SECOND QUARTER 2005, VOLUME 7, NO. 2

IEEE COMMUNICATIONS SURVEYS
The Electronic Magazine of Original Peer-Reviewed Survey Articles

www.comsoc.org/pubs/surveys

MULTICAST RECEIVER AND SENDER ACCESS CONTROL AND ITS APPLICABILITY TO MOBILE IP ENVIRONMENTS: A SURVEY

MOUNIR KELLIL, IMED ROMDHANI, AND HONG-YON LACH, MOTOROLA LABS — PARIS, FRANCE
ABDELMADJID BOUABDALLAH AND HATEM BETTAHAR, HEUDIASYC

ABSTRACT

Ensuring secure access control to multicast delivery trees is a challenging issue that is still largely open. Moreover, the impact of host mobility on the access control to the delivery tree has not been investigated. In this article we address the receiver and sender access control problems to the delivery tree and extend the interest to the mobile IP environment by taking into account its particular issues and requirements. To achieve this, we review the existing approaches by classifying them into three classes: *digital signature-based* solutions, *shared secret-based* solutions, and *hybrid* solutions. We also investigate their efficiency and limitations with respect to the specified requirements both in stationary and mobile cases. Our study shows that four main problems arise among the existing approaches. First, few approaches addressed the sender access control problem. Second, both the digital signature- based solutions and hybrid solutions are vulnerable to DoS attacks. Third, the existing solutions do not provide an efficient user exclusion mechanism. Fourth, the defined access control mechanisms result in a number of problems in mobile IP environments.

With the increasing number of multicast applications such as multimedia conferences, video games, and military communications, and the evolving need for multicasting, the Internet community is facing new problems that are slowing down the deployment of IP Multicast. The lack of the appropriate security solution is one of the main factors preventing a broader deployment of multicast technology over the Internet.

Securing IP Multicast has not been addressed while the IP multicast model was being specified. The underlying goal of the Internet Engineering Task Force (IETF) was to provide an open IP Multicast model. This model provides public multicast addresses while keeping the receivers anonymous for their sources as well as the multicast routers. In fact, the subnet multicast router does not maintain host's identity after processing its membership request and does not transmit such an identity upstream in the delivery tree. Furthermore, any host can request traffic from or send traffic to any multicast group. Such options simplify the management of multicast groups and enable IP multicast scaling to large groups. However, this is achieved at the expense of introducing an important security hole in the multicast infrastructure. This security hole is due to the lack of receiver and sender access control mechanisms to the delivery tree. This is one of the main concerns of network corporations and network service operators for which the interest in multicasting is increasing, but the lack of efficient control of multicast traffic transmission to/from their own networks is discouraging their interest [1].

The receiver and sender access control problems have been addressed as part of the multicast security problem [2]. In fact, two main security schemes are emerging: *end-to-end data security* and *multicast infrastructure security*. The end-to-end data security scheme ensures the protection of the multicast traffic content, i.e., *data confidentiality*, *source authentication*, and *data integrity*. The multicast infrastructure security scheme encloses the sender and receiver access control to the delivery tree. Concretely, the multicast infrastructure security service protects the multicast distribution tree. This consists in preventing malicious hosts from impersonating multicast routers, joining illegitimately particular multicast groups, or sending bogus traffic to multicast groups (i.e., extra traffic and Denial of Service (DoS) attacks[1]). Those three problems affect both parts of the multicast infrastructure, namely the *core* and the

[1] *DoS attacks consist in sending bogus traffic against networks to generate traffic overheads, and toward network devices (e.g., a router) to overflow their memory and overload their CPU by processing many useless packets.*

edge [3] (Fig. 1). The core is composed of multicast routers and multicast routing protocols that are used to build and maintain the delivery tree. The edge includes the edge multicast routers, hosts, and Group Membership Management protocols. These protocols operate between hosts and edge multicast routers to maintain the group membership information.

Attacking the core consists in altering the construction of the delivery tree by impersonating multicast routers using fake multicast routing control messages. To overcome this problem, it is enough to secure the control messages of the multicast routing protocols. The methods used to secure multicast routing protocols are specific to each of those protocols, such as for PIM-SM [4] and CBT [5]. Actually, securing exclusively multicast routing protocols ensures an efficient protection neither for multicast infrastructure nor for the core itself. Indeed, malicious hosts can still illegitimately join groups via fake membership control messages (*Report* messages), or send bogus multicast traffic, and hence generate DoS attacks against the multicast infrastructure. Although these problems affect the core, they originate from the edge of the multicast infrastructure. In brief, an important security hole exists in the multicast infrastructure even though the multicast routing protocols are secure. Therefore, it is highly relevant to secure primarily the edge of the multicast infrastructure [3]. This is achieved by providing receiver and sender access control at the edge level of the multicast infrastructure, and hence at the edge of the distribution tree.

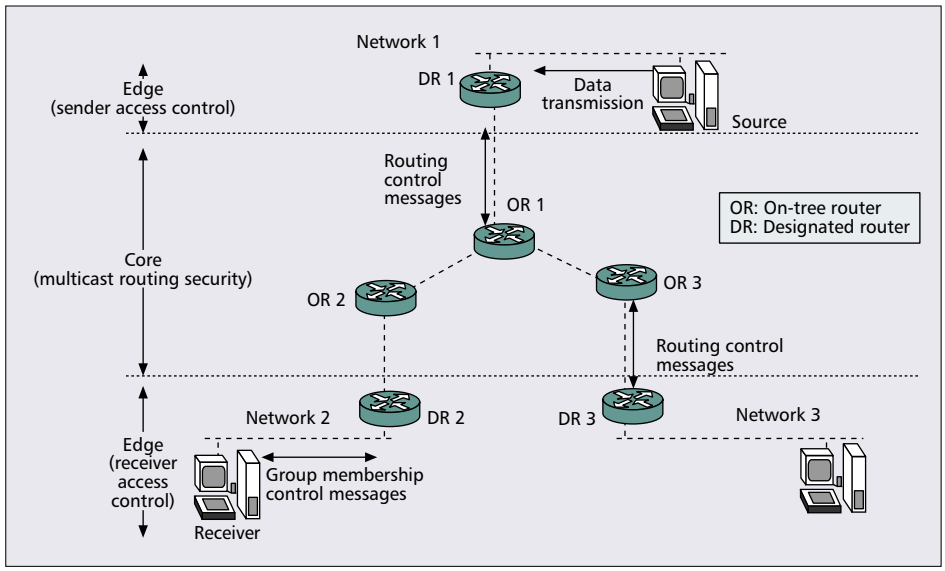


Figure 1. *The IP multicast security infrastructure problem.*

Several solutions addressed the access control problem to the delivery tree. We will review and classify them while taking into account the mobility of users. In fact, as mobility is becoming a primary need for most Internet users, providing access control for senders and receivers must be coupled with the basic requirements and considerations of mobile users and their devices, in particular: fast access control to reduce the join latency, and limited resource capacities (computations and memory storage). The remainder of this article is organized as follows. We define the basic concepts of this survey, in particular: IP multicast, mobile IP, and access control. We highlight the receiver and sender access control problems and draw attention to the impact of user mobility. We give an overview of the requirements that need to be satisfied to ensure an efficient receiver and sender access control both in stationary and mobile IP environments. We review the existing solutions that we classify into three types: *digital signature-based* solutions, *shared secret-based* solutions, and *hybrid* solutions. We end this section by providing a comparative study of the approaches and showing their limitations. Finally, we conclude our study.

Background

IP Multicast Model

The Internet multicast technology (IP Multicast) [6] has been defined to handle new types of applications based on one-to-many or many-to-many communications. The IP multicast model provides new techniques that overcome the limitations of both broadcast and unicast communications. In fact, such a model allows for an optimal use of network bandwidth and avoids source processing overheads since it is based on sending a single packet to a *group* of hosts, identified by a multicast address, without unnecessary duplications. To achieve this goal, the multicast model defines two types of protocols: Multicast Routing Protocols (such as MOSPF [7], CBT [5], PIM [4]) and Group Membership Protocols (IGMP [8, 9] and MLD [10, 11]). The first type is used to build and maintain a multicast tree composed of *multicast routers* that replicate optimally and forward the data packet copies toward the intended receivers. The second concept focuses on managing the group membership information. In the following subsection we will briefly review the group membership protocols, since they are concerned with the receiver access control problem.

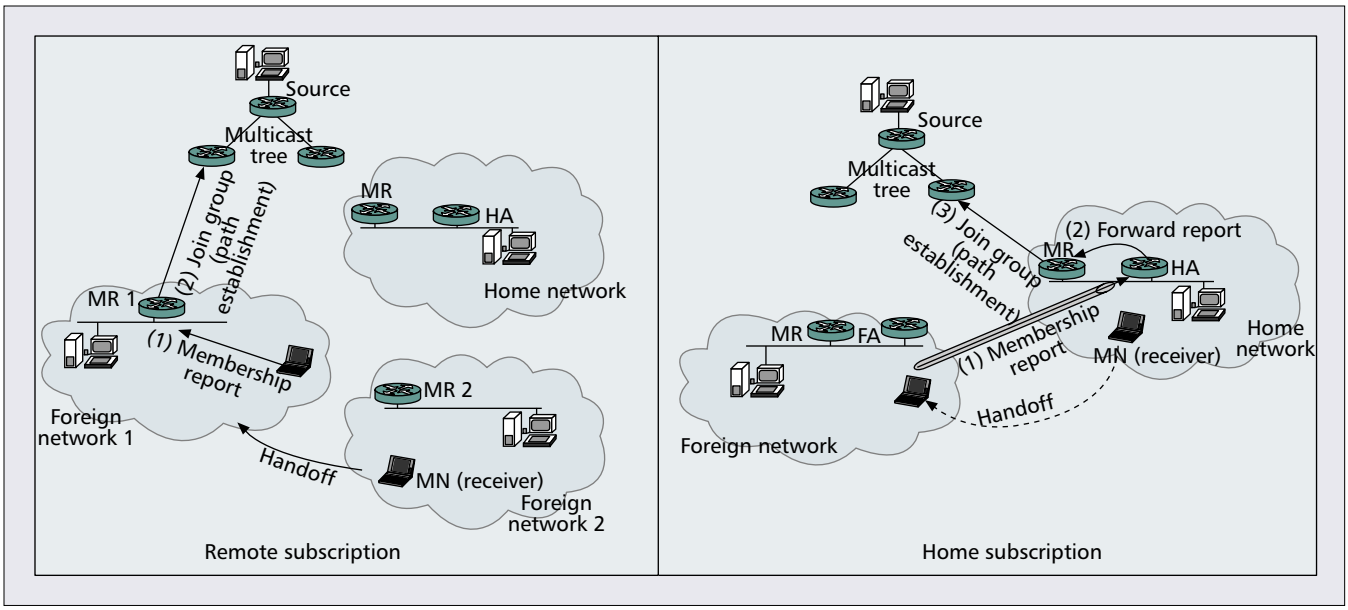
Group Membership Protocols — The group membership protocols have been defined in order to manage the group membership information of receivers (join and leave operations at the edge) for particular multicast groups.

There are two types of group membership protocols: Internet Group Management Protocol (IGMP), defined for the IPv4 protocol, and Multicast Listener Discovery (MLD), defined for the IPv6 protocol.

The last versions of IGMP and MLD (IGMPv3 and MLDv2, respectively) are defined based on their corresponding previous versions. However, IGMPv3 [9] and MLDv2 [11] extend their respective former versions to enable receivers to select the sources of their multicast groups. IGMPv3 and MLDv2 define similar functionalities that are based on two message types: *query* and *report*. Query messages are sent by the *querier* (elected edge multicast router) to all the local network hosts to learn whether there are any hosts (*listeners*) wishing to join particular multicast groups (*specific queries*), or any multicast group (*general query*).

On the other hand, the listeners (the interested hosts) are expected to reply to the queries by reporting the list of multicast groups they wish to listen to, to continue listening to, or to cease to listen to.

When a host wishes to join a given multicast address (and source(s), if any), it sends an MLD/IGMP Report message to *all MLDv2* (respectively: *IGMPv3*) *routers'* multicast addresses. This message informs the neighboring routers about the multicast addresses that the new host (the listener) is interested



■ **Figure 2.** *Remote and home subscription options.*

in. In addition, when a host wishes to update (*include*/*exclude*) the list of multicast groups that the host is listening to, it sends a Report message to join (*include*) or leave (*exclude*) particular multicast groups.

The received Report messages are used by the edge multicast router to maintain the membership information about local hosts. Based on this membership information, the multicast routers trigger the multicast routing procedure to attach to or leave the multicast delivery tree.

Mobile IP Protocol

Moving from an attached network to another while working and continuing communications is becoming a primary need for Internet users. In order to ensure both transparency and management of user mobility in the Internet, the Internet Engineering Task Force (IETF) has defined the Mobile IP protocol. There are two Mobile IP versions: Mobile IPv4 [12] and Mobile IPv6 [13]. The Mobile IP protocol allows a mobile node (MN) to continue communicating with its correspondent node (CN) while changing network location (handover). The MN is identified at its home network by an IP address called the home address (HoA). When the MN moves from its home network to another network (foreign network), it obtains a new IP address, called the care-of-address (CoA), which identifies its new location. This MN uses the CoA to ensure communication reachability to its current location. However, the MN continues using its HoA in order to ensure the transparency of IP address change (due to mobility) for transport and higher-level protocols. A home agent (HA) in the home network of MN is responsible for keeping track of mobile nodes that moved out of the home network to another network in order to tunnel the traffic to or from those mobile nodes. To achieve this goal, each time the MN moves to a new network it registers its (new) CoA address with its HA, which then caches the MN's (new) CoA.

In Mobile IPv4 the CoA registration procedure may be performed directly between MN and HA or via a mobility agent within the foreign network, called the foreign agent (FA). This agent is responsible for intercepting packets originating from the MN's HA in order to deliver them to the MN and vice versa.

In Mobile IPv6 the CoA registration procedure is quite different from Mobile IPv4 since the FA does not exist in Mobile IPv6. With Mobile IPv6, when the MN moves to a new network, it sends a *Binding Update* message to the HA. This message binds the MN's HoA to its new location (CoA).

Mobile IP and Multicast

Mobile IP is intended to support multicasting since IP Mobile Multicast communications is becoming an attractive perspective. As a result, Internet users will be able to keep their subscriptions to multicast sessions while moving between IP networks.

With mobile IP, when a mobile host wishes to receive multicast traffic, it joins the multicast tree via either its (current) foreign network or its home network. These two approaches are called, respectively, *remote subscription* and *home subscription* (Fig. 2). In the remote subscription approach, the mobile receiver sends to the local multicast router its membership report message using its CoA address as a source address of the message. This router then triggers the establishment of the tree branch for the requested multicast group. Hence, each time the mobile receiver moves to a new network, it sends a membership report message to the local multicast router of that network.

With the home subscription or the *bi-directional tunneling* approach the HA is assumed to be a multicast-capable entity and is responsible for periodically forwarding multicast group membership control messages to its mobile receivers that are out of their home network. As Fig. 2 shows, when a receiver wishes to join a multicast group using the home subscription approach, it establishes a bi-directional tunnel with its HA in order to tunnel its membership report message to the HA. When the HA receives this tunneled message, it decapsulates it and forwards the receiver's membership report message to the local multicast router of the home network. Then, when the HA receives multicast traffic, it forwards the traffic using the tunnel to the intended receivers.[2]

Similarly to a mobile receiver, a mobile sender can send multicast traffic either on the visited network or via a tunnel to its HA. In the first case, the mobile sender uses its CoA as the IP source address. In case the mobile sender prefers tun-

[2] *Note that in Mobile IPv4 it is possible that the tunnel ends at the FA instead of the MN in case the MN uses an* FA CoA *[12].*

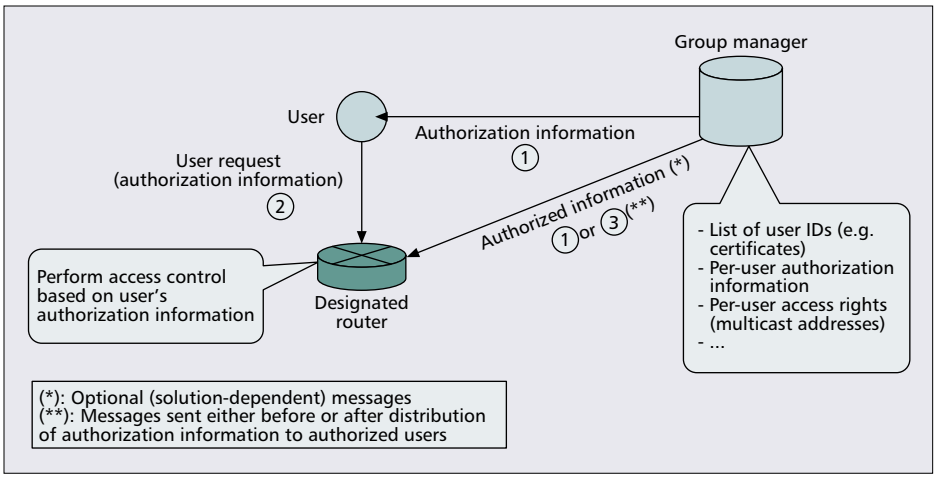


Figure 3. *Access control to the multicast delivery tree (involved entities).*

neling its traffic to its home agent, it uses its home address as the IP source address of the inner multicast packet. This assumes that the home agent is a multicast router.

These are the basic proposed approaches to support Mobile IP with multicasting. Extensions of these approaches have been proposed through multiples studies, and are summarized in [14].

The Access Control Service

The Access Control service is a required and relevant security element for any system and application. Ravi *et al.* [15] stated that "the Access Control seeks to prevent activity that could lead to a breach of security." More specifically, the access control operates according to a *security policy* in order to protect system resources against two risks. The first risk is an unauthorized access to system resources such as viewing, modification, or copying of file information on a computer. The second risk consists in improperly using system resources (e.g., network resources) by both authorized and unauthorized entities [16]. Entities requesting access to particular resources should have the appropriate *access rights* defined by a security policy. The meaning of access right depends on the object being accessed, such as "read/write" for files.

Two entities are directly involved in the access control: the user who claims that it is normally authorized to use the system (e.g., computer, network resources, etc.), and the access control system, which performs user authorization after the user has been successfully *authenticated*.

Authorization: Note that the term "authorization" is naturally used to describe the access control. In fact, authorization and access control terms are usually unintentionally interchanged. The authorization represents rather the right (or a permission) that is granted to a system entity to access a system resource [16]. An "authorization process" is a procedure for granting such rights. The authorization procedure is based on authorization information — referred to as *credentials* — presented by the user to the authorization entity. The credentials represents the secure proof that the user has the required information (e.g., password) to be authorized by the authorization entity. Through our study of the access control and authorization concepts we concluded that there is a subtle difference between them. In brief, the access control is *the goal* and the authorization is *the procedural means* to achieve this goal. Hence, in this survey we will often use the term "authorization procedure" in the description of the existing access control solutions.

Authentication: Note that the access control concept is different from authentication [15]. Indeed, the authentication aims rather at correctly establishing the identity of users. The access control assumes that the authentication succeeds before the enforcement of the access control.[3] Note that it is possible that the *authentication information* used to authenticate the user represents as well its credentials for the authorization procedure. For example, a user may use a password for both authentication and authorization purposes. The authentication may be performed either by the access control entity (a peer-to-peer authentication) or by a trusted third party (TTP), which is known and trusted by both the user and the access control entity. A typical example of trusted third party-based access control is shown in Kerberos [18], and more specifically in the access control to the delivery tree in IP multicast.

Access control to the multicast tree: The access control to the multicast tree typically involves three entities: *group manager*, host, and router (Fig. 3). The group manager is a security entity that is responsible for managing multicast groups. In a general scenario of an access control to the delivery tree, the group manager performs user authentication and authorization to subscribe to particular multicast groups. A successful authorization process ends by providing the user with access rights and the corresponding credentials. The group manager may attribute the access rights to users based on a security policy [19]. An example of access rights may be the list of multicast groups the user wishes to subscribe to. The credentials may be, for example, a *host certificate* signed by the group manager.

Once the user (sender or receiver) receives the required access rights and credentials, it can present them to the multicast router of its network (Fig. 3). The multicast router then performs a user authorization procedure based on the received access rights and credentials. In this situation, the user authentication procedure at the multicast router side may be optional in case such a procedure has already been performed by the group manager. A necessary condition that makes such a scenario possible is that both the multicast router and the user know the group manager (e.g., the group manager's certificate is trusted by both the user and the multicast router).

As we can see, the access control to the delivery tree is almost distributed between the group manager and the multicast router. Figure 3 reflects the basic picture where the differences between the existing approaches appear, specifically, what kind of credentials are sent to the user, how they are securely sent to the multicast router, and how efficient they are to ensure receiver and sender access control to the delivery tree in both stationary and mobile IP environments.

Problem Statement

We now provide an overview of the access control problem to the multicast delivery tree in the case of receivers and senders.

[3] *Note that in this case a mutual authentication may be required (*two-way authentication*) [17].*

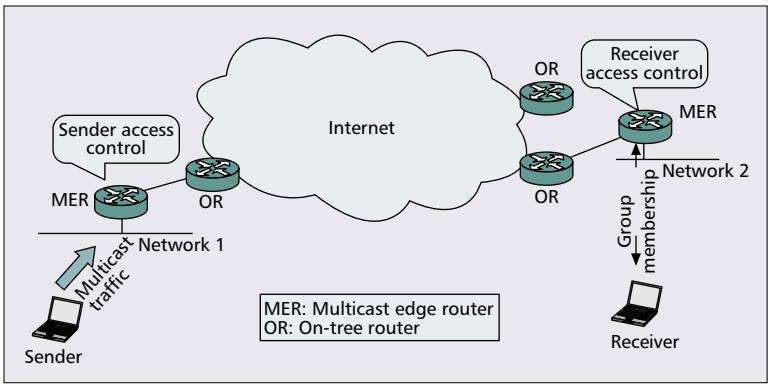


Figure 4. *Receiver and sender access control services.*

Receiver Access Control

Joining a particular multicast group as a receiver (from the viewpoint of attachment to a given multicast tree) is based on group membership message exchanges (*Query*/*Report*) between the receiver and the edge multicast router. Hence, ensuring a receiver access control service in the edge multicast router requires securing the control messages originating from the receiver, that is, *MLD*/*IGMP Report* messages [9, 11]. As described earlier, using Report messages the receiver reports its interest in receiving multicast traffic destined to a particular multicast address, and optionally originating from particular sources. The receiver sends Report messages to *All MLDv2* (respectively: *IGMPv3*) *Routers'* multicast addresses of its subnet (or to the multicast group address in the former versions of MLD and IGMP). Basically, the IGMP/MLD router maintains group membership information according to the received Report messages without performing user authorization.

As a result, using unsecured Report messages, an illegal host can send bogus subscriptions that generate the following:

- Wastage in resources (processing and memory) within the affected routers (i.e., risk of DoS attacks) as well as unnecessary extensions of the distribution tree toward networks where there are no legitimate hosts.
- Excessive bandwidth consumption in the subnet of the attacker, as fake Report messages open vulnerabilities to multicast traffic overload and potential risk for DoS attacks in the attacker's subnet.

Unfortunately, traffic encryption does not solve the problem[4] since a malicious host can still generate DoS attacks even if it cannot decrypt the multicast traffic. To face such attacks, the receiver needs rather to prove its membership right to a multicast router (e.g., an MLD/IGMP router). Currently, many efforts are being made to define the appropriate solution with respect to such an issue.

Sender Access Control

The sender access control (Fig. 4) aims at preventing unauthorized hosts from sending bogus multicast traffic. This problem is particularly challenging because the multicast model [6] allows any user to send its multicast traffic without prior request to the multicast router. Therefore, an attacker may send bogus multicast traffic for both non-existing and existing multicast groups, and hence create DoS attacks at a large scale of the Internet.

The impact of bogus multicast traffic toward 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 (e.g., EMSS [20]), these bogus packets will still generate traffic overhead over the scope of the multicast group.

The impact of bogus multicast traffic toward 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. For example, by exploiting the MSDP infrastructure[5] [21], an attacker may send bogus multicast traffic that generates extensive exchanges of *source active* messages (SA) between multicast routers, which may then suffer from memory and processing overheads. Methods that face such problems by predicting normal traffic patterns to deflect abnormal SA rates may reduce the risks [22]. However, those methods remain inefficient in cases where the bogus traffic is combined with spoofing attacks or this traffic is sent to existing multicast groups.

On the other hand, 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) [6] as the designated routers do not maintain state information about the senders. In addition, *Source Filtering* mechanisms provided by the Source-Specific Model (SSM) [23], the RPF check[6] [24], and other source-filtering approaches [1, 26, 27] do not efficiently resolve the problem because they use the sender's IP address-based filtering, which cannot prevent spoofing attacks originating from the network of a legitimate source.

Mobility-related Issues

The question of mobility implications will be addressed in this article from the viewpoint of multicast access control. Specifically, we will deal with the security considerations regarding the support of multicast traffic transmission/reception in Mobile IP [12, 13]. Other Mobile IP-specific security considerations (e.g., [27, 28]) are out of the scope of this article as they are independent of the IP Multicast model.

Besides, any initial procedure for network access [29] will not be addressed in this study since that aspect is application-independent. From these considerations, we now focus on and summarize the problems of coupling the receiver and sender access control issues with the Mobile IP environment.

- In the mobile environment, the communicating entities (e.g., mobile host-multicast router) may belong to different organizations, which are autonomously governed. This implies that the authorization entities (e.g., multicast router) may not be able to perform user authorization because they do not have the required information (e.g., keying material).

[4] *Traffic encryption provides access control to the multicast data content. Such an access control service, however, is different from the service used to provide authorized access to the delivery tree.*

[5] *MSDP (Multicast Source Discovery Protocol) describes a mechanism that connects multiple PIM Sparse-Mode (PIM-SM) domains together.*

[6] *Reverse Path Forwarding check (RPF) is a technique whereby the router checks its routing table, on the reception of a packet, to determine whether the interface that received the packet normally leads to the source of that packet. If the check succeeds, the router accepts the packet. Elsewhere, the packet is dropped. This reduces the risk of spoofing attacks and prevents looping of packets in the network. RPF is used by most multicast routing protocols such as PIM-SM [3] in order to forward multicast packets.*

Inter-Domain Interaction Issues: With mobile users, inter-domain interaction becomes more probable. That is, users are much more likely to want access to services and resources of a foreign network. In the case of multicasting, when a mobile host (sender or receiver) moves into a new administrative domain, it must be authorized by a local entity (e.g., an authorization server, a multicast router, etc) to continue sending or receiving multicast traffic for or from particular multicast groups. Such an authorization may require interaction between the local authorization entity and one of member's home domain. However, this interaction may not be possible because of interoperability issues or because of the scope of the access control service. Furthermore, in case an inter-domain interaction is possible, it may increase the rejoin latency for mobile members.

Time Information: Access control solutions based on time information may face problems in mobile environments, for example, in the case where a host uses timestamps or short-lived credentials. Indeed, that information may appear to be up-to-date in the current location of the host, but may be obsolete when the member moves to a new network. This particularly occurs when the member moves just before the expiration of its credentials or when the handoff latency is high.

Local Edge Multicast Router vs. Home Agent: The problem of multicast access control in the Mobile IP environment depends in particular on the way the user wishes to subscribe to the multicast group. In the case of receivers, a mobile receiver can send its membership report either to the multicast router of the current network (remote subscription) or via its HA (home subscription). In case the receiver uses its home subscription, it will avoid the problems encountered in the remote subscription. However, delegation mechanisms are required in order to enable the HA to be involved in the access control on behalf of receivers. Similarly, in the case of senders, the user may send its multicast traffic via either the local edge multicast router or its HA. Therefore, the sender will face the same constraints as those faced by receivers.

Hardware Characteristics: Mobile devices are usually very constrained in their resources (e.g., battery power, memory storage, processing power, etc). Hence, a heavy access control mechanism (e.g., based on digital signature) will severely impact mobile devices [30].

For the mobility scenario in this study, we will focus on the case where a user (sender or receiver) moving into a new network chooses to rejoin the delivery tree via the multicast router of that network, since the mobility-related issues are almost tied to this scenario exclusively.

Goals and Requirements

We now list the common requirements of receiver and sender access control solutions for IP Multicast with specific considerations to the Mobile IP environment.

- Performing receiver and sender access control typically requires three entities, namely: the host (sender or receiver), the group manager, and the edge multicast router (or an agent co-located with the router to perform particular tasks). The group manager is responsible for performing user authentication and authorization to enable the user to participate in particular multicast groups. The edge multicast router is typically a subnet multicast router such as a designated router (DR). This router performs user authorization (e.g., upon the reception of credentials from the user) to enable this user to send traffic to or receive traffic from particular multicast groups via the multicast distribution tree. Hence, the authorization procedure of hosts (senders and receivers) in the edge multicast router plays a key role in the access control of these hosts to the multicast distribution.
- A specific authorization infrastructure is required to provide receiver and sender access control, because of the following:
  - §The authorization procedure of the authorization authority must be performed in an effective fashion. In other words, such an authority needs to support group manager functionalities or interact with the group manager. This provides the authority with the knowledge of who participates and in which multicast group(s).
  - §Given the large range of multicast addresses (in both IPv4 and IPv6), the number and addresses of multicast groups that different users may subscribe to within a domain of a given authorization authority are unpredictable. Hence, dynamic authorization mechanisms are required to add/remove authorized multicast addresses.
- A user (sender or receiver) must provide the multicast router with authorization information (credentials) that proves that it is allowed (e.g., by the group manager) to subscribe to particular multicast groups. Besides, the router must be able to process the authorization information of the user.
- *User exclusion*: In order to avoid unnecessary bandwidth consumption and save network resources, a user exclusion mechanism is required (e.g., by setting a validity period for the authorization information (credentials)).
- *Reduced risk of Denial-of-Service (DoS) attacks*: As the main purpose behind the receiver and sender access control services is to prevent unauthorized access and improper use of the multicast delivery tree, which may lead to DoS attacks against multicast groups, and the distribution tree in particular, it is important that the solution does not open vulnerabilities to DoS attacks.
- *Anti-replay protection*: The access control mechanism should itself be immune from replay attacks.[7] This condition is required for both stationary and mobile environments. Indeed, in a stationary environment the protection consists in preventing replays against the same entity of a given network. In the mobile environment the protection consists in preventing replays against entities in different networks the attacker can visit.
- In mobile environments, the identity of senders and receivers (both local and visiting hosts) in a domain governed by a given authorization authority needs to be known by this authority, and the authorized access of senders and receivers needs to be performed in an effective fashion. As a part of this requirement, the mobile host may need to inform the group manager about its mobility (location change). This enables the group manager, for example, to update local information about registered hosts.
- A low-cost and fast access control solution is required in order to minimize delays in mobile environments (re-join delay).
- *Domain-independent access control*: The solution should not be restricted to an administrative domain since the multicast group may cover multiple domains governed by different authorization authorities, and the senders and receivers may move across different domains as well.

Receiver and Sender Access Control Solutions

Through our study of the existing approaches we noticed that

[7] *Replay attacks: an attacker can obtain a copy of a valid message (e.g., credential), store it and then re-send (replay) it at a later time in order to gain unauthorized access to particular resources.*

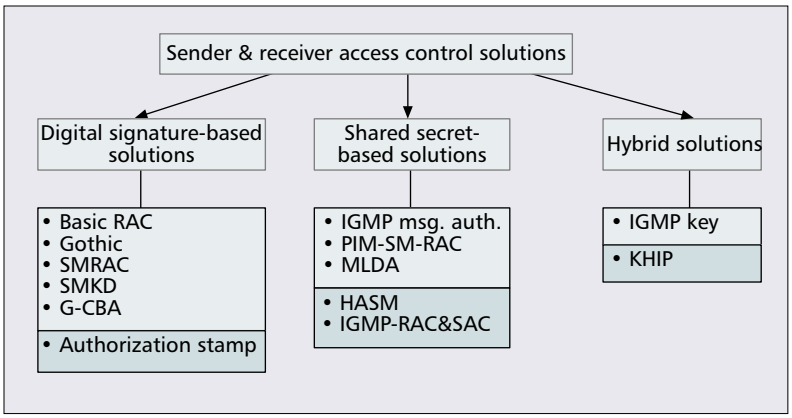


Figure 5. *Receiver and sender access control solutions. The solutions in the dark shaded background support both receiver and sender access control. The other solutions address only the receiver access control problem.*

the receiver access control problem has been more investigated than the sender access control. This latter might not be widely addressed, particularly because of the lack of protocols that provide message exchanges between the source and the edge multicast router. The only protocol that provides such a possible exchange is the Multicast Source Notification of Interest Protocol (MSNIP) [26]. This protocol enables the edge multicast router to inform the source whether there are receivers interested in its traffic. However, this protocol does not address the sender access control problem. The solutions mentioned in Fig. 5 address either the receiver access control problem or both the receiver and sender access control problems. Those solutions may be classified into three categories: *Digital Signature-based solutions, Shared Secret-based solutions,* and *hybrid solutions*. We now review the solutions of each category.

Digital Signature–based Solutions

The solutions we will review in this subsection use *Digital Signature* authentication methods to perform access control for hosts. The digital signature warrants the authenticity and integrity of messages as well as the non-rejection of message validity by a third party (*non-repudiation*). The Digital Signature scheme [31] defines a public-private key pair such that the owner of this key pair generates the digital signature based on its private key. The digital signature of an entity can be verified by any other entity using the signer's public key. The methods used to form and verify the digital signature depend on the approach in use (e.g., RSA, DSS, DSA, etc). With RSA, for example, the digital signature is formed by hashing the message [32] and encrypting the result with the signer's private key. The receiver of a signed message verifies the appended digital signature by hashing the message and decrypting the signature using the signer's public key. If the hash result and the decryption result match, the authentication succeeds.

In the solutions that we will review in the following subsection, the edge multicast router performs a Digital Signature verification of the messages originating from the host.

Basic Receiver Access Control — To ensure receiver access control, the security considerations section of IGMPv3 [9] suggests a method that we will refer to as Basic Receiver Access Control (Basic RAC). With this solution, when a host wishes to join a multicast group, it sends a digitally signed Report message to all-IGMPv3 routers' multicast addresses, as stated earlier.

Receiver Access Control Description — Basic RAC assumes that, within a subnet, all hosts need to know the public key of all routers, and all routers need to know the public key of all hosts. Knowing the public key of hosts assumes that these keys could be enclosed in certificates[8] that are distributed to multicast routers by a trusted entity (e.g., a group manager) during group setup. Otherwise, the host needs to transmit its certificate within its membership request message. In both cases, a *certificate infrastructure* is required to bind the public key with the corresponding host. Basic RAC, however, requires a large amount of keys and introduces a processing overhead and DoS attacks for the multicast router, due particularly to the high cost of Digital Signature processing of membership reports. Moreover, the proposed scheme does not prevent legitimate hosts from sending bogus subscriptions for non-existing multicast groups. Indeed, this solution does not specify any authorization procedure for authenticated hosts. In addition, the solution does not address the sender access control problem. Besides, it lacks specific considerations with regard to anti-replay protection as well as user exclusion.

[8] *The certificate is a data structure that binds a public key to an entity in an authentic way [33]. The certificates are validated, digitally signed, and issued to users by a trusted entity referred to as a certificate authority (CA).*

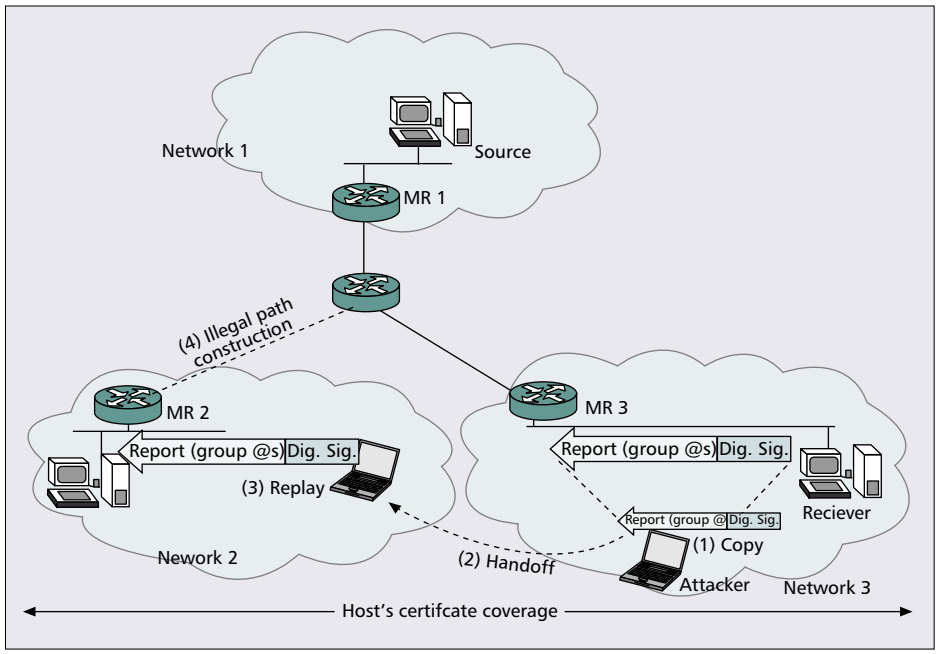


Figure 6. *A replay attack in basic receiver access control.*

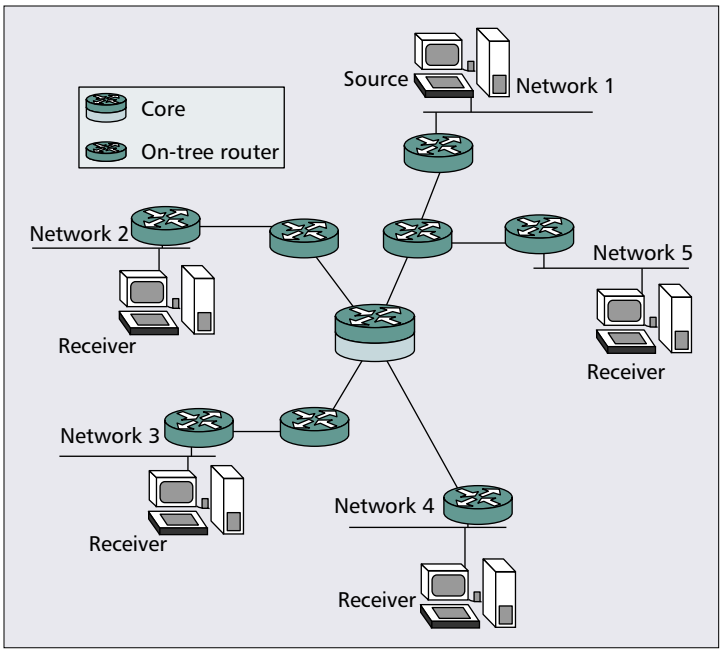


Figure 7. *Example of a CBT tree with one core.*

Mobility Considerations — When a mobile receiver moves from its current network to a new network, it may use either its home subscription or a remote subscription (or variants of these mechanisms) to rejoin the delivery. As we stated earlier, the access control to the delivery tree is concerned with mobility when the user (sender or receiver) rejoins the delivery tree via the visited network. This scenario will be the focus of our discussion about the mobility impact for all the studied approaches.

For the basic RAC solution, we can notice that frequent movements of mobile hosts may severely impact their resources, since the host needs to digitally sign each Report message it sends.[9] In addition, if the host IP address is not protected by the signature, a malicious host can get a signed membership request from its current network, and replay it later in another network after movement (Fig. 6).

Additionally, the multicast router of the visited network can authenticate membership requests of mobile hosts only if the router knows the public key of those hosts. This depends on the coverage of host certificates. If host certificates are distributed during group setup to a set of multicast routers within an administrative domain (e.g., corporate network), the host's membership request cannot be authenticated beyond that domain. To overcome this problem, the host needs to include its certificate within its membership request. This, however, cannot guarantee a successful authentication because the solution may face interoperability issues of public key infrastructures in mobile environments [30]. These issues will be discussed in the case of the Gothic approach.

Scalable Multicast Key Distribution (SMKD) — SMKD [34] defines a secure version of the Core Based Tree protocol (CBT) by integrating mechanisms for secure joining of CBT trees by routers, mechanisms for receiver access control, as well as a group key distribution and update method. The CBT protocol [35] uses a shared delivery tree scheme (Fig. 7), in which the tree is built around cores.[10] One selected core, called the *primary core*, will serve as a connection point for the other cores, called *secondary cores*. The core is responsible for receiving traffic from all the senders and distributes it onto the shared tree toward the group members.

In SMKD each group has its own group key distribution center (GKDC), and this function could be delegated to other routers when they join the tree. Initially, the primary core takes the role of the GKDC. The GKDC holds the group access control list (ACL) and distributes to authorized hosts and routers the group key and key encryption keys (KEKs) used for group key updates. The ACL list contains group membership information (inclusion and exclusion of hosts and routers).

Receiver Access Control Description — When a host wishes to join a tree, it sends an IGMP Report message including a digitally signed and self-generated token (Fig. 8). The token contains the host's unique identity, a timestamp, and a pseudo-random number. The host's token is authenticated either by the host's DR only (in case DR is a GKDC) or by both the DR and the GKDC. In this latter case, the DR first initiates the establishment of a new branch by forwarding the host's token to the core. As Fig. 8 shows, when the core verifies the token, it sends back to the requesting DR a digitally signed

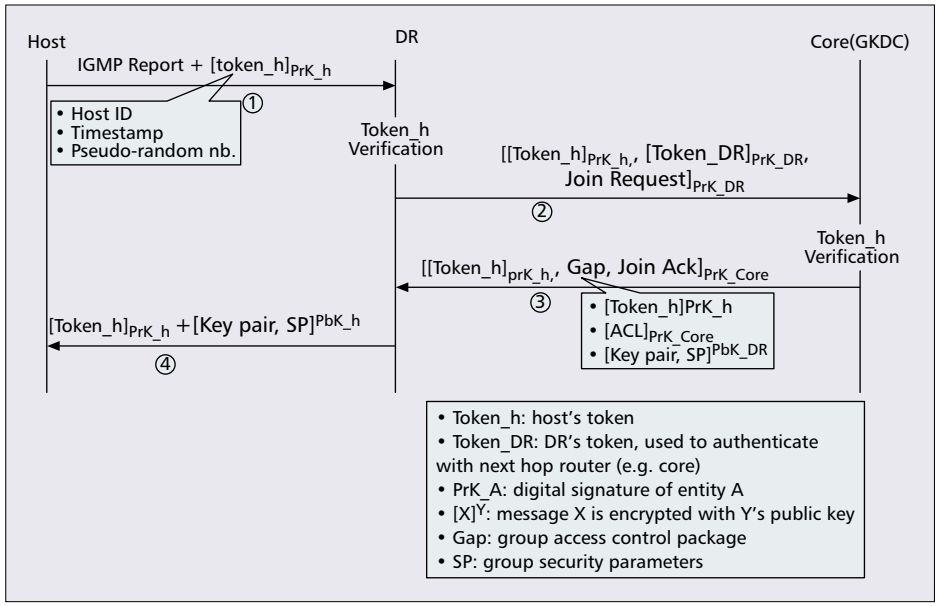


Figure 8. *SMKD protocol - receiver access control.*

[9] *Recall that performing public key operations requires high processing capacity.*

[10] *A core router is a delivery tree router that represents the convergence point of all traffic originating from multicast senders in order to be forwarded to the receivers.*

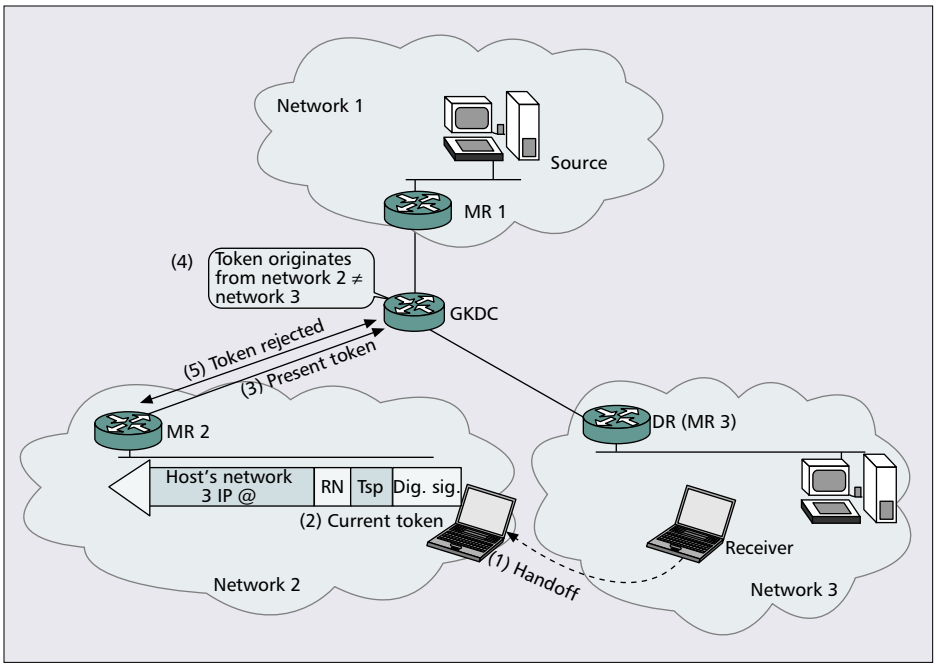


Figure 9. *SMKD-token invalidation because of network-based host ID.*

group access package including the host's token, a signed ACL, and other security parameters for multicast traffic (e.g., KEKs). Upon the construction of the new branch, the DR stores the group access package to act further as a new GKDC.

Compared to the basic RAC, SMKD provides authorization mechanisms since the GKDC is aware of which multicast groups the host wishes to join. This avoids the risk of bogus subscriptions from valid hosts. Besides, SMKD provides an anti-replay protection of the credentials (the token) using timestamps. However, SMKD does not provide a sender access control and does not ensure the user exclusion. Instead, the author suggests establishing a new group to revoke old members. Besides, this solution raises the risk of DoS attacks because of digital signature verifications of tokens at the both DR and the core.

Mobility Considerations — One of the key elements that could affect the remote subscription in SMKD is the host ID enclosed in the token. Such an ID may be either tied or not to a network location.

If the host ID is not tied to a network location, a valid token may be replayed by a mobile attacker. In fact, the attacker simply intercepts a token sent within a given network and replays it in another network during the validity period of the timestamp. In the case where the host ID is tied to a network location (e.g., IP address), the member cannot reuse its token for the remote subscription since the token verification phase at the routers (DR and root) will fail due to the difference between the host ID and the source address of the token originator (Fig. 9). Note that the token cannot be reused as well if the timestamp is outdated.

Mobile members can avoid the problems with invalid tokens by using the self-generation privilege of tokens. Specifically, a valid member can generate a new token with a new timestamp when it desires to use the remote subscription. In the case of a location-dependent host ID, the member requires first securely notifying its GKDC about its ID change using an out-of-band mechanism (a secure BU in the case of Mobile IPv6 [13]) (Fig. 10). Such a notification will enable the GKDC to be aware of the member's mobility, and hence avoid rejecting by mistake valid tokens specifying a location change. However, this useful extension is not free since it introduces additional processing and signaling costs between the member and the GKDC (ste[(2), (3), and (4) of Fig. 10). These additional costs contribute to increasing rejoin latencies for the mobile member. On the other hand, the authors did not specify in which data structure the public key and host ID are bound together. The solution requires that a public key infrastructure is in place. In that case, certificate-related problems in mobile environments need to be considered, as will be outlined in the next subsection.

As shown in Fig. 10, another mobility-related problem with SMKD is the scope of the access control service, which is limited to the bi-directional routing protocols integrating the secure joining and multicast key management functionalities.

Group Access Control Architecture for Secure Multicast

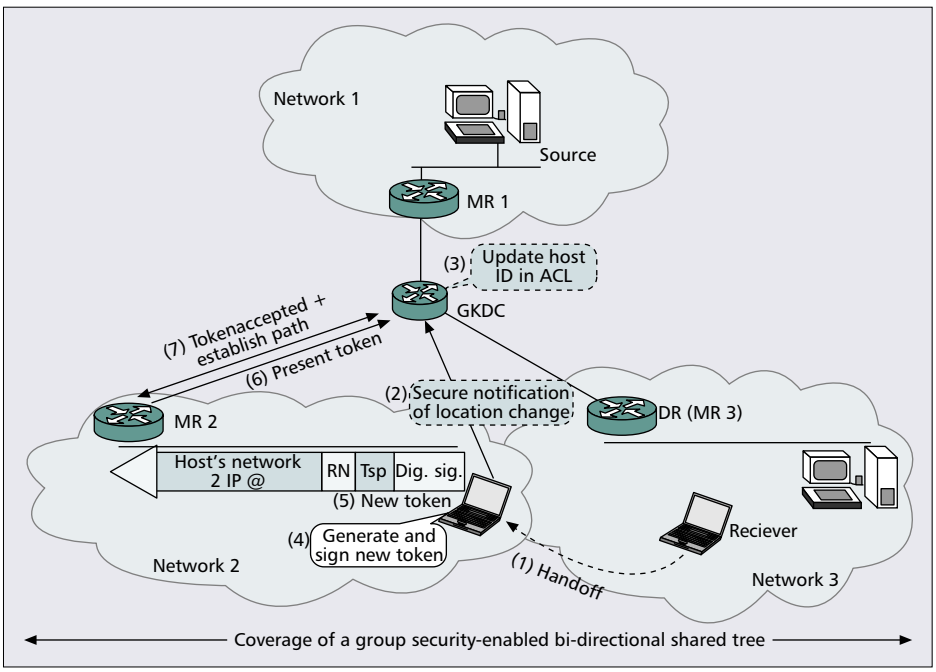


Figure 10. *SMKD applicability to support the remote subscription.*

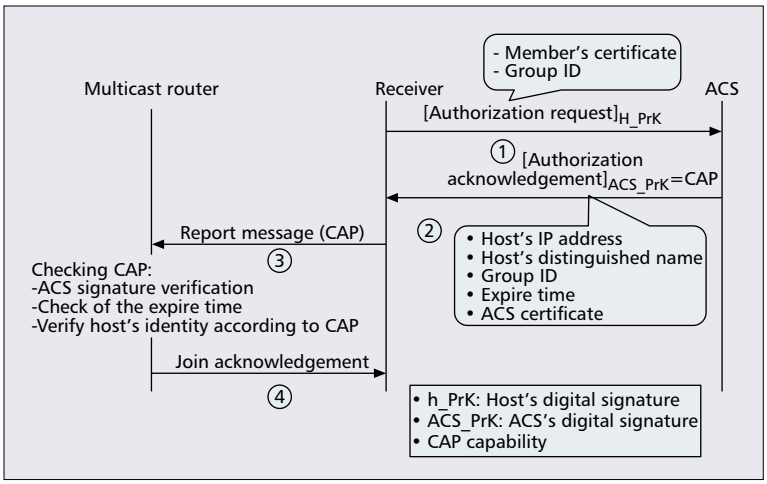


Figure 11. *Receiver access control in Gothic approach.*

and Anycast (Gothic) — The Gothic solution [19] provides receiver access control for both IGMP and MLD. More specifically, Gothic specifies access control functions based on a PKI infrastructure[11] [33]. Gothic functionalities provide authentication and authorization procedures to enable users to subscribe to multicast groups by presenting their credentials.

Receiver Access Control Description — The credentials, called *capability*, is provided by the group manager — the Access Control Server (ACS) — to authorized hosts when they wish to subscribe to particular multicast groups. The capability is digitally signed by the ACS, and consists in particular of member's IP address, the multicast address, and the public key certificate of the ACS.

When a host wishes to join a multicast group (as a receiver), it sends its join request enclosing its capability to the multicast router (Fig. 11). When the multicast router receives the Report message, it checks the validity of the capability by verifying the ACS's signature, and checking the host's identity against the one enclosed in the capability. Once the verification is completed, the router sends to the host a *Join Acknowledgment* message stating a successful or an unsuccessful join.

Compared to SMKD, the Gothic approach is attractive in the sense that it avoids the interaction between the group manager and routers. Hence there is no need for a pre-established secure channel or communication between those entities. Instead, all the access control information (capability) generated by the ACS is transmitted by the host to the router. Besides, Gothic provides a user exclusion mechanism based on an *expire time*. Hence, when the time of a given capability expires, this capability will be rejected by the multicast router.[12] This could be attractive in the case where membership duration is predefined (e.g., *prepaid services*) so that the ACS simply fixes the certificate period according to the membership duration. This, however, cannot be efficient in a typically dynamic environment, where the group membership duration of the user is unknown. For example, if the multicast router stops forwarding traffic because the validity period of a capability expired,

[11] A Public Key Infrastructure (PKI) is defined within an administrative domain. This infrastructure provides various certificate management functionalities, such as user registration and key pair generation, certificate generation and distribution to end users, renewing certificates when they expire, revoking certificates, etc.

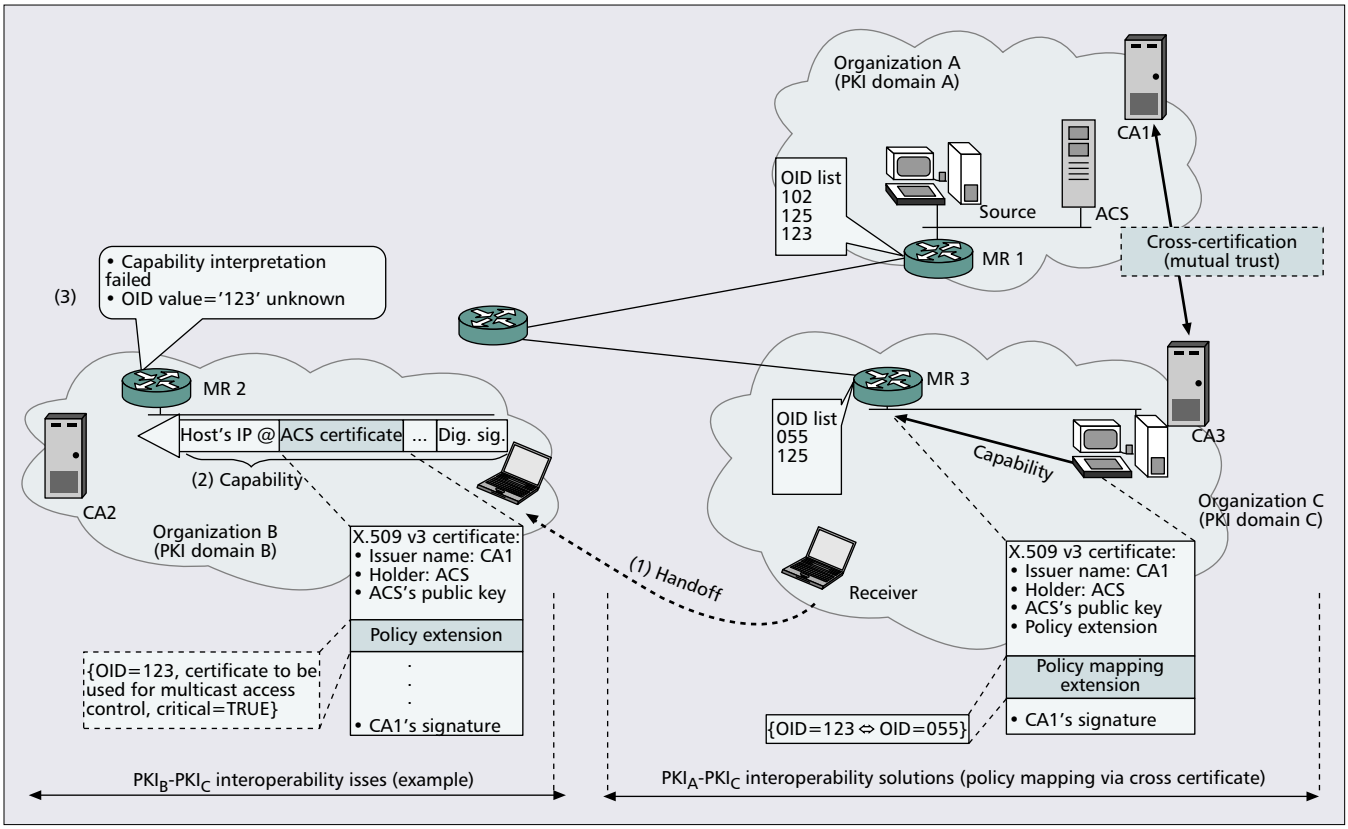


Figure 12. *The PKI-PKI interoperability problem in Gothic.*

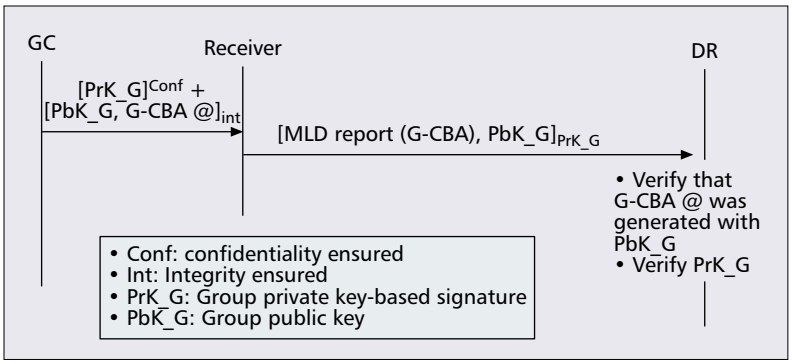


Figure 13. *Receiver access control in G-CBA (basic scheme).*

the host needs to request a new capability to continue its subscription to its multicast group. Moreover, the capability is not protected against replay attacks. These attacks, however, are effective only when all the valid hosts of a given network left their group while a corresponding capacity has not yet expired. In this situation, an unauthorized host that has received the capacity can send it later during its validity period to force the edge router to continue forwarding unnecessarily multicast traffic.

In addition, the Gothic approach does not address the sender access control problem. Besides, this scheme is weighty because of verification cost of the digital signature at the multicast router. This may introduce processing overheads in the router and a high risk of DoS attacks due to the public key authentication method.

Mobility Considerations — From the point of view of mobility support, this scheme seems to be well adapted since there is no need for a pre-established context between routers and ACS. If we look at the capability, however, we can notice that it is tied to the host's IP address. Hence, if a member prefers using remote subscription when it moves to a new network, it needs to request a new capability from the ACS because the multicast router verifies the host's IP address as part of the verification process of the capability. This requires that the member first inform the ACS about its mobility (as in SMKD). All these constraints will increase the join latency for mobile members and reduce the performance of Gothic in the mobile environment. In addition, constraints related to mobile host capacities (e.g., authentication with ACS) may affect the efficiency of the access control mechanism in highly mobile environments, as shown in the basic receiver access control approach and SMKD. Besides, PKI-related problems may rise when a member moves to a network where the multicast router is covered by a distinct public key infrastructure. Indeed, due to possible interoperability issues between public key infrastructures [30], the multicast router of the visited network may not be able to verify the capability (Fig. 12).

The interoperability issues arise from different factos such as technical factos (e.g., certificate formats, semantics of name attributes), policy factors, business factors, etc. However, in Gothic the verification is based on the ACS's public key, which is enclosed in the ACS's certificate.[13] Hence, if the multicast router does not recognize the ACS certificate format or any enclosed extension,[14] it will reject the host's request. For instance, in the PKIX certificate standard [33], unrecognized extensions introduce the rejection of the certificate when they are marked as *critical*. On the other hand, the enforcement of non-standard certifications or domain-dependent security policies both in the members' home network and in the visited network may also prevent those members from rejoining the tree via the visited network.

Figure 12 illustrates an example of a policy-related interoperability issue among three PKIs: PKI_A, PKI_B, and PKI_C. Each PKI initially has its own policy. Besides, let the ACS's certificate enclose a critical policy extension (e.g., a "certificate to be used for multicast access control"), which is not identifiable in domain B. When a member entering domain B presents the ACS's certificate to the multicast router MR2, this router will reject the ACS's certificate because it does not recognize the critical extension.

To overcome the PKI interoperability issues, specific methods are required to enable entities from different PKIs to be able to trust and understand the certificate of each other. Those methods are based on connecting different CAs to form a larger PKI. The most commonly known methods are *Cross Certificate* and the *Bridge Certification Authority* architecture (BCA) [36]. As illustrated through Fig. 12, using a cross-certification structure, the policy-related interoperability problem between PKI_A and PKI_C can be resolved. Concretely, the cross-certification establishes a mutual trust between PKI_A and PKI_C. Using this trust relationship, each PKI can statically map the OID (*policy identifier)* of the other PKI (*policy mapping*). The policy mapping [33] allows the OIDs generated in a certificate issued by one organization to be recognized in

[13] In addition to the public key, a typical certificate (e.g. x.509 [33]) contains other fields such as issuer name, owner name, a validity period, and optional extensions. An example of such extensions could be policies governing a certificate in an administrative domain.

[14] Certificate extensions may have standardized and proprietary values. The difference between extensions is a source of the existence of different certificate formats profiled for specific uses. These format differences may cause various PKI interoperability problems that may exist between different administrative domains [30].

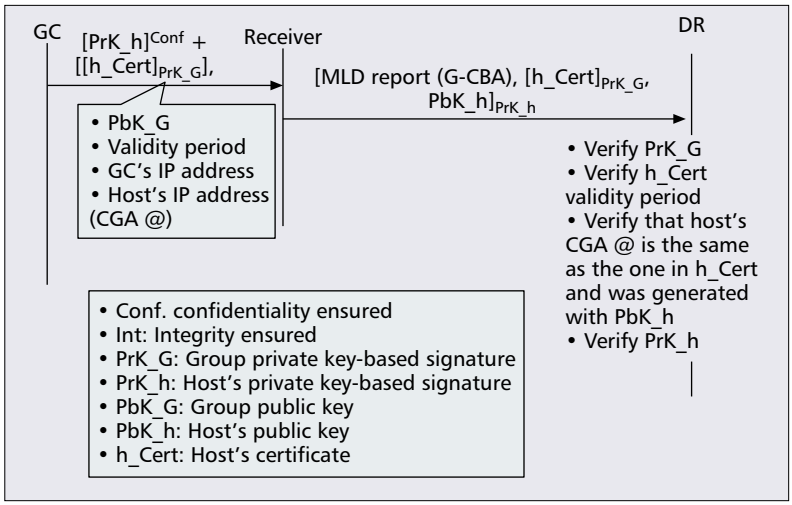
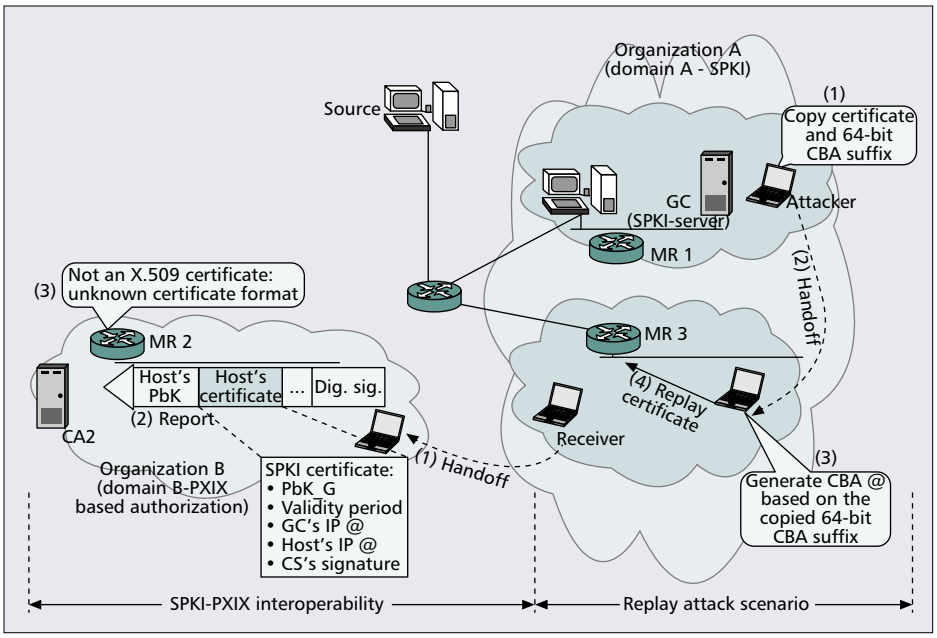


Figure 14. *Receiver access control in G-CBA (certificate-based scheme).*

[12] The router may not need to store the capability, but could for example send a periodic Query *message to re-request the capability from members.*



■ **Figure 15.** *CS Issues in mobile environments.*

another organization. Hence, in Fig. 12 the OID "123" is mapped into OID "055" in domain C.

The problem with the cross certificate and BCA techniques is that they are not broadly deployed, and are still in test phases. In fact, the complexity of current standards and technical divergences are making difficult the achievement of an efficient interoperability structure.

Group Cryptographically Based Addresses (G-CBA) — In [37] C. Castelluccia and G. Montenegro proposed a solution that provides a receiver access control mechanism for multicast groups in IPv6 environments. The proposed solution is based on the Cryptographically Based Address (CBA) scheme [38]. This scheme associates to each IPv6 node (host, server, router, etc) a public-private key pair and derives the node's IPv6 address (a *CBA* address) from the node's public key using a Hash-Message Authentication Code (HMAC) function.[15] Specifically, the public key is used to generate the 64-bit suffix of the CBA address, whereas the 64-bit prefix represents the subnet prefix.

The authors proposed to extend the CBA concept to group addresses (G-CBA) in order to secure MLD Report messages. The G-CBA protocol defines two schemes to solve the proof-of-membership problem: a basic scheme and certificate-based scheme.

Receiver Access Control Description — In the basic scheme (BS), the group controller (GC) generates a group public-private key pair and derives from it the G-CBA (group address).[16] The generated key pair is then securely distributed to authorized group members. When a host wishes to join or leave the group, it includes the group public key and signs the resulting message with the group private key (Fig. 13). Once the designated router (DR) receives a Report message for a group CBA address, it verifies the host's proof-of-membership to the group by verifying that:

- The G-CBA was generated from the group public key.
- The signature is valid.

If the proof-of-membership is correct, the router accepts the Report message. In addition, to avoid replay attacks in BS, the authors suggest including nonces[17] during the Query-Report exchange between routers and hosts.

Similarly to Gothic, the BS scheme avoids the interaction between routers and the GC. This approach, however, does not provide user exclusion. As a result, an old member can illegitimately send a Report message to the router with a valid public key and private key pair since these keys remain unchanged during the group session duration. In addition, the approach introduces risks for DoS attacks due to high-cost operations at the DR when authenticating fake Reports.

The alternative scheme, called the certificate-based scheme (CS), extends the basic scheme to ensure user exclusion using certificates. Specifically, each member will be attributed a distinct public/private key pair. The member's public key is used to generate its CBA address, as explained earlier. This CBA address is enclosed within an authorization certificate (SPKI certificate[18]) issued by the GC. Aside from the CBA address, the certificate includes the group public key, its related G-CBA address, and a validity period (Fig. 14). When a host wishes to join or leave the group, it includes its certificate and public key, and signs the resulting messages with its private key. On receipt, the DR verifies the validity of the certificate and uses its content to perform several validity checks, including the verification of the G-CBA and CBA addresses (Fig. 14). On the other hand, the authors recommend using short-lived certificates to overcome replay attack risks in the CS scheme.

The certificate-based scheme is attractive in the sense that it allows for excluding members based on the validity of their certificate. Also, this scheme avoids interactions between the DR and the group controller. The problem with this scheme, however, is that the user exclusion mechanism (certificate validity period) has the same limitations as the Gothic approach. In addition, as with the previous scheme, the certificate-based scheme is weighty, time-consuming, and vulnerable to DoS attacks because of the public key authentication. Finally, as a common conclusion, both the BS and CS schemes do not support sender access control.

Mobility Considerations — The G-CBA solution is attrac-

[15] HMAC is a one-way function that transforms the concatenation of a message (of any size) with a key to a fixed-size hash value usually used for authentication purpose. The One-Way property ensures that knowing a hash value and the hash function, it is computationally very hard to find the original message.

[16] G-CBA is generated by hashing the public key only.

[17] Nonce is a random value that is included in data exchanged between a pair of communicating entities. The randomness of nonces makes it possible to detect and protect against replay attacks.

[18] Simple Public Key Infrastructure (SPKI) defines a standard form of an authorization-oriented digital certificates [39]. Holders of SPKI certificates are identified by their public keys only rather than the pair (name, public key).

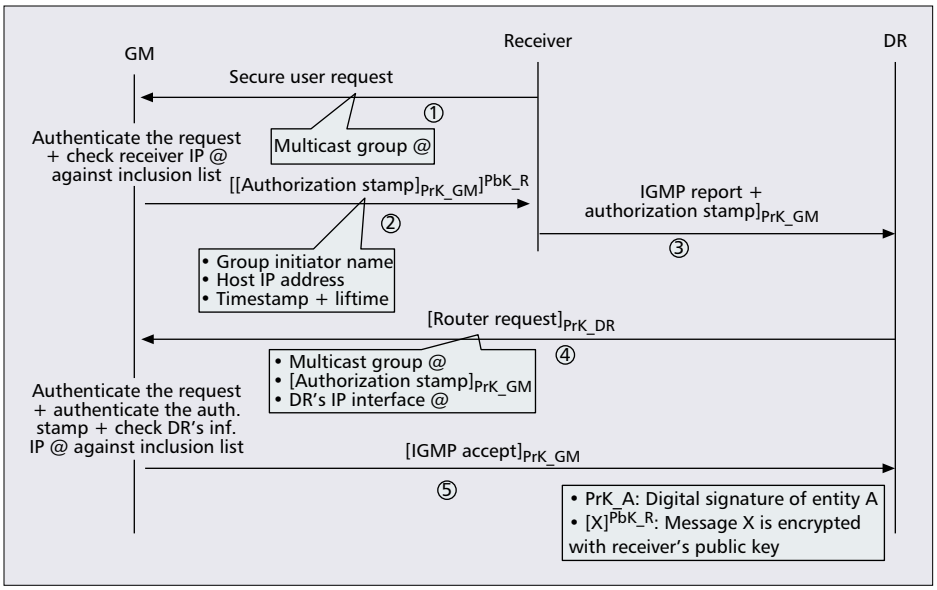


Figure 16. *Authorization stamp - receiver access control.*

tive with regard to mobility support. In fact, the router is required to neither store any pre-established context nor interact with the GC to perform host access control. Indeed, all the information required to verify the host's validity is included in its membership request (Fig. 13 and Fig. 14). Also, in the CS approach, the member's IP address change (i.e., CBA change due to mobility) does not invalidate the member's certificate. In fact, using the host's public key, the router can just verify the validity of the fixed hash representing the 64-bit suffix of the CBA address rather than the whole CBA address (i.e., including the subnet prefix). However, this opens vulnerabilities to replay attacks. Indeed, a mobile attacker could intercept the certificate and the CBA address of a victim, and then copy the relating 64-bit suffix to replay the certificate in another network (Fig. 15). To overcome such an attack, the authors suggest using short-lived certificates. With this option, however, if the member's certificate expired while the member needs to present it through a remote subscription, a new certificate should be requested from the GC. Such a constraint generates high operation costs at members (a secure binding update [13] and recovery of the new certificate), and hence increases rejoin latencies.

On the other hand, the CS scheme relies on SPKI infrastructure. Hence, the access control of hosts using a remote subscription will be ensured as long as those members move within SPKI domains covered by the GC service. To support the remote subscription in a domain that is not SPKI-based (e.g., a PKIX-based authorization domain [33]), the solution should first overcome the interoperability issues that arise when coupling a SPKI certificate format with other certificate formats (Fig. 15).

Finally, the CS scheme generates and verifies the validity of CBA addresses based on the Static Uniqueness and Cryptographic Verifiability (SUCV) algorithm, that is, the node's public key and the node's random value as inputs. However, other CBA schemes are emerging, such as [40], where the CBA address is generated based on the subnet prefix as an input parameter. This introduces additional interoperability issues for the CS scheme in mobile environments in cases where the router of the visited network does not support the SUCV algorithm.

Authorization Stamp — In [41] T. Ballardi and J. Crowcroft defined receiver and sender access control mechanisms for CBT trees. Each time a multicast group is created, the group manager generates a *multicast certificate* for that group. This certificate will be used by the group manager to perform user authorization procedures. The certificate contains a validity period, an IP multicast group address, group inclusion (or exclusion) list, that is, subnets where hosts are authorized (respectively, non-authorized) to become members, and a sender list (a list of members authorized to send to the group).

Receiver Access Control Description — A host interested

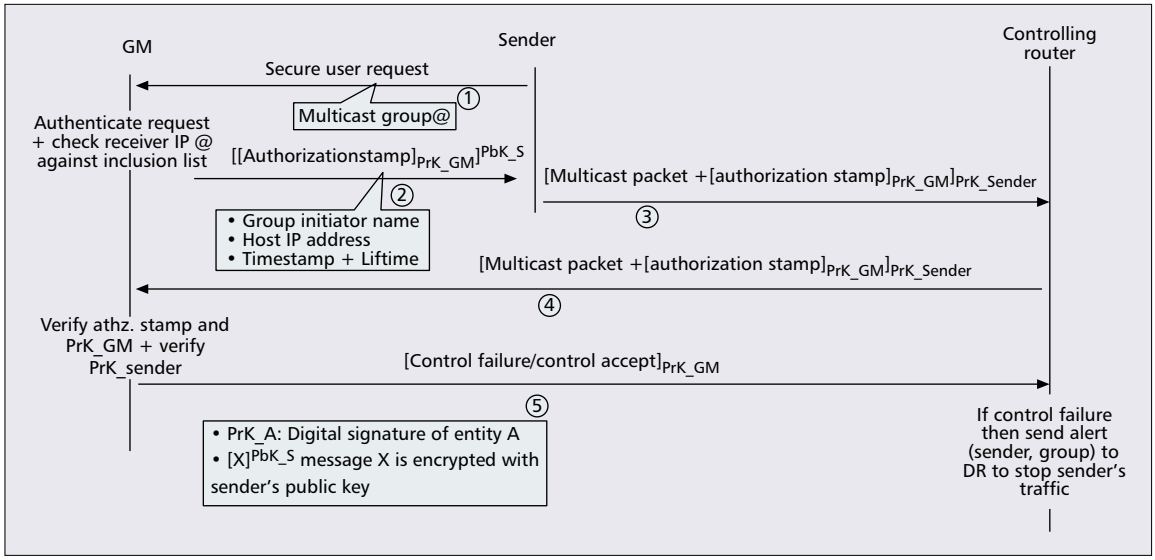


Figure 17. *Authorization stamp - sender access control.*

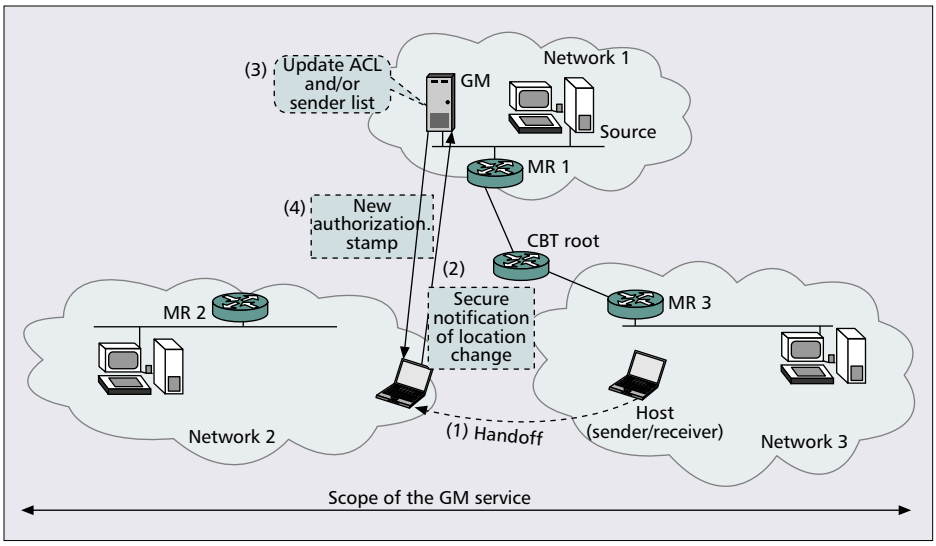


Figure 18. *Extension of authorization stamp approach to support a remote connection to the tree.*

in subscribing to a particular multicast group sends a signed *User-Request* message to the group manager (Fig. 16). If the check of user's request against the multicast certificate succeeds, the group manager generates and securely transmits to the host an *authorization stamp* that includes the host's IP address, a timestamp, and a lifetime to be used in data packets (Fig. 16). The host uses the authorization stamp as a credential when it sends its IGMP Report to the designated router (DR). To make a decision on the host's request, the DR securely forwards that request to the group manager. After the group manager receives the DR's message (Fig. 16), it checks the validity of the enclosed authorization stamp and verifies that the member's Report message was sent within one of the authorized subnets (*inclusion list*). After all the checks have been competed, the group manager replies to the DR with an acceptance or rejection of the member's request.

Sender Access Control Description — After a host receives the authorization stamp from the group manager, it can start sending traffic to the claimed multicast group (Fig. 17). To achieve this, the sender includes the authorization stamp in each multicast packet it transmits and digitally signs the packet. An on-tree router is expected to forward regularly to the group manager the packets it receives from a sender. If the group manager detects an unauthorized packet (Fig. 17), such as a fake packet signature, a *control failure* packet is returned to the requesting router. On receipt, the router generates an *alert* packet specifying the affected (source, group) pair. The alert packet is then transmitted to the DR of the malicious sender, so that the DR stores the IP address of the attacker and stops forwarding traffic originating from that address.

The authors suggest using the lifetime of the authorization stamp as a replay protection of the sender's traffic. Upon lifetime expiration, the sender should request a new authorization stamp to continue transmitting data.

Compared to the previous approaches, this solution supports both receiver and sender access controls. Also, this approach provides an anti-replay protection using a timestamp in the authorization stamp. Effective protection, however, requires short-lived authorization stamps at the expense of decreasing the efficiency of the protocol. In fact, with that scenario the host should frequently request a new authorization stamp from the group manager to maintain its connection to the tree. Also, the solution is vulnerable to DoS attacks where a malicious user gets the control routers involved in extensive exchanges with the group manager to verify bogus traffic. Moreover, the sender access control mechanism has two limitations. First, the exchange between the DR and the group manager provides a weak protection against bogus traffic, since only some packets are controlled among the whole traffic flow. Second, an attacker that impersonates a valid source can send bogus traffic to generate an alert packet that penalizes the valid source. In addition, the user exclusion mechanism is based on a pre-defined lifetime of the authorization stamp. This may increase latencies and disturb multicast sessions. Indeed, the sender needs to request a new authorization stamp before the expiration of the current one.

Mobility Considerations — This approach is attractive with regard to its applicability in the mobile environment given its reliance on public key infrastructure. In fact, although the authorization stamps are signed by the group manager, they are exclusively verified by that entity. Hence, when a valid host (sender or receiver) moves to a new network and wishes to rejoin the tree via that network, the router does not need to verify the authorization stamps, as they will be forwarded to the group manager (Fig. 17). The main problem that arises, however, is that the authorization stamp may be rejected by the group manager. In fact, this approach faces the same

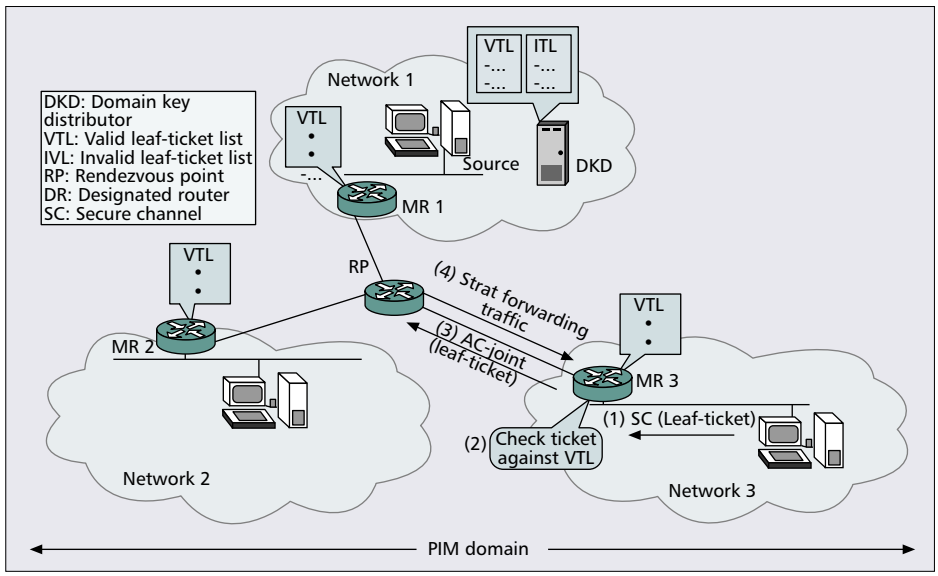


Figure 19. *Receiver access control in a PIM domain.*

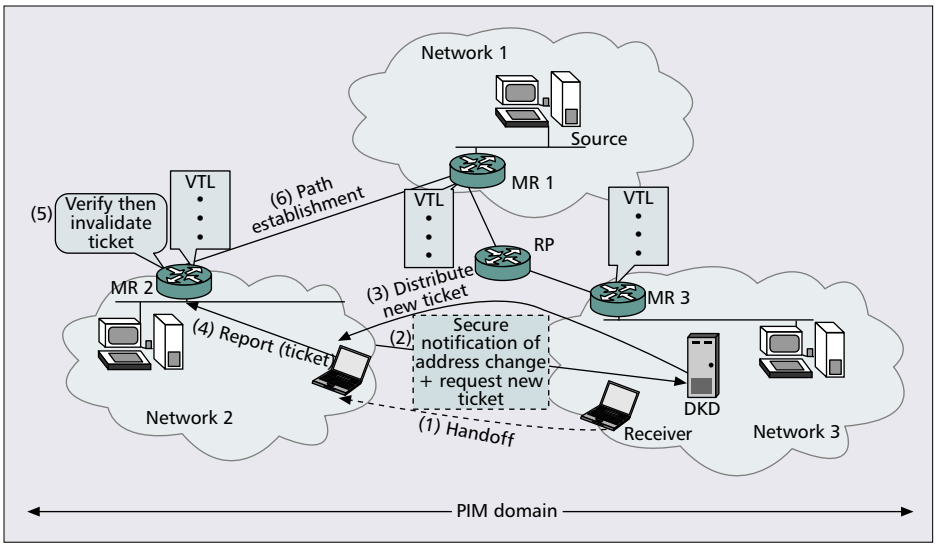


Figure 20. *PIM-SM-RAC applicability to support the remote subscription..*

problems in the mobile environment as with Gothic with respect to the change of the host IP address. This is because the host IP address is tied to the network where the user subscribed to the group. To avoid this problem, the host needs to request a new authorization stamp each time it rejoins the tree via its current network (Fig. 18). This, however, will introduce the same problems as G-CBA CS (i.e., increased rejoin latency and processing overhead at the host in a highly mobile environment). Also, access control is limited to the scope of the group manager's service, because the DR needs to interact with the group manager.

Shared Secret–based Solutions

In shared secret-based solutions a pair of communicating nodes, in our scenario a host and multicast router, authenticate each other based on secret information (typically known by those machines exclusively). To achieve this, the machine applies to the message being transmitted an authentication algorithm (e.g., HMAC) based on a shared (*symmetric*) key as a secret. Another alternative would be to enable a host to provide the proof to its communicating peer that it knows the secret it shares with that peer. This may be achieved using *Challenge/ Response* procedures [42] in which a *server* (e.g., the multicast router) sends an unpredictable *challenge value* (typically a random value) to the *client* (host), who computes the response using a transform on the received challenge value. Such a transform may be an encryption (symmetric or asymmetric) algorithm or a hash function applied on the concatenation of the challenge value along with a secret value (e.g., a key) shared between the client and the server. When the server receives the client's response, it applies the appropriate operation (it depends on the type of transform in use) in order to check whether the client's result matches the expected result. In the following sections we describe the existing receiver and sender access control solutions that are based on the concept of *shared secret*.[19]

Receiver Access Control in PIM-SM — A solution that extends mechanisms originally used to secure the control messages of PIM-SM protocol has been proposed in [46] to provide receiver access control. PIM routers use a key shared between them called the Equal Opportunity Key (K_{eq}) to authenticate their control messages. The defined receiver access control mechanism suggests using that key for two roles. First, the group manager, called the domain key distributor (DKD), generates different *leaf-tickets* by hashing K_{eq}

[19] *This concept is also exploited in [43, 44], and [45].*

[20] *The rendezvous point (RP) is a multicast router that represents the root of the delivery tree in PIM domains. All the multicast traffic in a PIM domain transits by the RP.*

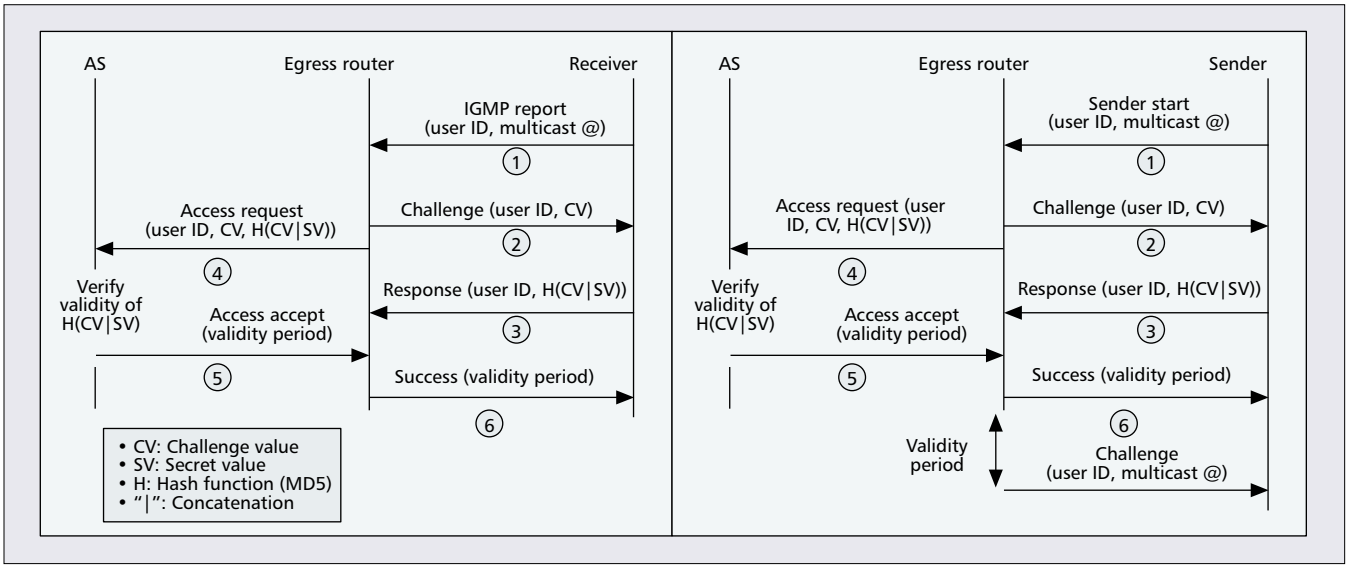


Figure 21. *Receiver and sender access control based on ingress/egress routers.*

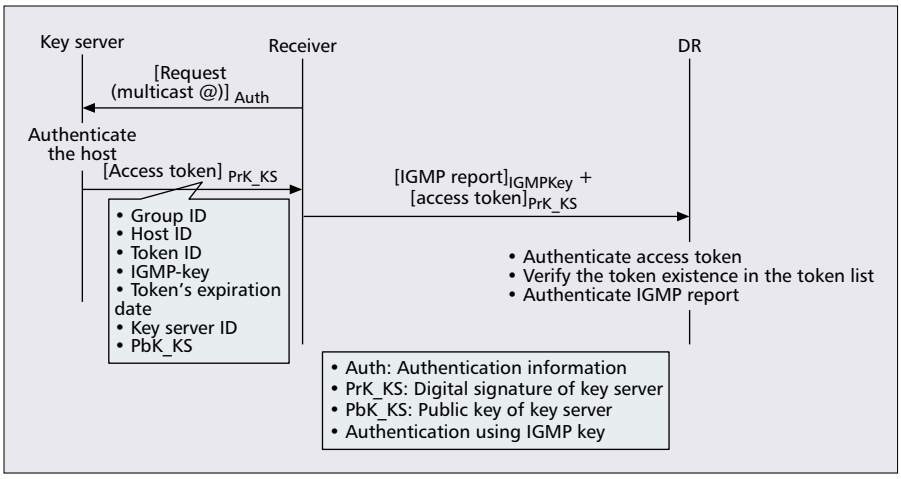


Figure 22. *Receiver access control based on IGMP-Key.*

with a random value. Second, the leaf-tickets are distributed periodically with their respective lifetime by the DKD in the form of a valid ticket list (VTL) encrypted with the K_{eq} key to all the PIM router of the PIM domain. The DKD also distributes the VTL list to the designated routers using a secure channel.

Receiver Access Control Description — When a host wishes to join a multicast group, the DKD provides him an unused leaf-ticket to prove its membership to the designated router. Once used, the ticket is included by the DKD in the invalid ticket list (ITL). This list holds the tickets that can no longer be used in the PIM domain for several reasons, e.g. the ticket has been attributed to a host or the lifetime of the ticket has expired. The DKD regularly distributes the updates of the ITL list to all the domain PIM routers so that they delete invalidated tickets from their VTL list (Fig. 19).

The joining host presents its ticket to the DR using a shared key to authenticate and encrypt the ticket (e.g., IPsec ESP channel). When the DR receives the ticket, it checks it against the VTL list (Fig. 19). If the ticket is valid, the DR sends a new-defined PIM message, called an Access-Controlled-Join (AC-Join) message, that includes the ticket, toward the rendezvous point (RP)[20] (Fig. 19). On receipt, the RP (or an on-tree router holding the VTL list) triggers the normal PIM join procedure to start forwarding multicast traffic requested by the joining host.

This solution provides anti-replay protection. Indeed, after the token is used, it will be invalidated by the DKD and routers so that any attacker cannot replay a used token.

Besides, the present solution provides user exclusion as the ticket is invalidated after it is attributed by the DKD to a joining host. Given this consideration, the author, however, does not describe how a valid host can successfully join the multicast tree. Indeed, a synchronization mechanism is required between the DKD and the routers in order to avoid multicast routers (e.g., DR) inadvertently excluding a joining host.

On the other hand, the defined user exclusion mechanism may not be efficient in a dynamic environment for the reasons we explained earlier. In addition, bogus subscriptions with a valid ticket are possible because the ticket is not tied to the requested multicast addresses.

Also, this approach is specific to PIM-SM domains and requires a high deployment cost since all the domain multicast routers need to support the receiver access control mechanism, and not the DR only, as in the previous solutions. Moreover, the scalability of this solution is questionable because the PIM routers may store a large VTL list. In addition, this approach does not address the sender access control problem.

Mobility Considerations — When a member moves to a new network and uses a remote subscription to rejoin the tree, it may face two problems. First, the ticket is distributed within a PIM-SM domain. Hence, a member that moves out of this domain cannot use its ticket. Second, since the ticket is invalidated after it is used, when the member moves even within the same domain it is necessary to request a new ticket from the DKD (Fig. 20). All these constraints may increase member join latency and affects computation resources.

IGMP Extension for Authentication of Receivers and Senders (IGMP-RAC&SAC) — In [47] Ishikawa *et al.* proposed a solution to authenticate senders and receivers based on an extension of IGMPv2 to allow for the use of a Challenge/Response procedure. In this approach, the first hop routers of the delivery tree represent ingress routers (for senders) and egress routers (for receivers). An authentication server (AS) holds a secret value for each host. This value will be verified by the authentication server when the host wishes to subscribe to a particular multicast group.

Receiver Access Control Description — When the host wishes to receive multicast traffic of a particular group, it sends its IGMP Report, including its host ID (e.g., email

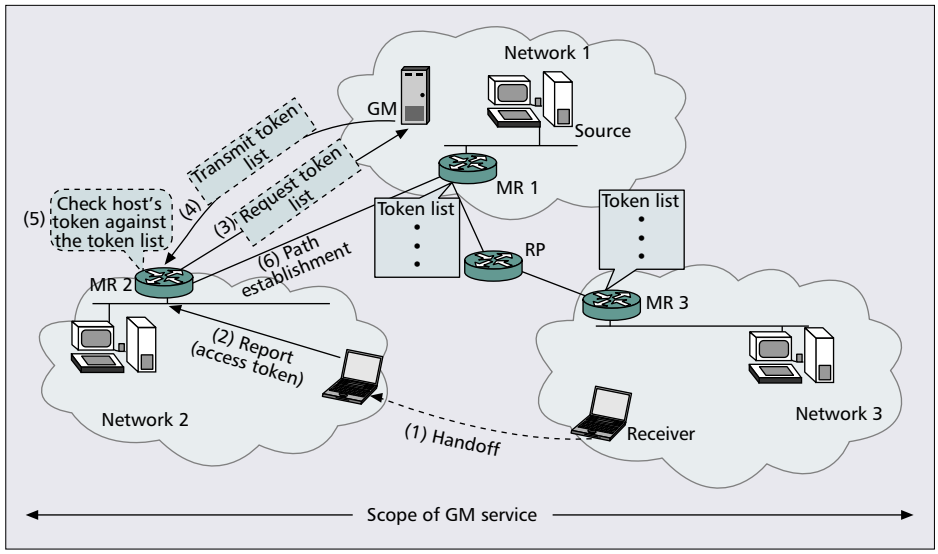


Figure 23. *Dynamic inclusion of multicast routers to support the remote subscription in the IGMP key method.*

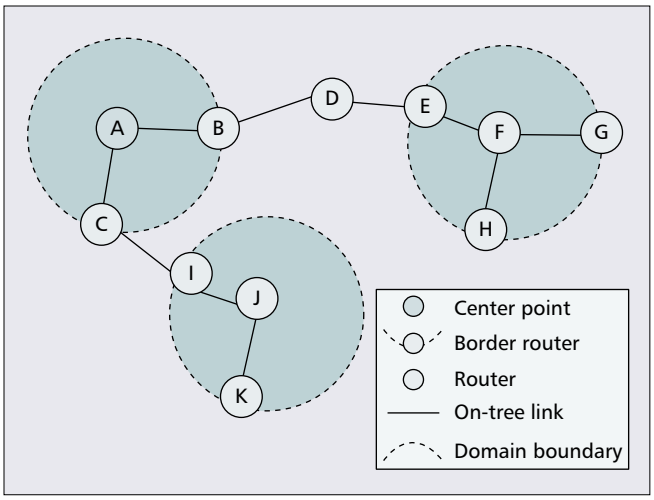


Figure 24. *HIP tree structure.*

address), to the egress router. After the message is received, the egress router triggers with the new receiver a Challenge/Response procedure (Fig. 21). The result of the challenge is calculated by the receiver based on its secret value. The egress router forwards that result along with the host ID to the authentication server in order to authenticate the host. When it receives the forwarded message, the authentication server calculates the expected hash result and compares it with the received result. If both results match, the authentication server sends to the egress router an *Access-Accept* message stating a successful authentication (Fig. 21). The egress router then informs the new receiver about the authentication success, sets a validity period for the requested group, and starts forwarding multicast traffic. When the validity period expires, the egress router sends a group-specific query to trigger a new Challenge/Response procedure with any interested receiver.

Sender Access Control Description — When a sender starts sending multicast packets, it transmits a *Sender Start* message to an *ingress router*. This message holds the user ID (e.g., email address) and the multicast group address. The remainder of the sender access control mechanism works in a similar way as in the receiver case (Fig. 21). Upon a successful authentication the ingress router starts forwarding the sender's traffic.

The present solution provides anti-replay protection based on the Challenge/Response process. In fact, an attacker cannot replay a response of a valid host because any response is tied to a random value (CV) previously generated by the router (Fig. 21). However, the problem with this solution is the lack of an effective authorization procedure. In fact, egress routers (respectively, ingress routers) do not prevent legitimate hosts from sending bogus subscriptions (respectively, bogus multicast traffic) because the ingress/egress routers are not aware of which multicast addresses the host wishes to subscribe to, or send traffic to. Besides, the proposed Challenge/Response approaches are based on static values (passwords). This provides a weak protection for passwords against *dictionary attacks* [48]. In other words, an attacker that observes both the challenge and response can test random passwords against the known challenge, and hence may discover the transmitted password. This problem is due to the low entropy of passwords, and may arise in the case of the described solution since the same password is used for all requested multicast address.

In addition, the sender access control mechanism opens vulnerabilities to bogus traffic. Indeed, an attacker may spoof the IP address of a valid sender, and then send bogus traffic during the validity period of the multicast traffic originating from the valid sender. Also, the solution does not support user exclusion.

Mobility Considerations — From a mobility perspective, the IGMP-RAC&SAC solution is interesting. Indeed, when a host rejoins the tree via the visited network, the ingress/egress router does not need to be aware of the host's validity (i.e., SV validity), as the verification will be passed to the AS (Fig. 21). This, however, comes at the cost of requiring multicast routers in the visited network that play the role of egress/ingress filtering entities. Hence, this solution is only applicable within the scope of the AS's service.

Hybrid Solutions

Hybrid solutions combine both digital signature and shared secret schemes in order to perform access control of hosts at the designated router.

IGMP Key – T. Hardjono and B. Cain [5] defined a receiver access control mechanism based on a one-time token sent along with IGMP Report messages. The token contains in particular a group ID, a host ID, an expiration date, and a symmetric key called the IGMP-key that is used by receivers to authenticate their Report messages.

Receiver Access Control Description — During group setup, the key server (KS) transmits digitally signed tokens to authorized hosts (Fig. 22). The key server also distributes to a set of multicast routers an *access token list* identified by a triple (group ID, token ID, and IGMP-Key).

When a host wishes to subscribe to a particular group, it sends an IGMP Report message along with the access token (Fig. 22). On receipt, the designated router (DR) verifies the digital signature of the token using the public key of the key server.[21] The DR then checks its access token list to verify whether an entry exists for the requested multicast address and its corresponding IGMP-key. If the verification succeeds, the multicast router validates the host's membership report and deletes the corresponding triple (group ID, token ID, IGMP-Key) from its list.

Compared to Gothic, the IGMP Key approach reduces the

[21] *Note that although the server's public key is enclosed in the token, the authors assume that the routers hold the certificate of the key server (e.g., to securely bind the server's ID to the server's public key).*

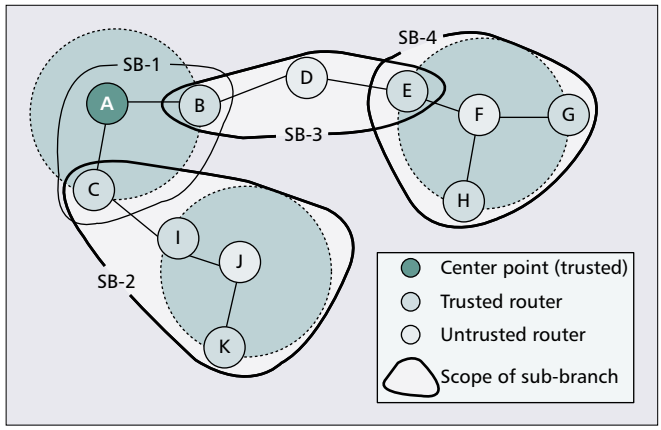


Figure 25. *Secure HIP tree under KHIP.*

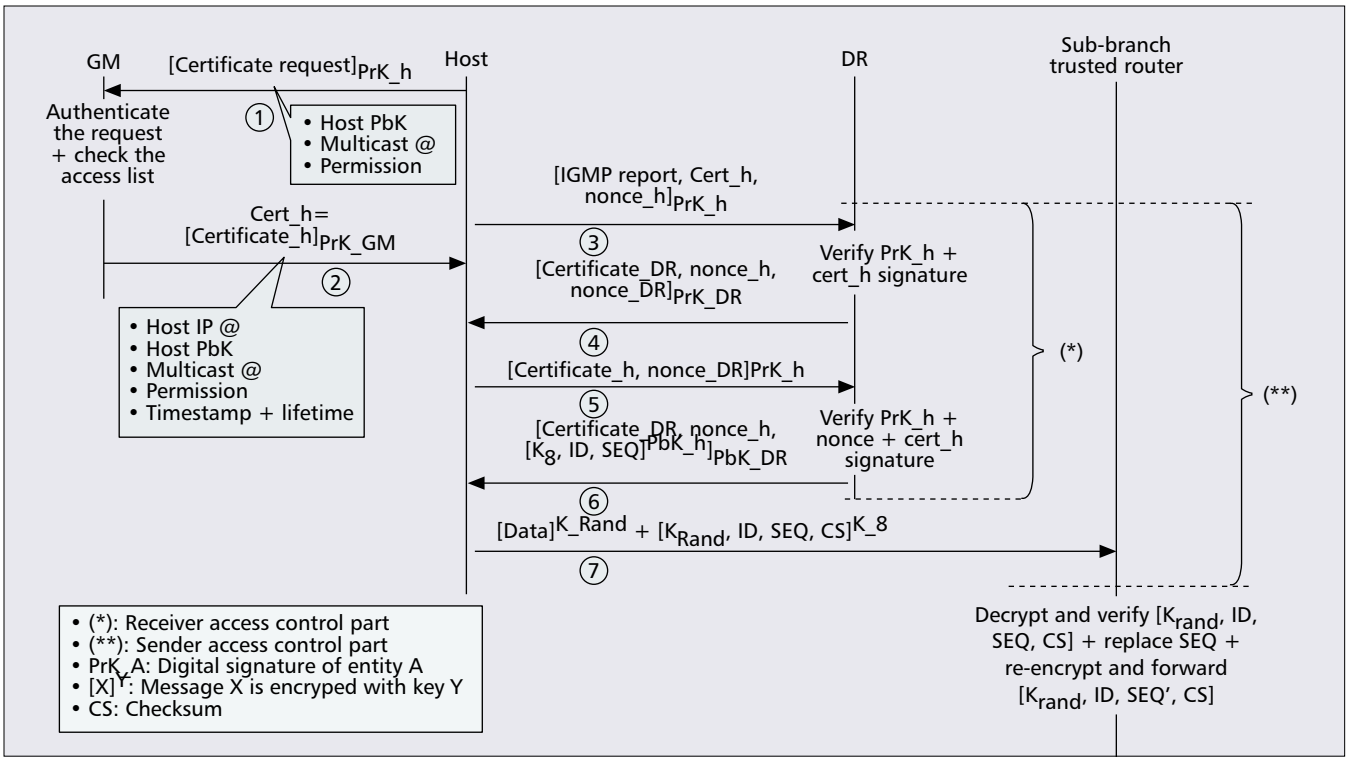


Figure 26. *Receiver and sender access control under KHIP.*

risk of replay attacks of a valid credential (token) by enabling the DR to delete the corresponding entry from the token list after the token is used. In addition, this approach provides a user exclusion mechanism as the token contains a validity period. However, the exclusion mechanism may be inefficient for the same reasons as in G-CBA CS, for example. In addition, the solution does not address the sender access control problem, and is vulnerable to DoS attacks when the multicast router receives bogus subscriptions with fake tokens. In this case, it will experience processing overheads due to extensive digital signature verifications. Also, the performance of this approach at both the receiver and the multicast router sides is limited because the receiver needs a distinct access token for each group, with a distinct IGMP key, whereas the edge multicast router may have a large amount of access tokens.

In order to reduce the memory storage at the edge router, T. Hardjono and B. Cain suggested an extension to the above approach so there will be no need to store tokens at the routers [49]. However, the proposed extension is very similar to Gothic, and hence inherits its advantages and drawbacks.

Mobility Considerations – In the IGMP Key approach, the multicast router can verify the token validity only if the router holds the corresponding token list. Otherwise, a dynamic mechanism is required to ensure the distribution of token lists to current and new routers (Fig. 23). This is particularly useful in mobile IP environments when the host wishes to use the remote subscription.

However, the dynamic distribution of tokens will be limited to the scope of the access control service of the key server. On the other hand, the host ID in the enclosed token may raise problems in the mobile environment. Indeed, if the host ID is a network-based ID (e.g., IP address), the host cannot use the remote subscription. To overcome this problem, the mobile host needs to request a new token from the key server. This, however, will increase the rejoin latency and introduce a processing overhead at the host (re-authentication with the key server and key decryption operations). If the host ID is not tied to a network location (e.g., in the case of email addresses), an unauthorized host can copy the token from its current network, move to a new network, and replay the token in an unauthorized membership request to the local multicast router. If that router holds the appropriate token list, it may validate the token.

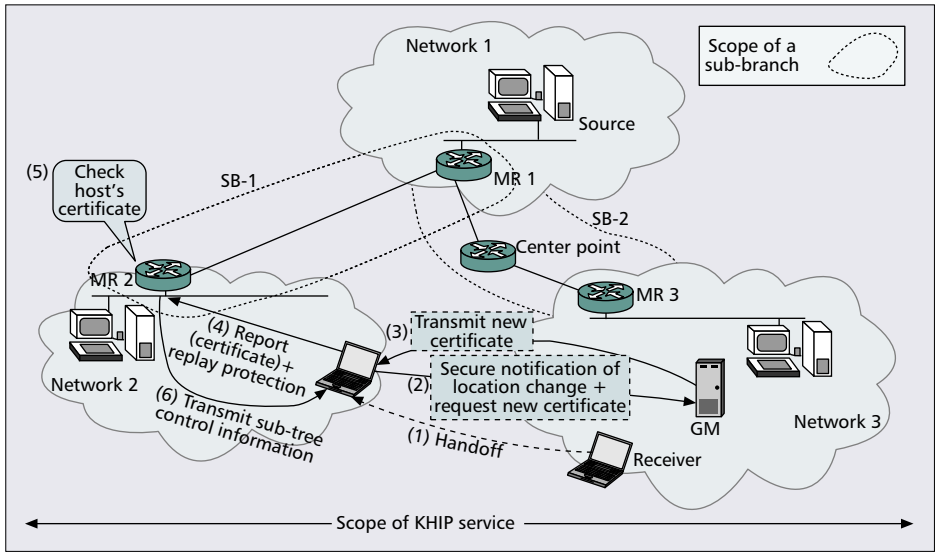


Figure 27. *KHIP applicability to support the remote connection to the tree.*

Keyed Hierarchical Multicast Routing Protocol (KHIP) — KHIP (Keyed Hierarchical Multicast Routing Protocol) [50] is a secure, hierarchical multicast routing protocol that was specified for securing the multicast routing protocol (against untrusted routers), but provides as well receiver and sender access control mechanisms, and integrates the distribution of encryption keys. KHIP extends the Hierarchical Multicast Routing Protocol (HIP) by introducing mechanisms for the authentication and authorization of hosts and trusted routers. The HIP protocol [51] is based on the Ordered Core Based Tree protocol (OCBT)[22] [52] and enables the routing of multicast data between heterogeneous multicast domains (each domain uses its proper multicast routing protocol). In HIP, the multicast tree is constructed of OCBT routers and *virtual OCBT routers*. Each virtual OCBT is mapped to a domain by organizing the border routers of the domain to simulate the output of a single OCBT router (Fig. 24). Also, HIP uses border routers of the multicast domain as OCBT *cores*.

KHIP (Fig. 25) places trust in OCBT cores and some routers to maintain correctly the multicast tree (protection against untrusted routers)[23] and help to ensure receiver and sender access control. Also, the multicast tree is divided into a number of sub-branches, each with an OCBT core as a root.

Receiver Access Control Description — 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 (Fig. 26) such as the member's IP address, its public key, the range of authorized addresses, and per-group permission (*initiator*, *sender*, *receiver*, and *group terminator*). The authors did not describe how host access control could be performed in the DR, and they only proposed using the same mechanisms as those enabling trusted routers of a given sub-branch to authenticate with their core.[24] We now briefly explain how the mechanisms used by trusted routers could be interpreted from the viewpoint of receiver access control.

First, the host initiates with the DR two exchanges of digitally signed messages, holding the certificate of the transmitter along with a random nonce for replay protection (Fig. 26). The DR terminates the exchanges by validating the host's membership request and transmitting to the host the required information to start receiving or sending multicast traffic (Fig. 26). That information includes a *starting sequence number* and a branch key (K_B)[25] both used for data transmission.

Sender Access Control Description — As Fig. 26 shows, the sender access control mechanism encloses the receiver access control. After this latter succeeds, a receiver can send multicast traffic as a new authorized sender. To achieve this, the receiver creates a random encryption key (K_{Rand}) for data encryption. It then appends to the data an amount of control information to form the whole multicast packet. The control information is encrypted with the branch key (K_B) (Fig. 26). This information consists of the random key (K_{Rand}), the host's branch ID, the next sequence number, and a checksum of the encrypted data. The branch ID along with the sequence number (both received from the DR) will be used by the sender as nonces in order to prevent replay attacks. Once the packet is formed, it is transmitted from the sender's sub-branch over the whole tree. During the transit of the sender's traffic, the included control information is controlled by trusted routers interconnecting different branches (Fig. 25) to ensure a proper transmission of the source's traffic.[26]

KHIP limits the effect of flooding attacks to the scope of a sub-branch, because the sender's packets are controlled by a trusted router before being forwarded to another sub-branch. In addition, KHIP provides nonce-based anti-replay protection both for the sender's traffic and the receiver's membership requests. However, the access control mechanism may introduce a high processing cost and risks for DoS attacks at both DRs and cores. Indeed, DRs and cores may perform multiple digital signature verifications to validate the host's subscription. Also, the sender access control mechanism is not performed only at the edge of the delivery tree. Instead, the sender's packets are controlled and reprocessed sub-branch by sub-branch. This will increase data delivery delays and introduce a high deployment cost as multiple on-tree routers may be involved together in controlling a single sender. In addition, the user exclusion mechanism has the same drawbacks as G-CBA CS, since the host's certificate has a pre-defined lifetime. Furthermore, although not described in this section, frequent removals and reconstructions of branches due to the departure of trusted routers will decrease even more the efficiency of the protocol. In fact, when a trusted router leaves its sub-brunch, the root updates that sub-branch with a new branch key and a new starting sequence number, both encrypted with the public key of each remaining router and sub-branch member.[27]

Mobility Considerations — Some of the mobility issues that arise in KHIP have already been seen through the previous approaches. First, the host's IP address is tied to the host's certificate, while the sub-branch key relates to the branch to which the user is connected. Hence, if an authorized host wishes to rejoin the tree via the visited network upon its movement, this host should request a new certificate from the group manager and request the corresponding control information from the DR of the new sub-branch, including a sub-branch key and a starting sequence number (Fig. 27).

This, however, will increase the rejoin latency and introduce processing overheads at the host (re-authentication with thegroup manager and message exchanges with the DR).

On the other hand, the solution is limited to the scope of the KHIP service, which only covers OCBT domains.

[22] OCBT extends CBT in order to eliminate message loops that may occur in a CBT tree. This is achieved by ordering the way in which multicast routers and cores join the multicast tree.

[23] Control messages exchanged between trusted routers carry nonces (for replay protection) and are digitally signed.

[24] The router authenticates with the core through two secure message exchanges that include the exchange of their respective certificates. The core also sends to the router the branch key, the branch ID, and a starting sequence number for data forwarding.

[25] Members of the same sub-branch keep track of a common sequence number and share the same branch key.

[26] When a trusted router receives traffic from one of its sub-branches, it decrypts, verifies, and then updates the received control information. The update consists in replacing the sequence information with a new one proper to the next sub-branch. The control information is then re-encrypted and transmitted to that sub-branch.

[27] The root acts as a subgroup-manager, and thus it should know the hosts of its sub-branch even if the root is not a DR.

Approach			IP protocol used	Used credential	RAC	SAC	Host exclusion	Anti-replay protection	Bogus subscription w/ valid cred.	Overhead risks in multicast router	DoS risks in multicast router
Dig. sig.	Basic receiver access ctrl.		IPv4	Digital signature	Y	N	N	N	Y	Digital sig. verification of membership request	High
	SMKD		IPv4	Token	Y	N	Y	Y	N	Digital sig. verification (token + router-GKDC message exchanges)	High
	Gothic		IPv4 & IPv6	Capacity	Y	N	Y	Y[1]	N	Digital sig. verification of cap.	High
	SMRAC		IPv4	Token	Y	N	Y	Y[1]	N	Digital sig. verification of the token	High
	G-CBA	BS	IPv6	GC's signature	Y	N	N	Y	N	Digital sig. verification of membership request	High
	G-CBA	CS	IPv6	Auth. Certificate	Y	N	Y	Y	N	Digital sig. verifications (certificate + membership request)	High
	Auth. stamp		IPv4	Auth. stamp	Y	Y	Y	Y	N	Digital sig. verification (auth. stamp + DR-GM message exchanges)	High
Shared secret	IGMP mess. auth.		IPv4	GSA shared key	Y	N	N	Y	N	—	High
	MLDA		IPv6	Password	Y	N	N	Y	Y	—	Low
	PIM-SM-RAC		IPv4 & IPv6	Ticket	Y	N	Y	Y	Y	Memory storage of tickets + ticket verifications	High
	HASM		IPv4	Ticket	Y	Y	Y	Y	Y	—	Low
	IGMP-RAC&SAC		IPv4	Secret Value (e.g., password)	Y	Y	Y	Y	Y	Memory storage of secret values	Low
Hybrid	IGMP-key		IPv4	Access Token	Y	N	N	Y	N	Memory storage + digital signature verification of the access token	High
	KHIP		IPv4	Auth Certificate	Y	Y	Y	Y	N	Digital sig. verification of certificates + data decryption/ re-encryption	High

[1] Replay attacks are not very likely as host IP address is tied to the capability

■ Table 1. *Comparative table: stationary environment.*

Approach			Credential tied to user location	Invalid cred. when rejoining	Fast access ctrl. cost upon a rejoin	Risk of replay cred. in another network	PKI inter-operability issues?	Solution scope
Dig. sig.	Basic receiver access ctrl.		N	Y	N	Y	Y	Interoperable PKI domains
	SMKD		?	Y	N	Y	Y	Bi-directional shared trees with multicast security functionalities
	Gothic		Y	Y	N	N	Y	Interoperable PKI domains within the scope of ACS service
	SMRAC		Y	Y	N	N	Y	Interoperable PKI domains within the scope of the GM service
	G-CBA	BS	N	N	N	N	N	Global[5]
		CS	Y	N	Y	N	Y	GC service coverage
	Auth. stamp		Y	Y	Y	N	Y	GM service
Shared secret	IGMP msg. auth.		N	N	Y[2]	N	N	GDOI-capable IGMP routers[6]
	MLDA		N	N	Y[3]	N	N	MLDA-capable routers
	PIM-SM-RAC		N	Y	N	N	N	PIM-SM domains
	HASM		Y	Y	Y	N[4]	N	A/A service coverage
	IGMP-RAC&SAC		N	N	Y	N	N	Egress/ingress routers within AS's service
Hybrid	IGMP-Key		N[1]	N[1]	N	N[1]	Y	Key server service scope
	KHIP		Y	Y	N	N	Y	OCBT domains

"?": Not specified in the solution.

[1] If host ID is a network-based ID, then the values of the second, third, and fifth columns will be "Y".

[2] It might be "N" in case the DR of the visited network requires contacting the GCKS as a new GSA member.

[3] It might be "N" in case of an inter-domain movement.

[4] It might be "Y" in case host ID is a network-based ID.

[5] The router should support the G-BCA algorithm.

[6] GDOI: Group Domain of Interpretation [55] is a group key management protocol.

■ Table 2. *Comparative table: the mobile IP environment.*

Although this may avoid interoperability issues of PKI infrastructures on the scope of the KHIP service,[28] an authorized host cannot use its certificate beyond OCBT domains.

Summary

This section will sum up the characteristics of the different approaches we presented in the previous sections, and give a comprehensive view of their limitations.

First of all, few solutions addressed the sender access control problem (Table 1). Also, some of the proposed mechanisms lack efficiency, e.g. IGMP-RAC&SAC and authorization stamp, where a security hole exists because the sender's traffic is periodically controlled. KHIP resolves the problem by involving the router in a continuous control of the sender's traffic. This control, however, may be a router's bottleneck because the router may be involved in high-cost operations (decryption/encryption operations and data sequence updates). On the other hand, if we look at the types of credentials introduced by the existing approaches, we can note that some solutions only use the authentication information as credentials. This is particularly true for Basic RAC and IGMP-RAC&SAC. In these solutions, the access control at the multicast router is limited to authenticating host requests. Hence, the multicast router has no control of host access

[28] *For example, a PKI infrastructure could be mapped to the KHIP service.*

rights, such as the authorized multicast addresses. This will open vulnerabilities to bogus subscriptions by valid (authenticated) members.

Besides the G-CBA-BS solution uses group authentication-based access control rather than an individual authentication of hosts. In this solution the multicast address is generated based on a group public key so that its corresponding private key is used to authenticate the host's request. With this scheme, the access control at the multicast router can succeed only if the router successfully authenticates the host's request based on the group public key. As we can note, by providing a group authentication-based mechanism rather than an individual authentication of hosts, we can provide a type of authorization procedure at the multicast router.

The problem with the proposed group authentication-based access control is that the authentication information is tied to a single multicast group. Hence, the multicast router will perform for a given host as many authorization procedures as there are requested multicast groups. This may have a negative impact on solution performance, especially when the authentication is based on digital signatures (e.g., G-CBA). This problem is not due to the group authentication-based access control concept, as it may arise as well for the solutions where the credentials (e.g., certificates) enclose a few or a single multicast group (e.g., Gothic). SMKD resolves the problem by enclosing multiple group IDs in the credential so that the multicast router can perform a single host authorization procedure for multiple groups. This is particularly valuable for the access control support of hosts wishing to subscribe to multiple groups.

Regarding the access control cost, compared to shared secret-based solutions, both digital signature-based solutions and Hybrid solutions may introduce a high processing cost at the multicast router due to the authentication information. In fact, hash authentications, typically used in the shared secret-based approaches, have a low computational cost compared to digital signatures. More specifically, hash authentications are about two to four order of magnitude faster than digital signatures [53]. Moreover, the high authentication cost of digital signature increases the risk of DoS attacks in the network entity that verifies digital signatures [54]. In the case of digital-signature based approaches, the multicast router may be the main victim of such attacks because of the verification of host requests.

On the other hand, many solutions defined a user exclusion mechanism. However, this issue has not been efficiently addressed since almost all the proposed approaches use a validity period for the user's credential. This, however, will not be efficient in the case where membership duration is unknown.

Mobility Considerations — Our study of the applicability of the existing solutions in mobile IP environments highlighted several issues and challenges. Table 2 summarizes the issues that may be encountered if a mobile member rejoins the tree via the visited network. In brief, the mobile member may face two main problems.

First, the credential may be invalid in the new network because of one of the following reasons:

- The host's credential is tied to its network location (e.g., the host's IP address in Gothic).
- A pre-established security context. For instance, the router needs to hold the host's public key (Basic Receiver Access Control), or tokens (IGMP-Key) before performing host access control.
- One-time credential usability as an anti-replay attack mechanism (e.g., IGMP Key, PIM-SM-RAC).

The invalidation of the member's credentials may generate time-consuming operations for mobile members. This is particularly true when the member needs to re-authenticate with the group manager and routers based on digital signatures (e.g., Gothic and G-CBA- CS). Furthermore, such expensive operations increase the rejoin latencies.

The second main problem relates to the scope of the access control service. In fact, protocol-dependent solutions such as KHIP, SMKD, and PIM-SM-RAC do not work beyond the domains where the underlying protocol (respectively, OCBT, bi-directional shared trees, and PIM-SM domains) has been deployed .

Other domain-dependent issues may arise due to interoperability problems, such as with the solutions that are based on certificate infrastructures (e.g., Gothic and G-CBA-CS). These solutions may face PKI interoperability issues if a mobile member moves out of its PKI domain. In this case, the certificate enclosed in the member's credentials may appear invalid in the new PKI domain, and hence the member's credentials will be rejected.

Interoperability appears as a key condition for the extensibility of the scope of the multicast access control service. Such extensibility leads to a broader support of multicast access control in mobile IP environments. From the perspective of the mobility question in our study, we can classify the interoperability issues into two categories: *intra-infrastructure interoperability* and *inter-infrastructure* interoperability.

The first class concerns the interoperability between homogeneous infrastructures, such as PKI-PKI interoperability. Regarding that category, some multicast access control solutions are built upon infrastructures that show more interoperability potential than others. For example, Gothic is built upon a PKI infrastructure, which could benefit from interoperability structures such as cross certificates and BCA [36]. Other infrastructures may be more vulnerable to interoperability issues. For example, the problem of interoperability has not been addressed for the group key management schemes (group key distribution and update), which differ in several features, such as the physical architecture (centralized, decentralized, distributed) [56]. Hence, the SMKD solution, which is based on a proper decentralized architecture (i.e., a GKDC hierarchy-based) to ensure the group key management, is potentially less extensible to a larger scope than Gothic.

The second interoperability class is more problematic as it deals with the interoperability between heterogeneous infrastructures such as a PKI infrastructure and a group key management infrastructure. A basic solution to this interoperability problem could be to provide the member with multi-access control support so that it can execute the appropriate multicast access control service that corresponds to its current location.

Finally, although the G-CBA-BS solution lacks both a user exclusion mechanism and the support of sender access control, it overcomes the above mobility-related issues. Therefore, G-CBA-BS could be the solution that shows the best applicability in mobile environments. It is true that if the mobile member continues to send or receive multicast traffic via tunneling with its home agent, the access control mechanisms may not face the issues we summarized above. However, that option has some limitations, such as non-optimal routing of multicast traffic and QoS-related issues [14]. This is why other options for re-subscription via the visited network have been proposed [14]. As a result, the access control mechanism needs to consider those options.

CONCLUSION

In this article we studied the existing solutions for receiver and sender access control, and investigated their efficiency both in stationary and Mobile IP environments. We classified the existing solutions into three classes: Digital Signature-based, Shared Secret-based, and Hybrid solutions. Each solution has some advantages and drawbacks with respect to its applicability both in the stationary and mobile scenario. We will now summarize the main issues and challenges among the existing solutions. We will also provide considerations that help define a scalable and flexible multicast receiver and sender access control service with the support of mobile members.

• **Sender access control**: Few solutions addressed the sender access control problem, and almost all of them open vulnerabilities to bogus traffic. This problem needs to be addressed in depth, as recommended in [57]. Indeed, bogus traffic of an illegitimate sender may have a higher impact than bogus Report messages (i.e., illegitimate receiver) because the distribution tree acts as an *amplifier* of the source's traffic to ensure the distribution to the whole group.

• **User exclusion**: Some proposals are based on fixing a validity period for membership duration. Although this might work in some scenarios, it will not be efficient in the case where membership duration is unpredictable.

• **DoS attack risks**: The public key authentication has a high cost. Hence, Digital Signature-based and Hybrid solutions are vulnerable to DoS attacks. Although these risks are concentrated on the edge of the multicast tree, their consequences may impact several groups and network applications because the attacked router may interact with several network devices (e.g., routers, servers, etc). In brief, overcoming bogus subscriptions (from illegitimate receivers) and bogus traffic (from illegitimate senders) at the edge of the multicast tree is attractive. However, this needs to be achieved with lightweight mechanisms in order to avoid additional DoS attack risks due to the access control mechanisms themselves.

• **Mobility impact**: The impact of member mobility on the access control solutions depends on how the member wishes to continue its subscription to the group, via the home agent (i.e., home network) or via the visited network. In the case of a connection to the home network, the access control service will behave as if the member was a fixed entity. In this case, there will be no mobility-related issues. However, other options for re-subscription via the visited network exist as an alternative to home agent-based re-subscription [14]. Those options need an appropriate access control support to the delivery tree. Without such a support, the access control solutions may challenge two main issues. First, member credentials may be invalid in the visited network. To acquire a new credential, the mobile member may perform high operation costs and suffer from re-join latencies. The second problem that can arise in the case of a re-subscription via the visited network is the scope of the access control service, which may be limited to specific domains. Hence, members cannot be assured of rejoining the tree locally if they move beyond the scope of the access control service (i.e., defined domains). As part of this problem, interoperability issues may arise, for example in the case of PKI-dependent access control.

In addition to the limitations we describe above, there are features that need to be considered.

• **Dynamic access control of senders and receivers**: The group manager needs to provide a dynamic per-user access right (e.g., authorized multicast addresses) in order to support membership change (join/leave) of a member during the time. This dynamic access control may include, as well, the control of the multicast address space usage [1].

• **Flexible receiver access control**: The receiver access control service should consider the behavior of the group membership protocol. Specifically, the IGMP/MLD routers may send Query messages periodically or in response to Report messages. The question of adapting the receiver access control service to the router's queries has not been explored by the existing schemes, and merits particular attentions.

• **Group security policy**: A specific security policy is needed to provide security-related rules for receiver and sender access control to the delivery tree. For example, such a policy may specify the conditions upon which an authorized user can join an additional multicast group, the conditions for user exclusion, an authorization level (e.g., a range of authorized multicast addresses for a user), etc. It would be attractive that the expected policy be part of, or at least interact with, other multicast security policies [58]. In fact, T. Harjdono and B. Weis [58] suggest using a policy management framework for possible rules governing different multicast security services, such as user registration, group rekeying, and source authentication. We believe there may be common rules governing those services and the access control service to the delivery tree, for example, user exclusion in the case of access control to the delivery vs. user exclusion (*revocation*) during group rekeying.

• **Centralized vs. hierarchical/distributed authorization infrastructures**: 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 subgroup managers. This is also useful for mobile environments where a mobile member needs well adapted access control services when it moves into foreign "domains."

• **Mobility support**: In mobile environments, the multicast application should be aware of the scope of the access control service. In this situation, an authorized user that moves to a new network should react quickly to reconnect with its home agent, and hence reduce rejoin latencies. Alternatively, a global access control mechanism that enables multicast routers to efficiently perform a location-independent access control of mobile members could be an attractive perspective that needs to be investigated in depth, for example basing access control on *attribute certificates* [59]. Finally, another factor that should be considered in a mobile scenario is to address the problem of identifying trusted multicast routers when the host reconnects to the multicast tree via the visited network.

REFERENCES

[1] R. Lehtonen and J. Harju, "Controlled Multicast Framework," *Proc. 27th Annual IEEE Conf. Local Comp. Net. (LCN)*, Florida, 2002, pp. 565–71.

[2] T. Hardjono, and L. R. Dondeti, *Multicast and Group Security*, Artech House — Computer Security Series, 2003.

[3] T. Hardjono and B. Cain "Key Establishment for IGMP Authentication in IP Multicast," *ECUMN*, France, Oct. 2000, pp. 247–52.

[4] B. Fenner *et al.*, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)," Internet draft, draft-ietf-pim-sm-v2-new-11.txt, Oct. 2004 (work in progress).

[5] D. Ballardie, "Core Based Trees (CBT version 2) Multicast Routing Protocol Specification," Internet RFC 2189, Sept. 1997.

[6] S. Deering, "Host Extension for IP Multicasting," Internet RFC 1112, Aug. 1989.

[7] J. Moy, "Multicast Extensions to OSPF," Internet RFC 1584, Mar. 1994.

[8] W. Fenner, "Internet Group Management Protocol, Version 2," RFC 2236, Nov. 1997.

[9] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Internet Group Management Protocol, Version 3," RFC 3376, Oct. 2002.
[10] S. Deering, W. Fenner, and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6," Internet RFC 2710, Oct. 1999.
[11] Rolland Vida *et al.*, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," RFC 3810, June 2004.
[12] C. Perkins, "IP Mobility Support for IPv4," RFC 3344, Aug. 2002.
[13] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.
[14] I. Romdhani *et al.*, "IP Mobile Multicast: Challenges and Solutions," *IEEE Commun. Surveys and Tutorials*, vol. 6, no. 1, 1st Quarter 2004.
[15] R. S. Sandhu and P. Samarati, "Access Control: Principle and Practice," *IEEE Commun. Mag.*, vol. 32, no. 9, 1994, pp. 40–48.
[16] R. Shirey, "Internet Security Glossary," RFC 2828, May 2000.
[17] G. P. Kumar and P. Venkateram, "Security Management Architecture for Access Control to Network Resources," *IEEE Proc. Comp. and Digital Techniques*, vol. 144–6, Nov. 1997, pp. 362–70.
[18] J. Kohl, and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, Sept. 1993.
[19] P. Judge and M. Ammar, "Gothic: A Group Access Control Architecture for Secure Multicast and Anycast," *IEEE INFOCOM*, New York, June 2002, pp. 1547–56.
[20] A. Perrig *et al.*, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *Proc. IEEE Symp. Security and Privacy (S&P 2000)*, May 2000, pp. 56–73.
[21] B. Fenner and D. Meyer, "Multicast Source Discovery Protocol (MSDP)," RFC 3618, Oct. 2003.
[22] P. Rajvaidya, K. Ramachandran, and K. C. Almeroth, "Detection and Deflection of DoS Attacks against the Multicast Source Discovery Protocol," Technical Report, Department of Computer Science, University of California, Santa Barbara, July 2002.
[23] S. Bhattacharyya *et al.*, " An Overview of Source-Specific Multicast (SSM)," RFC 3569, July 2003.
[24] Y. K. Dalal and R. M. Metcalfe. "Reverse Path Forwarding of Broadcast Packets," *Commun. ACM*, vol. 21, no. 12, Dec. 1978, pp. 1040–48.
[25] N. Wang and G. Pavlou, "Scalable IP Multicast Sender Access Control for Bi-directional Trees," *Proc. 3rd Int'l. Wksp. Networked Group Commun. (NGC'2001)*, London, J. Crowcroft, M. Hofmann, Eds., Springer, Nov. 2001, pp. 141–158.
[26] B. Fenner *et al.*, "Multicast Source Notification of Interest Protocol," IETF draft, draft-ietf-magma-msnip-05.txt, Mar. 2004, (work in progress).
[27] C. Perkins, P. R. Calhoun, and J. Bharatia, "Mobile IPv4 Challenge/Response Extensions (revised)," Internet draft, draft-ietf-mip4-rfc3012bis-03.txt, Dec. 2004 (work in progress).
[28] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," RFC 3776, June 2004.
[29] Protocol for Carrying Authentication for Network Access (pana), http://www.ietf.org/html.charters/pana-charter.html.
[30] J. Dankers *et al.*, "Public Key Infrastructure in Mobile Systems," *Electronics & Commun. Eng. J.*, vol. 14, Oct. 2002, pp. 180–90.
[31] G. Montenegro and C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses," *ISOC NDSS'02*, 2002.
[31] National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) PUB 186, Digital Signature Standard (DSS), U.S. Department of Commerce, 19 May 1994.
[32] National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) PUB 180-1, Secure Hash Standard (SHS), U.S. Department of Commerce, Washington, 1995.
[33] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280, Apr. 2002.
[34] A. Ballardie, "Scalable Multicast Key Distribution," RFC 1949, May 1996.
[35] A. Ballardie, "Core Based Trees (CBT version 2) Multicast Routing," RFC 2189, Sept. 1997.
[36] W. T. Polk, N. E. Hastings, and A. Malpani, "Public Key Infrastructures that Satisfy Security Goals," *IEEE Internet Computing*, vol. 7, July–Aug. 2003, pp. 60–67.
[37] C. Castelluccia and G. Montenegro, "Securing Group Management in IPv6 with Cryptographically Based Addresses," *Proc. 8th IEEE Int'l. Symp. Comp. and Commun.*, Turkey, July 2003, pp. 588–93.
[39] C. Ellison *et al.*, "SPKI Certificate Theory," RFC 2693, Sept. 1999.
[40] T. Aura "Cryptographically Generated Addresses (CGA)," *ISC'03*, Oct. 2003, pp. 29–43.
[41] T. Ballardie and J. Crowcroft, "Multicast-Specific Security Threats and Counter-Measures," *Proc. IEEE Symp. Net. and Distributed System Security*, 1995, pp. 2–16.
[42] W. Simson, "PPP Challenge Handshake Authentication Protocol (CHAP)," RFC 1994, Aug. 1996.
[43] T. Hayashi *et al.*, " Multicast Listener Discovery Authentication Protocol (MLDA)," Internet Draft, draft-hayashi-mlda-02.txt, Apr. 2004 (work in progress).
[44] A. Van Moffaert and O. Paridaens, "Security Issues in Internet Group Management Protocol version 3 (IGMPv3)," Internet Draft, draft-irtf-gsec-igmpv3-security-issues-01.txt, Feb. 2002 (work in progress).
[45] B. Coan *et al.*, "HASM: Hierarchical Application-Level Secure Multicast," Internet Draft, draft-coan-hasm-01.txt, Oct. 2002, (Work in Progress).
[46] T. Hardjono, "Router-Assistance for Receiver Access Control in PIM-SM." *Proc. IEEE Int'l. Symp. Comp. Commun. (ISCC)*, Antibes, France, July 2000, pp. 687–92.
[47] N. Ishikawa, N. Yamanouchi, and O. Takahashi, "An Architecture for User Authentication of IP Multicast and Its Implementation," *IEEE/APAN Internet Wksp. '99 (IWS'99)*, Japan, Feb. 1999, pp. 81–87.
[48] E. Rescorla, "A Survey of Authentication Mechanisms," Internet Draft, draft-iab-auth-mech-03.txt, Mar. 2004 (work in progress).
[49] H. He, T. Hardjono, and B. Cain, "Simple Multicast Receiver Access Control," Internet draft, draft-irtf-gsec-smrac-00.txt, Nov. 2001 (work in progress).
[50] C. Shiels and J. J. Garcia-Luna-Aceves, "KHIP: A Scalable Protocol for Secure Multicast Routing," *Proc. ACM SIGCOMM'99*, 1999, pp. 53–64.
[51] C. Shields and J. J. Garcia-LunaAceves, "The HIP Protocol for Hierarchical Multicast routing," *Proc. ACM SIGACT-SIGOPS Symp. Principles of Distributed Computing (PODC '98)*, Mexico, June 1998, pp. 257–66.
[52] C. Shields and J. J. Garcia-Luna-Aceves, "The Ordered Core Based Tree Protocol," *Proc. IEEE INFOCOM '97*, Apr. 1997, pp. 884–91.
[53] L. Eschnehauer and V. D. Gligor, "A Key Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conf. Comp. and Commun. security (CCS'02)*, Nov. 2002, pp. 41–47.
[54] C. Meadows, "A Formal Framework and Evaluation Method for Network Denial of Service," *Proc. 12th IEEE Computer Security Foundations Wksp.*, 1999, pp. 4–13.
[55] M. Baugher *et al.*, "The Group Domain of Interpretation," RFC 3547, July 2003.
[56] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Computing Surveys (CSUR)*, vol. 35, Sept. 2003, pp. 309–29.
[57] P. Judge and M. Ammar, "Security Issues and Solutions in Multicast Content Distribution: A Survey," *IEEE Network*, 2003, pp. 30–36.
[58] T. Hardjono and B. Weis, "The Multicast Group Security Architecture," RFC 3740, Mar. 2004.
[59] S. Farrell, and R. Housley, "An Internet Attribute Certificate Profile for Authorization" RFC 3281, Apr. 2002.

ADDITIONAL READING

[1] S. Kent and R. Artkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.

[2] D. Harkens and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998.
[3] R. Rivest, "MD5 Digest Algorithm," RFC 1321, Apr. 1992.
[4] J. Vollbrecht *et al.*, "AAA Authorization Framework," RFC 2904, Aug. 2000.
[5] S. Glass *et al.*, "Mobile IP Authentication, Authorization, and Accounting Requirements," RFC 2977, Oct. 2000.
[6] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Info. Theory*, 1976, pp. 644–54.
[7] W. Stallings, *Cryptography and Network Security: Principle and Practices*, 3rd Ed., Prentice Hall, 2003.
[8] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, 1978, pp. 120–26.

BIOGRAPHIES

MOUNIR KELLIL (Mounir.Kellil@motorola.com) is a Ph.D. student and research engineer in Motorola Labs-Paris, and a member of the networking team of the HeuDiaSyc Laboratory of the University of Technology of Compiegne (UTC), France. He received an engineer diploma in computer sciences from the University of Science and Technology Houari Boumediène (USTHB), Algiers in 1999, and a M.Sc. in networking from the University of Versailles (UVSQ), France in 2001. His current research interests include multicasting, wireless networks, Mobile IP, wireless security, and multicast security.

IMED ROMDHANI (Imed.Romdhani@motorola.com) is a Ph.D. student and research engineer at Motorola Labs-Paris, and a member of the networking team of the HeuDiaSyc Laboratory of the University of Technology of Compiegne (UTC), France. He received an engineer diploma in computer sciences from the National School of Computer Sciences (ENSI), Tunis, Tunisia in 1998, and a M.Sc. in networking from the Louis Pasteur University of Strasbourg (ULP), France in 2001. His current research interests include multicasting, wireless and moving networks, mobile IP, and QoS.

HONG-YON LACH (Hong-Yon.Lach@motorola.com) received a B.S. degree in computer science, with a minor in economics, in 1987 from the American University of Paris, France. He is currently managing a team of researchers at Motorola Labs-Paris, working on IP-based mobile multiparty multimedia networking. He has extensive experience in the research and development of OSI and IP communication protocols. He is a contributor to standardization projects, including ETSI Project HIPERLAN Type 1, ETSI Project MESA, and IETF. He also participates in many EU projects in the ESPRIT, ACTS, FP5, and FP6 programs.

ABDELMADIID BOUABDALLAH (bouabdal@utc.fr) received the engineer diploma in computer science from the University of Technology of Algiers (USTHB) in 1986, and received the Master (DEA) degree and Ph.D. from the University of Paris-sud Orsay (France) in 1988 and 1991, respectively. From 1992 to 1996 he was assistant professor at the University of Evry-Val-d'Essonne, France. Since 1996 he has been a professor in the department of computer engineering at the University of Technology of Compiegne (UTC), where he leads the networking and optimization research group. His research Interests include Internet QoS and security, unicast/multicast communication, and fault tolerance in wired/wireless networks and distributed systems.

HATEM BETTAHAR (bettahar@utc.fr) received the M.S. degree and Ph.D. degree in computer science for work on multicast routing and QoS in IP networks from the University of Technology of Compiegne (UTC), France in 1998 and 2001, respectively. Since 2001 he has been an assistant professor in the department of computer engineering at UTC. He is a member of the networking and optimization research group within the Heudiasyc UMR-CNRS-6599 Laboratory. His research Interests include Internet QoS routing, multicast communication, multicast security, and Mobile