International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# X.1101

(05/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Multicast security

## Security requirements and framework for multicast communication

Recommendation ITU-T X.1101

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY**

| | |
|---|---|
| PUBLIC DATA NETWORKS | X.1–X.199 |
| OPEN SYSTEMS INTERCONNECTION | X.200–X.299 |
| INTERWORKING BETWEEN NETWORKS | X.300–X.399 |
| MESSAGE HANDLING SYSTEMS | X.400–X.499 |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | X.600–X.699 |
| OSI MANAGEMENT | X.700–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | X.850–X.899 |
| OPEN DISTRIBUTED PROCESSING | X.900–X.999 |
| INFORMATION AND NETWORK SECURITY | |
| General security aspects | X.1000–X.1029 |
| Network security | X.1030–X.1049 |
| Security management | X.1050–X.1069 |
| Telebiometrics | X.1080–X.1099 |
| SECURE APPLICATIONS AND SERVICES | |
| **Multicast security** | **X.1100–X.1109** |
| Home network security | X.1110–X.1119 |
| Mobile security | X.1120–X.1139 |
| Web security | X.1140–X.1149 |
| Security protocols | X.1150–X.1159 |
| Peer-to-peer security | X.1160–X.1169 |
| Networked ID security | X.1170–X.1179 |
| IPTV security | X.1180–X.1199 |
| CYBERSPACE SECURITY | |
| Cybersecurity | X.1200–X.1229 |
| Countering spam | X.1230–X.1249 |
| Identity management | X.1250–X.1279 |
| SECURE APPLICATIONS AND SERVICES | |
| Emergency communications | X.1300–X.1309 |
| Ubiquitous sensor network security | X.1310–X.1339 |
| CYBERSECURITY INFORMATION EXCHANGE | |
| Vulnerability/state exchange | X.1520–X.1539 |
| Event/incident/heuristics exchange | X.1540–X.1549 |
| Exchange of policies | X.1550–X.1559 |
| Heuristics and information request | X.1560–X.1569 |
| Identification and discovery | X.1570–X.1579 |
| Assured exchange | X.1580–X.1589 |

*For further details, please refer to the list of ITU-T Recommendations.*

# Recommendation ITU-T X.1101

## Security requirements and framework for multicast communication


### Summary

Recommendation ITU-T X.1101 defines the network and service models used for multicast communication. It addresses potential security threats and the required countermeasures. Potential threats are defined from the general, mobility-oriented and multicast specific perspectives, and multicast-specific threats are analysed in particular detail. As such, the security requirements, framework and functions are defined and explained as the main focus of the Recommendation.



### History

| Edition | Recommendation | Approval | Study Group |
|---|---|---|---|
| 1.0 | ITU-T X.1101 | 2010-05-29 | 17 |

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## CONTENTS

# Recommendation ITU-T X.1101

## Security requirements and framework for multicast communication

### 1 Scope

The purpose of this Recommendation is to analyse the potential security threats and vulnerabilities that can arise during multicast communication at the application and IP layers, which provides efficient multiparty group communication, as well as to define the basic security requirements, and provide the security objects and functionalities, the security structure and multicast security technology for the efficient implementation of security to support such communication.

### 2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.603] Recommendation ITU-T X.603 (2004) | ISO/IEC 16512-1:2005, *Information technology – Relayed multicast protocol: Framework*.

[ITU-T X.603.1] Recommendation ITU-T X.603.1 (2007) | ISO/IEC 16512-2:2008, *Information technology – Relayed multicast protocol: Specification for simplex group applications*.

[ITU-T X.604] Recommendation ITU-T X.604 (2010) | ISO/IEC 24793-1:2010, *Information technology – Mobile multicast communications: Framework*.

[ITU-T X.604.1] Recommendation ITU-T X.604.1 (2010) | ISO/IEC 24793-2:2010, *Information technology – Mobile multicast communications: Protocol over native IP multicast networks*.

### 3 Terms and definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 access control** [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

**3.1.2 anonymity** [b-ITU-T X.1252]: A situation where an entity cannot be identified within a set of entities.

NOTE – Anonymity prevents the tracing of entities or their behaviour such as user location, frequency of a service usage, and so on.

**3.1.3 application service provider (ASP)** [b-ITU-T X.1121]: An entity (person or group) which provides application service(s) to mobile users through an application server.

**3.1.4 authentication** [b-ITU-T X.800]: See data origin authentication and peer-entity authentication.

**3.1.5 authorization** [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

**3.1.6 confidentiality** [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

**3.1.7 content protection** [b-ITU-T X.1191]: Ensuring that an end user can only use the content that he/she already acquired in accordance with the rights granted to him/her by the rights holder; content Protection involves protecting contents from illegal copying and distribution, interception, tampering, unauthorized use, etc.

**3.1.8 data integrity** [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

**3.1.9 data origin authentication** [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

**3.1.10 integrity** [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner

**3.1.11 IP multicast** [ITU-T X.603]: Realizes a multicast scheme in the IP network with the help of multiple multicast-enabled IP routers.

**3.1.12 key** [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

**3.1.13 key management** [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

**3.1.14 masquerade** [b-ITU-T X.800]: The pretence by an entity to be a different entity.

**3.1.15 mobile network** [b-ITU-T X.1121]: A network that provides wireless network access points to mobile terminals.

**3.1.16 mobile terminal** [b-ITU-T X.1121]: An entity that has wireless network access function and connects a mobile network for data communication with application servers or other mobile terminals.

**3.1.17 mobile user** [b-ITU-T X.1121]: An entity (person) that uses and operates the mobile terminal for receiving various services from application service providers.

**3.1.18 multicast** [ITU-T X.603]: A data delivery scheme where the same data unit is transmitted from a single source to multiple destinations in a single invocation of service.

**3.1.19 peer-entity authentication** [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

**3.1.20 personally identifiable information (PII)** [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

**3.1.21 security policy** [b-ITU-T X.800]: The set of criteria for the provision of security services (see also identity-based and rule-based security policy).

**3.1.22 shoulder surfing** [b-ITU-T X.1121]: A security threat which collects information in busy places by watching keystroke, reading mobile terminal's screen, or listening to sound from a mobile terminal.

**3.1.23 threat** [b-ITU-T X.800]: A potential violation of security.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 backward access control**: Feature by which joining members are not allowed to decrypt past data.

NOTE – This definition is consistent with [b-IETF RFC 4046].

**3.2.2 forward access control**: Feature by which joining members are not allowed to access to future group data.

NOTE – This definition is consistent with [b-IETF RFC 4046].

**3.2.3 group and membership control (GMC) agent**: An agent that is in charge of user and membership authentication, authorization for accessing a group, group management, etc.

**3.2.4 group identifier**: An identifier used to represent a specific group.

**3.2.5 group key management**: The secure distribution and refreshment of keying material.

**3.2.5 group key management (GKM) agent**: An agent which has a responsibility for the creation, distribution, renewal and maintenance of group keys.

**3.2.6 individual key**: A key shared between a user and a session manager through group and membership control (GMC), after a successful user authentication.

**3.2.7 membership authentication**: Mechanism that identifies whether a node is a genuine member of a multicast session group.

**3.2.8 multicast communication**: A communication using multicasting technologies, i.e., IP multicast or overlay multicast.

**3.2.9 overlay multicast network**: An overlay multicast network pertains to a network wherein legacy IP multicasting schemes are not fully supported, where multicast application data are delivered using unicast transport such as TCP, UDP, or IP-in-IP tunnelling schemes.

**3.2.10 receiver security agent (ReSA)**: An agent assuming responsibility for the corresponding security functions of the sender security agent (SSA), the group and membership control (GMC) agent and the group key management (GKM) agent such as a membership authentication and group key update.

**3.2.11 sender security agent (SSA)**: An agent which is to perform contents protection and the corresponding security functions of the receiver security agent (ReSA), the group and membership control (GMC) agent and the group key management (GKM) agent.

# 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| ACK | ACKnowledgement |
| CP | Contents Provider |
| DoS | Denial of Service |
| DMA | Dedicated Multicast Agent |
| DVMPR | Distance Vector Multicast Routing Protocol |
| FA | Foreign Agent |
| FEC | Forward Error Correction |
| GKM | Group Key Management |
| GM | multicast Group Member |

GMC Group and Membership Control
HA Home Agent
IGMP Internet Group Management Protocol
IP Internet Protocol
ISP Internet Service Provider
LMC Local Mobility Controller
MA Multicast Agent (including HA and FA)
MAID Multicast Agent IDentifier
MCS Multicast Contents Server
MLD Multicast Listener and Discovery
MMA Mobile Multicast Agent
MMC Mobile Multicast Communications
MN Mobile Node
MOSPF Multicast Open shortest Path First
MR Multicast-enabled Router
NAK Negative AcKnowledgement
PIM Protocol Independent Multicast
ReSA Receiver Security Agent
RMA Receiver Multicast Agent
RMCP Relayed MultiCast Protocol
RMT Reliable Multicast Transport
SM Session Manager
SMA Sender Multicast Agent
SSA Sender Security Agent
TCP Transmission Control Protocol
UDP User Datagram Protocol

## 5 Conventions

None.

## 6 Overview of multicast communication

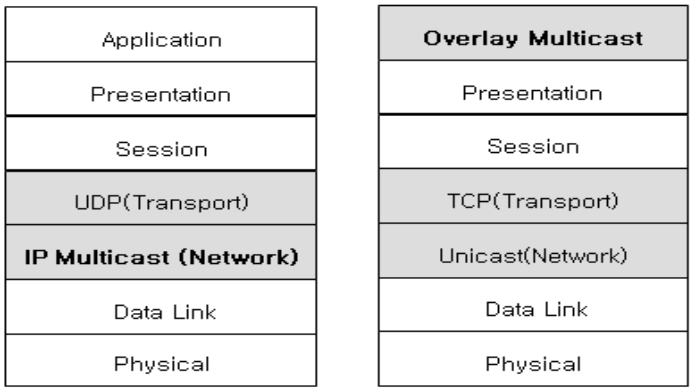
Multicast transport technology provides bandwidth-efficient group communications. It is classified into three types – IP multicast transport, overlay multicast transport and reliable multicast transport (RMT), which has been standardized by the Internet Engineering Task Force (IETF). Multicast transport technology focuses mainly on reliable transport through either the creation of a reliable multicast transport tree or the use of a forward error correction (FEC) code. The tree is used for determining how to send an acknowledgement (ACK) or a negative-acknowledgement (NAK) of the multicast data in IP multicasting. Forward error correction (FEC) is also used to ensure the reliability of real-time data. RMT is outside the scope of this Recommendation.

IP multicast assumes that multicast-enabled routers have been deployed in the network. After receiving packets with a multicast address in the multicast-enabled network, the multicast-enabled router determines the output multicast interface, copies the multicast packets and forwards them to the next appropriate routers, i.e., to routers to which multicast group members are attached, or to other intermediate routers. However, IP multicast is not currently supported in the open Internet. Internet service providers (ISPs) disable the multicast function in their routers to avoid side effects, like security threats and network management problems. In consideration of the above, overlay multicast, which operates at the application layer and uses unicast IP packets, is being developed. Overlay multicast configures a virtually multicast network in the unicast communication environment.

Also, since multicast data can be delivered over wireless networks, mobile multicast is considered, in terms of security requirements over the IP and framework over overlay multicast networks.

## 6.1 Network and service models on multicast communication

The IP and overlay multicast protocol stacks are shown in Figure 1. IP multicast transmits data using multicast IPv4 and IPv6 addresses (see [b-IETF RFC 791] and [b-IETF RFC 2460]). Also, IP multicast uses the UDP protocol to transport data. In contrast, overlay multicast is located at the application layer. Overlay multicast forwards data on a virtual multicast tree using unicast communication by means of a unicast address over the TCP protocol.




a) IP multicast b) Overlay multicast

**Figure 1 – Multicast protocol stack**

### 6.1.1 IP mixed and overlay multicast communication

[ITU-T X.603], [ITU-T X.603.1] and [ITU-T X.604] define overlay and IP multicast communication over wired and wireless networks.

#### 6.1.1.1 Wired environment

The relayed multicast protocol (RMCP) framework and its protocols (see [ITU-T X.603] and [ITU-T X.603.1]) describe the network and service models for overlay multicast.

The model described in [ITU-T X.603] is composed of a session manager, intermediate multicasting receivers, senders and end-receivers. Multicast-enabled routers can be used or not, as shown in Figure 2.

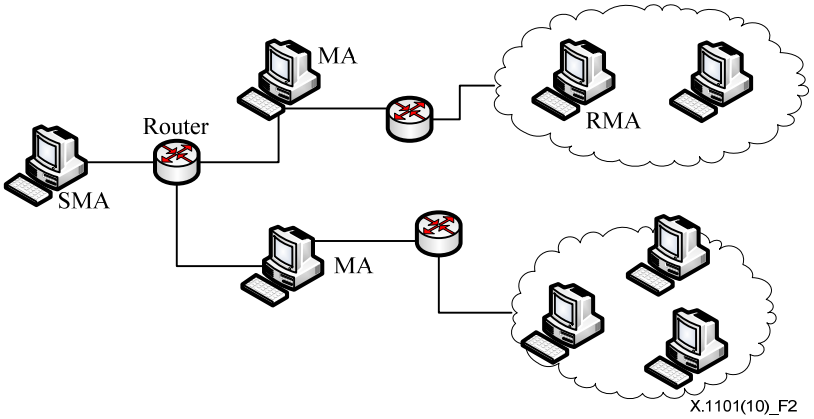



**Figure 2 – Overlay multicast network [ITU-T X.603]**

The [ITU-T X.603.1] service model, which is depicted in Figure 3, includes intermediate relay servers or receivers as well as one sender and multiple receivers. The intermediates are responsible for data forwarding in an overlay multicast tree, which they construct themselves through unicast communication.

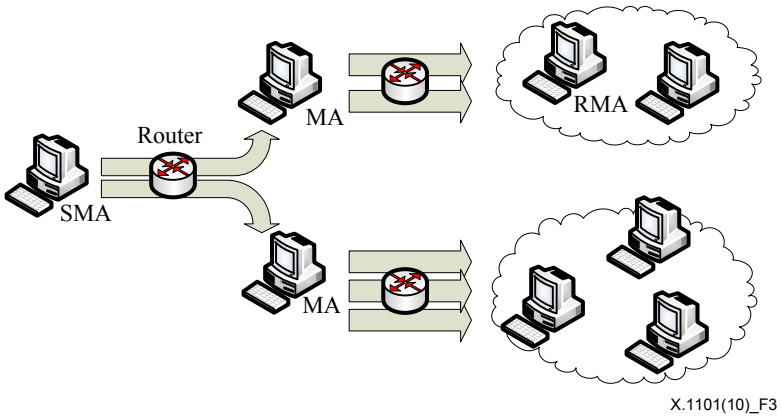



**Figure 3 – Overlay multicast service [ITU-T X.603.1]**

Figure 4 shows a mixed service model with IP and overlay multicast services. If an area permits IP multicast communication, multicast data can be delivered. Of course, other areas use overlay multicast communication to forward the data.

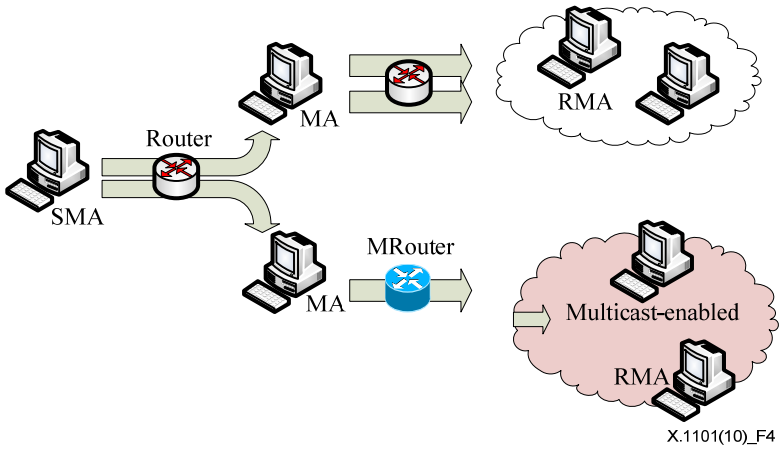
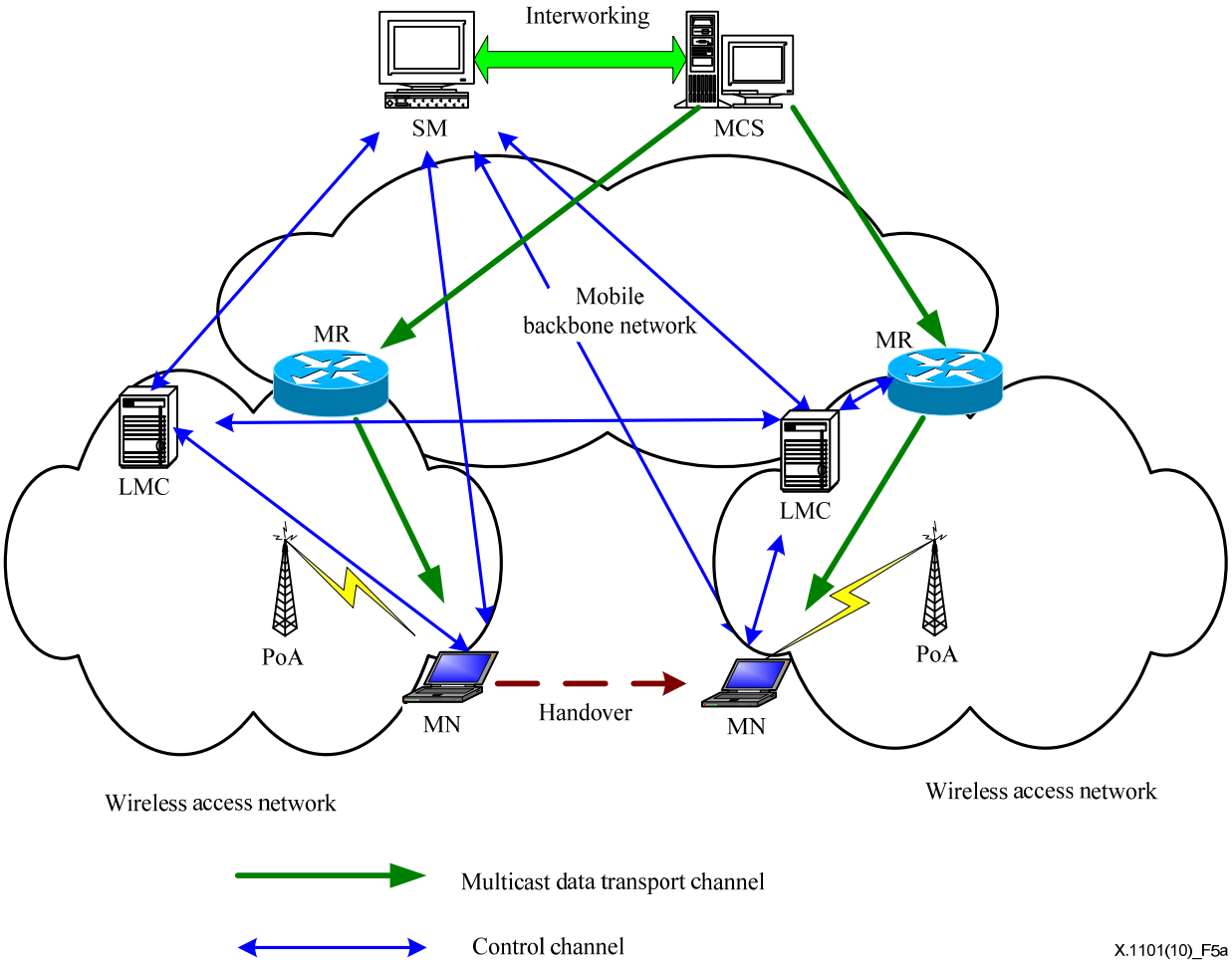


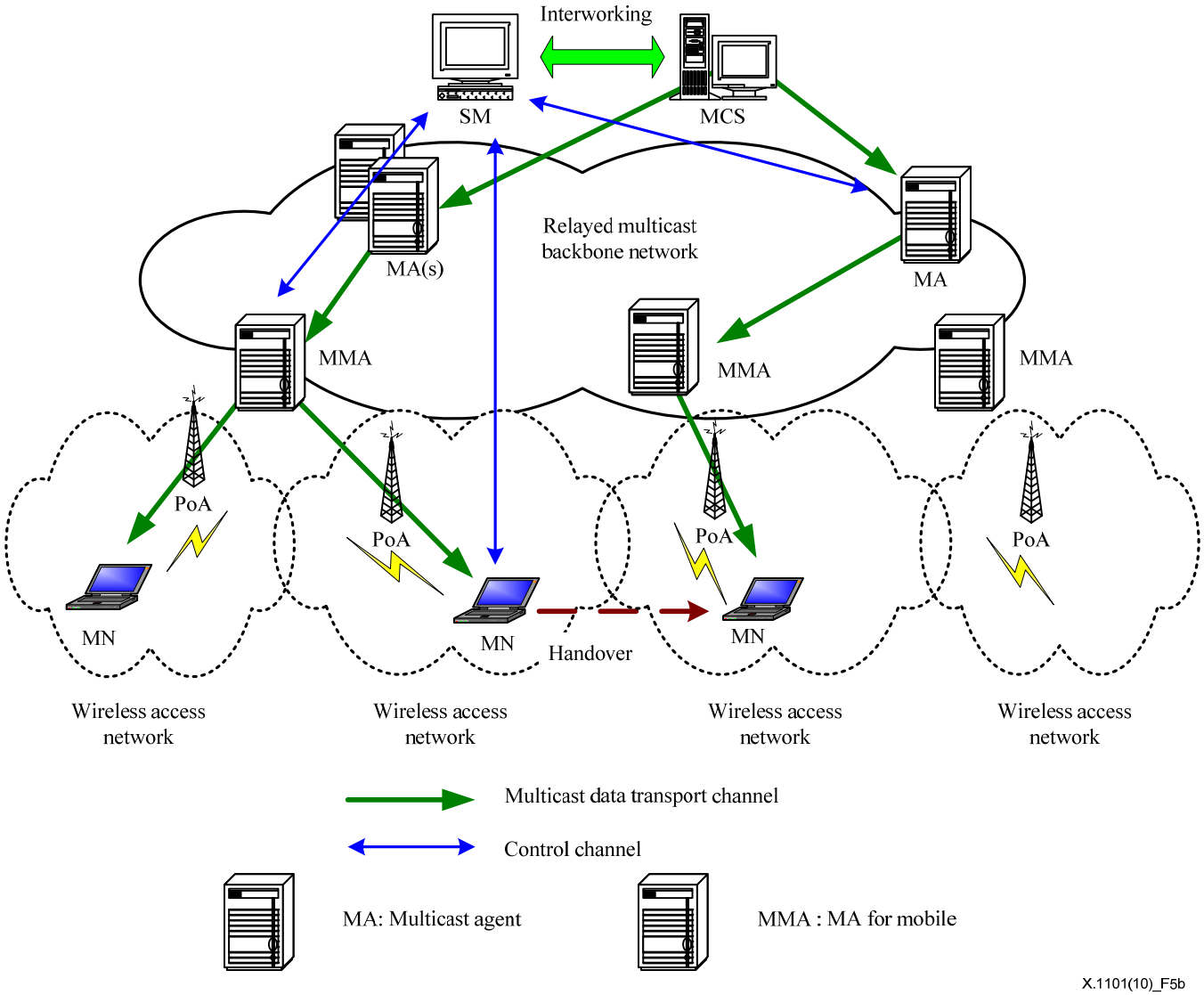

**Figure 4 – Overlay and IP mixed multicast service [ITU-T X.603.1]**

### 6.1.1.2 Wireless environment

[ITU-T X.604] describes the network and service models for mobile multicast communication. There are two types of mobile multicast models, both of which establish separated control and multicast data transport channels. Figure 5-a shows how the IP multicast data is delivered through multicast-enabled routers (MRs) without the intervention of the local mobility controller (LMC). Figure 5-b shows how the multicast contents server (MCS) forwards the multicast data while simultaneously managing the control channel over the overlay network.




**a) Mobile multicast over IP multicast**




**b) Mobile multicast over overlay multicast**

**Figure 5 – Mobile multicast model [ITU-T X.604]**

### 6.1.2 IP multicast communication

[b-IETF RFC 791] and [b-IETF RFC 2460] allow for IP multicast communications.

#### 6.1.2.1 Wired environment

The IP multicast network is composed of multicast-enabled routers, senders and multicast receivers, as shown in Figure 6. In the IP multicast network, packets get through using the IP multicast address [b-IETF RFC 3171].

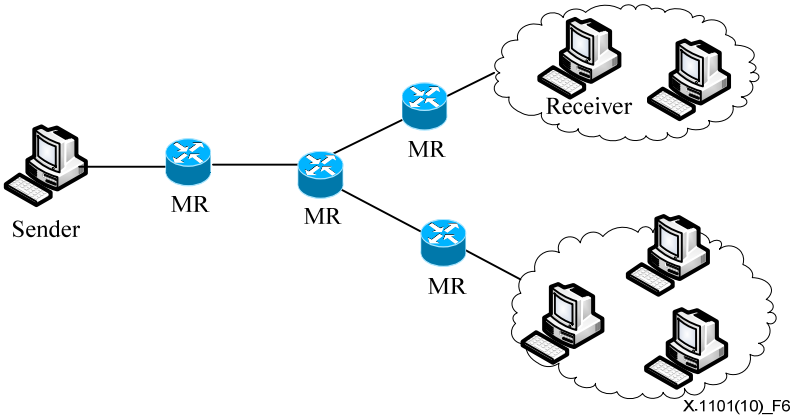



**Figure 6 – IP multicast network**

MRs replicate and forward the packets towards the multicast group members until these arrive at the multicast receivers, making use of the IGMP or MLD protocol used by the MRs to forward the IPv4 or IPv6 packets. If there are any receivers joined directly to any access MR, the MR can join its parent MR using the multicast routing protocol mechanism described in [b-IETF RFC 1075], [b-IETF RFC 3569], [b-IETF RFC 3973] and [b-IETF RFC 4601].

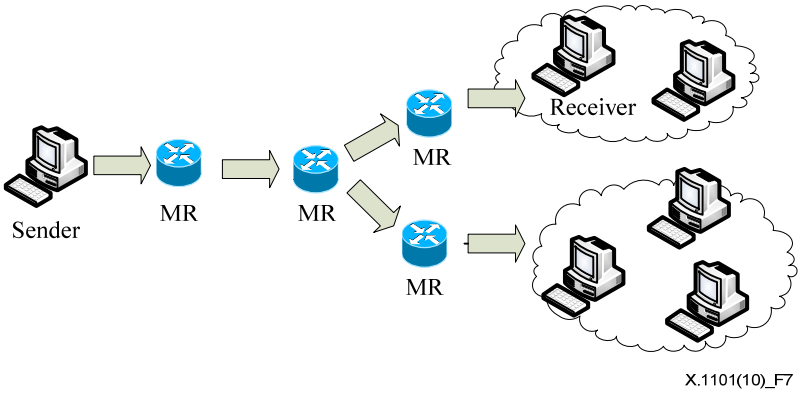



**Figure 7 – IP multicast service [b-IETF RFC 3171]**

### 6.1.2.2 Wireless environment

Mobile multicast only considers an interval of HA/FA/MA and mobile terminal. The HA can join a multicast group on behalf of its mobile terminals. Thus, the HA takes charge of forwarding data to its mobile users directly or by tunnelling even if the users move on another area.

The remote subscription method defines the FA as a multicast group member. So, the FA sends multicast packets to its mobile users. In the case of movement to another area, the moved user should re-join a new FA in the area. The mobile user can then receive the multicast data from a new FA, as shown in Figure 8-b.

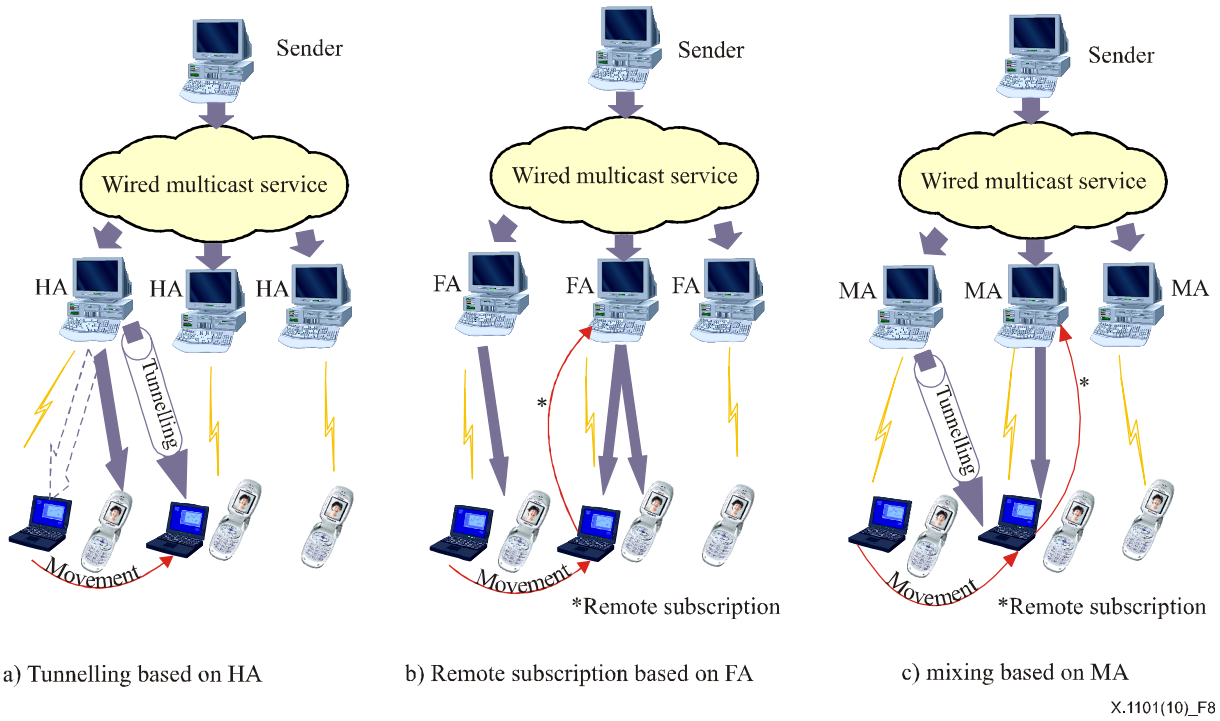



**Figure 8 – Network and service model for mobile multicast described in [b-IETF RFC 3344] and [b-IETF RFC 3775]**

Figure 8-c illustrates the way in which a mobile user receives multicast data from its MA, which may be an HA or an FA. After movement has been detected, the user obtains the data through a tunnel from the previous MA, while at the same time the user terminal tries to establish a remote subscription to a new MA. The tunnel is released once the remote subscription has been established.

## 6.2 Characteristics of multicast communications

### 6.2.1 Few senders and many receivers for the same data

Multicast communication requires that there be few senders and many receivers who receive the same data. The multicast service is classified into 1-to-n and m-to-n communication where m is much smaller than n. In the case of 1-to-n, one sender transmits data to n numbers of receivers. The IPTV service is an example of a 1-to-n service. The service provides large amount of broadcasting contents to receivers wanting to watch the show. Also, software distribution can be done through 1-to-n group communication. m-to-n distribution is applicable for teleconferencing, where some of the attendees speak using microphones and their voices are delivered to the listeners attending the meeting via Internet.

### 6.2.2 Group identifier

A multicast group, defined as a set of receivers to obtain the same data through multicast communication, has an identifier. The overlay multicast group identifier of [ITU-T X.603.1] and [ITU-T X.604] defines a set of MAIDs that may be used as identifier of the MA and MMA nodes that make part of virtual multicast routing tree. Likewise, IP multicast described in [ITU-T X.604.1], [b-IETF RFC 791] and [b-IETF RFC 2460] defines a multicast address as an identifier.

**Table 1 – Multicast group identifier definition**

| Network environment | | Group identifier definition |
|---|---|---|
| Wired/mobile | IP multicast | – IPv4: Class D multicast addresses<br>– IPv6: Addresses that begin with "FF" |
| | overlay multicast | – The identifier MAID group of MAs participating in the overlay multicast tree |

### 6.2.3 Dynamic group management

Any member is able to join or leave its multicast group at any time. The members that compose a group are dynamically changed. Overlay multicast group manages the membership at the MA or the MMA. In contrast, group management of IP multicast is done by the IGMP and the MLD protocol for IPv4 and IPv6, respectively. The management nodes are responsible for the join and leave procedures, at the member's request. The overlay group management agent is located at the application layer, while IP multicast management is performed at the IP layer.

Membership control for a mobile receiver is also required in mobile multicast. Thus, the node supports mobility by seamlessly grafting and pruning the members of the groups.

**Table 2 – Group managers**

| Network environment | | Functionality | Operating entity |
|---|---|---|---|
| Wired | IP multicast | Subscribe/ Unsubscribe | – Access router (MR) with IGMP of IPv4<br>– Access router (MR) with MLD protocol of IPv6 |
| | Overlay multicast | | – MA participating in overlay multicast tree |
| Mobile | IP multicast | Move | – HA/FA on access router (MR)<br>– LMC at the last access router (MR) |
| | Overlay multicast | | – MMA participating in overlay multicast tree |

### 6.2.4 Multicast routing tree

The multicast data is transported via an established path through a multicast routing mechanism. The overlay configures a virtual tree among the MAs, MCS and MMA. The path is made at the application level in the unicast environment. Otherwise, the MRs perform the standard routing mechanism such as DVMRP, MOSPF, PIM, etc. [b-IETF RFC 1075], [b-IETF RFC 3569], [b-IETF RFC 3973], [b-IETF RFC 4601] for IP multicasting.

**Table 3 – Components of multicast routing tree**

| Network environment | | Routing tree components |
|---|---|---|
| Wired | IP multicast | – sender, MR, GM |
| | Overlay multicast | – SMA, MA, RMA |
| Mobile | IP multicast | – sender, MR, HA or FA, MN<br>– MCS, MR, MN |
| | Overlay multicast | – MCS, MA, MMA, MN |

## 7 Security threats to multicast communication

A multicast communication faces different threats than unicast because it provides one-to-many or many-to-many communication, rather than end-to-end communication between peers. As such, threats have a greater and deeper effect on the network or system.

## 7.1 General multicast security threats in wired networks

### 7.1.1 Eavesdropping/disclosure/interception

An attacker scans or eavesdrops on multicast packets to obtain the group identifier over the network. It sends a graft message to an access multicast router or system to join the multicast group using a spoofed group identifier.

It attempts to intercept multicast data or join/leave messages, in order to interfere with or interrupt normal operation of the service. The attacker collects the encrypted data by eavesdropping or interception, and tries to infer the group key which protects data confidentiality.

**Table 4 – Eavesdropping/exposure/interception threat**

| Attack target | Details |
|---|---|
| Multicast group subscribe/unsubscribe message | The attacker illegally acquires group identifiers, send/receive IP addresses, subscribe/unsubscribe information exposed by eavesdropping/intercepting of subscribe/unsubscribe messages sent to the multicast group |
| Multicast data | The attacker illegally acquires data received from a multicast group through eavesdropping/interception |
| Critical messages including group key information and user access rights management/service information | The attacker illegal acquires group keys exchanged for multicast security or information for user access right management, major service information |

### 7.1.2 Injection and modification of data

The attacker tries to inject abnormal multicast data into the spoofed IP address or group identifier, so members may receive noisy or wrong data.

The attacker may modify main control messages such as the join or leave messages from a member, making it impossible for attacked members to receive the service, while anyone not joining the group may receive unexpected multicast data. This results in a denial of service attack. In the case of mobile multicast, the effects of this type of attack are more serious.

The multicast packet may be modified and transferred by the attacker, so members may receive forged data through a normal group identifier which belongs to a group normally joined by them.

**Table 5 – Threat of the injection of abnormal data and forging/modification of normal data**

| Attack target | Details |
|---|---|
| Multicast group subscription message | The attacker induces service malfunction by forging or modifying subscribe/unsubscribe messages |
| Multicast data | The attacker distorts service content by forging or modifying multicast data |
| Critical messages including group key information, user rights management, and service information | The attacker induces service malfunction by forging or modifying security related critical messages such as group keys and service information |
| Senders such as MCS and SMA, relay agents MA, IP multicast addresses | The attacker induces service malfunction by disguising itself as a sender or relay agent who is forwarding multicast data, thereby causing normal recipients to receive noise data and other multicast data |

### 7.1.3 Communication jamming

This threat is the same as that posed to unicast communication. Intentional or unintentional interference overpowers the sender or receiver of a communication link rendering the communication link useless. This can result in a DoS attack.

### 7.1.4 Interruption

The attacker sends to the MR or MA a forged leave message on behalf of any normal member. As a result, the normal member will not receive multicast data. The attacker creates the forged message by intercepting a normal leave message and IP address or through group identifier spoofing.

**Table 6 – Service disruption**

| Target of attack | Details |
|---|---|
| Multicast group unsubscribe message | – The attacker forges/modifies an unsubscribe message so that a normal subscriber cannot receive multicast data |
| Multicast and general control message | – The attacker floods the multicast transmission and other control messages so that the service cannot be provided |

### 7.1.5 Unauthorized access

The attacker sends a service registration message, which is a previously intercepted and modified message, or a spoofed message, to a service administrator in order to access the service normally.

When the MA, LMC, HA, FA, or MMA relays multicast data, the attacker poses as an MA, LMC, HA, FA, or MMA, whereupon the fake MA, LMC, HA, FA, or MMA receives and forwards multicast data from and to a real MA, LMC, HA, FA, or MMA. At the end, the fake node will be able to access and join the multicast service as an administrative node.

If any of the members is a mobile node, the fake node will send a moving message to its MA, LMC, HA, FA, or MMA in order to receive data seamlessly. Once this procedure is complete, the attacker may access the service as a member that has not moved from the previous area. Furthermore, it may access the service as a new incoming mobile member in any multicast group area, even if the normal member has not moved.

In the case of an IP multicast network, the mobile member moves and re-joins the multicast group by sending a multicast join message to its access router through a newly configured unicast address. This type of attack is the same as an unauthorized access and joining of the group by sending a spoofed multicast join message.

**Table 7 – Unauthorized access**

| Attack target | Details |
|---|---|
| Multicast group subscription message | Multicast data can be received illegally by forging/modifying a subscription message |

### 7.1.6 Repudiation

Repudiation is understood as the denial by one of the entities involved in a communication of having participated in all or in part of the communication.

## 7.2 Mobile multicast security threats in a wireless network

Security threats in a wireless multicast environment could be more serious than those of a unicast environment, since multiple users are affected by the threats.

### 7.2.1 Eavesdropping

In mobile multicast, an attacker is able to listen to the multicast data more easily by intercepting radio signals or by performing a fake moving action. In other words, the attacker pretends to be a moving or an unmoving member of a new multicast area, independently of whether the normal member moves or does not move. Thus, the attacker acquires multicast data more easily as a normal member.

**Table 8 – Eavesdropping/exposure/interception threat**

| Attack target | Details |
|---|---|
| Message for movement to multicast group in other region | The attacker illegally acquires the IP addresses or group identifier of moving node or multicast group related information by eavesdropping on or intercepting the movement messages generated when a multicast recipient moves to a different region |

### 7.2.2 Injection and modification of data

In mobile multicast, an attacker is able to inject abnormal messages or nodes to make the MMA or HA/FA/MA believe the victims are moving or not moving.

**Table 9 – Threat of injection of abnormal data and forging/modification of normal data**

| Attack target | Details |
|---|---|
| Message for movement to other region's multicast group | – The attacker induces service malfunction by forging/modifying subscribe/unsubscribe messages related to movement |
| Relay agents MMA and HA/FA | – The attacker induces service malfunction by disguising itself as a relay agent MMA who is forwarding multicast data, or as an HA/FA, thereby causing normal recipients to receive noise data and other multicast data |

### 7.2.3 Communication jamming

In mobile communications, there are two types of attacks: jamming against a mobile terminal and jamming against a network element. The former allows a rogue mobile terminal to impersonate the legal mobile terminal. The latter impersonates the legitimate network element interfacing with the mobile terminal through the wireless interface [b-ITU-T X.1121].

### 7.2.4 Shoulder surfing

This occurs when an attacker collects information in busy places by watching keystrokes, reading a mobile terminal's screen, or listening to sound from a mobile terminal. This results in leakage of information [b-ITU-T X.1121].

### 7.2.5 Lost mobile terminal

This security threat may occur as the mobile terminal is carried around by the mobile user. This can result in the loss or destruction of information stored in the mobile terminal [b-ITU-T X.1121].

### 7.2.6 Stolen mobile terminal

This threat may also occur as the mobile terminal is carried around by the mobile user. This can cause leakage of information stored in the mobile terminal and data deletion resulting from unauthorized access of the stolen mobile terminal in addition to the loss of information stored in the mobile terminal [b-ITU-T X.1121].

### 7.2.7 Unprepared communication shutdown

This is a security threat caused by unstable communications or the limitation of power supply. This can result in data deletion [b-ITU-T X.1121].

### 7.2.8 Misreading

This is a security threat caused by the use of the small displays of mobile terminals. This can result in data deletion by masquerading of ASP [b-ITU-T X.1121].

### 7.2.9 Input error

This is a security threat caused by the difficulty of inputting data via a small keyboard or the keypad of a mobile terminal. This can cause the failure of user authentication [b-ITU-T X.1121].

### 7.2.10 PII Infringement

The PII data, like location information and ID, can be illegally intercepted and collected by an attacker. It can also be misused for tracing the location of some mobile members.

If data is transferred through IP multicast, the attacker can collect it easily by unauthorized joining of the multicast group.

## 8 Security requirements for multicast communication

### 8.1 Security requirements

#### 8.1.1 Confidentiality

The confidentiality of multicast data is achieved through a group key. Multicast data should be encrypted over the wired and/or wireless networks as follows:

a) Data protection for the overlay multicast network [ITU-T X.603.1]:
   i) Overlay multicast data from the SMA and the RMAs via the MAs.
   ii) Control data between the SM and others, between the SMA and the MA, between the MAs, and between the MA and the RMAs.

b) Data protection for IP multicast [b-IETF RFC 3171]:
   i) IP multicast data from sender to receivers via the MRs.
   ii) Control data between sender and receivers.

c) Data protection for mobile multicast [b-IETF RFC 3344], [b-IETF RFC 3775]:
   i) IP multicast data from the MCS to MNs [ITU-T X.604.1].
   ii) Control data between the SM and the MMC, and the SM and the MNs [ITU-T X.604.1].
   iii) Overlay multicast data from the MCS to the MNs via the MAs and the MMAs [ITU-T X.604].
   iv) Control data between the SM and others i.e., MAs, MMAs, MNs [ITU-T X.604].
   v) Protection of IP multicast data from the sender to the HA/FA/MA.

vi) Protection of IP multicast data at the wireless interval between the HA/FA/MA and the recipient.

vii) Control data protection between the HA/FA/MA and the recipient.

### 8.1.2 Group key management

An update of the group key affects all multicast group members. Also, the renewal of the group key is required more frequently than with unicast – whenever a new member joins, when an existing member leaves or at periodic updates. Such updates of the group key should take into account the performance of the renewal for all multicast members.

a) Rekey management of group key.

i) Forward access control:

- A leaving member shall not read any message sent after it leaves the group.

ii) Backward access control:

- A new group member shall not read messages sent before it joined the group.

iii) Periodical protection:

- Group keys should be protected from exposure by updating them periodically.

b) Rekey management of group key by movement:

i) A new group key should be created and distributed following the movement of a mobile node to another MA's region.

### 8.1.3 Integrity

Forging/modification of multicast data, subscribe/unsubscribe and movement messages should be prevented. The integrity of other messages considered critical should be assured.

### 8.1.4 Authentication

It should be verified whether the user has been authenticated; furthermore, a user is authenticated to check membership before it joins a group. The origin of the multicast data should also be verified.

a) Source authentication:

i) A receiver needs to make sure that the message was originated by an authentic source.

b) Membership Authentication:

i) New members that subscribe to the group should be authenticated by the administrator.

ii) Mobile users should be authenticated by the new relayed server system whenever they move.

### 8.1.5 Access control

It is required that more than one administrator control access to a group.

a) Authorization of a new member to a group:

i) Users should be authorized to join a group.

b) Authorization for sending multicast contents:

i) A sender or an administrator might authorize a user to provide multicast contents.

### 8.1.6 Group management

In case of a closed group, there should be more than one administrator performing secure session advertisement and managing the availability of the group information.

### 8.1.7 Protection of bidirectional tunnelling of data

If tunnelling of a multicast packet is used by a mobile user, the inner and outer tunnelled packet header information should be verified and protected.

### 8.1.8 Location information concealment by movement to another multicast area

As location information could be revealed by an unauthorized user that follows the movement of an authorized user, the administrator needs to manage the information by providing anonymity and protection of the data.

## 8.2 Relationship between security threats and requirements in multicast communications

The relationship between threats and requirements for multicast security over wired and wireless networks is shown in Tables 10 and 11, respectively.

**Table 10 – Wired multicast communication**

'Y' indicates that a security requirement solves the correspondent security threats

| Requirements / Threats | Confidentiality | Group key management | Integrity | Authentication | Access control | Group management |
|---|---|---|---|---|---|---|
| Eavesdropping/Disclosure/Interception | Y | Y | | | | |
| Injection and modification of data | | | Y | Y | | |
| Communication jamming | | | | | Y | Y |
| Interruption | Y | Y | Y | Y | Y | Y |
| Unauthorized access | | | | | Y | Y |
| Repudiation | | | | Y | | Y |

**Table 11 – Mobile multicast communication**

'Y' indicates that a security requirement solves the correspondent security threats

| Requirements / Threats | Confidentiality | Group key management | Integrity | Authentication | Access control | Group management | Protection of bidirectional tunnelling of data | Location-information concealment by movement to another multicast area |
|---|---|---|---|---|---|---|---|---|
| Eavesdropping / Disclosure/Interception | Y | Y | | | | | Y | Y |
| Injection and modification of data | | | Y | Y | | | Y | |
| Communication jamming | | | | | Y | Y | | |
| Interruption | Y | Y | Y | Y | Y | Y | | |
| Unauthorized access | | | | | Y | Y | Y | Y |
| Repudiation | | | | Y | | Y | | |

# 9 Security framework for multicast communication

This clause suggests a security framework and the functions required for secure multicast communications.

## 9.1 Multicast security architecture

The following elements can be deployed to provide secure multicast communications: A GMC capable of managing authorization to multicast groups and of authenticating recipients intending to subscribe; a GKM agent capable of managing group keys; and SSA and ReSA which can guarantee data integrity, security and source authentication. Depending on the issue of implementation, the GMC and the GKM can exist together or separately.

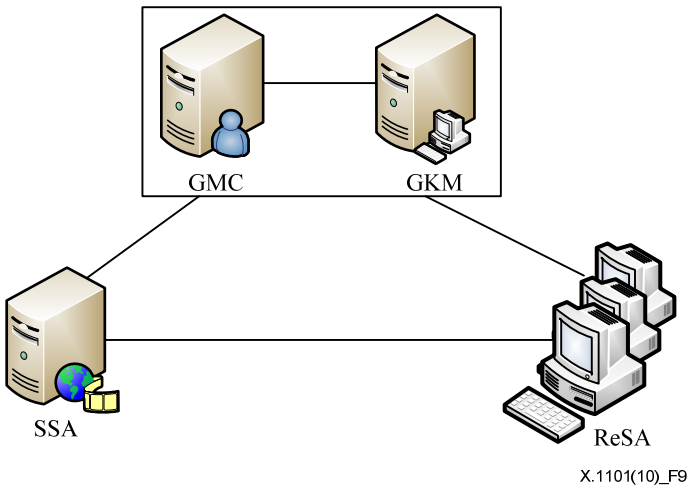



**Figure 9 – Overview of a multicast security architecture**

– GMC: Group management, authentication of users intending to subscribe.

– GKM agent: Generation and management of group keys for the safe sending/receiving of multicast data.

– SSA: In charge of multicast security at the sending end.

– ReSA: In charge of multicast security at the receiving end.

### 9.1.1 Security architecture for wired IP multicast

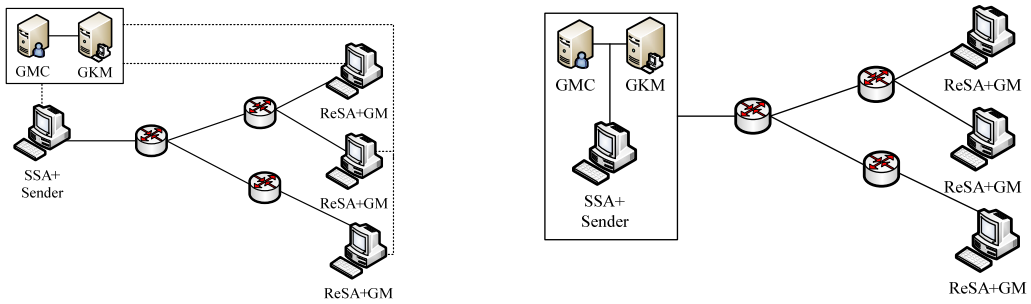



**Figure 10 – Security architecture for IP multicast**

In wired IP multicast communication, the GMC and GKM can be implemented in a security server, while security modules related to sending/receiving can be installed in sender/recipient's terminals. The GMC, GKM and SSA can be installed in the sender's server at the sending end to enable consolidated operation. Separated operation is applied in the case of large-scale service

deployments, while the integrated model is applied in the case of small-scale services, such as personal broadcasting. In the separate model, the GMC and GKM can reside in the same or in different servers, depending on the needs. Only the GMC or the GKM can be installed at the sending end. This is not considered an implementation issue.

### 9.1.2 Security architecture for wired overlay multicast

The security architecture for overlay multicast in a wired environment has been defined in Amendment 1 to [ITU-T X.603.1]. The Global-GMC and Session-GKM are in charge of security management for the overlay multicast session, while Local-GMC and Local-GKM are responsible for group security management of their child groups in the multicast tree.

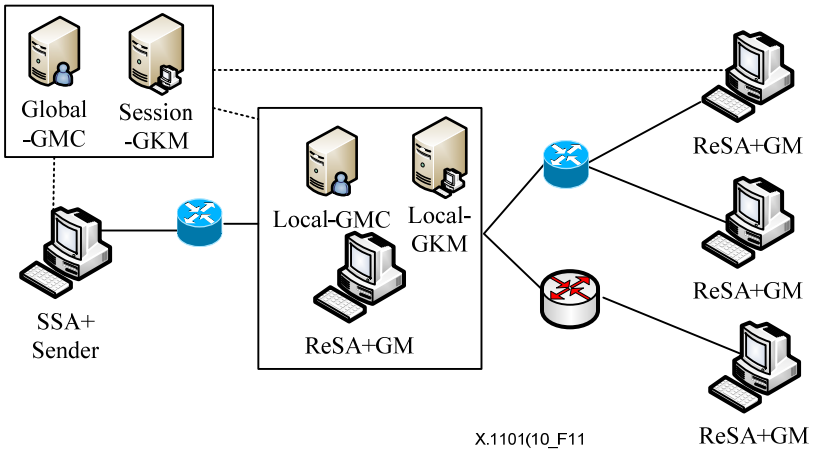



**Figure 11 – Multicast security architecture for wired overlay multicast**

### 9.1.3 Mobile multicast security architecture for IP multicast

Multicast under a wireless environment consists of multicast in the wired interval from sender to the access multicast enabled router and the MMA, and of multicast in the wireless interval from the access multicast enabled router and the MMA to the MN. The security architecture in a wired multicast environment follows the IP multicast architecture in a wired environment; for mobile multicast in the wireless interval, Mobile-GMC and Mobile-GKM are required to authenticate mobile members and perform group key management. The Mobile-GMC and Mobile-GKM can be implemented as one security server or separately. As a multicast component of the IP multicast network environment developed by ITU-T, the LMC can play roles of both Mobile-GMC and Mobile-GKM.

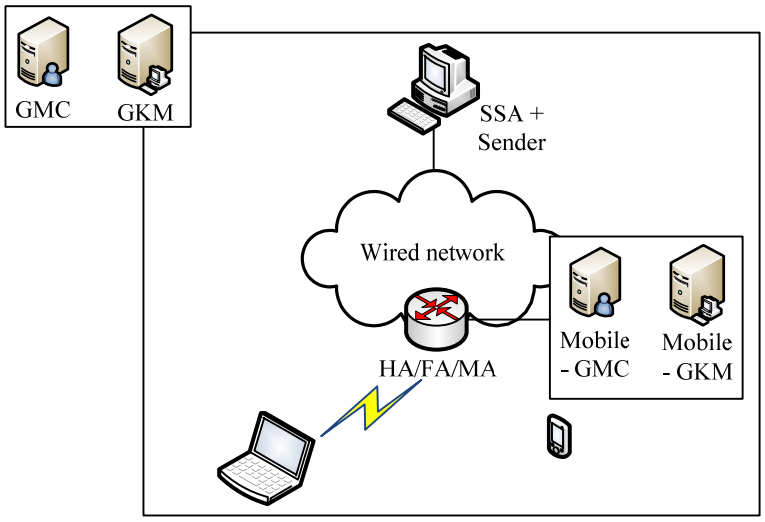



**Figure 12 – Security architecture for mobile multicast in an IP multicast network**

### 9.1.4 Mobile multicast security architecture for overlay multicast

For overlay multicast in a wireless environment, [ITU-T X.604] defines an MMA server as playing the role of managing mobile nodes and transmitting multicast data to them. Therefore, the Mobile-GMC and Mobile-GKM can be either installed together on the MMA server, or else they can operate separately.

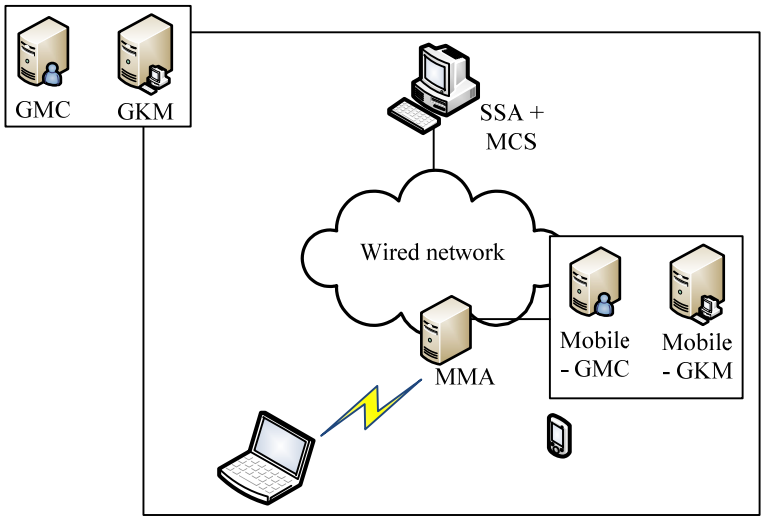



**Figure 13 – Security architecture for mobile multicast over overlay multicast network**

## 9.2 Multicast security functions satisfying the security requirements

Table 12 shows the relationship between the security requirements and the entities which satisfy them.

**Table 12 – Summary of functionalities to be provided by each entity**

| | Confiden-tiality | Group key manage-ment | Integrity | Authen-tication | Access control | Group manage-ment security | Protection of bidirectional tunnelling of data | Location-information concealment by movement to another multicast area |
|---|---|---|---|---|---|---|---|---|
| GMC | | | | Y | Y | Y | | |
| Global-GMC | | | | Y | Y | Y | | |
| Local-GMC | | | | Y | Y | Y | | |
| Mobile-GMC | | | | Y | Y | Y | Y | Y |
| GKM | | Y | | | | | | |
| Session-GKM | | Y | | | | | | |
| Local-GKM | | Y | | | | | | |
| Mobile-GKM | | Y | | | | | Y | Y |
| SSA | Y | Y | Y | Y | | | | |
| ReSA | Y | Y | Y | Y | | | | Y |

### 9.2.1 Functions of the sender security agent

The SSA is a sender security module that mainly performs the encryption and decryption of multimedia contents; it should provide a message authentication method to guarantee the integrity of the multicast data and the major control information sent by the SSA. In addition, to prevent the repudiation of transmitted multicast data and control information, source authentication should be provided.

**Table 13 – Functions of the sender security agent**

| Functions | Roles |
|---|---|
| Contents protection | Provision of confidentiality for or protection of rights of multicast contents |
| Source authentication | Non-repudiation of multicast contents |
| User authentication | Authentication for subscription to multicast service session |
| Contents access authorization | Controls access to multicast contents |
| Membership authentication | Authentication to join the multicast group by x-GMC, where x stands for Global, Local or Mobile |
| Secure user information management | If the SSA manages the information of group members, secure management of member information is needed |
| Group key management | Creation or updating, revocation for a group key by a defined rekey method |
| Secure channel | Establishment of a secure channel between the SSA and an administrator, or between the SSA and a contents provider (CP) if the CP is different from the SSA |
| Individual key management | Key management shared with the SSA, and Global-GMC or the SSA and the CP |

### 9.2.2 Functions of the receiver security agent

The receiver security agent (ReSA) should be able to ensure the confidentiality and integrity of major messages related to subscription and subscription cancellation, movement-related data, etc., and should be capable of performing group key update and management according to the defined group key management method. In addition, integrity checking and source verification of multicast

messages and sent major control messages should be supported. Furthermore, privacy information such as location information arising from movement should be protected from exposure by providing anonymity.

**Table 14 – Functions of the receiver security agent**

| Functions | Role |
|---|---|
| User authentication | Authentication for subscription to a multicast service session |
| Contents access authorization | Admit access to multicast contents (performed by the SSA) |
| Membership authentication | Authentication to join the multicast group by x-GMC, where x stands for Global, Local or Mobile |
| Group key management | Creation, updating or revocation for a group key by the defined rekey method |
| Secure channel | Establishment of a secure channel between the ReSA and x-GMC while exchanging controls such as privacy or key materials, where x stands for Global, Local or Mobile |

### 9.2.3 Functions of group and membership control

GMC performs multicast group access authorization and authentication of users intending to subscribe.

– Global-GMC: Performs authentication and session management upon subscription to a multicast session.
– Local-GMC: Manages the MA's child node groups in overlay multicast communication; performs membership authentication when a user subscribes to the parent MA.
– Mobile-GMC: Manages mobile member groups; performs authentication of a mobile user's group subscription and membership authentication due to movement.

**Table 15 – Functions of group and membership control**

| Functions | Role |
|---|---|
| Admission control | Authentication of an SSA, or ReSA to subscribe to a multicast service session |
| Membership authentication | Membership authentication for the ReSA to join a multicast group |
| Re-membership authentication for mobile users | Light-weight re-membership authentication for a member moving to a new network |
| Contents access control | Maintains user authorization for multicast service |
| Group key management | Creation, updating and revocation from a group performed by the sender, the GMC and the GKM |
| Secure user information management | Secure management of user information in a multicast session |
| Secure channel | – Establishment of a secure channel between the GMC and other nodes with the ReSA if required<br>– Establishment of a secure tunnel between the Mobile-GMC and the ReSA if Mobile-GMC is mounted on the MA or HA |

### 9.2.4 Functions of the group key management agent

The GKM agent performs the initial generation, updating, deletion and safe management of group keys.

– Session-GKM: Creates, deletes and updates group keys according to the group key management method, defines the group key for a session if a common key has to be used in the multicast session; capable of providing data secrecy via the group key.
– Local-GKM agent: Creates, updates and deletes group keys so that the MA can manage group keys for its child groups; ensures the secrecy of data through the group key.
– Mobile-GKM agent: Performs rekey key management for mobile members within the wireless interval; in particular, performs group key management according to members' movements.

**Table 16 – Functions of the group key management agent**

| Functions | Role |
|---|---|
| Group key management | Mainly responsible for group key management of ReSA members or between administration nodes – SSA, GMC and x-GKM where x stands for Session, Local or Mobile |
| Individual key management | Exchanges and maintains individual keys after user authentication in a multicast session |
| Mobile group key management | Manages group keys for moving mobile users |
| Secure channel | Establishes a secure channel between the GKM and the GMC |

# Appendix I

## Use cases for wired mobile multicast communication standards

(This appendix does not form an integral part of this Recommendation)

### I.1 Multicast in a wired environment

#### I.1.1 [ITU-T X.603.1] for 1-to-n group communication over the overlay network

Amendment 1 to [ITU-T X.603.1] has already specified the security functions on [ITU-T X.603.1] for 1-to-n group communication. It defines four entities – SM, SMA, DMA and RMA. It takes the form shown in Figure 11 where their functions are identical to those of the SSA, GMC, GKM and ReSA.

**Table I.1 – Security support in [ITU-T X.603.1]**

| Entity | Identical functional entities |
|---|---|
| SM (session manager) | Global-GMC, Session-GKM |
| SMA (sender multicast agent) | SSA |
| DMA (dedicated multicast agent) | Local-GMC, Local-GKM |
| RMA (receiver multicast agent) | ReSA |

It defines the framework shown in Figure I.1, which has almost the same form shown in Figure 11. The SMA provides the functions of the SSA, such as contents protection and access authorization, source and user authentication, etc., as shown in Table 13. The SM plays the role of Global-GMC and Session-GKM in Tables 15 and 16. In Amendment 1 to [ITU-T X.603.1], the SM is in charge of session admission management, session-key management for the RM-group, access control list management, secure group and membership management, security policy and message encryption/decryption.

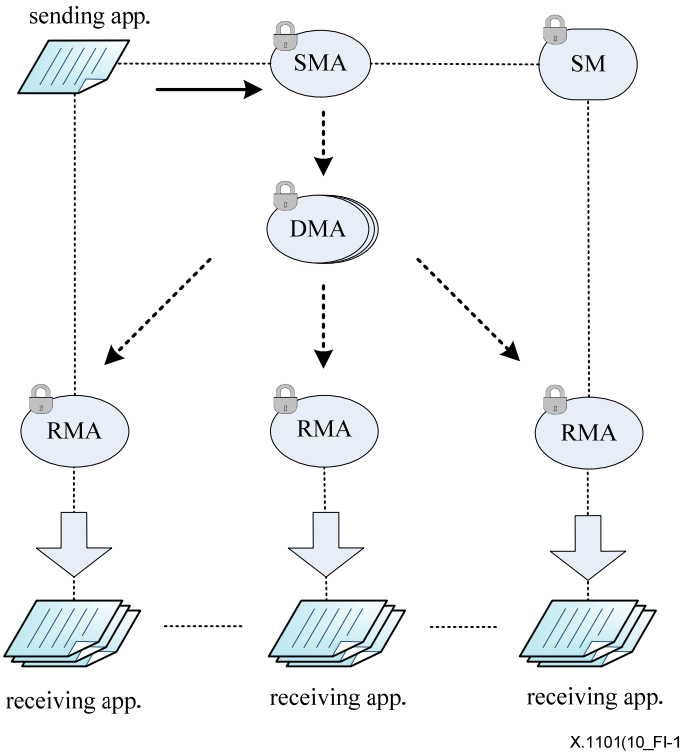



**Figure I.1 – Multicast security architecture in [ITU-T X.603.1], Amd.1**

The DMA is responsible for secure tree configuration, and secure group and membership management, as shown in Table 15, as well as for group key management and message encryption/decryption, as shown in Table 16, together with contents encryption key management to ensure the efficient secure delivery of multicast contents. The SMA and the RMA perform similar roles to those of the SSA and the ReSA.

### I.1.2 Use case for security supplements for n-to-m group communication in an overlay multicast environment

Figure I.2 demonstrates a transport protocol for providing n-to-m group communications over the overlay network. The service model is similar to the one in [ITU-T X.603.1]. However, in this type of n-to-m group communication there are several senders and corresponding SMAs. There are also core MAs connected in the form of a ring or mesh structure, and edge MAs connected in a tree topology.

**Table I.2 – Security supports in case of n-to-m group communication**

| Entity | Identical functional entities |
|---|---|
| SM (Session Manager) | Global-GMC, Session-GKM |
| Edge MA | SSA, ReSA |
| Core MA | Local-GMC, Local-GKM |

The SM could play the role of the Global-GMC and Session-GKM, as in Amendment 1 to [ITU-T X.603.1], where the edge MA would be an SSA or ReSA, as the edge is able to become an SMA or RMA. The edge MA could dynamically join or leave the n-to-m group to become an SSA or ReSA. On the other hand, only the core MA should be the Local-GMC and Local-GKM, as trust party, because the GMC and GKM are key components that provide multicast security.

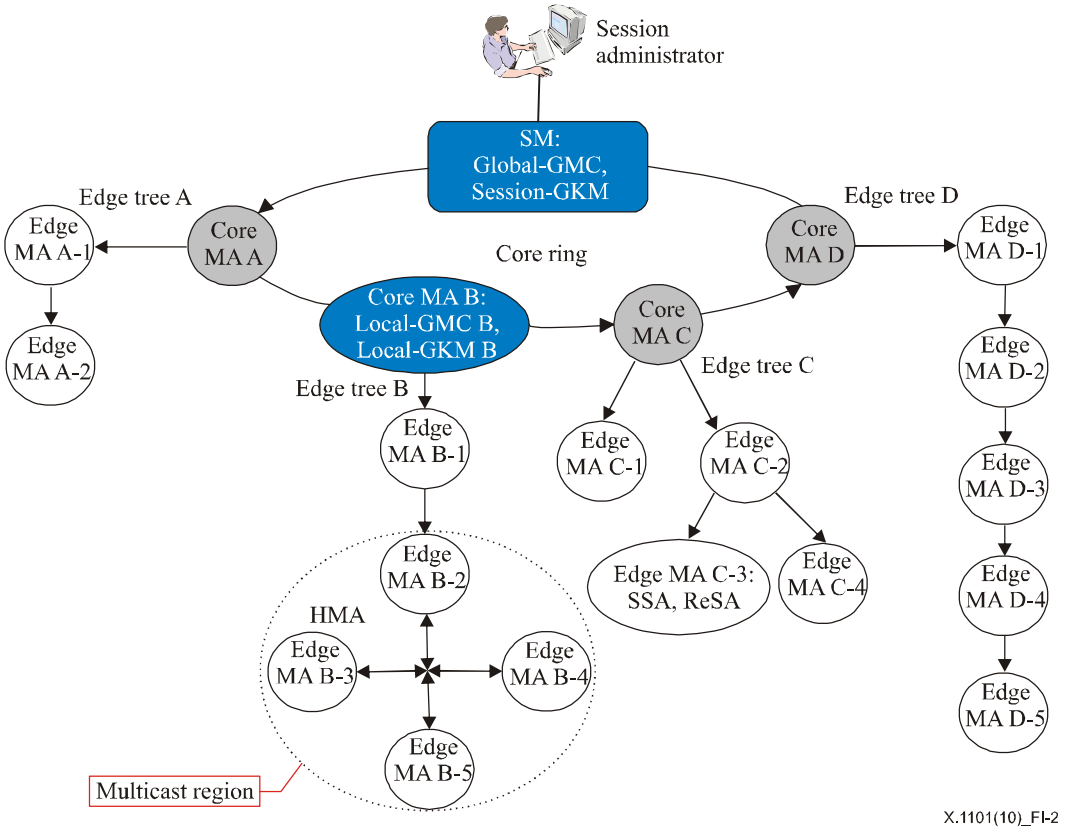



**Figure I.2 – Use case of security support for n-to-m group communication**

### I.1.3 Use case for IP multicast in a wired environment

In IP multicast communication, there are many IETF RFCs for multicast security. Table I.3 shows the various multicast security technologies that are suitable for each multicast entity.

**Table I.3 – Security support for IP multicast**

| Entity | Technologies that can be applied |
|---|---|
| SSA | MGSA, GKMA, TESLA, MEIP |
| GMC | GDOI, MGSA, GKMA, MEIP |
| GKM | GDOI, MGSA, MIKEY, GKMA, MEIP |
| ReSA | MGSA, GKMA, TESLA, MEIP |

Figure I.3 shows a relationship of GKM with each entity in this Recommendation. GKM has five functional blocks for policy infrastructure, authorization infrastructure, GCKS, sender(s) and receiver(s). The two infrastructures are mainly in charge of multicast security policy and service access control that belong to the GMC. GCKS is a key component to provide group membership, key management and data security. GMC is responsible for group membership, and GKM is in charge of group key management and data security.

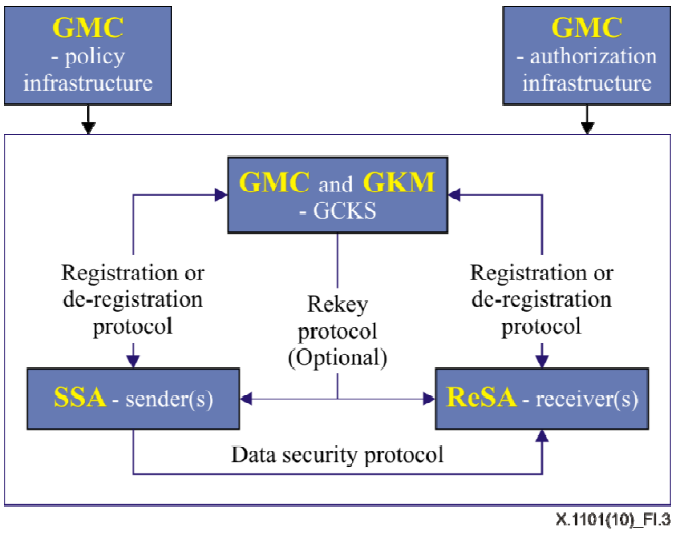



**Figure I.3 – Example of security correspondence with GKMA**

## I.2 Multicast in wireless networks

### I.2.1 Use cases of security for mobile multicast over IP multicast network [ITU-T X.604.1]

[ITU-T X.604.1] supports group communication over the IP multicast network. As shown in Table I.4, there are four entities – SM, MCS, LMC and MN. The SM manages an overall multicast session, and the MCS and the MN are the sender and the receiver, respectively. The LMC is a mobile controller and provides mobile multicast communication as a main component.

The SM would be the Global-GMC and the Session-GKM, which are responsible for admission control and multicast service access control, etc., as shown in Tables 15 and 16. The MCS and the MN serve as the SSA and the ReSA, respectively. The LMC is in charge of group key management, membership authentication, etc. as the Local-GMC and the Local-GKM, as shown in Tables 15 and 16.

**Table I.4 – Security support in the case of [ITU-T X.604.1]**

| Entity | Identical functional entities |
|---|---|
| SM (session manager) | Global-GMC, Session-GKM |
| MCS (multicast contents server) | SSA |
| LMC (local mobility controller) | Local-GMC, Local-GKM |
| MN (mobile node) | ReSA |

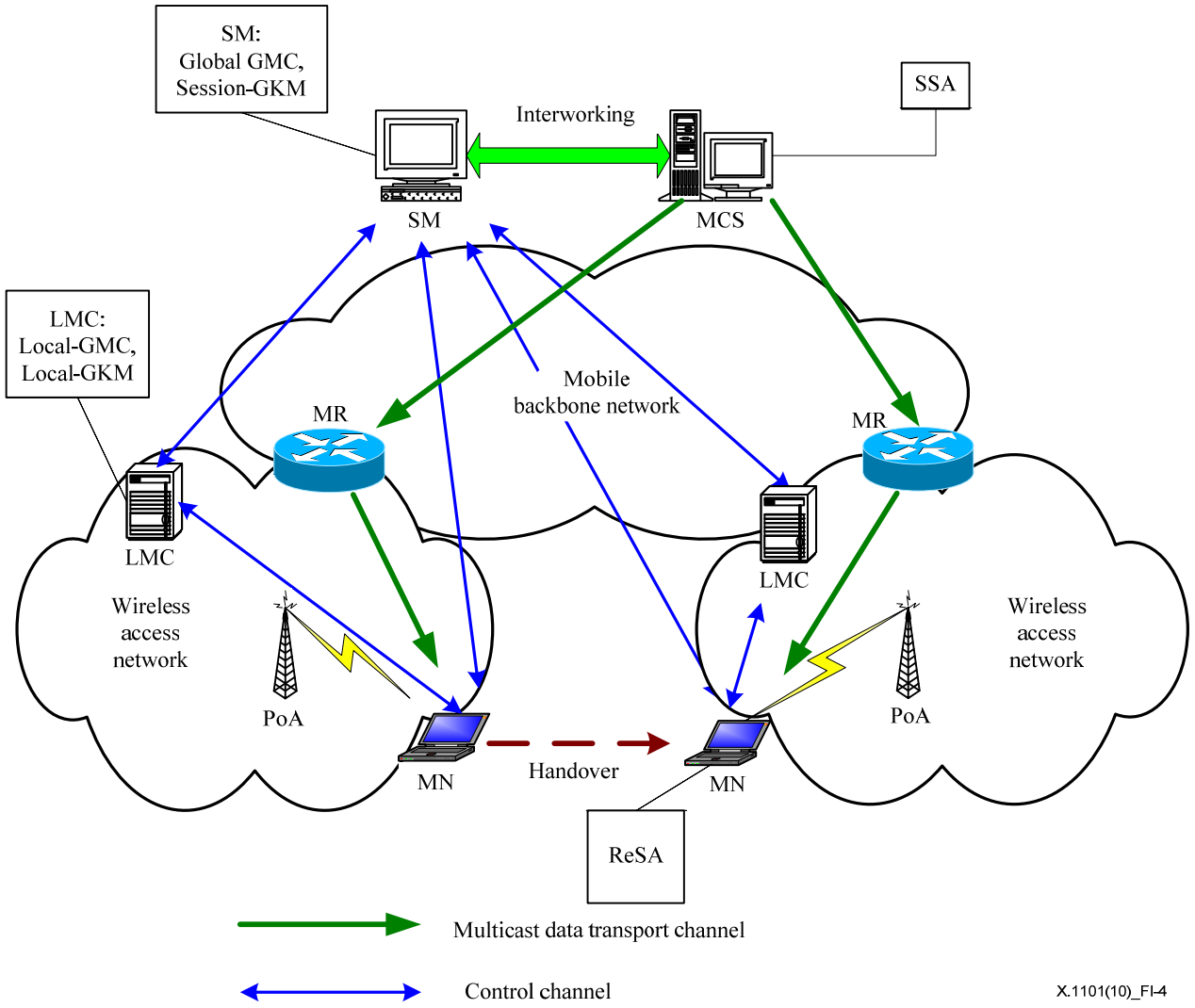



**Figure I.4 – Use case of security support for [ITU-T X.604.1]**

### I.2.2 Use cases of security for mobile multicast over overlay networks [ITU-T X.604]

[ITU-T X.604] has been developed for multicast transmission over the overlay network. It is composed of the SM, MCS, MA, MMA and MN. The SM would be the Global-GMC and Session-GKM for security, as with [ITU-T X.604.1]. Also, the MCS and the MN are the SSA and the ReSA, respectively. The functions of the Local-GMC and the Local-GKM would be performed in the MMA. Here, the MA is the same as that of [ITU-T X.603.1] SMA, RMA and DMA.

**Table I.5 – Security support in the case of [ITU-T X.604]**

| Entity | Identical functional entities |
|---|---|
| SM (session manager) | Global-GMC, Session-GKM |
| MCS (multicast contents server) | SSA |
| MMA (mobile multicast agent) | Local-GMC, Local-GKM |
| MN (mobile node) | ReSA |

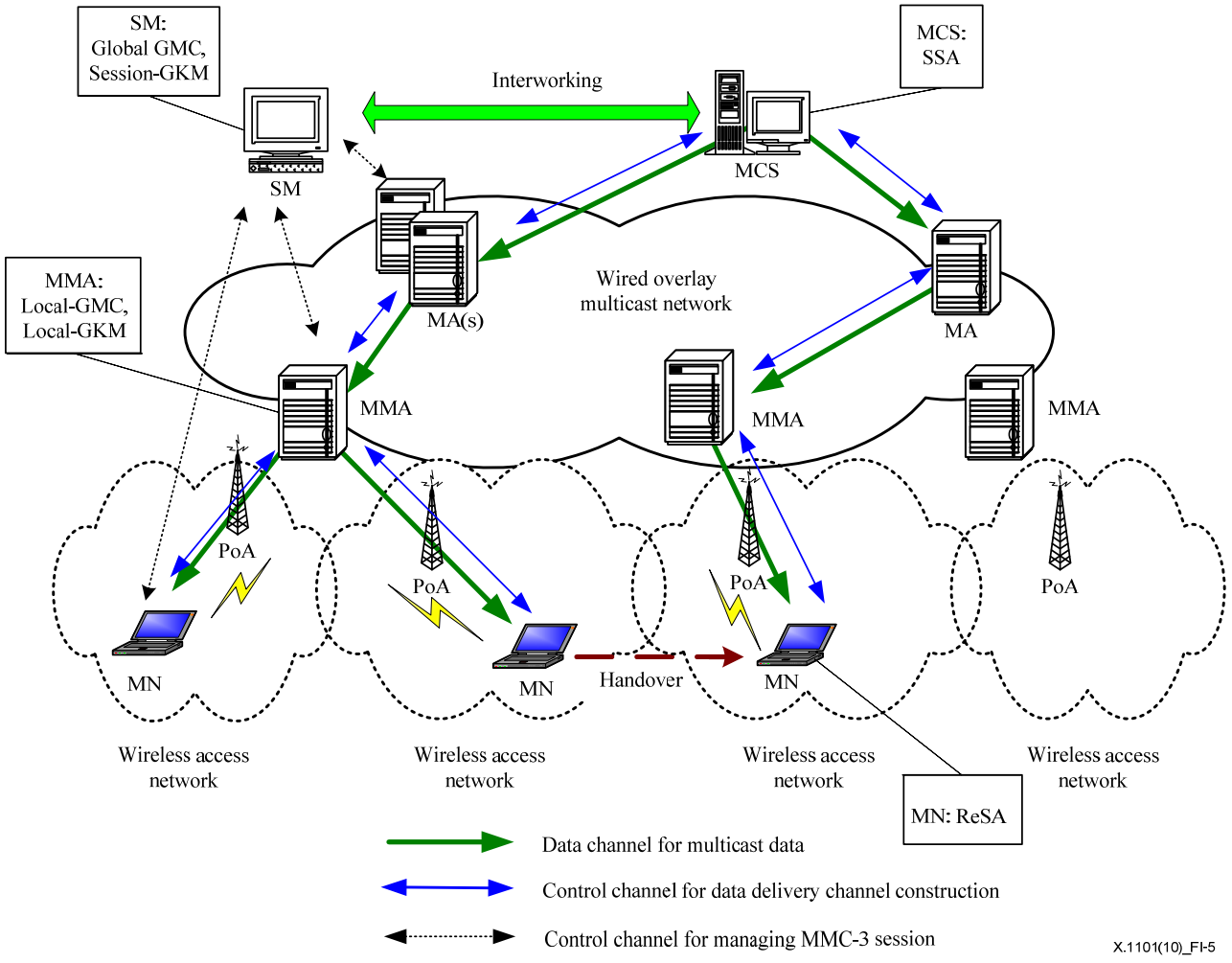



**Figure I.5 – Case of security support for [ITU-T X.604]**

### I.2.3 Use cases for security in the mobile multicast model [b-IETF RFC 3344], [b-IETF RFC 3775]

Mobile multicast in the IETF consists of the HA, FA and MN. The HA can be the Global-GMC and the Session-GKM, while the CN is the SSA. The ReSA is adopted by the MN as a client security agent. The FA plays the role of the Local-GMC and the Local-GKM.

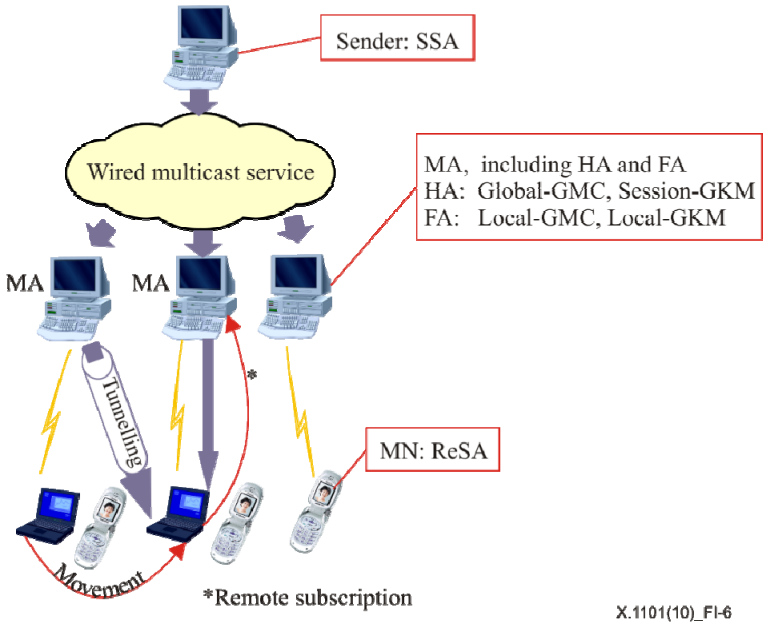



**Figure I.6 – Case of security support for mobile IP**

# Appendix II

## Security technologies for multicast communication

(This appendix does not form an integral part of this Recommendation)

Technologies capable of providing security for multicast communication can be largely divided into group key management techniques and standard technologies for message authentication to ensure data integrity. In addition, the security architecture is defined for the management of multicast group keys. ITU-T is also standardizing the security specifications for overlay multicast transmission to provide a 1:n group communication service (see Amendment 1 to [ITU-T X.603.1]).

**Table II.1 – Multicast security standards**

| Category | Abbreviation | Title of the standard | Standard |
|---|---|---|---|
| Group key management architecture and method | KDC | Group Key Management Protocol (GKMP) Architecture | [b-IETF RFC 2094] |
| | GKMP | Group Key Management Protocol (GKMP) Specification | [b-IETF RFC 2093] |
| | GDOI | The Group Domain of Interpretation | [b-IETF RFC 3547] |
| | MIKEY | Multimedia Internet KEYing | [b-IETF RFC 3830] |
| | GSAKMP | Group Secure Association Key Management Protocol | [b-IETF RFC 4535] |
| | LKH | Key Management for Multicast: Issues and Architectures | [b-IETF RFC 2627] |
| | MGSA | The Multicast Group Security Architecture | [b-IETF RFC 3740] |
| | GKMA | Multicast Security (MSEC) Group Key Management Architecture | [b-IETF RFC 4046] |
| | MEIP | Multicast Extensions to the Security Architecture for the Internet Protocol | [b-IETF RFC 5374] |
| Providing integrity | TESLA | Timed Efficient Stream Loss-Tolerant Authentication | [b-IETF RFC 4082], [b-IETF RFC 4383] |
| ITU-T X.603.1 security extensions | Secure RMCP-2 | ITU-T X.603.1 \| ISO/IEC 16512-2/Amd.1: Relayed multicast protocol-Security extensions | [ITU-T X.603.1], Amd.1 |

# Bibliography


[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications.*

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*

[b-ITU-T X.1111] Recommendation ITU-T X.1111 (2007)*, Framework of security technologies for home network*.

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004)*, Framework of security technologies for mobile end-to-end data communications*.

[b-ITU-T X.1191] Recommendation ITU-T X.1191 (2009)*, Functional requirements and architecture for IPTV security aspects*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010)*, Baseline identity management terms and definitions*.

[b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[b-IETF RFC 791] IETF RFC 791 (1981), *Internet protocol*.

[b-IETF RFC 1075] IETF RFC 1075 (1988), *Distance Vector Multicast Routing Protocol*.

[b-IETF RFC 2093] IETF RFC 2093 (1997), *Group Key Management Protocol (GKMP) Specification*.

[b-IETF RFC 2094] IETF RFC 2094 (1997), *Group Key Management Protocol (GKMP) Architecture*.

[b-IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[b-IETF RFC 2627] IETF RFC 2627 (1999), *Key Management for Multicast: Issues and Architectures*.

[b-IETF RFC 3171] IETF RFC 3171 (2001)*, IANA Guidelines for IPv4 Multicast Address Assignments*.

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4*.

[b-IETF RFC 3547] IETF RFC 3547 (2003), *The Group Domain of Interpretation*.

[b-IETF RFC 3569] IETF RFC 3569 (2003), *An Overview of Source-Specific Multicast (SSM)*.

[b-IETF RFC 3740] IETF RFC 3740 (2004), *The Multicast Group Security Architecture*.

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.

[b-IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

[b-IETF RFC 3973] IETF RFC 3973 (2005), *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification*.

[b-IETF RFC 4046] IETF RFC 4046 (2005), *Multicast Security (MSEC) Group Key Management Architecture*.

[b-IETF RFC 4082] IETF RFC 4082 (2005), *Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction*.

[b-IETF RFC 4383] IETF RFC 4383 (2006), *The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in the Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 4535] IETF RFC 4535 (2006), *GSAKMP: Group Secure Association Key Management Protocol*.

[b-IETF RFC 4601] IETF RFC 4601 (2006), *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification*.

[b-IETF RFC 5374] IETF RFC 5374 (2008), *Multicast Extensions to the Security Architecture for the Internet Protocol*.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Cable networks and transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Terminals and subjective and objective assessment methods |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| **Series X** | **Data networks, open system communications and security** |
| Series Y | Global information infrastructure, Internet protocol aspects and next-generation networks |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2010