architecture, and Multicast Address Allocation Architecture (MAAA). The elements of the PIM-SM/MBGP/MSDP architecture are the following: (i) improved BGP inter-domain routing protocol, Multiprotocol BGP (MBGP) that can handle not only unicast, but also multicast inter-domain routing [6]; (ii) PIM-SM intra-domain multicast routing protocol [7], [8]; and (iii) Multicast Source Discovery Protocol (MSDP) that links PIM-SM and MBGP to enable Internet-wide ASM routing [9].

The idea behind the use of the MBGP for multicast routing was to use hierarchical multicast routing based on hierarchical unicast routing [17]. MBGP uses peering mechanism to exchange multicast routing information between MBGP routers (between domains). Every MGBP peer links connects two MBGP routers via TCP protocol, and the peers cover all the Autonomous Systems (AS). Using MBGP routers does not need to know all the other routers, but the directly connected ones. Obviously every MBGP router has to participate in the intra domain routing for the domain it belongs to. MBGP handles unicast and multicast inter-domain routings as well; however, it uses different peer connections between domains for unicast and multicast routing [10].

One of the most relevant members of the dynamic allocation group is MAAA [11], [1]. MAAA uses three-level hierarchy for address allocation; domain, intra-domain, and host-to-network levels. The Address Allocation Protocol (AAP) is used for intra-domain address allocation, and the Multicast Address Dynamic Client Allocation Protocol (MADCAP) is used by hosts to obtain multicast addresses from a Multicast Address Allocation Server (MAAS). It is noteworthy that the MAAA infrastructure is quite complex, and this disadvantage makes hard to implement the system Internet-wide.

Static Allocation Group. GLOP is a typical member of the static allocation group. It uses static (limited) assignment of multicast addresses based on AS numbers [13]. The AS number is hardcoded into GLOP address arrays. GLOP uses the 233/8 (233.0.0.0... 233.255.255.255) address range only. Every AS has 233.X.Y/24 multicast address range, where X and Y are related to the sequence number of a specific AS. Besides its simplicity, GLOP has two major disadvantages. First, every AS has only 255 multicast addresses, and there is no possibility to extend the range, if it is not enough inside the AS. Second, GLOP has not any method to allocate the multicast addresses inside the ASs.

SSM is another good example for the limited (static) allocation group [14], [15]. SSM reuses every multicast address in every host having unicast address as well, because the SSM session is identified by the multicast group address and the unicast address of the source at the same time (S, G states in routers). Although SSM is a creative solution for the limited multicast address range, it has hard limitations. SSM uses different distribution trees for every source, and in addition every listener (drain) has to join every distribution tree in a multisource environment [12]. Therefore, it is necessary to use an application level protocol to identify the sources related to a specific multicast session.

Evidently, there is no need for a complicated address allocation using SSM, but an effective, Internet wide address allocation mechanism is needed for ASM. In addition, the drawback of SSM comes from the one-way source rooted trees it uses, because the routers have to set up different distribution trees for every source in a multi-source session, and also an Application Level mechanism is needed to let receivers to get information about sources, and to join all the trees rooted at the sources.

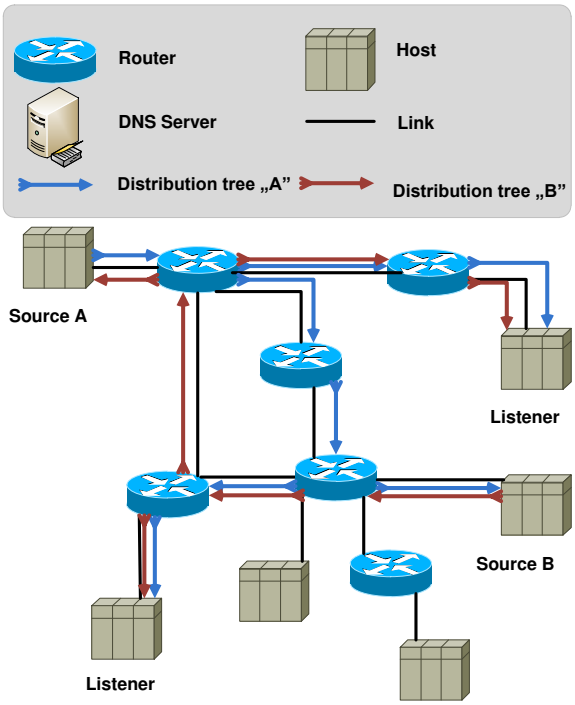

Fig. 1. Multisource SSM session.

3 Solution

A novel method called Responsible Source Multicasting (RSM) was developed to eliminate the drawbacks of existing SSM and ASM routing mechanisms, and to incorporate advantages of them.

3.1 Overview of RSM routing

The proposed routing mechanism, the RSM uses ASM routing, but it assigns a responsible source (RS) unicast IP address for every multicast session (multicast group). The assignment of unicast IP addresses enables to use the DNS system for registration of the dynamically allocated multicast IP addresses. Furthermore the RSM multicast routing protocol uses this unicast address of the RS to maintain routes in MRIB table. RSM routing uses information taken directly from the unicast routing table related to unicast address of the RS. MRIB is populated with the interface for a given RSM multicast group address that is the same interface from the unicast routing table for the unicast address of the RS related to the given multicast group.

RSM routing can be implemented as an extension for PIM multicast routing. PIM relies on an underlying topology-gathering protocol to populate a routing table (MRIB) with routes. The routes in MRIB may be taken directly from the unicast routing table, or it may be different and provided by a separate routing protocol such as MBGP or RSM [9]. Regardless of how it is created, the primary role of the MRIB in the PIM protocol is to provide the next hop router along a multicast-capable path to each destination subnet. The MRIB is used to determine the next hop neighbor to which any PIM Join/Prune message is sent. Data flows along the reverse path of the PIM Join messages. Thus, in contrast to the unicast RIB, which specifies the next hop where a data packet would take to get to some subnet, the MRIB gives reverse-path information, and indicates the path that a multicast data packet would take from its origin subnet to the router that has the MRIB. Using RSM as a PIM extension eliminates the need of inter-domain routing mechanisms and usage of RPs, while provides the same functionality as ASM multicast routing has. Moreover, the participants can be sources and listeners at the same time in one single session, the sessions can be multi-source. Using source routed trees it provides the robustness of SSM.

The RSM is ready for easy Internet wide deployment, because only the new routing extension is needed at the router side and the rest (DAMA protocol) can be handled on the clients (as an operating system or application level standard library) that provides the followings: (i) simple (DNS based) service registration/discovery, (ii) dynamic address allocation, and (iii) fair allocation mechanism (network topology related).

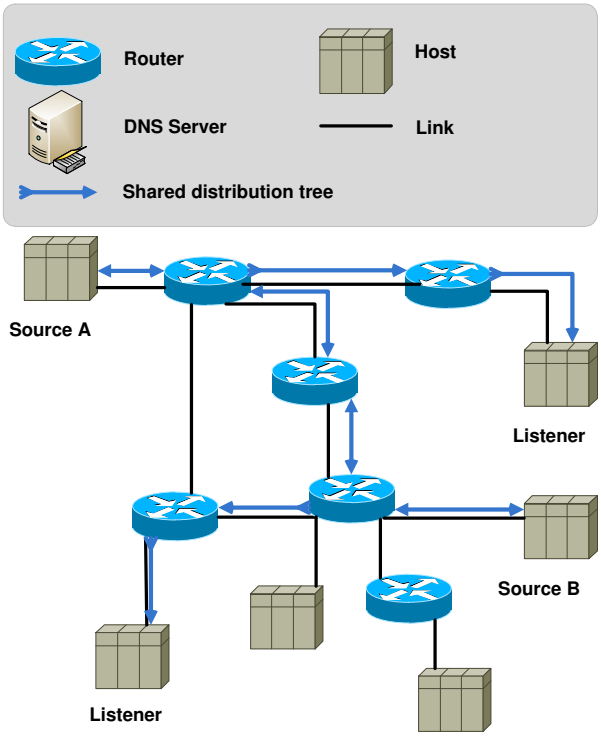

Fig. 2. Multisource RSM session.

3.2 Dependency on DAMA protocol

The Responsible Source Multicasting (RSM) uses Dynamic Address Allocation of Multicast Addresses (DAMA) protocol for dynamic address allocation, service registration, and service discovery. RSM inherits the favorable properties of DAMA like simple distribution and penetration, robustness and fairness. The RSM multicast routing uses Responsible Source Rooted Trees as distribution trees. Each Responsible Source Rooted Tree is identified by a multicast group address and a responsible source unicast address. The multicast routing can use simple Reverse Path Forwarding or Shortest Path Forwarding algorithms to make routing decisions, because the location of the root of the tree, (the responsible source) determined by its unicast IP address. This solution eliminates the need for complex hierarchical multicast routing.

For an RSM session the usage of the DAMA protocol is only necessary by the first member of the session for the registration of the Responsible Source. After this, any other member can easily join the RSM session using standard ICMP protocol or simply sending IP packets to the multicast group address.

3.3 Overview of DAMA protocol

In the DAMA project a protocol was constructed from the idea about using existing well-tried Domain Name System (DNS) for communication needs of multicast address allocation and service discovery. DAMA is an operating system software library for applications and a modified DNS server for the special DAMA top level domain implementing the address allocation and RS registry.

The applications use the operating system extension, the DAMA Library to allocate multicast address and for service discovery. The operating system extension offers the following services to the application: (i) obtaining new (free) RSM multicast address for the service; (ii) releasing unused multicast addresses after usage; (iii) finding services of given hosts; and (iv) finding sources of multicast sessions based on multicast address (querying RS unicast IP address).

The DAMA Library uses DAMA DNS server as distributed database system. DAMA uses standard DNS protocol [11] for communication between DAMA library at hosts and the DAMA DNS server. The database records for address allocation are stored in standard DNS Resource Records.

For starting an RSM multicast session (session initialization) a server needs a multicast address. It asks the DAMA library for it. Every host has IP-multicast address tables with 256 addresses for unicast addresses each. The DAMA library asks the DAMA name server to allocate an address based on its unicast address. If the DNS queries goes through network address translation NAT the altered unicast address; visible for DAMA name server will be used. If the name server has unmapped IP-multicast address, it maps to the unicast address of the host (in the host map every unicast address has 256 slots for multicast addresses). If there is an error or no more addresses available, then DAMA name server returns an error to the DAMA library. DAMA library allocates the offered address for the unicast address, and sends it to the applications, or signals the error. When the multicast session finishes (session termination) the application sends dispose message to the DAMA library, which sends unmap messages to the name server.

Every allocated and mapped address has timeout assigned. Within the timeout keep-alive message must arrive to renew the allocation (session holding). Every keep-alive message must be acknowledged. If a keep-alive message had not been acknowledged or renewal refused, the application must finish sending to the related multicast address (session failure).

3.4 RSM protocol description

Responsible source (RS) is a unicast IP address of the host assigned as responsible source for a given RSM multicast address by DAMA protocol. This RSM multicast group address and RS unicast IP address assignment information is freely available using DAMA. RS is identified by the RSM multicast group address and its responsible IP address for the RSM multicast group address. Member is a host participating in the RSM multicast session and is different from RS. Fake source is an RS that is not participating in the RSM multicast session (not sending or receiving

packets). Sender is a member or the RS that sends packets for the RSM multicast session. Receiver is a member or the RS that receives packets for the RSM multicast session.

Basics of RS unicast address registration. The dynamic allocation of RSM multicast group addresses is handled by DAMA protocol. For the basic understanding it is necessary to highlight the address allocation process in general.

The DAMA process starts when a host wants to initiate a new RSM multicast session. It calls the DAMA registration function to ask for a new RSM multicast group address. It is noteworthy that RSM multicast group addresses planned to come from a dedicated RSM multicast group address range reserved by IANA in the future. DAMA protocol assigns the RS unicast address of the requester to a new RSM multicast group address and makes it available as a DNS zone entry under the dama.org zone. If a DNS "IN A" query initiated for the dama.org zone in DAMA format containing the RSM multicast group address the RS unicast address for the multicast group would be the response. If an RSM capable router needs to join the given RSM multicast group it initiates the DNS query mentioned above, and selects the interface from the unicast routing table related to the unicast IP address come as results for the query. This interface will be populated to MRIB for the (*,G) routing state, where the G is the multicast IP address of a multicast group.

As a result from the above procedure it is obvious that at least one host per RSM session has to be capable of using DAMA protocol to register its unicast IP address as the Responsible Source. It is advised for every participant to use DAMA as service registry anyhow.

3.5 Workflow

Initialization. One DAMA capable host in the RSM session obtains an available multicast group address and registers its unicast IP address as Responsible Source for that multicast session using DAMA protocol. In such a way, it becomes the RS.

Maintenance. Any host can freely send packet to the given multicast group address implicitly joining the session or can explicitly join using IGMP protocol. These hosts become members. If a router receives a multicast packet from a directly connected source or receives an IGMP register message for a given group address (for the DAMA multicast address range) it uses PIM protocol for routing decisions. If an MRIB query is performed to find the RPF neighbor during PIM routing a DAMA formatted DNS query is made to insert the relevant entry to the MRIB. This entry is constructed regarding the unicast routing information related to unicast IP of the RS of the given multicast group. Any host can freely leave the session using IGMP explicitly or implicitly as a result of reaching PIM timeouts.

Disposal. On request from the RS for disposal or on reach of session timeout the dynamically allocated RSM multicast address is freed in DAMA and become reusable. Depending on PIM MRIB entry timeouts the freed multicast group addresses can be alive for a short period, so immediate allocation of disposed addresses should be avoided in DAMA protocol.

4 Performance issues of RSM

The main issues of RSM are the consequences of using DNS system. Routing decisions have to be made quickly, but if a protocol used during the routing mechanism is an application level network protocol like DAMA significant delay can occur. Therefore instead of waiting for the result of the DAMA DNS query, RSM drops or delays the packet after a new DAMA query initiated. When the DAMA response arrives, the necessary information for the (*,G) session is populated to MRIB and upcoming multicast packets for the given multicast group can be routed as normal – based on the PIM-SM protocol. This asynchrony behavior between the initialization of collecting the necessary information for MRIB during routing decision and MRIB updates on arrival of information can cause significant delays between a new member starts joining process and technically joins the session (receives packets). This delay occurs on every router between the joining member and the distribution tree, as every router has to query the RS IP address using DAMA. This delay can be reduced significantly if PIM JOIN message contains the RS IP address and eliminates the uses of DAMA at intermediate routers.

Another performance related problem is that RSM can have only a limited address range from the available multicast group address ranges. All the RSM session over the Internet shares this address range. If the number of RSM session needed are higher than the size of the available address range no more sessions can be started until one of the existing sessions closes. The address allocation takes place in order of the arrival of the allocation requests; therefore Denial of Service (DOS) attacks can be easily made against RSM. To reduce the negative effect of DOS attacks and to provide low level fairness, DAMA divides the available address range based on IP address classes. This limits effects of DOS attacks to C class subnetworks and shared the address range equally between these networks. To make address allocation more effective and allow the allocation of whole available address range even when the requirements are coming from a limited set of sub networks, some improvements on temporary address range handover and forced takeover must be implemented in DAMA.

Additional performance improvement can be realized taking into account that a responsible source distribution tree can be suboptimal for multiple sources. In RSM always the RS is the root of the tree regardless of the link properties and utilization and the characteristics of the traffic. An application layer protocol can be used to select the RS from the participants of the session prior RSM initialization. This protocol can take into account the given application specific traffic pattern and expected topology for the RS selection making the distribution tree optimal.

Multisource sessions can suffer from overloading low bandwidth members when high bandwidth sources and other high bandwidth members are exists. If an application can handle receiving from limited set of source to take care of low bandwidth members the high bandwidth members and sources can share high bandwidth traffic while low bandwidth members still be part of the session and receives lower bandwidth traffic. Some minor improvements can be added for handling the denial of some sources due to this bandwidth limitation. This can be

achieved by maintaining exclusion list for sources and RSM multicast groups for interfaces (like SSM does in its membership database) at router side.

5 Conclusions

The proposed novel service model, Responsible Source Multicasting (RSM) lets fast penetration of multisource multicast application became reality. The most significant advantage of RSM in penetration point of view is that there is no need for complex setup either at intra domain or at local network level. The PIM RSM Extension is planned to be submitted as Internet-Draft. On its acceptance, future PIM implementations and routers sold will support it. It will make possible for a user having a modern RSM capable router to easily join to RSM sessions without complex network and routing configuration tasks.

While RSM model incorporates the advantages of the different multicast address allocations and routing protocols, eliminates their disadvantages having been blocking their penetration. However, further simulations and experimental measurements are necessary to validate the model and to provide performance measures.

Besides the RSM lets multicasting penetration Internet-wide, it is far away to start deployment. The standardization of the underlying DAMA protocol is needed first, and then an RSM protocol implementation and standardization is necessary in order to let deployment begin. Finally routers need to be upgraded with RSM PIM extension to get RSM work. Beside this process looks quite complex, it is far simpler than processes necessary for the deployment of any other solutions.

A novel method for IP level multisource multicast routing was developed to address the problem of slow penetration of multisource multicasting capable routing protocols. The new method called Responsible Source Multicasting (RSM) can be easily deployed Internet wide not having dependencies on non-widely used complex application level protocols that have to be maintained both intra domain and inter domain scopes like MAA but providing the same functionality as ASM. RSM routing is implemented as PIM extension and depends only on DNS that makes its penetration simple. The delay caused by the Dynamic Address Allocation of Multicast Addresses (DAMA) protocol at routers can be reduced significantly if PIM JOIN message contains the RS IP address and eliminates the uses of DAMA at intermediate routers. This PIM JOIN extension with RS IP address in case of RSM group address range is given planned to be implemented shortly.

RSM service model planned to be applied to Mobile Ad-Hoc Networks (MANET) [18] and can significantly reduce the multicast routing protocol overhead that is necessary for tree building in MANET Multicast routing protocols. Multicast OLSR (MOLSR) [19] protocol uses SOURCE CLAIM message to identify the multicast source for a given multicast group and use the information from this message to build a source rooted tree. The SOURCE CLAIM messages are flooded over the MANET regularly resulting large routing overhead. RSM service model planned to be applied for MOLSR where SOURCE CLAIM messages will be replaced by DAMA

registration messages. The RSM for MOLSR uses RS as “Originator Address” defined in the protocol.

The DAMA fairness, DOS prevention mechanism and temporary address handover/takeover mechanisms are going to improved, implemented in the next phase of the DAMA project.

6 Acknowledgement

The work reported in the paper has been developed in the framework of the project “Talent care and cultivation in the scientific workshops of BME”. This project is supported by the grant TÁMOP - 4.2.2.B-10/1–2010-0009.

References

1. M. Orosz, G. Hosszú, F. Kovács: “Global Address Allocation for Wide Area IP-Multicasting” chapter in book, Encyclopedia of Multimedia Technology and Networking, Second edition (3 Volumes, 1756 p.), Editor: Margherita Pagani, Information Science Reference, Hershey, USA, 2009, Vol. II, pp. 574-580, ISBN 9781605660141
2. Daniel Zappala, Virginia Lo, and Chris GauthierDickey: The Multicast Address Allocation Problem: Theory and Practice. Special Issue of Computer Networks, Elsevier Science, 2004
3. Fenner, B., Handley, M., Holbrook, H., Kouvelas, I.: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised), Internet Engineering Task Force, Network Working Group, Request for Comments (RFC) 4601 (2006)
4. Holbrook, H., Cain, B.: Source-Specific Multicast for IP. Internet Engineering Task Force, Network Working Group, Request for Comments (RFC) 4607 (2006)
5. Hosszú G.: Az internetes ko*mmunikáció informatikai alapjai*, Első kiadás, Novella Kiadó, Budapest, 2005, 640 oldal, ISBN 963 9442 51 8.
6. Hosszú, G.: Current Multicast Technology. In M. Khosrow-Pour (Ed.), Encyclopedia of Information Science and Information Technology Vol. I-V, (pp. 660-667). Hershey, PA: Idea Group Reference, 2005
7. Kim, D., Meyer, D., Kilmer, H., & Farinacci, D.: Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP). Internet Engineering Task Force, Network Working Group, Request for Comments (RFC) 3446 (2003)
8. M. Orosz, G. Hosszú, F. Kovács: “DNS-Based Allocation of Multicast Addresses” chapter in book, Encyclopedia of Internet Technologies and Applications, Editors: Mário Freire and Manuela Pereira, Information Science Reference, Hershey, USA, 2007, ISBN: 978-1-59140-993-9, pp 157-164.
9. McBride, M., Meylor, J., Meyer, D.: Source Discovery Protocol (MSDP) Deployment Scenarios. Internet Engineering Task Force, Network Working Group, Request for Comments (RFC) 4611, Best Current Practice, BCP: 121 (2006).
10. Meyer, D., & Lothberg, P.: GLOP Addressing in 233/8. Internet Engineering Task Force, Network Working Group, Request for Comments (RFC) 3180, Best Current Practice, BCP: 53 (2001)

11. Mockapetris, P.: Domain names - implementation and specification, STD 13, Internet Engineering Task Force, Network Working Group, Request for Comments (RFC) 1035 (1987)
12. Bhattacharyya, S. (Ed.): An Overview of Source-Specific Multicast (SSM). Internet Engineering Task Force, Network Working Group, Request for Comments (RFC) 3569 (2003)
13. Rajvaidya, P. & Almeroth, K.: Analysis of routing characteristics in the multicast infrastructure. In Proceedings of the IEEE INFOCOM (pp. 1532-1542). San Francisco: IEEE Press, 2003
14. S. Kumar, P. Radoslavov, D. Thaler, C. Alaettinoglu, D.Estrin, & M. Handley: The MASC/BGMP Architecture for Interdomain Multicast Routing in ACM SIGCOMM, August 1998.
15. Savola, P.: Lightweight Multicast Address Discovery Problem Space. Internet-Draft. Internet Engineering Task Force, MBONE Deployment, 2006, work in progress.
16. Savola, P.: Overview of the Internet Multicast Addressing Architecture. Internet-Draft. Internet Engineering Task Force, PIM Working Group, 2006, work in progress.
17. Savola, P.: Overview of the Internet Multicast Routing Architecture. Internet-Draft. Internet Engineering Task Force, PIM Working Group, 2007, work in progress.
18. Badameh, O., Kadoch, M.: Multicast Routing Protocols in Mobile Ad Hoc Networks: A Comparative Survey and Taxonomy. EURASIP Journal onWireless Communications and Networking (January 2009)
19. Laouiti, A., Jacquet, P., Minet, P., Viennot, L., Clausen, T., Adjih, C.: Multicast Optimized Link State Routing, INRIA research report RR-4721 (2003)