Distributed Conditional Multicast Access for IP TV in High-Speed Wireless Networks (Destination Specific Multicast)

[1, 2] Jan Fesl, [1] Richard Klee , [1] Marie Dolezalova

[1] Institute of Applied Informatics , Faculty of Science, Univers of South Bohemia
Ceske Budejovice, Branisovska 31, 37001, Czech Republic

[2] Department of Computer Science, Faculty of Electrical Engineering, Czech Technical University
Prague, Karlovo namesti 13, 12135, Czech Republic

Abstract - IP TV has become very popular discipline in last years. Many internet service providers provide their own dedicated IP TV solutions. Common situation is that some TV channels are provided as free and some as paid service. In the past IP TV was mostly provided through optical fiber networks, but now, there is an ever increasing demand by more and more customers to have IP TV over wireless links. In practice most multicast solutions are based on Protocol Independent Multicast (PIM) sparse mode mechanism. PIM does not contain mechanism for the determination between free and paid service. Solutions for wireless networks should focus on using minimal needed line capacity. We propose PIM-SM based distributed conditional access mechanism for paid IP TV service suitable for present commercial metropolitan wireless networks mostly based on IEEE 802.11 a/b/g/n/ac standards.

Keywords- *Multicast, PIM, sparse-mode, conditional access, IP-TV*

1. Current common IP-TV Solutions

1.1. IP TV network

Typical IP TV solution consists of an IP TV streaming server and a routed IP network. The Signal for IP TV streaming server is provided by terrestrial or satellite broadcasting. The broadcasting is mostly encoded into other video format (typically mpeg4/h264) for the minimization of needed traffic flow. So far some proprietary solutions for paid services based on data flow encryption [2][4] have been proposed, but it is very complicated to implement such a solution into a common home network infrastructure. Types of IP TV broadcasting are based on unicast or multicast solutions. Each solution has its advantages. Unicast solution is better traversal for network address translation (nat), but requires more backbone capacity in comparison to the multicast solution. Standard dynamic unicast routing mechanism such as ospf, rip or i-bgp is a common component of every modern computer network. Multicast flow is today typically received by laptops, smart-phones or intelligent home tv devices.

1.2. IP TV Multicast Network

The picture below shows the multicast advantage. Only one packet flow is needed for multiple receivers in the same broadcasting direction, which is very useful for wireless networks (capacity of links is very limited compared to optical networks). It's important to say, that wireless network must save line capacity and it means, that connecting to a multicast tree is advantageous only, when a broadcasting subscriber exists. PIM sparse mode mechanism is valid for this situation, because the multicast traffic tree is periodically modified or pruned and traffic passes through the network backbone only at the time, when a multicast subscriber (receiver) exists.

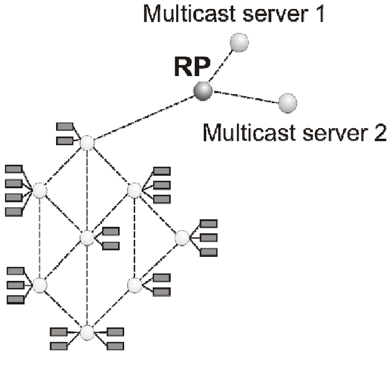

Fig. 1 – IPTV network topology
(servers, RP, backbone nodes and receivers)

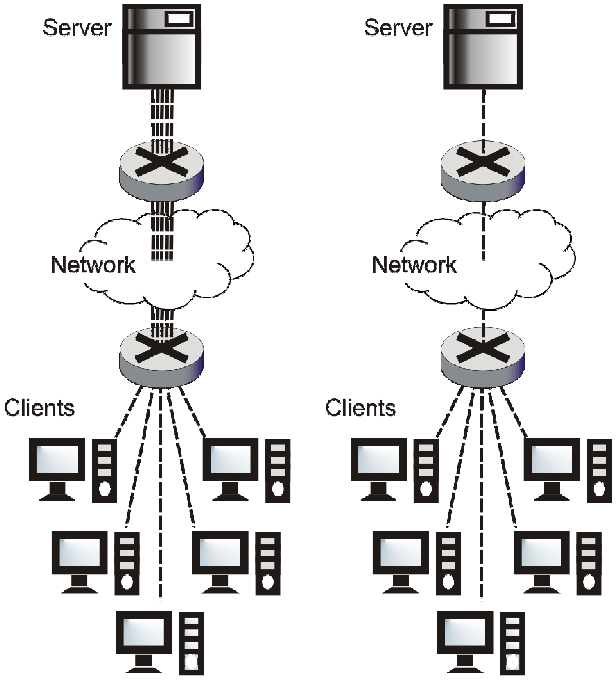

Fig. 2 – Unicast vs. multicast solution comparison

2. PIM Sparse Mode Description

Protocol independent multicast [1] is a multicast routing protocol, which provides creation of distribution trees for multicast flow. For wireless networks based on radio links, the best solution is based on the sparse mode, because bandwidth for IP TV traffic flow should be reserved only for real time, when it's used.

There are two solutions for multicast source implemented in PIM. First is called ASM (any source multicast), that means – the receiver joins a multicast group through any node in a multicast group. SSM (source specific multicast) means that the receiver joins only to multicast group with a specific multicast source. PIM-SM consists of three main parts, discussed in the next section.

2.1. Joining to Multicast Group

In phase one, a multicast receiver expresses its interest in receiving traffic destined for a multicast group. Typically it does this using one of the receiver's local PIM routers, which is elected as the Designated Router (DR) for that subnet. Upon receiving the receiver's expression of interest, the DR then sends a PIM Join message towards the Rendezvous Point (RP) for that multicast group. The RP is a PIM-SM router that has been configured to serve in a bootstrapping role for certain multicast groups. This Join message is known as a (*,G) Join because it joins group G for all the sources to that group. The (*,G) Join travels hop-by-hop towards the RP for the group, and in each router it passes through, multicast tree state for group G is instantiated. Eventually the (*,G) Join either reaches the RP, or reaches a router that already has a (*,G) Join state for that group. When many receivers join the group, their Join messages converge on the RP, and form a distribution tree for group G that is rooted at the RP. This is known as the RP Tree (RPT), and is also known as the shared tree because it is shared by all sources transmitting to that group. Join messages are resent periodically as long as the receiver remains in the group. When all receivers on a leaf-network leave the group, the DR will send a PIM (*,G) Prune message towards the RP for that multicast group. However if the Prune message is not sent for any reason, the state will eventually time out.

A multicast data sender just starts sending data destined for a multicast group. The sender's local router (DR) takes those data packets, unicast-encapsulates them, and sends them directly to the RP. The RP receives these encapsulated data packets, decapsulates them, and forwards them onto the shared tree. The packets then follow the (*,G) multicast tree state in the routers on the RP Tree, being replicated wherever the RP Tree branches, and eventually reaching all the receivers for that multicast group. The process of encapsulating data packets to the RP is called registering, and the encapsulation packets are known as PIM Register packets. At the end of phase one, multicast traffic is flowing encapsulated to the RP, and then natively through the RP tree to the multicast receivers.

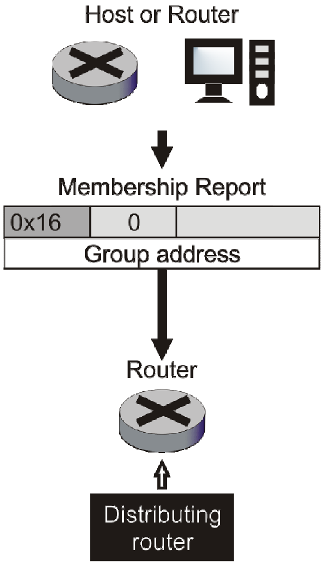

Fig. 3 – IGMP join (message format)

Joining to specific to multicast group is realized by sending IGMP Membership Report message. On network layer (IP protocol) is this operation realized by sending ip packet to network destination address 224.0.0.2 (all routers), source address is original IP address of IGMP Membership Report message sender.

2.2. Register-Stop

Although Register-encapsulation may continue indefinitely, for the reasons above, the RP will normally choose to switch to native forwarding. To do this, when the RP receives a register-encapsulated data packet from source S on group G, it will normally initiate an (S, G) source-specific Join towards S. This Join message travels hop-by-hop towards S, instantiating (S, G) multicast tree state in the routers along the path. (S, G) multicast tree state is used only to forward packets for group G if those packets come from source S. Eventually the Join message reaches S's subnet or a router that already has (S, G) multicast tree state, and then packets from S start to flow following the (S, G) tree state towards the RP. These data packets may also reach routers with (*, G) state along the path towards the RP - if so, they can short-cut onto the RP tree at this point.

While the RP is in the process of joining the source-specific tree for S, the data packets will continue being encapsulated to the RP. When packets from S also start to arrive natively at the RP, the RP will be receiving two copies of each of these packets. At this point, the RP starts to discard the encapsulated copy of these packets, and it sends a Register-Stop message back to S's DR to prevent the DR unnecessarily encapsulating the packets.

At the end of phase 2, traffic will be flowing natively from S along a source-specific tree to the RP, and from there along the shared tree to the receivers. Where the two trees intersect, traffic may transfer from the source-specific tree to the RP tree, and so avoid taking a long detour via the RP. It should be noted that a sender may start sending before or after a receiver joins the group, and thus phase two may happen before the shared tree to the receiver is built.

2.3. Shortest-Path Tree optimization

Although having the RP join back towards the source removes the encapsulation overhead, it does not completely optimize the forwarding paths. For many receivers the route via the RP may involve a significant detour when compared with the shortest path from the source to the receiver. To obtain lower latencies, a router on the receiver's LAN, typically the DR may optionally initiate a transfer from the shared tree to a source-specific shortest-path tree (SPT). To do this, it issues an (S, G) Join towards S. This instantiates state in the routers along the path to S. Eventually this join either reaches S's subnet, or reaches a router that already has (S, G) state. When this happens, data packets from S start to flow following the (S, G) state until they reach the receiver.

At this point the receiver (or a router upstream of the receiver) will be receiving two copies of the data - one from the SPT and one from the RPT. When the first traffic starts to arrive from the SPT, the DR or upstream router starts to drop the packets for G from S that arrive via the RP tree. In addition, it sends an (S, G) Prune message towards the RP. This is known as an (S, G, rpt) Prune. The Prune message travels hop-by-hop, instantiating state along the path towards the RP indicating that traffic from S for G should NOT be forwarded in this direction. The prune is propagated until it reaches the RP or a router that still needs the traffic from S for other receivers. By now, the receiver will be receiving traffic from S along the shortest-path tree between the receiver and S. In addition, the RP is receiving the traffic from S, but this traffic is no longer reaching the receiver along the RP tree. As far as the receiver is concerned, this is the final distribution tree.

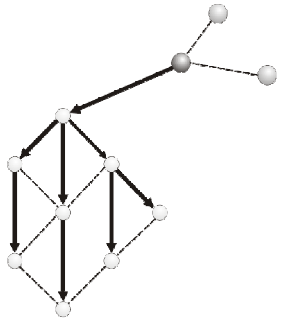

Fig. 4 – Multicast distribution tree creation

3. Distributed Conditional Multicast Access

Central direction point of PIM-SM mechanism is the RP. The RP contains detailed information about connected routers, which form the distribution tree backbone.

A typical situation can arise, when receivers (with known IPs) want to join a multicast group but only some receivers are allowed to join, which the current PIM mechanism does not support.

The RP is a point of the network, which is typically situated in the root of the distribution tree and is very suitable for maintaining access control list (ACL). ACL contains the following information. There is a list of unicast IPs, which are allowed to receive multicast traffic of this group, for every unique multicast group (typically multicast address of one IP TV channel).

ACL is list of pairs <*unicast ip prefix of valid receiver, specific multicast group*>

Because only some nodes (receivers) are allowed to receive traffic determined for specific multicast group, this multicast type is called **destination specific multicast**. Central authorizations for every valid receiver are realized remotely on the RP node. The RP node has knowledge of all the trusted receivers of whole network.

3.1. Specific Multicast Groups

Specific multicast group SMG is defined as couple of multicast address type ip prefix and name, which usually represent paid tv channel (which is more acceptable to humans). Only authorized receivers are able to receive traffic valid for this group.

SMG <multicast address type ip prefix, group name>

3.2. Cooperation between Unicast and Multicast Routing Algorithm

There are two separated “address worlds”, which create the distributed system for multicast iptv. Unicast and multicast address types have their own routing mechanism and it is suitable to combine information from both of them. Most modern internet service providers have implemented some type of dynamic routing mechanism such as OSPF, RIP or BGP and needed information can be derived from the local routing tables.

Unicast routing mechanism knows the closest forwarding nodes (mostly their gateways) to multicast receivers, which are defined by a specific unicast address. Multicast routing mechanism knows the path from a specific multicast source to all the receivers. Cooperation of routing algorithms is important for destination specific multicast mechanism.

3.3. Destination specific multicast

The RP maintains information about permitted receivers of specific multicast groups. Solution for wireless (or low speed) networks should respect the following fact, which is that multicast join for an unauthorized receiver should be dropped at the nearest multicast router to this receiver. But only the RP has at first the valid information, which receivers (nodes) are allowed to receive the multicast traffic.

A solution could be based on the following idea. After the creation of PIM shortest path tree, the next phase, in which will be delivered information about specific multicast groups (paid tv channels) via Specified Multicast Group Message (SMGM) from RP to all PIM routers. This information is the same for all PIM routers and after receiving this message all the routers will set the default dropping of igmp joins for this groups. This operation is easy to implement via broadcasting to all PIM routers, similar to implementing OSPF routing algorithm. It is necessary to set expiration time of incoming SMGM message at the node.

SMGM <list of all specific multicast groups>

The next phase, after sending specific multicast groups, is sending information to concrete PIM routers, which serve as getaways for multicast receivers. Destination Specific Multicast Message (DSMM) is a message, which contains information about trusted receivers for specific multicast group. It is necessary to set expiration time of incoming DSMM message for the router. The DSMM message contains an id (generated by the RP), what guarantees freshness of the message. DSMM messages are periodically resend from the RP.

DSMM <specific multicast group, list of all ip prefixes able to receive traffic>

3.4. Specific multicast groups message delivery

SMGM sending is initiated by the RP. The RP sends SMGM to all the PIM nodes, which are directly interconnected with the RP. Routers store this information and send it to all of their neighbors except to the one from which the original SMGM came from. All routers store ids of the last SMGM messages. If a message with a smaller or the same id as has been stored comes, it is rejected. This is done periodically until all the routers have this information.

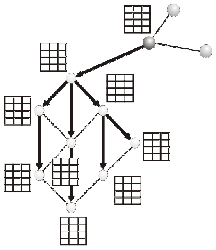

Fig. 5 – Specific multicast groups delivering to all nodes in network

3.5. Destination Specific Multicast Message Delivery

Algorithm uses information from unicast routing mechanism.

1. RP sends parallel DSMMs to all the neighbors of all multicast groups. Sending is done as follows. One DSMM is divided into as many DSMMs, as there are different outgoing interfaces on the router. Specific DSMM is sent via specific interface and contains only unicast ip prefixes, which are reachable via this interface. This step radically lowers the size of the transmitted messages.

2. The routers compare their local IP ranges with ip prefixes from the DSMM. If the ip prefixes match the local ranges are excluded from the DSMM, and set as allowed for igmp connection to the current router into local ACL.

3. After exclusion of ip ranges from the DSMM, the rest of the DSMM is again divided into subsequent DSMM and transmitted the same way as in step 1.

4. The operation terminates in the case that there are no more address prefixes for the DSMM delivery (empty) or there is no route to reach a specific destination prefix.

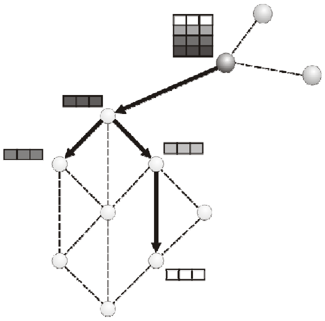

Fig. 6 – DSMM delivering to destination nodes

3.6. Application of SMGM and DSMM Messages

After receiving a SMGM, multicast routers obtain information about multicast specific groups. After receiving the DSMM list, the specific router knows, which ip prefixes from a local range are allowed to receive specific multicast traffic. Routers, through receiving the igmp message, only compare ip of the source and ip of the multicast group to local ACL, and allow or reject the join message.

Advantages of this solution

This solution respects low speed capacity of wireless networks and it can be easily implemented for all versions of the IGMP protocol. A certain amount of traffic is necessary for SMGM & DSMM message delivery, but in comparison to multicast flow it is negligible.

4. Conclusion

PIM-SM is a very useful and widely used mechanism for spreading multicast flow in computer networks. Our destination specific multicast solution utilizes all the advantages of the PIM protocol efficiency and adds the possibility to create conditional access for some subscribers. The main advantage of this solution is compatibility with all common devices, which are able to receive multicast traffic via sending igm join connect message. Required message flow for igmp message control is lowered thanks to DSMM message sending policy. Our solution is suitable to use in modern wireless networks because it is fast and fully compatible with the current standard. Security of this solution depends on what type of multicast user authentication mechanism is used. Self PIM protocol message communication is available only between backbone nodes.

References

[1] RFC4601, PIM protocol specification, available online, http://www.ietf.org/rfc/rfc4601.txt.

[2] Sysmaster ltd., IP TV broadcaster, http://www.sysmaster.com/products/iptv_broadcaster.php, available online.

[3] Jessica H. Fong, available online, http://web.eecs.umich.edu/~martinjs/papers/fgks_journal.pdf.

[4] Panaccess ltd. , IPTV CAS Solution , available online, http://www.panaccess.com/doc/sl_pr_iptv_en.pdf.

Jan Fesl was born in Ceske Budejovice, Czech Republic in 1982. His M.Sc. Diploma received in Computer Science in 2007 at the Czech Technical University of Prague, Czech Republic. Currently, he is an assistant professor at the University of South Bohemia and he is a Ph.D. student at the Czech Technical University of Prague. His current research is focused on computer networks and distributed computing.

Richard Klee works as an assistant professor at the University of South Bohemia, his areas of research are VLSI and embedded computer systems.