Security and Routing Scoped IP Multicast Addresses

Imed Romdhani, Ahmed Al-Dubai
Edinburgh Napier University
School of Computing
10, Colinton Road, EH10 5DT Edinburgh, UK
{I.Romdhani, A.Al-Dubai}@napier.ac.uk

Mounir Kellil
CEA LIST, Laboratoire des Systèmes Communicants
Point Courrier 94, Gif-sur-Yvette, F-91191 France
Mounir.Kellil@cea.fr

***Abstract*— IP multicast is an efficient and scalable network layer delivering method for multimedia content to a large number of receivers across the Internet. It saves the network bandwidth and optimizes the processing overhead of the source. However, current IP multicast deployment is still facing many deployment complexities. In particular, the duality and the strong relationship between multicast addressing and routing along with the absence of an integrated multicast access control security mechanism have prevented a broader deployment of multicasting over large and public network infrastructures such as the Internet. To solve multicast scoping and autonomic multicast routing triggering issues, we propose a new scope based and hierarchical multicast control and routing protocol[1]. Our approach introduces a new multicast addressing scheme that embeds simultaneously a plurality of hierarchical scopes and associates each scope with a specific access control and routing method. We evaluate the performance of our solution with respect to access control overhead and we analyse its strengths and limitations compared to related works.**

Keywords-component; *IP Multicast, Many-to-Many, Access Control, Multicast Routing and IPv6.*

I. INTRODUCTION

Multicast communication is an elementary service and fundamental for many applications in networked and distributed systems. In addition, multicast communication itself is not only central to many important real-world distributed applications but is also fundamental to the implementation of higher-level communication operations such as gossip, gather, and barrier synchronisation. In general, the primary benefits of a packet reaching multiple destinations from a single transmission are threefold: bandwidth minimization, the exploitation of parallelism in the network and the optimization of transmitter costs. However, current IP multicast deployment figure is still far away behind the expectations of both Internet Service and Content Providers due to several deployment complexities. These deployment complexities are due to an increasing gap between the state-of-the-art and the real deployment [1], [2]. While current routing devices and internetwork operating systems are IP multicast enabled for both IPv4 and IPv6 addressing schemes, Internet Service Providers (ISPs) are resisting to a large public use of IP multicast. This deployment resistance and fear can be justified by the lack of comprehensive and deployable secure multicast architecture that fulfils ISP requirements in terms of access control, source authentication, network management and billing [3][4]. Unfortunately running IP multicast applications in a similar and smooth manner as IP unicasting is not realistic due to fundamental differences between the two communication models. Compared to unicast, multicast communications require transactional state to be maintained by the network layer forwarding entities along the delivery path from the source to the set of receivers. While IP multicast addressing schemes constitute the key foundation on top of which all other routing, security and management operations will be built upon, they suffer from different limitations. First, a group communication address, whether it is an Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) based address [5], is identified by an owner or a group creator, a fixed distribution scope boundary, a lifetime, a group lifetime, and it is implicitly or explicitly associated with a particular class of multicast routing protocol. Therefore, before starting a multicast session, a network administrator needs to check first the ownership, the correctness of the IP address and the validity of all its parameters prior to enabling the routing and the security processes on the network. Unfortunately, such a verification and validation process is not yet automated and there is a lack of integrated Internet standard to ease the complexity of such a task. On the other hand, multicast source verification is required for several raisons. First, the verification process is necessary to detect and prevent various types of attacks including address spoofing and Denial of Service (DoS). Second, unnecessary multicast routing states will not be inserted in multicast routing tables and thus associated multicast routing control messages will not be exchanged between routers. As a result, the former will avoid constructing multicast branches or the whole multicast delivery tree, which saves, in return, their processing capabilities. Finally, potential multicast receivers will be prevented from being locked up, paralyzed, or waiting endlessly for a multicast content that will not arrive. While the source verification is important, the activation of the multicast routing process to construct the multicast delivery tree should be optimized and well scheduled. In fact, multicast routers cannot trigger automatically a unidirectional or a bidirectional multicast

[1] Patent Pending, patent application number GB0820316.8, assigned to Edinburgh Napier University, UK, field on 06 November 2008.

1530-2016/09 $26.00 © 2009 IEEE
DOI 10.1109/ICPPW.2009.81

routing protocol unless they are manually configured to use a specific routing protocol for a predetermined pool of IP multicast addresses. The pool of IP multicast addresses itself may has ambiguous and contradictory semantic from one ISP network to another with respect to one-to-many or many-to-many capabilities or scope distribution boundaries. While it is possible today to secure the multicast payload content thanks to end-to-end security keying and cryptographic methods, the access control for both senders and receivers remains a costly and time consuming process. The access control can be further complicated if the scope boundaries cannot be properly defined and controlled or the receivers have conflicting access rights and preferences. In reality, there are many collaborative multicast applications where the receivers can be clustered into different well-known sub-groups each of which has its own sending and receiving rights. These sub-groups may be isolated from each others as they may coexist in a nested manner in the network topology.

To ease and combine multicast router dynamic auto-configuration and access control check, we propose and analyze a combined approach that encompasses an enhanced multicast address scoping scheme. Thanks to a new scope field format for both IPv4 and IPv6 networks, we automate both access control and routing triggering for both one-to-many and many-to-many multicast applications. By using our enhanced multicast addressing approach and in order to lower the complexity of the network layer, we introduce a new scope based multicast routing protocol. Our protocol exploits the hierarchical feature of network topologies and builds in parallel a global multicast delivery tree for a given group by interconnecting heterogeneous and mixed per-scope unidirectional and bidirectional based sub-trees. Thus, a coherent interaction between addressing, routing and security access control is introduced.

Our paper is organized as follow. In Section 2, we introduce the background for IP multicast. Then, we describe in Section 3 the multicast scoping and access control issues. In Section 4, we present our solution and we analyse its performances with respect to access control overhead in Section 5. Finally, we conclude by discussing the strengths and the limitations of our solution and the future work.

II. BACKGROUND

Today, IP multicast relies on two main membership models: Any-Source Model (ASM) and Source-Specific Model (SSM) [5]. These models have different multicast address ranges and different terminologies. In fact, IP multicast defines a special IP multicast address to identify the group of interested receivers. Senders (multicast sources) send to the multicast address without prior knowledge of the multicast receivers. IP multicast does not require senders to a group to be members of the group. To set-up a multicast session and distribute the multicast data, the group of interested receivers should be identified. A multicast address is a specific IP address used to identify a set of hosts to deliver IP packets to. The multicast address can be allocated from a specific range of IP addresses dedicated for sending to groups. Each address has a specific scope, which limits the flooding of multicast packets. Currently, multicast scoping technique uses either the "*Time To Live*" field in the IPv4 packet header or the scope field in case of IPv6. In IPv6, the scope field is an integrated part of the multicast address itself. The IETF has particularly defined guidelines that explain how to assign and allocate IP multicast address for both the ASM and the SSM models. To allocate a multicast address, two mechanisms can be used. The first mechanism is a centralized one where the allocation is carried out by an authorized entity. Hence, a multicast address has to be requested from this authority and cancelled when the multicast session ends. The second mechanism is a distributed one. The distributed allocation is done locally through multicast address allocation servers and requires specific protocol like the Multicast Address Dynamic Client Allocation Protocol (MADCAP) [6]. Compared to the centralized mechanism, the distributed mechanism does not guarantee the uniqueness of the multicast address, but it is more flexible than the centralized mechanism. To avoid confusion and reduce the probability of IP multicast address collision, both IPv4 and IPv6 multicast address architecture have been revised to embed unicast prefixes in multicast addresses [7][8][9]. By delegating multicast addresses at the same time as unicast prefixes, network operators will be able to identify their multicast addresses without running an inter-domain allocation protocol. Once a multicast address is allocated, the multicast source or the group manager describes the multicast session to be launched using the multicast Session Description Protocol (SDP) [10] and advertises this description using the multicast Session Announcement Protocol (SAM) [11].

The exiting multicast address allocation schemes have not defined yet a common strategy to allocate one-to-many and many-to-many multicast addresses. While multicast routers are capable to distinguish between ASM and SSM pool of addresses, they are unfortunately unable to trigger an optimal multicast routing protocol (i.e. unidirectional or bi-directional) for a given application. For instance, the PIM-SM protocol provides both one-to-many and many-to-many multicasting capabilities as it builds a shared unidirectional shared tree rooted on a Rendezvous Point, however the switching mechanism from the Rendezvous Point shared tree to a source-routed shortest path tree is inadequate for many-to-many communications where the number of sources could be very large. For scalability reasons, interactive multimedia applications could not be implemented as multiple instances of one-to-many.

To receive multicast traffic, an interested receiver requires a mechanism to join the multicast group. The receiver notifies its local router that it is interested on a particular multicast group address; the receiver accomplishes this task by using a membership protocol such as IGMP (Internet Group Management Protocol for IPv4 hosts) [12] or MLD (Multicast Listener Discovery Protocol for IPv6 hosts) [13]. To build a distribution tree from the senders to all receivers as indicated in Figure 1, multicast capable routers need a multicast routing protocol to handle the duplication of multicast traffic and conveying multicast packet across the built tree [14][15][16]. Several multicast routing protocols are proposed for the use on the Internet. Since the early routing protocols such as DVMRP and MOSPF were designed to handle dense multicast groups, new other protocols are proposed to offer better scalability. Sparse-mode protocols like PIM-SM provide efficient multicast communication between members that are sparsely distributed. Such protocols use a single unidirectional shared

tree that spans all members of a group. Consequently, multicast traffic for each group is sent and received over the same delivery tree, regardless of the source. Compared to share tree protocols, SSM routing protocols construct a specific delivery tree per source.

While multicast technology offers group-oriented communication settings with reduced overheads and low group management costs, its advantages are achieved at the expense of raising various scoping and security problems. This limitation prevents a border deployment of multicasting over large and public network infrastructures such as the Internet. In the next sections, we are going to detail briefly theses issues with some examples.

III. MULTICAST DEPLOYMENT ISSUES

A. *Addressing and scoping problem*

The Internet community has designed different unicast addressing schemes to be used independently of the underlying unicast routing protocol to be used. In contrast, multicast addressing and routing approaches have a strong relationship and dependency between them. In fact, a multicast address is matched either implicitly or explicitly with a specific multicast routing protocol. This means that for example a multicast application that uses an IP multicast address allocated from the Any-Source Multicast (ASM) pool should be configured with a unidirectional multicast routing protocol such as PIM-SM. However, if the address is a Source-Specific Multicast (SSM) address, in this case, an SSM compatible routing protocol should be used instead of a shared tree based one. While this association is easily distinguishable, many-to-many multicast application still require extra network administration settings to bind a pool of multicast addresses to a specific bi-directional routing protocol such as Bidirectional PIM-SM or CBT [16]. This duality of semantic is further complicated by the allocation strategy to be put in place and that is why new addressing strategies have been recently introduced by the Internet Engineering Task Force (IETF) to simplify and ease multicast address allocation process and make it similar or inspired from unicast addressing. This attempt covers for both IPv4 and IPv6 networks [7] [8]. While, we do believe that these solutions can help to reduce the complexity of multicast addressing and guarantee the uniqueness of a multicast address across the Internet, there is still a vital need to address the other related addressing issues such as the scope boundary definition and the security access rights. In fact, several multicast applications involve the exchange of sensitive information such as private multimedia conferences, pay-per-view, and military communications. These applications are particularly concerned with the security and distribution problems as multicast traffic can cross insecure links and unwanted large network areas. Hence, an attacker may alter (modify) data content, read sensitive information, or exploit the multicast infrastructure to launch Denial of Service attacks (DoS). Lo limit multicast flooding issue and avoid multicast data being forwarded beyond well defined administrative boundaries, administratively scoped IP multicast addresses have been proposed to overcome the limit of the IPv4 TTL packet header technique [17]. These well-known addresses intend to guarantee local significance within every organization and permit address reuse while having topological meaning. In terms of deployment, a router at an administrative boundary should be configured with one or more per-interface security access filter, which induces a manual setting and network management overheads. To announce scope zone boundaries, the Multicast-Scope Zone Announcement Protocol (MZAP) [18] is used between multicast routers. Compared to IPv4, IPv6 uses a simple method that embeds the scope field into the multicast address itself. Thus, a multicast router can detect automatically the distribution scope limit based on the value of the scope field and consequently, no announcement protocol is required. Table 1 illustrates the different scopes in IPv4 and IPv6.

Table 1: Multicast scopes in IPv4 and IPv6

Scope Field Value (IPv6)	Scope [RFC 4291]	IPv4 Prefix [RFC 2365]
1	Interface-Local scope	Not assigned
2	Link-local	224.0.0.0/24
4	Admin-Local	Not assigned
5	Site-local	239.255.0.0/16
8	Organisation-local	239.192.0.0/14
E	Global	224.0.1.0 - 238.255.255.255

B. *Access control problem*

Defining efficient security solutions for multicasting is a challenging task. Indeed, multicast sessions are subject to different constraints, including group characteristics (e.g. membership dynamism and group size), multicast application requirements (e.g. QoS, level of security and resource requirements), etc. Such constraints complicate the multicast security problem. As a result, the multicast security community has made extensive efforts to study the multicast security issues, and propose a variety of solutions. Four key blocks of the multicast security issue are emerging: Multicast source authentication and data integrity, group key management, multicast routing security, and multicast receiver and sender access control. In this paper, we will focus on the receiver and sender access control issues only. The sender access control aims at preventing unauthorized hosts from sending bogus multicast traffic. This problem is particularly challenging because the open multicast model style allows any user to send its multicast traffic without prior request to the multicast router. The authorization represents the right (or a permission) that is granted to a system entity to access a system resource. An "authorization process" is a procedure for granting such rights and it is triggered once the entity to be authorized has been successfully authenticated. The authorization can be seen as a function that links a user ID with a set of permissions (or privileges). User ID could be transmitted by the member during the registration phase, otherwise the group manager (or subgroup manager) can simply store and map user ID to its access rights or credentials. In a dynamic access control environment, the message exchange rate between the group manager and the members may increase considerably (e.g. to refresh the access rights of members). In this situation, the

group manager may suffer from processing overheads. This problem may be resolved by deploying a hierarchal or distributed architecture that distributes the access control tasks among multiple sub-group managers. The impact of bogus multicast traffic towards existing multicast groups increases with the scope of the targeted multicast groups. Although packets originating from an illegal source can be discarded by the receivers using a source authentication mechanism, these bogus packets will still generate traffic overhead over the scope of the multicast group. In addition, the impact of bogus multicast traffic towards non-existing multicast groups may be dramatic for the delivery trees as well as Internet communications. In fact, an attacker may generate DoS attacks against multicast routers by involving them in extensive exchanges of control messages. Although the ingress filtering mechanism eliminates the risk for remote attacks, an attacker localized within the same link as a legitimate sender can impersonate it (spoofing) and send bogus multicast traffic. Furthermore, the problem is particularly complicated in the Any Source Model (ASM) as the designated routers do not maintain state information about the senders. In addition, source filtering mechanisms provided by the Source-Specific Model (SSM), the RPF check, and other source-filtering approaches do not efficiently resolve the problem because they use sender's IP address-based filtering, which cannot prevent spoofing attacks originating from the network of a legitimate source.

To overcome the scoping and access control issues, new solutions are therefore required. These solutions should be easy to deploy and manage. In the next section, we attempt to propose a combined approach that integrates security access control and routing by enhancing the multicast scoping feature.

IV. NEW MULTICAST ADDRESSING AND ACCESS CONTROL METHOD

Multicast application requirements influence both security and routing approaches to be used. Hierarchical multicast management approaches are required to fulfil multicast application specificity, topology engineering and routing, and security access control requirements. In the next sections, we are going to highlight these requirements and explain how hierarchical design can ease multicast management and deployment. Then, we will propose a new solution that exploits the hierarchical feature of multicast groups and we prove how it can help to improve both multicast addressing allocation and routing configuration.

A. Requirements for a hierarchical solution

Multicast application requirements: depending on the sender access right, multicast applications can be classified into two main classes: one-to-many and many-to-many. In one-to-many group communication, only a unique source is allowed to send to the whole group. This type of communication can be compared to a master/slave communication where the master controls all operations. However; in many-to-many multicast applications, a subset or the entire receivers are entitled to send data to the rest of the group at any time. Transmission coordination and synchronization may be required to allow one source to send once a time using either a round-robin fashion or any other timing or access control based mechanisms. This classification of multicast applications is not really realistic as different levels of access rights may be required for heterogeneous receivers. These receivers may be located in separate and identifiable zones or levels of a network topology (Virtual local area networks, sites, branches, etc.) or they may co-exist in the same topology or geographic location due to network deployment, management or mobility constraints (e.g. military and tactical networks). In such circumstances, the multicast traffic is required to be addressed to these receivers according to their security accessibility allowance and their available network resources. Therefore a clustering approach is required to isolate those who are allowed to receive the data from those who are not at both security and routing levels.

Topology design requirements: According to [19] layering concept is highly recommended when designing network topologies in order to ease network management, optimise equipment efficiency, plan network traffic patterns, enhance routing information aggregation, implement routing policy and manage traffic forwarding and admittance into the network. By using vertical logical division, a network topology can be broken into two or three-layer hierarchies. Each layer may have several zones, whereas a zone designates a logical set of routers within the layer. In practice, networks are divided into two or three layers which are: core, distribution and access. In addition, network using link-state routing protocols are for example divided into areas (OSPF) or domains (IS-IS). This engineering practice is inline with many conceptual and analytical Internet topology models and studies [20] [21] that proved the hierarchical property of the Internet topology in both router and AS (Autonomous System) levels. Thanks to layering points, network administrator can control the amount of data that each networking device needs to manage. Arguably, this is highly recommended for IP multicast as controlling the scope of the distribution of multicast data and defining security access control points to control multicast traffic forwarding and admittance are the major problems to be addressed for any successful multicast deployment. Therefore, we do believe that exploiting the hierarchical nature of network topologies can help to design multicast solutions that solve both routing and access control issues.

Security requirements: In a dynamic access control environment, the message exchange rate between the group manager and the members may increase considerably (e.g. to refresh the access rights of members). In this situation, the group manager may suffer from processing overheads. This problem may be resolved by deploying a hierarchal or distributed architecture that distributes the access control tasks among multiple sub-group managers. This is also useful for mobile environments where a mobile member needs well-adapted access control services when it moves into foreign "domains". An example of hierarchical security solution is the KHIP protocol. KHIP (Keyed Hierarchical Multicast Routing Protocol) was specified in the purpose of securing the Hierarchical Multicast Routing Protocol (HIP) [22]. HIP protocol enables for routing multicast data between heterogeneous multicast domains (each domain uses its proper multicast routing protocol). The domain is defined by a set of

OCBT routers. Besides, HIP uses border routers of the multicast domain as OCBT cores. KHIP (Figure 1 and 2) places trust in OCBT cores and some routers to maintain correctly the multicast tree (protection against untrusted routers) and help to ensure receiver and sender access control. Besides, the multicast tree is divided into a number of sub-branches, each with an OCBT core as a root.

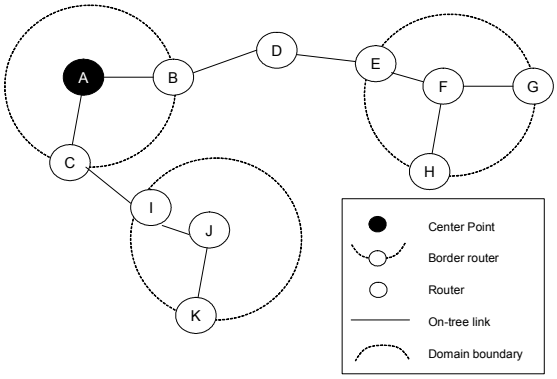

Figure 1: HIP Tree Structure

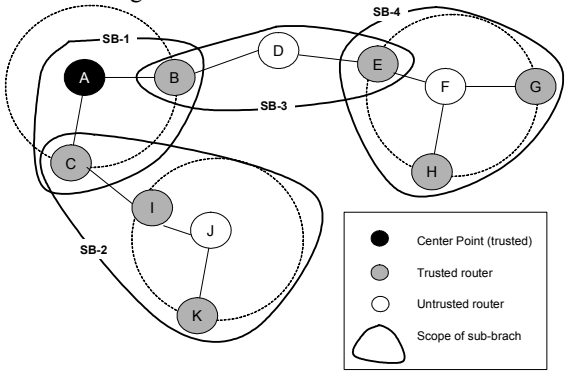

Figure 2: Secure HIP Tree under KHIP

In KHIP, a group manager maintains an access list for each multicast group and securely issues digitally signed multicast certificates to authorized members. The certificate includes several fields such as member's IP address, its public key, the range of authorized addresses, and per-group permission (initiator, sender, receiver, and group terminator). When a host wishes to receive or send multicast traffic for a multicast group, it sends its Report message along with its certificate. When the DR receives host's messages, it determines the validity of host's request based on the enclosed certificate. If successful, the DR transmits to the host a starting sequence number and a branch key (KB) both used for data transmission. To act as a new sender, the new member creates a random encryption key (KRand) for data encryption. This key is then encrypted with KB and transmitted with each data packet. Sender's traffic is then controlled (decryption, verification, and re-encryption) by trusted routers interconnecting different branches.

B. New IPv6 Multicast Address Format

To differentiate between one-to-many and many-to-many multicast addresses and to embed the different access rights of the group into the multicast address itself, we propose a new multicast addressing scheme for IPv6. Our solution is also applicable for IPv4, but for simplicity reason, we will limit our discussion to IPv6. The new IPv6 multicast address has an expanded scope field, which enables a plurality of hierarchical distribution scopes. The length of the new scope field is extended beyond the standard 4-bit value as illustrated in Figure 4. In fact, the standard IPv6 addressing format defines one single distribution scope per multicast address, which is explicitly coded in the multicast address by using the hexadecimal value of all the 4 bits. However in the new format, a plurality of distribution scopes is consecutively and simultaneously coded in each multicast address. The order of coding defines and differentiates explicitly each hierarchical scope (sub-scope). Consequently, this method will improves the multicast address allocation mechanism by avoiding allocating a multicast address per a single scope basis. In the conventional allocation method, the distribution scopes are mutually exclusive, while in the new method the distribution scopes could collocate. The definition of the hierarchies will depend on network topology and the structures of user groups for a given organization, but as an example where there are six hierarchies these could relate to interface-local, link-local, admin-local, site-local, organization-local, and global scopes with respect to the latest IPv6 standards. The size of the scope field will therefore govern how many hierarchies can be embedded. A an example, a 12-bit value scope field can be used to provide a basis for the definition of six ordered hierarchies, with two bits being allocated for the identification of each of the six hierarchies.

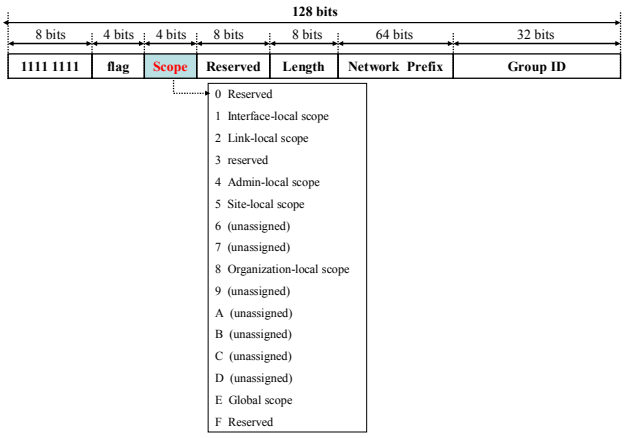

Figure 3: Conventional IPv6 multicast address format with respect to the specification of RFC 3306.

Figure 4 shows an embodiment wherein the scope field is extended to a 12-bit value in accordance with RFC 3306, with the additional eight bits being borrowed from the reserved field. It is to be appreciated that in other embodiments the format, the length, and the placement of the scope field could be changed, and distribution scopes could be added, removed, reordered, or changed. The same extension can be also applicable to the IPv6 address format as proposed by RFC4291. In this case, eight bits need to be borrowed from the Group ID field (Figure 5).

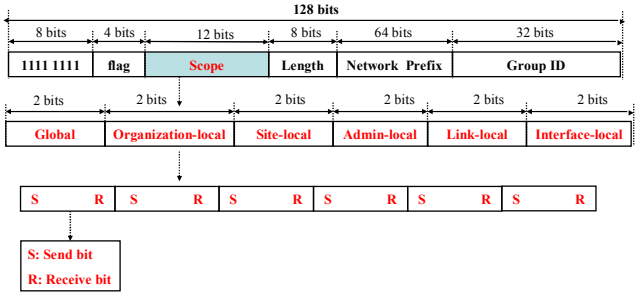

Figure 4: Our extended scope format with respect to RFC 3306

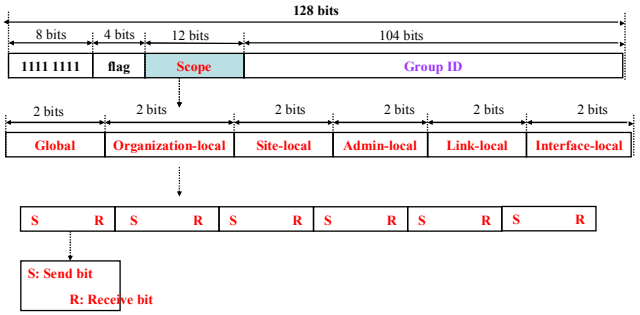

Figure 5: Our extended scope format with respect to RFC 4291

To differentiate the access rights for multicast receivers and senders within each distribution level (sub-scope), we defined in the same scope field the correspondent access right modes for the group members. Conventionally, the access right for a given multicast group is defined by external mechanisms such as security access lists or security keying which are configured by the network administrator. Moreover, this access right is applicable and valid for the whole group as a single unit. However in our new format, the access rights are encoded in the multicast address itself. There are many ways in which the access rights can be encoded. In one embodiment, the access rights can be encoded by using two bits that define send and receive permissions for each sub-scope. The binary combination of these two bits allows four permission rights. One bit (for example the highest) can be reserved for a "transmission" right and one bit (for example the lowest) can be reserved for a "reception" right. The other bits can define other intermediate permissions. For example, within each sub-scope multicast receivers may be assigned with one of the following access rights: denial of access, receive only, send only, or send and receive simultaneously. The numeric hexadecimal value of each bit is either one or zero. These are illustrated in Figures 4 and 5, where each of the scopes is of a 2 bit size with the bits encoding data regarding the send and receive permissions for each of the scopes.

C. Scope Based RoutingProtocol

Thanks to our new addressing and access control method, a multicast controller, for instance a multicast router, can dynamically auto-configure itself by using one or multiple optimal multicast routing protocols, either per whole multicast group basis or per scope basis. When different multicast routing protocols are used simultaneously for the same multicast group address, multicast routers within a specific scope can choose to run the same routing protocol.

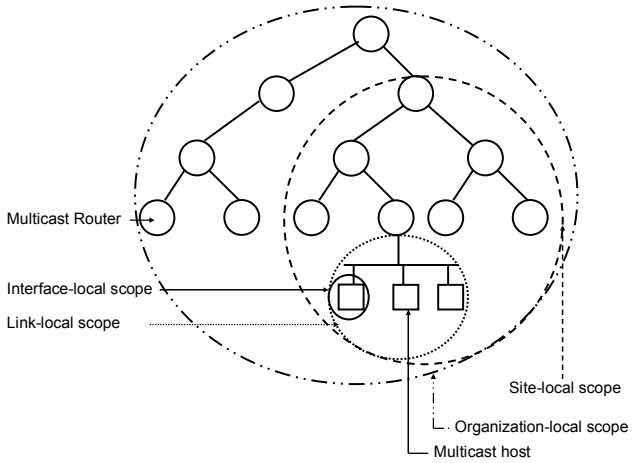

Figure 6: Examples of hierarchical scopes

The selection of a given multicast routing protocol within a given scope depends on the access right values for that scope level. The multicast routing protocols for all the distribution scopes may be the same. Thus, our solution introduces for the first time a hierarchical scope-based multicast routing method where unidirectional and bidirectional multicast routing protocols can co-exist and used simultaneously to construct a multicast delivery tree for a given multicast group. Multicast routing protocols can be triggered per scope basis or per whole address basis (Figure 7).

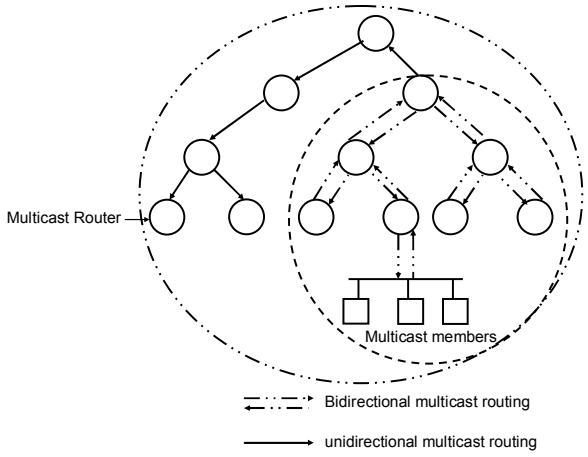

Figure 7: Hybrid unidirectional and bidirectional multicast routing

To construct unidirectional or bi-directional trees, multicast border routers have to play a key role. These routers need to run different routing protocol instances if their routing interfaces are connected to different scopes. If a unidirectional shared three is needed to be built inside for a given scope or a network topological level, one of these scope border routers can be elected as a rendezvous point or core router for that shared tree, thus the distribution of multicast content can be fasten and tree maintenance is improved. In brief, our solution does not introduce a new routing protocol, but it changes the

way existing unidirectional and bidirectional multicast routing are deployed. These two types of multicast routing protocols can be used simultaneously for a single multicast group. By using hybrid multicast routing protocols for the same group, multicast tree maintenance overhead is minimized as routing protocols are used on-demand based on the security access control requirements.

V. PERFORMANCE EVALUATION

Our new multicast addressing scheme enhances multicast source filtering for receivers with different multicast data admittance and forwarding preferences. Classic filtering approaches uses either different multicast addresses for each specific group users' preference or they use one single multicast address and allow the receivers to do filtering themselves with coordination with their multicast access routers [23][24]. If we evaluate the number of different combinations of users preferences in terms of sending and receiving access rights for all possible scopes of a multicast group, we can conclude that this number follows the formula ($2^{2L} - 1$), whereas L is the number of scopes (e.g. link-local, site-local, organization, etc.). In this formula, we assume that if all the scope bits are set to zero (i.e. S=R=0), the multicast address is reserved and can not be used. As illustrated in Figure 8, the new scope field saves a considerable number of multicast addresses especially when the number of possible hierarchical scopes is high.

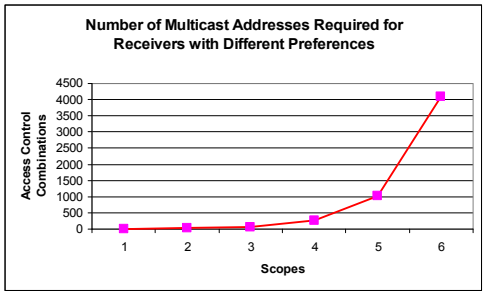

Figure 8: Access control combinations

Beyond the access control feature of our solution discussed above, our solution gives rise to many other advantages. The expanded scope field means that a standardized allocation or assignment method of multicast addresses that differentiates between one-to-many and many-to-many address ranges can be provided. In addition, the encoding of all scopes in the expanded scope field avoids the need to implement complex security mechanisms such as security access lists and avoids the need for a third party to filter unauthorized multicast receivers and sources for the matching and binding of specific ranges of multicast addresses to specific multicast routing protocols, as is required by multicast routing policies. Furthermore, by encoding both distribution scopes and the associated access rights in the multicast address itself, our solution helps to auto-configure multicast capable routers with the appropriate multicast routing protocols and therefore ease network management. Compared to the access control solution introduced in [25], in our solution access list forwarding is avoided between routers. In addition, multiple multicast routing protocols can be deployed for the same multicast group instead of using a single multicast routing protocol for all hierarchical distribution scopes in association with many confusing security access lists to perform the same results. Also, multicast routers within an administrative domain will share the same view of what type of multicast routing protocol to be used (for the scope and for the whole multicast group) and what are the associated access rights to be verified. The access rights may follow the network topological design or the users' distribution across the network. Finally, the new addressing, access control and routing methods are simple to implement and deploy and they ease autonomic multicast capable router configuration, in contrast to conventional methods which are complex to deploy. To be deployed in IPv4 networks, our solution requires changing the interpretation of the IPv4 TTL packet header when multicast is used. Another alternative for IPv4 consists of introducing new routing control packets and exchanging them between multicast routers. In all cases, more in-depth simulation and analysis is still required to measure the impacts of our solution on the routing overhead and on the properties of multicast tree structures in the Internet [26]. Future work will focus on these points to enhance our proposed solution.

VI. CONCLUSION

To ease autonomic multicast router configuration, we have proposed a new extension to the IPv6 multicast address format. Our extension consists of embedding a plurality of ordered hierarchical scopes with their associated access rights on the multicast address itself. Such integration will be used by multicast routers to trigger the appropriate multicast routing protocol per sub-scope basis. Our solution constitutes an attempt to lower the complexity of the network layer and to introduce a coherent cross-layer interaction between the multicast addressing, multicast routing and multicast security levels. Future work will focus on how to extend this interaction to merge more other levels (multicast announcement, multicast description, and multicast router discovery, etc.), to secure multicast address allocation and avoid multicast scope alteration.

REFERENCES

[1] S. Ratnasamy, A. Ermolinskiy, and S. Shenker, "Revisiting IP Multicast", Proceedings of SIGCOMM, pp. 15-26, September 2006.

[2] Kevin C. Almeroth, "Multicast Help Wanted: From Where and How Much?", Workshop on Peer-to-Peer Multicasting 2007 (P2PM'07), at IEEE Consumer Communications and Networking Conference 2007 (CCNC 07), Las Vegas, NV, USA - January 11, 2007.

[3] Hiroaki Satou, Hiroshi Ohta, Christian Jacquenet, Tsunemasa Hayashi, Haixiang He, "AAA and Admission Control Framework for Multicasting", IETF Internet Draft, Work in Progress, January 28, 2009.

[4] B. Quinn, K. Almeroth, "IP Multicast Applications: Challenges and Solutions", RFC 3170, September 2001.

[5] P. Savola, "Overview of the Internet Multicast Addressing Architecture", IETF Internet Draft, Work in Progress, October 2006.

[6] S. Hanna, B. Patel, and M. Shah, "Multicast Address Dynamic Client Allocation Protocol (MADCAP)", IETF Standards Track, RFC 2730, December 1999.

[7] B. Haberman and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", IETF Standards Track, RFC 3306, August 2002.

[8] D. Thaler, "Unicast-Prefix-based IPv4 Multicast Addresses", IETF Internet Draft, Work in Progress, March 9, 2009.

[9] B. Haberman, "Allocation Guidelines for IPv6 Multicast Addresses", IETF Standards Track, RFC 3307, August 2002.

[10] Mark Handley, Van Jacobson, and Colin Perkins, "SDP: Session Description Protocol", IETF RFC 4566, July 2006.

[11] Mark Handley, Colin Perkins, and E. Whelan, "Session Announcement Protocol", IETF Standards Track, RFC 2974, October 2000.

[12] Brad Cain, Steve Deering, Bill Fenner, Isidor Kouvelas, and Ajit Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[13] Rolland Vida, and Luis Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", Internet Draft, RFC 3810, June 2004.

[14] P. Savola, "Overview of the Internet Multicast Routing Architecture", IETF RFC 5110, January 2008.

[15] B. Haberman, J. Martin, "Multicast Router Discovery", IETF RFC 4286, December 2005.

[16] Mark Handley, Isidor Kouvelas, Tony Speakman, Lorenzo Vicisano, "Bi-directional Protocol Independent Multicast (BIDIR-PIM)", IETF RFC 5015, October 2007.

[17] M. Handley, D. Thaler, R. Kermode, "Multicast-Scope Zone Announcement Protocol (MZAP)", RFC 2776, February 2000.

[18] D. Meyer, "Administratively Scoped IP Multicast", RFC 2365, July 1998.

[19] Russ White, Alvaro Retana, Don Slice, "Optimal Routing Design", Cisco Press, ISBN-10: 1587051877, June 17, 2005.

[20] H. Haddadi, M. Rio, G. Iannaccone, A. Moore, R. Mortier, "Network topologies: inference, modeling, and generation", IEEE Communications Surveys & Tutorials, vol.10, Second Quarter 2008, pp. 48–69.

[21] Siganos Georgos, Tauro Sudhir Leslie; Faloutsos Michalis, "Jellyfish: A conceptual model for the AS Internet Topology", Journal of communication and networks, Vol. 8, no3, Pages 339-350, 2006.

[22] C. Shields and J.J. Garcia-Luna-Aceves, "KHIP—A scalable protocol for secure multicast routing", Proceedings of ACM SIGCOMM'99, 1999, pp. 53 – 64.

[23] De-Nian Yang Wanjiun Liao Chang-Jung Kao, "Source Filtering in IP Multicast Routing", IEEE Transactions on Broadcasting, Volume: 52, Issue: 4, Pages: 529-542, December 2006.

[24] Salekul Islam, J. William Atwood, "The Internet Group Management Protocol with Access Control (IGMP-AC)", Proceedings of 31st IEEE Conference on Local Computer Networks, Tampa, Florida, U.S.A., November 14--16, 2006.

[25] N. Wang and G. Pavlou, "Scalable IP Multicast Sender Access Control for Bi-directional Trees", Proceedings of the 3rd International Workshop on Networked Group Communication (NGC'2001), London, J. Crowcroft, M. Hofmann eds, Springer, November 2001, pp. 141-158.

[26] Danny Dolev, Osnat (Ossi) Mokryn, Yuval Shavitt, "On Multicast Trees: Structure and Size Estimation", IEEE/ACM Transactions on Networking, vol. 14, no. 3, June 2006.