Information Technology Journal 3 (1): 95-105, 2004
ISSN 1682-6027

New Multicast Technology "Survey and Security Concerns"

Jean-Pierre Avognon
Huazhong University of Science and Technology,
502#, Foreign Guest House,
Bldg No 7, Wuhan 430074, Hubei, People's
Republic of China

Zhi Tang Li
Huazhong University of Science and Technology,
502#, Foreign Guest House,
Bldg No 7, Wuhan 430074, Hubei, People's
Republic of China

Abstract: IP multicast capable network is increasingly becoming an important technology for commercial and even military distributive and group-based application. As any network session, the security aspect of multicast is a very important problem to be resolved. This article is a first part of a continuous work that will end up on the IPsec-based security aspect of the IP multicast communication. In this article, we first make an overview on the multicast fundamental and its routing protocols as well as the distribution trees they are based on. Various techniques that have been currently proposed to enforce IP multicast security and reliability are qualitatively discussed.

Key words: IP multicast, security

INTRODUCTION

The Internet today provides the possibility of communication in different modes for the convenience of the interlocutors. Among those multiple communication modes we can cite the Unicasting, the Broadcasting, the Anycast communication, the point-to-point communication and also the multicast communication that will be the topic in this article.

The multicast communication is a typical group-oriented communication that permits to send efficiently information to one or more receivers at the same time so that packets are not sent several times from the same sender, to minimize redundant transmission on the network.

Generally talking, the inherent cost and resources benefits of multicast routing and data delivery are obvious, however the group-oriented communication paradigm presents new and unique technical challenges more severe than traditional networks routing and security approaches.

Fundamental of multicast: Multicast communication is a feature developed and used originally on LANs. Ethernet is the best example of a Local Area Multicasting. However, there is a more complex level of multicasting that is the Wide Area Multicast. This diverges from the first from both its principle and its application.

Local Area Multicast (LAM): The local level of multicast technology mainly takes advantage and feasibility from the possibility of the Ethernet to support multicast because of its diffusion nature. It is based on the LAN architecture, but will concern only host that belong to the group that the multicast packet is sent to. The LAM is generally a close multicast session that may not necessary base on the Internet.

In this case the security issue is less urgent as long as there is no packet relaying bridge (say router on the Internet) in direct or indirect connection to the LAN

Wide-Area Multicast (WAM): The Wide-Area Multicast transmission requires the presence of routers, i.e. some hosts capable of building and managing the multicast distribution tree at logical level. From the level and role of the routers in the network, we may distinguish:

- The leaf router, which is characterized by its possibility to discover and to locate the presence of hosts belonging to the multicast group.
- The transit router situated in the transit network and that participates into the distribution and forwarding of the packets to other transit routers or leaf routers, as shown in the Fig. 1.

The multicast session and addressing: In general, a multicast session is defined as either public or private (clear is the difference between LAM and private session and also WAM and public session). Any multicast session is characterized by a group of members who adhere to the group by the only membership property that is the multicast IP address. Thus, unlike in the unicast

Corresponding Author: Jean-Pierre Avognon, Huazhong University of Science and Technology, 502#, Foreign Guest House, Bldg No 7, Wuhan 430074, Hubei, People's Republic of China, Tel.+86 27 87820651-517, Fax: +86 27 87820658 E-mail: jean-pierre.avognon@alstom-wuhan.com

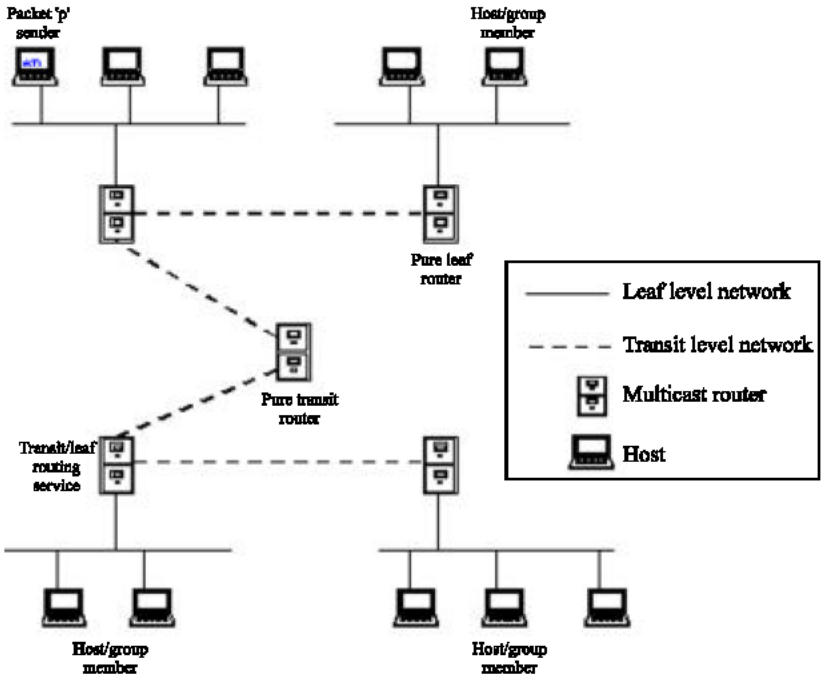

Fig. 1: Wide Area Multicast

communication, a given multicast IP address indicates and determines a group of members but not a member of the group.

The IP address range used in the multicast communication is given as follow:

- The range 224.0.0.0 to 239.255.255.255 that represents the class D address range in IPv4, as defined by RFC 1112[1]. Those addresses are characterized by "1110" as their high-order four bits. In this IP range, there are specific addresses primarily or already assigned to some special multicast groups, that are regularly published in the "Assigned Number " RFC[2]. Here, let's present some of them:
  - 224.0.0.1 is the "all-hosts" group address in the subnet. If you ping that group, all multicast capable hosts on the network should answer, as every multicast capable host must join that group at start-up on all its multicast capable interfaces,
  - 224.0.0.2 is the "all-routers" group. All multicast routers must join that group on all its multicast capable interfaces,
  - 239.0.0.0 to 239.255.255.255 defined by RFC 2365[3] as "Administratively Scoped IPv4 Multicast Space".

In any case the range from 224.0.0.0 through 224.0.0.225 is reserved for local uses (administrative and maintenance purpose). Any router never forwards packets destined to these addresses.

- IPv6 multicast addresses are distinguished by the value of the high-order octet of the addresses that is 0xFF (binary 11111111), as defined by RFC 2373[4,5].

The assignment rule is presented by the following format:

Bits number	8	4	4	120 bits
Value	11111111	flgs	scop	Multicast group ID

  - "Flgs" is a set of 4 flags with the 3 more significant bits always initialized to 0. The lower order bit takes the value "0" for a permanently assigned multicast address and the value "1" in case of a non-permanently-assigned multicast address.
  - "Scop" is a 4-bit multicast scope value used to limit the scope of the multicast group. It takes the hexadecimal "1" for node-local scope, "2" for link-local scope, "5" for site-local scope, "8" for organization-local scope and "E" for global scope; the values "0" and "F" are reserved.

    Ex: The IPv6 address FF02:0:0:0:F001:0:0:1 is a permanently assigned multicast address of a multicast group that ID is ::F001::1 and on the same link as the sender.

Multicast address mapping to ethernet address: A block of MAC addresses have been reserved for multicast address to identified multicast Ethernet or FDDI. That

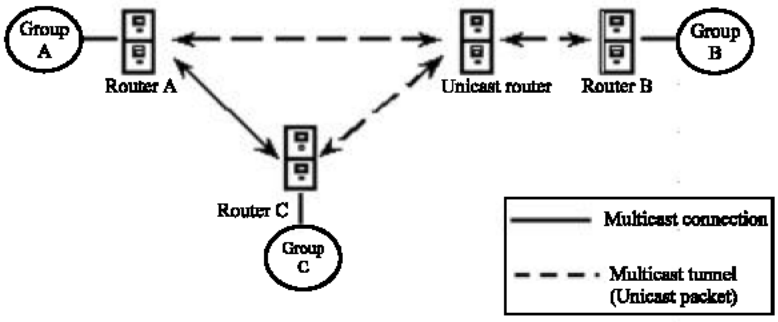

Fig. 2: Mbone architecture

range is 01-00-5E-00-00-00 to 01-00-5E-FF-FF-FF (hex). Thus, every Ethernet/FDDI frame that destination address is within that address range contains data for a multicast group. The prefix 01-00-5E identifies the frame as multicast; the next bit (24th from the least significant bit of the Ethernet address) is always 0.The complete multicast Ethernet address is then created by copying the low 23 bits of the IP multicast address in 01-00-5E-00-00-00.

Ex: Multicast IP address 224.0.10.09 will map to Ethernet address 01-00-5E-00-0A-09.

As IP multicast groups are 28 bits long (4x8bits minus 4 bits corresponding to "1110"), the IP-Ethernet address mapping cannot be one-to-one. Only the 23 least significant bits of the IP multicast group are placed in the frame. The remaining 5 high-order bits are ignored, resulting in several multicast groups being mapped to the same Ethernet/FDDI address. As a consequence 32 different IP multicast addresses that are only distinguished by the nine most significant bits lead to the same multicast Ethernet address. It means that each time a multicast frame is received, the IP layer will have to decide whether to accept the frame the data-link passed to it.

Multicast Backbone (MBONE) structure: Mbone is a virtual multicast network supported by Internet, a hash of IP tunnels between multicast routers joining multicast-capable local networks (Multicast islands) together. IP datagrams addressed to a multicast group are tunneled between multicast routers, i.e., they are encapsulated into another IP datagram and sent to other appropriate multicast routers as unicast datagrams.

Then Routers in the middle would not have any protocol support problems, as they would be dealing with unicast type traffic. Finally, in the receiving site, traffic would be de-encapsulated and sent to the island in the original multicast format. Two ends converting from multicast to unicast and then again to multicast define what is called a multicast tunnel.

In the Mbone architecture presented above, router A, B and C support multicast, but the unicast router does not.

From the Fig. 2, it is clear that the Mbone is made so that multicast groups with multicast routers between them could communicate directly. It should be remarked also that it is not necessary that the packet sender belongs to the multicast group, i.e., is a member of the multicast group.

IP multicast protocols: After a brief introduction to the multicast technology, it is important to notice how restrictive is its implementation, in spite of its originality. This restriction is a fact of the unavailability of a complete set of functions and the non-flexibility in worldwide applications which currently characterize the IP multicast technology. The most representative arguments are the protocols; specially the routing protocols. In fact the protocols their self may not be compatible if the algorithm on which there are designed are not. Following are presented some algorithms used in the protocols design.

The flooding algorithm: The flooding algorithm is a distributing approach with the following characteristics:

- Each multicast router node acts as both a transmitter and a receiver of a multicast packet.
- Each multicast router tries to forward every message to every one of its network neighbors, except the one it received the packet from.
- Router should forward the same packet only once to a given node. A second reception of the same packet at a node is dropped. To ensure the "first reception" test, the node should remember all the packets received so far, or mark each of them so that each packet contains the list of all routers that it goes through.

- Discharge the network by allowing messages to eventually expire from the system.

The principle of the flooding algorithm[6] can be resumed as following:

Suppose mP is the multicast packet received from the source S on the interface I:

if (Forwarding_Parameters=Enable)

Forward mP to all neighbors' nodes except S;

else

Drop mP;

The forwarding parameters should include the verification of the datagram relative TTL (Time to live).

In IP multicast, the limit value of the packet TTL is called threshold[6]. It defines the areas that the multicast datagram can only cross if its TTL is superior to the threshold. Following are some conventional threshold values:

- 32: defines the "organization boundary",
- 64: defines the "region boundary",
- 128: defines the "continent boundary".

The mean disadvantage of this distribution algorithm is the huge memory and network resource consumption that it engenders.

The flood-and-prune algorithm: This is a variant of the Reverse-Path-Forwarding (RPF) algorithm that enables the pruning of all useless branches that are not on the path of a receiver. This algorithm is consisted of two major sequences: the Flooding and the Pruning. Description of the flood-and-prune distribution tree as follow:

- A source sends a datagram that is addressed to a given IP multicast group on its local network. An immediate attached router receives the packet and sends it to all its outgoing interfaces.
- Each router that receives a packet performs a Reverse-Path-Forwarding check to verify if the incoming interface is the one the router would use as the outgoing interface to reach the source with the shortest possible path. Such an interface is named the router's RPF interface for this multicast packet. That is the verification of shortest reverse path to the source. Thus, only incoming packets received on the relative RPF interface are forwarded on the outgoing interfaces; the others are discarded.
- A leaf router checks group members on its attached subnets by periodically sending IGMP[1] queries (Internet Group Management Protocol). If there is a member existing, the leaf router sends the packet on the subnet. Otherwise, the router will send a "Prune Request" message towards the source, from its reverse-path-forwarding interface to the closest node on the shortest reverse path to the source.
- Thus, "Prune Request" message are forwarded back towards the source; and routers along the way create a "Prune State" for their interfaces on which the prune message is received. That will prevent the router from forwarding relative datagrams on these links. If prune messages are received on all the multicast packet-outgoing interfaces, the router will send a prune message of its own toward the source through the RPF interface. In this way, a reverse shortest path tree in created for this IP multicast group.

The main advantage of the Flood-and-Prune distributing algorithm is to restrict the distribution tree to only the useful nodes and shortest paths. Its best performance occurs when used in a densely populated topology. That makes routers assume that there are group members downstream and so forward packets. Only when an explicit prune message is received the router does not forward multicast datagram. If a group is densely populated, routers are unlikely to ever need to prune!

The main disadvantage is that it requires each router to keep state information for each multicast source, no matter whether that router is on a path to a receiver or not. There is a periodical flooding to discover the connection of new group members. Thus in case there is a new member connected, the router will cancel the "Prune Request" for confirmation. It is clear that if a group is not densely populated, significant state will be stored in the network with less hope of new member connection and a significant amount of bandwidth may be wasted. The principle of the flood-and-prune routing tree is represented as follow:

Let mP be the multicast packet received from a source S on the interface I,

if (Forwarding_Parameters=Enable)

Forward mP to all downstream interfaces without Prune Request;

else

register multicast group info;

send a Prune Request upwards;

The forwarding parameters include to verify whether or not I is on the shortest path to S and also if there exists any downstream node that has not send a "prune request"

Core Based Tree (CBT): For this algorithm[7] a core is first chosen for the multicast group and then the receivers (the last-hop routers) send their subscription request to the core through intermediate routers (if existing). Each intermediate router remembers the node from which this request has been received so that it will be included in the distribution tree. The so created tree, also named Share Tree, is the same for each source that sends message to the same multicast group. The CBT provides a bi-directional routing capability for the derived protocol, but not designed for shortest path[8,9].

This architecture presents the advantage of that there is less memory resource used and the transmission is restricted to only the routers that are on the path to a receiver. However it is to be noticed the high concentration of traffic that is engenders around the core.

The spanning tree: The Minimum Spanning Tree (MST) is also used in the design of some IP multicast routing protocols. In this algorithm, it is selected a subset of the physical links to create an acyclic tree that includes all the nodes and at a minimal cost. In the case the minimum cost condition is not considered, the spanning tree will be simplified to the following:

- Proceed to the selection of a core,
- Keep only the links that are on the shortest path from this core to the other nodes.

This algorithm requires only a little memory because there are some links that are not involved. However the multicast datagram traffic may be highly concentrated at the fixed subset of the physical layers, regardless the spreading of the receivers.

The intra-domain protocols

Distance Vector Multicast Routing Protocol (DVMRP): DVMRP[10] is the original dense mode IP multicast routing protocol based on Distance Vector technology that is used on the Mbone. The latest version of DVMRP is the version 3. It is an implementation of the truncated RPF algorithm and is designed to run over both multicast capable LANs (like Ethernet) as well as through non-multicast capable routers. In this case, the IP multicast packets are "tunneled" through the routers as unicast packets in an encapsulated DVMRP protocol message. This encapsulation requirement is proper to DVMRP-v3 and contributes to enhance the security aspect of data during traffic and facilitate the firewall configuration at the tunnel end-point. This will engender a replication of the packets (multicast packets tunneled into new unicast packets) and then will have an effect on performance, but it could then ensure the inter-connectivity of multicast-capable routers with those that are not.

DVMRP maintains the "multicast routing table" updated by exchanging the distance vector information among routers, like the unicast analog RIP, Routing Information Protocol (in fact, RIP proceeds the routing and forwarding of datagrams to a given destination, whereas the purpose of DVMRP is to keep track of the return paths to the source of multicast datagrams). Each vector entry contains the source and the distance expressed in hops. Theses updates are send to each multicast capable node and each multicast tunnel. This allows a possibility of having a consistent view of a distribution tree that is then created using the flood-and-prune algorithm and the distance database of DVMRP.

After the routing tree created, some packets regularly flood the whole Mbone as far as the TTL makes it possible, in order to update the distribution tree by including new receivers and dropping those who have sent a prune message in the meantime.

Multicast OSPF (MOSPF): MOSPF[11] is the addition of the multicast enhancement to the Open Shortest Path First[12] (OSPF) to provide efficient multicasting within an autonomous system. The enhancements have been added in a backward compatible fashion.

In OSPF, each router periodically sends link-states to all other routers in the network, so that each router builds up a complete network map. With this information each router is able to compute the shortest-path to every destination in the network using the Dijkstra's algorithm[12]. MOSPF extends these link-states to also carry information about multicast group membership. Thus, MOSPF routers basically flood an OSPF area with information about multicast group receivers, i.e. each router advertises the presence of multicast group receivers attached to it. Therefore each MOSPF router can construct a shortest path multicast tree for each source and group. There is no multicast data forwarding while group membership report are flooded through the OSPF area.

The MOSPF is very dependent on the OSPF and its link-state routing paradigm; it can be considered as a dense mode protocol because membership information is broadcasted to each MOSPF router. It can be also considered as an explicit join protocol because data is only sent to the receivers that are specially interested with it, but not in the entire network.

Protocol Independent Multicast (PIM): PIM is an IP routing protocol independent that relies on unicast routing protocols to perform the multicast forwarding function. It uses the unicast routing table to perform the Reverse-Path-Forwarding (RPF) check function instead of building up its own multicast routing table. The protocol independent multicast has been originally split into two

protocols, a dense mode version called PIM-DM and a sparse mode version called PIM-SM. But a new variant of PIM-SM is being designed now: the BIDIR-PIM.

PIM Dense Mode (PIM-DM): PIM-DM[13] is very similar to DVMRP. In PIM Dense Mode (PIM-DM), the PIM router initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. When this process repeats periodically, the routers accumulate their state information by receiving the data stream. These data streams contain the source and group information so that downstream routers can build up their multicast-forwarding table. Since PIM-DM supports only source trees, i.e., (Source, Group) entries, it cannot be used to build a shared distribution tree.

PIM Sparse Mode (PIM-SM): The PIM Sparse Mode as presented in[14] (PIM-SM) is a multicast routing protocol that builds both source and shared trees for the distribution of multicast packets. PIM-SM shared trees are unidirectional in nature and are rooted to special routers called Rendezvous Points (RP). An RP is unique for each multicast group and all routers in the network should be capable to identify the RPs and their correspondent multicast group.

In unidirectional PIM-SM, there are two possible methods for distributing data packets on the shared tree that actually depend on the way packets are forwarded from the source to the RP:

- Initially when a source starts transmitting, its first hop router encapsulates data packets in special control messages (Registers) that are unicast to the RP. After reaching the RP the packets are decapsulated and distributed on the shared tree.
- A transition from the above distribution mode can be made at a later stage. This is achieved by building source specific state on all routers along the path between the source and the RP. This state is then used to natively forward packets from that source.

In PIM Sparse Mode (PIM-SM), only subnets with active receivers that have explicitly requested the data will be forwarded the traffic. So the receivers are expected to send explicit "Join" message. These join messages are then forwarded to the RP by the shortest reverse path.

Each source sends multicast data packets that are then forwarded to the receivers.

There are two differences between PIM-SM and CBT:

- PIM-SM[14] uses unidirectional shared tree while CBT uses a bidirectional one,
- PIM-SM used the reverse shortest path shared tree while CBT uses only a shared tree and is not designed for shortest path tree.

Bi-Directional PIM (BIDIR-PIM): This is a new variant of PIM-SM being in development[15] capable of building bi-directional share trees connecting multicast sources and receivers. This routing protocol builds the bi-directional tree on the base of Designated Forwarders (DF) election mechanism that exists on each link of the multicast topology, except the Rendezvous Point Link (RPL). The concept is original but uses the same format as the PIM-SM.

In BIDIR-PIM, the Rendezvous Point Address (RPA) is an address configured to be used as "the root" of the distribution for a given range of multicast groups. That address (RPA) is a conceptual address that does not need to correspond to an address for an interface on a real router (as in case of PIM-SM), but must be routable from all routers in the PIM domain. In the BIDIR-PIM domain, the RPA belongs however to a particular physical link that is the Rendezvous Point Link (RPL).

Join messages send by the multicast group members of a BIDIR-PIM domain will be forwarded hop-by-hop to the RPA. A single DF exists for each RPA on every link within a BIDIR-PIM domain. This DF will correspond to the router that has the best route to the corresponding RPA from the link. Its role is to ensure forwarding downstream traffic onto its link and forwarding upstream traffic from its link towards the RPL. It does this for all the bi-directional groups that map to the RPA. It's also responsible of processing Join messages from downstream routers on the link as well as ensuring that packets are forwarded to local receivers.

Inter-domain multicast: Inter-domain multicast has been developed from the need to provide scalable, hierarchical and worldwide multicast. The protocols to be used to achieve the inter-domain multicast have always been the key problem. In fact, the routing algorithms of the different protocols present a very clear divergence in principle that makes the problem more complicated.

Multicast Source Discovery Protocol (MSDP) and the Multiprotocol BGP (MBGP): The operation of the unidirectional PIM-SM is difficult in the inter-domain level because routers are not all multicast capable. Since PIM-SM relies on the unicast routing protocol to construct multicast trees, join messages may reach non-multicast routers, complicating PIM's job. The use of PIM-SM in the inter-domain level still has two problems:

- Designing a scalable mechanism for mapping multicast groups to RPs,
- ISPs do not desire to depend on other ISPs' facilities, because the RP location for some ISPs will not be acceptable by other ISP in many cases.

The short-term solution to these problems resides in the use of combination of Multiprotocol Extensions for BGP-4 (MBGP[6]), PIM-SM and the Multicast Source Discovery Protocol[16] (MSDP[17]).

MBGP allows multiple routing tables to be maintained for different protocols. This way, routers may construct one routing table with unicast-capable routes and another with multicast-capable routes. PIM can then send join messages detouring non-multicast routes.

MSDP provides a solution to the ISP interdependence problem. ISPs run PIM-SM within their own domain with their own set of RPs. RPs within the same domain are interconnected and are connected to RPs in other domains using MSDP to form a loose mesh. MSDP sets up a group-shared tree within each domain. When a source in a specific domain starts sending, the RP in this domain sends a Source Active message to RPs in other domains. Joining members in others domains send source-specific join messages following the MBGP routes in the inter-domain level. This solution solves PIM-SM problem in only the near-term because every RP in every domain must be told about every source, so MSDP does not scale with the number of senders.

Border Gateway Multicast Protocol (BGMP): BGMP[18] is a scalable multicast routing protocol that responds to the internet-wide need of multicast technology. Like CBT and PIM Sparse Mode, BGMP chooses a global root for a delivery tree. But unlike those routing trees where the meeting point is a single router, the root of the BGMP is a domain. That is to strengthen the multicast routing system so that if there is any path available to the domain, connectivity could be maintained.

BGMP is an inter-domain protocol in that it adopts particular design features of BGP familiar to providers. Two of these features follow: it uses TCP connections for the transfer of routing information and it has a state machine (with error notifications) similar to BGP.

BGMP can build three types of multicast trees: Both unidirectional source and shared trees and bidirectional shared trees. This has the advantage to accommodate different applications and backward compatibility.

The root of the shared trees of this protocol is an Autonomous System that is associated with the multicast group address of the tree. Having the root of the tree at the Autonomous System that is associated with the address is logical because there are likely members in that domain. Rooting the trees at an Autonomous System level also provides stability and inherent fault tolerance. To clearly establish the mapping of autonomous system with multicast addresses, BGMP disposes of two means: The Multicast Address-Set Claim (MASC)[19] and the Globally Assignable Multicast Addresses (GLOP).

The MASC protocol supports address allocation between domains. It includes mechanism to insure that address collisions are immediately removed. It allocates temporary assignments from the IPv4 group D address space; it then distributes these assignments into Multiprotocol BGP (MBGP) so that BGMP will know which Autonomous System is associated with which group and, therefore, where to send join messages.

If Globally Assignable Addresses are available, then BGMP can use any static address architecture for obtaining an Autonomous System from a multicast group address.

The combination of BGMP and a large multicast address space (for example, IPv6 address space) provide the best scaling for all types of multicast applications.

Multicast reliability: We have surveyed the routing aspect of the IP multicast, i.e. how to send information to group members in a flexible and dynamic way. Actually this is only a little aspect of the service problem. The possibility to furnish a reliable transmission is as well commonly required.

Two major tasks are required for a reliable transmission service: The Error Detection and the Error Recovery[20,8].

Following, we give a brief description of three different types of loss recovery mechanisms used for providing a reliable multicast: The ACKs, NACKs and FEC.

- If using positive acknowledgement (ACKs), the sender transmits messages until ACKs from all destinations are received. Undoubtedly, this approach does not scale well because the flux of ACKs for each packet received will lead to serious network congestion (ACK implosion). In addition the source has to know the exact composition of the multicast group to be able to achieve this. Thus this approach seems not to work well with multicast.
- When using negative acknowledgments (NACKs), receivers transmit negative acknowledgment only when a packet loss is detected. In order to reduce the implosion problem different NACK suppression mechanisms could be applied.

- The Forward Error Correction (FEC)-based reliability solution consists in sending redundant packets (called parity packets) together with regular data packets. This approach reduces the end-to-end latency compared to the NACK approach because the receiver does not have to wait for the retransmission of lost packets any more. However, this will affect the available bandwidth since additional packets are sent systematically.
- Hybrid combinations of the FEC and the NACK approaches may lead to better solutions.

IP multicast monitoring: One recent tool that has been developed to facilitate multicast monitoring and debugging is the Multicast Reachability Monitor (MRM)[8,21]. MRM consists of two parts; a MRM management station configures test senders and test receivers in multicast networks. A multicast test sender or test receiver is any server or router that supports the MRM protocol and can source or sink multicast traffic. MRM provides the ability to dynamically test particular multicast scenarios; this capability can be used for fault isolation and general monitoring of sessions.

MRM is typically used to configure MRM-capable routers as test senders and test receivers from a management station. Routers configured as test senders send multicast packets periodically to a configured multicast group at a configured rate. Routers configured as test receivers monitor traffic to a group and keep statistics that can be reported back via RTP Control Protocol (RTCP) packets. Test receivers can be configured to send RTCP reports when a given condition has been reached or when polled by a management station. Although the MRM protocol is simple itself, it provides powerful capabilities that can be used by future multicast debugging applications.

Security concerns in IP multicast: Multicast security is more difficult than unicast security in several areas. There are some special problems with the secure multicast that won't arise with unicast and many security aspects that are not apparent in unicast are clear and should be resolved in IP multicast. Actually the security requirement and security level of an IP multicast session is relative to the application that is implemented. Generally, private session may require higher-level security than public session. The present section will give an overview on the general security goals in IP multicast[20].

- Confidentiality: Confidentiality requires that no non-trusted third parties can access the messages. Usually, confidentiality is achieved by encrypting the messages. If a symmetric cipher is used, all parties in the multicast transmission should know the shared key, including the members of the multicast group and all the senders. If an asymmetric cipher is used, the public keys of all the sending parties should be distributed to all the receiving parties and vice versa.
- Integrity or Data Authentication: Integrity requires that the messages cannot be altered during the transit without detection. Integrity can be achieved by using an encrypted checksum or a keyed hash function.
- Group Authentication: Authentication requires ensuring that the received message was actually sent by the claimed sender. Authentication in the multicast (unlike in the unicast) can be achieved with digital signatures. That is because when a system like MD5 or encrypted checksum is used, all the participants have to know the shared secret or key. It is impossible to make a difference between parties knowing the key.
- Access control: Access control must ensure that only proper parties can access resources, e.g. join into a multicast group. Access control can be achieved by using access control lists for key distribution or digital signatures. E.g., only parties whose signatures are accepted can join the multicast group or send data to the group. Without the proper access control it is extremely easy to eavesdrop multicast sessions. Multicast routing or key distribution mechanisms should support access control. For many applications, group membership is likely to vary over time. It is often required that members leaving a group lose access to future group communication and that members joining a group do not gain access to group communication that occurred before they joined.
- Non-repudiation: Non-repudiation[20] requires that the recipient can prove that the sender did send the message even if the sender denies sending it. Non-repudiation may require the use of a public key cryptosystem and digital signatures. Each message should be signed with the private key of the sender.
- Anonymity: This is a somewhat contradictory requirement with the Non-repudiation. It concern is keeping the identity of group members secret from outsiders or from other group members. The main purpose of the Anonymity is the protection from traffic analysis[22].

Base on the above requirements for securing an IP multicast session, it is obvious that the key management applicable to the group will be more complex. Since in the multicast communication the group membership is not static, there is a frequent need of re-keying[23].

Also, since the IP multicast communication is a sender-oriented communication (view from receiver), in the same group there should be a traffic protection between mutual untrusty members. Therefore, the data security issue should take in consideration intruders attacks from both inside and outside the group.

Because of the wide range of one-to-many multicast applications and the sometimes-conflicting requirements these applications exhibit, it is believed that a single protocol will be unable to meet the requirements of all applications. To resolve this problem, the notion of building blocks has been introduced. Building block can be instantiated by one or more protocols that will be interchangeable. The Reference Framework will not only describe one-to-many multicast, but also many-to-many multicast. An application may use different blocks together to create a protocol that meets its specific requirements.

The blocks being developed include data security transforms, group key management and group security association and group policy management.

Data security building block: This is to come up to the confidentiality and authentication services requirements for data being transported between group members. The main difficulty is about Authentication, because the algorithms used in IP multicast protocols should allow a group member "R" to authenticate data as being sent from a specific member "S" of the group but without being able to reproduce authentic message. This is to avoid an untrusted receiver to impersonate the sender and forge message to others receivers. Thus the secret used to authenticate the traffic must be shared between all sending and receiving parties, but any receiver cannot generate the signature for a message with its public secret key alone[24].

The standard approach to achieve such asymmetry for authentication is to use asymmetric cryptography, for instance a digital signature. The Timed Efficient Stream Loss-tolerant Authentication Protocol (TESLA)[24] is one of the building blocks designed for this purpose. It uses time for asymmetry.

TESLA is designed so that it retains the efficiency benefits of symmetric algorithms. It does not rely on any network propagation delay. A senders running TESLA use a hash chain of keys K_0, K_1, $K_2 \ldots K_n$, so that $K_i = F^{n-i}(K_n)$, $i<n$, to sign data. The function F is a one-way function (irreversible function) constructed by the sender based on a pseudo-random function (PRF)[24]. After each data is sent, the source releases its key in the chain a short interval later. If keys are lost during transmission, receivers can recomputed any key earlier in the sequence simply by repeatedly applying the hash function used to any later key received.

Group key management issues for multicast: The Key Management for multicast requires quite a lot more traffic compared to the key management for unicast. In applying a keying solution for secure multicast applications, it is very important to maintain protocol features that preserve multicast efficiency and scale well for one-to-many and many-to-many multicast sessions.

First, the common group key should be distributed to each group member and all the senders. If the traffic should also be authenticated, senders have to distribute their authentication key to all of the group members.

The concept of a group owner may provide simple solution to the problem of key management in a multicast group. Members send the join and leave requests to the group owner, which generates and distributes the needed keys.

The Multicast Group Key Management Architecture is being worked up by the multicast security (msec) workgroup of IETF and the general requirements are presented in the Internet draft[25].

The Group Key Management architecture as described in[25] provides a unified model for key management blocks[25]. A central Group Controller/Key Server (GCKS) provides Traffic Encrypting Keys (TEKs) or Key Encrypting Keys (KEKs) to new group members after authenticating them with a unicast protocol. This architecture permits all keys to be obtained by the unicast registration protocol[25]. The GCKS may also delegate some of its functions to other entities, improving scalability.

Three key registration-building blocks are being developed:

- The Group Domain of Interpretation (GDOI) that takes advantage on the Internet Security Association Key Management Protocol (ISAKMP)[26] to allow the creation and management of security associations for IPsec and other network or application layer protocols.
- Multimedia Internet Keying (MIKEY)[27] is targeted at real-time multimedia communications, particularly those using the Secure Real-time Transport Protocol (RTP) and can be tunneled over the Session Initiation Protocol (SIP).
- A Group Secure Association Key Management Protocol (GSAKMP)[28] along with a GSAKMP-Light profile, has also been developed[8].

Multicast group policy: The group policy[25] defines policies such as which roles various entities may play in the group; who may hold group information such as cryptographic keys; the cryptographic algorithms used to protect group data; and proof that the creator of a given policy is authorized to do so.

DISCUSSION

In the present publication we have made an overview of the IP multicast technology and presented the progressive work being deployed to enforce the worldwide secure implementation of that technology. But actually, a remark is made that the IPsec implementation to a secure multicast is not very developed. Obviously, the implementation of IPsec in the unicast security has shown remarkable results. The second part of our research will focus on the IPsec implementation in IP multicast communication. Thus, three critical points have to be discussed:

- How may the IP Security Architecture Support Multicast?
- What are the IPsec implementations in multicast today?
- What perspective for an IPsec-based secure multicast?

REFERENCES

1. Deering, S., 1989. Host Extensions for IP Multicasting. Network Working Group, RFC1112.
2. Anonymous, 2004. Internet Multicast Addresses. www.iana.org/assignments/multicast-addresses.
3. Meyer, D., 1998. Administratively Scoped IP Multicast. Network Working Group, RFC2365.
4. Hinden, R., Nokia and S. Deering, 1998. IP Version 6 Addressing Architecture. Network Working Group, RFC2373.
5. Anonymous, 2003. Internet Protocol version 6 Multicast Addresses. www.iana.org/ assignments/ipv6-multicast-addresses.
6. Vincent, R., L. Costa, R. Vida, A. Dracinschi and S. Fdida, 2000. A Survey of Multicast Technologies. Université Pierre et Marie Curie (Paris 6).
7. Cain, B., A. Ballardie and Z. Zhang, 2003. Core Based Trees (CBT version 3) Multicast Routing, Protocol Specification. Inter-Domain Multicast routing, Internet Draft, <draft-ietf-idmr-cbt-spec-v3-01.txt>.
8. Brown, I., J. Crowcroft, M. Handley and B. Cain, 2002. Internet Multicast Tomorrow. The Internet Protocol Journal.
9. Koh, S.J. and S.G. Kang, 2001. Enhancement of the CBT Multicast Routing Protocol. ICPADS., pp: 209-213.
10. Pusateri, T., 2003. Distance Vector Multicast Routing Protocol. Inter-Domain Multicast Routing, Internet Draft, <draft-ietf-idmr-dvmrp-v3-11.txt>.
11. Ranjitkar, P.G., I.M. Suliman, P. Geil, M. Kuipers and R. Prasad, 2000. IP Multicast Implementation Based on the Multicast Extensions to OSPF Protocol. IEEE, ICPWC.
12. Moy, J., 1997. OSPF Version 2. IETF, RFC2178, http://www.ietf.org/rfc/rfc2178.txt.
13. Adam, A., J. Nicholas and W. Siadak, 2003. Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification (Revised). IETF, Internet Draft, < draft-ietf-pim-dm-new-v2-04.txt >.
14. Fenner, B., M. Handley, H. Holbrook and I. Kouvelas, 2003. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised). IETF, Internet Draft, < draft-ietf-pim-sm-v2-new -08.txt >.
15. Handley, M., I. Kouvelas, T. Speakman and L. Vicisano, 2003. Bi-directional Protocol Independent Multicast (BIDIR-PIM). IETF, Internet Draft, < draft-ietf-pim-bidir-05.txt >.
16. Almeroth, K.C., 2000. The Evolution of Multicast: From the Mbone to Inter-Domain Multicast to Internet2 Deployment. IEEE Network.
17. McBride, M., J. Meylor and D. Meyer, 2003. Multicast Source Discovery Protocol (MSDP) Deployment Scenarios. IETF, Internet Draft, < draft-ietf-mboned-msdp-deploy-04.txt>.
18. Thaler, D., 2003. Border Gateway Multicast Protocol (BGMP): Protocol Specification. IETF, Internet Draft <draft-ietf-bgmp-spec-05.txt>.
19. Radoslavov, P., D. Estrin, R. Govindan, M. Handley, S. Kumar and D. Thaler, 2000. The Multicast Address-Set Claim (MASC) Protocol. Network Working Group, RFC2909.
20. Pekka, P., 1995. Secure Multicast. Department of Computer Science, Helsinki University of Technology.
21. Sarac, K. and K.C. Almeroth, 2000. Supporting Multicast Deployment Efforts: A Survey of Tools for Multicast Monitoring. Department of Computer Science, University of California.
22. Canetti, R., J. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas, 1999. Multicast Security: A taxonomy and Some Efficient Constructions. IEEE, INFOCOM., 2: 708-716.
23. Setia, S., S. Koussih and S. Jajodia, 2000. Kronos: A scalable Group Re-Keying Approach for Secure Multicast. IEEE, Symposium of Security and Privacy.

24. Perrig, A., R. Canetti, B. Briscoe, D. Tygar and D. Song, 2002. TESLA: Multicast Source Authentication Transform. IETF Internet Draft, <draft-ietf-msec-tesla-intro-01.txt>.
25. Baugher, M., R. Canetti, L. Dondeti and F. Lindholm, 2003. MSEC Group Key Management Architecture. IETF, Internet Draft, <draft-ietf-msec-gkmarch-06.txt>.
26. Maughan, D., M. Schertler, M. Schneider and J. Turner, 1998. Internet Security Association and Key Management Protocol (ISAKMP). IETF, RFC2408.
27. J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman and Ericsson, 2003. MIKEY: Multimedia Internet KEYing. IETF, Internet Draft, <draft-ietf-msec-mikey-08.txt>.
28. Harvey, H., U. Meth, A. Colegrove, A. Schuett, P. McDaniel, G. Kenny, H. Cruickshank, S. Iyengar and G. Gross, 2003. GSAKMP. IETF, Internet Draft, <draft-ietf-msec-gsakmp-sec-04.txt>.