SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2008; **1**:495–509
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.86

AuthoCast–a mobility-compliant protocol framework for multicast sender authentication

Thomas C. Schmidt[1*,†], Matthias Wählisch[1,2], Olaf Christ[1] and Gabriel Hege[1]

[1]*HAW Hamburg, Dept. Informatik, Berliner Tor 7, D-20099 Hamburg, Germany*
[2]*link-lab, Hönower Str. 35, D-10318 Berlin, Germany*

Summary

Mobility is considered a key technology of the next generation Internet and has been standardized within the IETF. Rapidly emerging multimedia group applications such as IPTV, massive mutliplayer games (MMORPGs) and video conferencing increase the demand for mobile group communication, but a standard design of mobile multicast is still awaited. The open problem poses significant operational and security challenges to the Internet infrastructure. This paper introduces a protocol framework for authenticating multicast sources (MSs) and securing their mobility handovers. Its contribution is twofold: at first, the current mobile multicast problem and solution spaces are summarized from the security perspective. At second, a solution to the mobile source authentication problem is presented that complies to IPv6 mobility signaling standards. Using an autonomously verifiable one-way authentication based on cryptographically generated addresses, a common design is derived to jointly comply with the mobile any source and source specific multicast (SSM) protocols that are currently proposed. This light-weight scheme smoothly extends the unicast enhanced route optimization for mobile IPv6 and adds only little overhead to multicast packets and protocol operations. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: Mobile multicast source authentication; multicast mobility management; mobile IPv6; cryptographically generated addresses; ASM; SSM

1. Introduction

Many of today's mobile devices carry individual IP addresses and Internet services are expected to extend to mobility management in the near future. The virginal availability of a new, truly mobile IP enabled network layer [1] offers connectivity to nomadic users at roaming devices, while preserving communication sessions beyond IP subnet changes.

Voice and video (group) conferencing, as well as large scale content distribution, e.g., IPTV or massive mutliplayer games (MMORPGs) are considered the key applications for the next generation ubiquitous Internet. Inexpensive, point-to-multipoint enabled technologies such as 802.16 or DVB-H/IPDC emerge on the subnetwork layer and facilitate large-scale group communication deployment. Unlike point-to-point mobility and despite of 10 years of active research, mobile

*Correspondence to: Thomas C. Schmidt, HAW Hamburg, Dept. Informatik, Berliner Tor 7, D-20099 Hamburg, Germany.
†E-mail: t.schmidt@ieee.org

multicast protocol development is still in an early, premature state [2]. Up until now, a security layer for mobile multicast senders is entirely absent. But the handover of a multicast sender introduces a new multicast channel at the routing layer and a re-direct of traffic on the multicast session layer. In a multicast environment that provides admission control and accounting, it is unfeasible to deploy mobility without reliable mechanisms of mobile source identification and authorization.

To address this problem at the IPv6 layer, we present a scheme along with a protocol design that permits receivers *and* Internet routers to authenticate mobile multicast senders. Credentials can be verified autonomously in the sense that all information required for sender admission control is provided within a single data packet, without the need of external signaling or pre-established trust relationships. The protocol named 'AuthoCast' equally applies to any source [3] and source specific multicast (SSM) [4], and all common schemes for a multicast mobility management. By extending standard unicast protocols, this work fills the gap of a missing security layer for mobile multicast, which is a severe hindrance to deployment.

In detail, the contribution of this work is twofold. At first, the current mobile multicast problem and solution spaces are summarized from the security perspective, and common requirements for a secure signaling are derived. At second, a solution to the mobile source authentication problem is presented that complies to IPv6 mobility management standards. Based on established protocol elements, a new protocol semantic is defined that smoothly extends unicast signaling to the case of multicast. Protocols and methods introduced along the line of this work apply beyond pure mobility management; in single source sessions, AuthoCast may be immediately used for a general source authentication to a multicast group, which may be extended to a multisource environment by conventional trust delegation.

This paper is organized as follows. We introduce the problem space of multicast sender mobility in Section 2 and present an overview about the major approaches for mobility management protocols and their requirements in Section 3. Design and operations of the AuthoCast protocol are outlined in Section 4, followed by an evaluation of the relevant aspects of the proposed solution in Section 5. Reference to work related to multicast sender authentication is given in Section 6. Finally, with discussions, conclusions and an outlook we close in Section 7.

2. Problem Statement

Multicast data transmission is built upon shared or source specific distribution trees, which replicate packets within the network towards a possibly large and far-flung group of receivers. As an essential functional characteristic, the general host group model of Deering [3] enables a communication from a source to receivers without prior contact or explicit authorization. In disseminating unauthorized data on previously established multicast trees, though, the network may easily be abused to facilitate distributed denial of service attacks, as well as to flood receivers with unwanted traffic. Depending on the multicast routing protocol in use, traffic of additional sources may create new states or even entire trees in network routers. In the example of protocol independent multicast - sparse mode (PIM-SM) [5], a new source actively issuing data to an existing group may initiate the construction of a new source specific tree spanning all receivers. The restrictive model of SSM foresees an explicit source filtering following source-based client subscriptions. However, an attacker using spoofed IP addresses can pose similar threats as in the open host group model to receivers and the network infrastructure.

A mobile multicast sender will face the problem of enabling a continuous forwarding of data to its group of receivers, while it undergoes roaming and network layer handovers. Its mobility protocol should facilitate a seamless transmission service and at the same time preserve transparency with respect to network and address changes at the receiver side.

Multicast listener applications are frequently source address aware. A mobile multicast source (MS) consequently must meet address transparency at two layers: To comply with reverse path forwarding (RPF) requirements, it has to use an address within the IPv6 basic header source field, which is in topological concordance with the employed multicast distribution tree. For application transparency, the logical node identifier, commonly the Home Address (HoA), must be presented as the packet source address to the transport layer at the receivers.

Network routing, at the complementary side, must comply with the sender movement without having network functionality compromised. It should realize native forwarding whenever possible to preserve its resources, but needs to ensure routing convergence even under a rapid movement of the sender. Mobility handovers should not enable new ways of abusing established distribution trees, but must prevent bogus

DOI: 10.1002/sec

nodes from feeding into established multicast sessions by issuing malicious mobility signaling.

Mobility support for MSs at the network layer thus poses a significant challenge to the infrastructure. A node submitting data to a group of receivers either defines the root of a source specific shortest path tree (SPT), distributing data towards a rendezvous point or receivers, or it forwards data directly down a shared tree, e.g., via encapsulated protocol independent multicast (PIM) [5] register messages. Native forwarding along source specific delivery trees will be bound to the source's topological network address due to RPF checks. A mobile MS moving to a new subnetwork is only able to either inject data into a previously established delivery tree, which may be a rendezvous point based shared tree, or to (re-)initiate the construction of a multicast distribution tree compliant to its new location. In the latter case, the mobile sender will have to proceed without controlling the new tree development, as it operates decoupled from its receivers.

Source address binding updates (BUs) raise the security issues. Multicast receivers that evaluate binding caches for source identification are subject to impersonation and a theft of service, unless BUs of a mobile source can be authenticated. However, unlike in the unicast case, the multicast distribution infrastructure is easily misused, as well, whenever a mobility-related address update at the infrastructure level will be accepted without verification. Attackers could hijack the tree by modifying source filters, force routers to recompute multicast trees frequently after iterated state updates, and perform distributed denial of service attacks through amplified flooding. Any source multicast (ASM)—even though designed to permit packet distribution from any voluntary sender—is bound to restrictions imposed by operators and by scoping and may require source authentication, cf. Section 6. Threats in particular apply to mobility agents, which facilitate routing with the help of binding caches. Security requirements specifically apply to SSM, where listeners may subscribe to or exclude any specific MS, and thereby want to rely on the topological correctness of network operations. The SSM design permits trust in equivalence to the correctness of unicast routing tables. Any SSM mobility solution should preserve this degree of confidence. BU security at the SSM infrastructure level is equivalent to BU security with a correspondent node in MIPv6. Any such BU authentication though has to proceed within unidirectional signaling, as feedback messages will violate the multicast communication paradigm.

3. Multicast Mobility Schemes

Seamless support for mobile multicast senders requires efforts significantly exceeding unicast mobility management schemes. The MIPv6 standard proposes bidirectional tunneling through the home agent as a generally applicable, minimal multicast support for mobile senders and listeners as introduced by Reference [6]. In this approach, the mobile MS always uses its HoA for multicast operations. Since home agents remain fixed, mobility is completely hidden from multicast routing at the price of triangular paths and extensive encapsulation.

Further schemes attempt to optimize temporal handover performance and to approach optimal multicast routing, thereby using its temporal Care-of Address (CoA). They all have in common a per handover change of source addresses and thus require an address duality management, i.e., a maintained *HoA*-to-*CoA* mapping, at end nodes, as well as at assistant infrastructure components. The infrastructure entities involved in mobility management depend on the routing protocol in use. Mainly, these are specialized multicast agents, sometimes all on-path multicast routers require mobility updates. Protocols are specialized with respect to the multicast model in use and are thus categorized according to ASM and SSM. For a current overview of multicast mobility solutions we refer to Reference [2].

3.1. ASM Solutions

In the following we give an overview of the key concepts for ASM mobility solutions. They all take advantage of infrastructural agents to which mobile sources associate and establish bindings. ASM receivers likewise operate binding caches to map packets from mobile sources to its appropriate HoA.

3.1.1. Rendezvous point based

Romdhani *et al*. [7] propose to employ the rendezvous points of PIM-SM [5] as mobility anchors, thereby following a shared tree approach. Operating on extended multicast routing states, these 'mobility-aware rendezvous points' (MRPs) hold a binding of the current CoA with the HoA. Mobile senders initially tunnel their BUs and data to MRPs within PIM register messages, which subsequently initiate the construction of a source specific tree to facilitate native forwarding from the mobile source at its location within the PIM domain. Focusing on interdomain mobile multicast, the authors

DOI: 10.1002/sec

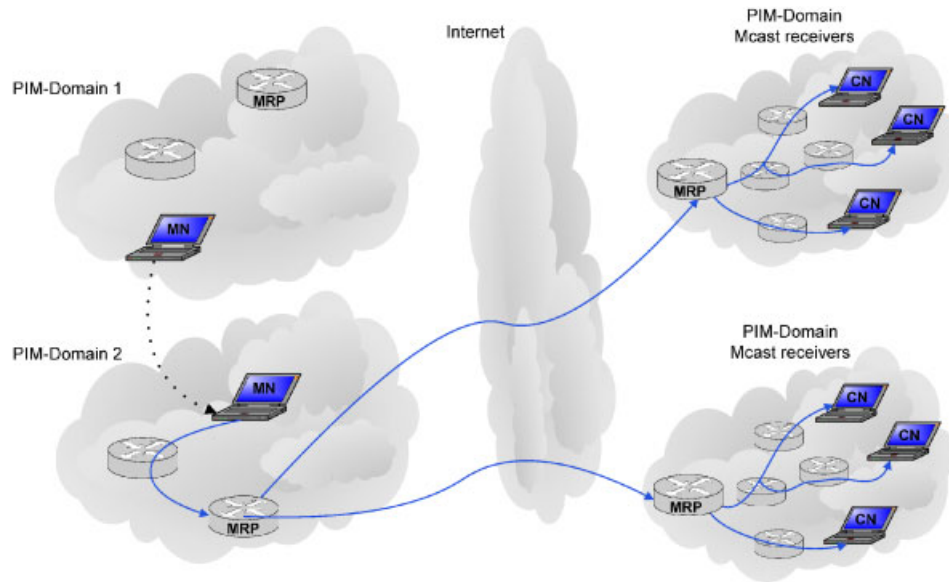

Fig. 1. Multicast source handover at a mobility-aware rendezvous point.

further design a tunnel– or SSM–based backbone distribution of packets between MRPs that is initiated by the primary MRP, which the source currently is attached to. As shown in Figure 1, the mobile performs address BUs with its directly associated rendezvous point to enable continuous data transmission after a handoff.

3.1.2. Mobility agent based

Alternate approaches rely on mobility-related anchor points serving as multicast agents, which aid the mobile source in compensating handover-related routing delays. They remain neutral with respect to the multicast routing protocol in use. The range-based mobile multicast (RBMoM) protocol [8] dynamically selects these agents based on advertisements, while multicast extensions for HMIPv6 [9], M-HMIPv6 [10], add multicast relay functions to HMIPv6 mobility anchor points (MAPs). A mobile source will transmit multicast packets via such agent, using the regional CoA allocated from the agent network as MS address. Whenever the source moves within a MAP domain, a BU with the anchor point is required, even though address changes are hidden to the multicast routing. In case of an inter-MAP handover, the mobile source rebinds with its previous MAP and takes its assistance for tunneling data into the previously established multicast tree as shown in Figure 2. This compensates for the delays until multicast routing has converged to follow the handover.

3.2. SSM Solutions

In this section the few existing solutions that support mobile sources in SSM are discussed. In contrast to any source multicast, receivers not only require source address updates to maintain binding caches, but need to actively subscribe to any new source identifier to initiate SSM channels. SSM filtering equally applies at the routing layer, causing the requirement of an active rejoin or state update at any on-tree multicast forwarder.

3.2.1. Control tree based

Thaler [11] proposes to construct a completely new distribution tree after the movement of a mobile source, following a receiver-initiated source specific join. This scheme relies on client notification, which is obtained from an additional, static control tree. Clients are permanently joined with the current data and the control tree, the latter distributing periodically source specific address states to the clients. The SSM control tree may be rooted at the Home Agent or some well known source address. Source specific state updates are to be tunneled to the control tree root and data tree handovers are activated on listener requests subsequently as shown in Figure 3.

3.2.2. Mobility anchor based

To reduce control-related update delays while working with client initiated tree reconstruction, Jelger and

DOI: 10.1002/sec

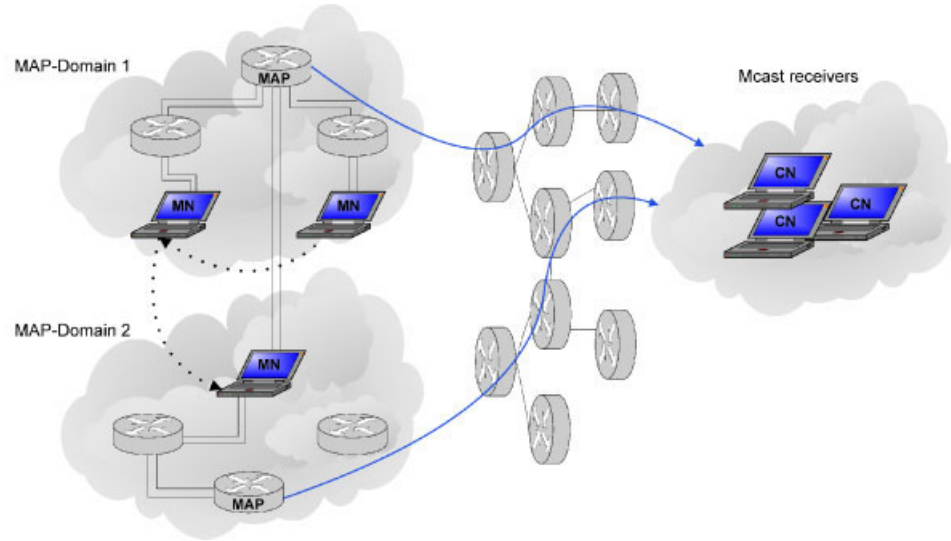

Fig. 2. Handover between mobility anchor points for multicast sources.

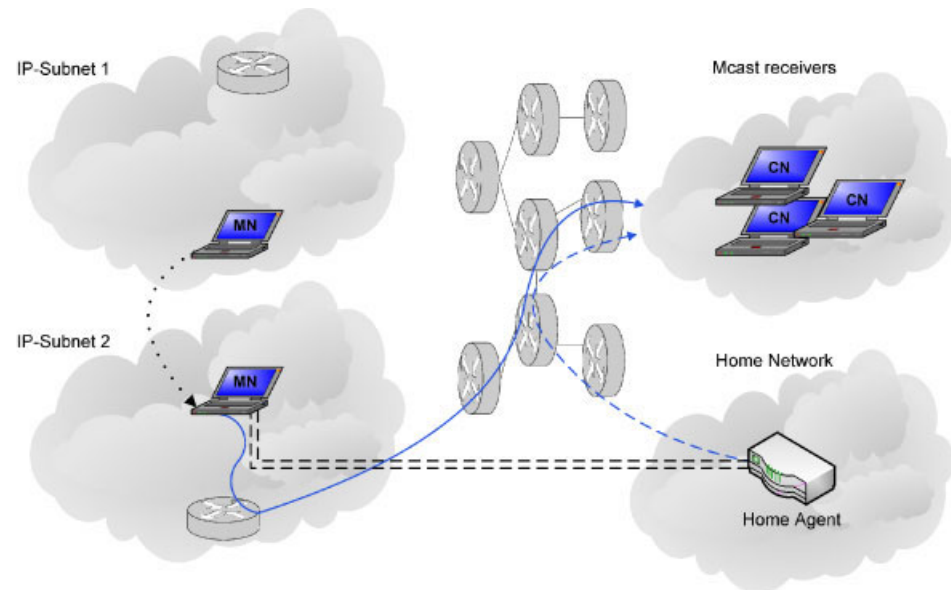

Fig. 3. Listener initiated SSM handover with control tree (dashed).

Noel [12] suggest to employ anchor points within the source networks. These persistent mobility agents will serve as a root of multicast distribution trees, cf. Section 3.1.2. Subsequent to handover, a moving source will rebind with its previous agent and tunnel multicast data via the already established source specific tree as shown in Figure 4. On reception of source address state updates, clients will join to the new (S, G) multicast channel and initiate a new shortest path tree. Client notification in the original proposal has been foreseen out of band, e.g., by SDR, but could equally be obtained by tunneling via the previous distribution tree.

This scheme, which suffers from the multicast-inherent problem of tree construction being unsynchronized with sources, does support a continuous data distribution during client-initiated handovers.

3.2.3. *Mobility-adaptive trees*

A routing protocol adaptive to SSM source mobility, the Tree Morphing has been introduced by the authors

DOI: 10.1002/sec

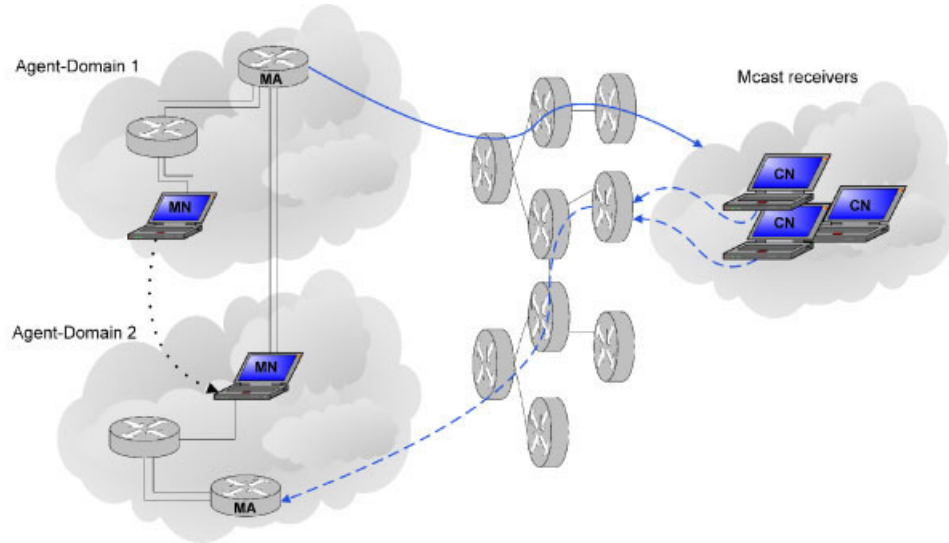

Fig. 4. Listener initiated SSM handover assisted by mobility agents.

in Reference [13]. A mobile MS away from home will transmit *unencapsulated* data to a group, using its HoA on the application layer and its current CoA on the Internet layer, just as unicast packets are transmitted by MIPv6. In extension to unicast routing, though, the entire Internet layer, i.e., routers included, will be aware of the permanent HoA. Maintaining address pairs in router states like in binding caches will enable all nodes to simultaneously identify (*HoA*, *G*)-based group membership and (*CoA*, *G*)-based tree topology. When moving to a new point of attachment, the MS will alter its address from previous CoA (pCoA) to new CoA (nCoA) and eventually change from its previous designated multicast router (pDR) to a next designated router (nDR). Subsequent to handover it will immediately continue to deliver data along an extension of its previous source tree. Delivery is done by elongating the root of the previous tree from pDR to nDR (s. Figure 5). All routers along the path, located at root elongation or previous delivery tree, thereby will learn MS's new CoA and implement appropriate forwarding states.

Routers on this extended tree will use RPF checks to discover potential shortcuts. Registering nCoA as source address, those routers that receive the state update via the topologically incorrect interface will submit a join in the direction of a new SPT and prune the old tree membership, as soon as data arrives at the correct interface. All other routers will re-use those parts of the previous delivery tree, which coincide with the new shortest path tree. Only branches of the new shortest path tree, which have not previously been established, need to be constructed. In this way, the previous SPT will be morphed into a next shortest path tree. This algorithm does not require data encapsulation at any stage.

3.3. Résumé

Multicast routing protocols compliant with moving sources span a wide solution space, but share the requirement to update the source address binding at a mobility-aware entry point of the distribution tree. This entity may be a dedicated agent or a common multicast router. In any case, it requires protection against misuse on the one hand, and may serve as a guard against unwanted packets forwarded down the distribution tree on the other. The AuthoCast protocol we define in detail in the following section will take advantage of this architectural semantic, which can be identified as an inherent invariant of the problem scope.

4. Protocol Design

In this section we will introduce the AuthoCast protocol framework for multicast address authentication of moving sources, which is jointly applicable to all multicast mobility management schemes, cf. Section 3. In admitting a design of equal extensions at the packet level, protocol operations will differ only at intermediate routers and receivers. Based on cryptographic address identifiers [14], all communication remains unidirectional. Following a handover, a mobile source

DOI: 10.1002/sec

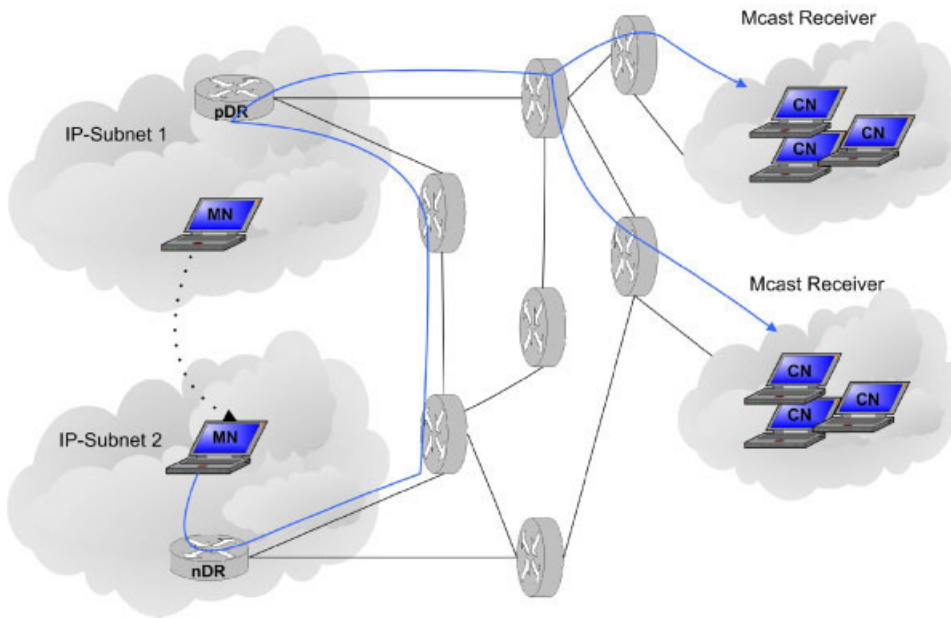

Fig. 5. Adaptive tree management: elongation and optimization in the Tree Morphing scheme.

is just obliged to send packets including its source authentication, without being aware of routing protocol or receiver specific requirements of the current distribution algorithms in use. The approach is thus compliant to the general multicast paradigm, where a sender only transmits packets, while receivers initiate routing, and the infrastructure conducts an appropriate data distribution.

4.1. Objectives

The multicast mobility management schemes introduced in the previous section have in common the requirements to update source address states at some routing entities and at the receivers. Presupposing properly established states at routers and receivers prior to handover, the AuthoCast protocol is intended to provide reliable source authentication and to sustain integrity at mobility-related state transitions. Such state updates, performed at Internet infrastructure nodes and at receivers, require a robust, cryptographically strong authentication.

A mobile MS contributing to group G needs to submit a forwarding state update, as soon as basic handover operations are completed. In order to implement processing at the tree maintenance layer, packets have to signal the update context given by (HoA, G) and the new multicast forwarding states ($nCoA$, G). These information correspond to mobility BUs as operated by MIPv6 at unicast end nodes. To ensure consistency and avoid signaling redundancy, update messages should simultaneously serve both, the routing infrastructure as well as receivers.

Since an additional signaling would add undesired overhead, a major objective lies in embedding BU information into the data packets immediately following the handover. Using a 'piggy-back' mechanism bears an additional advantage. Whenever packet disordering occurs at the network layer, data packets are prevented from passing protocol signaling messages. Even though payload packets can still arrive in an incorrect order, the design should guarantee that the first packet received contains the update instructions. Additional control to improve reliability should be foreseen.

4.2. Authentication Mechanism

In the mobile regime, handover authentication is equivalent to providing a proof-of-ownership for the HoA, which serves as the permanent node identifier. Multicast signaling is *bound to a one-way authentication* of the mobile source, i.e., the owner of the HoA has to provide proof of authenticity for the update packets without returning messages to the originator. Currently, the only appropriate method known for achieving this goal is the use of cryptographically generated addresses (CGAs) [14]. By choosing its HoA of CGA kind, a sender can provide cryptographically strong proof of HoA ownership within a *single*, autonomously verifiable update packet.

DOI: 10.1002/sec

A HoA can serve as a cryptographic identifier by obtaining the IPv6 interface identifier from five coded bits and 59 bits of the SHA-1 hash of the public key of an RSA key pair generated prior to mobility operations. Packets qualifying for autonomous authentication then need to carry the original public key along with a signature of the mobility data. Mobility data contain the CoA, the group address, the BU message including the mobility header and all options up to the last CGA Parameters option, as specified in Reference [15]. Standardized IPv6 protocol extension headers have been defined to place these data structures, as will be shown in the following section.

The implementation of AuthoCast is therefore realized by combining existing protocol structures with minimal extensions. Existing protocol implementations for multicast routing, like PIM-SM [5], or enhanced route optimization for MIPv6 [15] can easily be adapted, since all processing functions are already available. Furthermore this lightweight approach bears advantages for the protocol robustness, as standardized headers and protocols have already been analyzed thoroughly and have been used in real life scenarios.

4.3. Packet Design

Signaling a change of MS address after a Mobile IPv6 handover is implemented on the network layer by inserting additional headers into the data packets. The required information, group address, HoA and CoA, as well as proof of authentication can already be extracted from BU messages sent by mobiles to correspondent end nodes subsequent to every handover. The State Update Message needed for multicast can therefore be composed of several Mobile IPv6 headers, and there is no need to define a full new protocol. AuthoCast messages can thus be processed transparently with regular, CGA authenticated [15] BUs. Nevertheless they need to be interpreted by routers along the packet's path.

To enable visibility at routers of such transparent multicast mobility signaling, a Router Alert Option is inserted in a Hop-by-Hop Option Header [16]. Extension header processing is normally omitted according to the IPv6 base specification [17]. By placing a specific alert in the Hop-by-Hop Option Header, predefined further instructions are processed by every router receiving the extended packet on its path.

The full AuthoCast signaling is built by chaining the IPv6 extension headers as to be piggy-backed with the first data packet(s). Figure 6 shows the combined packet format used after source handover. The mobile source sends the packet exactly as instructed by the multicast

Fig. 6. AuthoCast IPv6 header sequence for authenticated state updates of mobile multicast sources.

mobility management scheme in operation, using either its previously valid CoA, when tunneling applies, or its current CoA, whenever unencapsulated transmission is foreseen.

According to the extension header order of Reference [17], the first header has to be the Hop-by-Hop Option header containing the Router Alert Option as described above. The Mobility Destination Options header follows next. It contains the HoA Option [1], which signals the HoA to routers and receivers. The CGA Parameter Option and the CGA Signature Option are stored in the Mobility Header [1]. These two options are specified in Reference [15] and contain the data necessary for CGA authentication. Finally, the upper layer header including data is the last part of the message.

4.4. Protocol Operations

The AuthoCast protocol operations jointly applicable to all mobile multicast routing solutions add the extension headers and thereby ensure that sender authentication is synchronously performed with the first packet at the entry point of the multicast tree. This common signaling scheme is visualized in Figure 7. Distinguished semantics only apply at the router level, whereas sources and receivers remain agnostic of the particular mobility management scheme in operation.

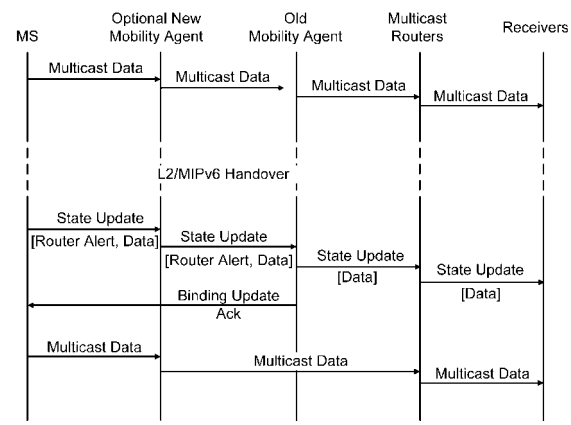

Fig. 7. AuthoCast signaling flow subsequent to handover.

DOI: 10.1002/sec

4.4.1. Operations of the mobile source

After address configuration have completed at a Mobile IPv6 handover, the MS continues to send its payload to the multicast group. Thereby, it follows the algorithm set by the mobile multicast routing scheme in use as described in Section 3. It augments its first packet(s) with the AuthoCast update header sequence shown above.

In rigorously reliable networks without packet loss or re-ordering, the state update message could be sent only once in the first packet after a MS handover. Since real networks are error-prone, error resilient mechanisms have to be used for the source to successfully inject its new state. Since Hop-by-Hop Alerts increase routing load, the mobile source should implement a conservative strategy of repeating the AuthoCast header extension within a first number of packets. According to network conditions and the mobility scheme deployed, the update message may be acknowledged by the corresponding multicast agent or pDR. A Mobile IPv6 Binding Acknowledgement Message [1] sent to the mobile source indicates the reception of a new state update message and leads the mobile source to return to regular multicast packet transmission conformal to the routing scheme it uses.

4.4.2. Operations of network agents

The mobility management schemes introduced in Section 3 jointly rely on some agent permanently positioned within the network that assists in mobile source handovers. Agent choices have been made to take advantage of the home agent, of a mobility-aware PIM rendezvous point, regional MAPs or multicast designated routers. The common function of all agents is to serve as transit point between the new location of the mobile source and a previously established multicast distribution tree. They hold mobility binding information to identify a source at its current location and receive mobile sender updates through a tunnel, as unicast messages, via a source route, or some multicast forwarding mechanism.

On the reception of a state update packet, the multicast agent will apply ingress filters to narrow the window for CGA spoofing and for the misuse of Hop-by-Hop option headers, which require analysis according to Reference [17]. Thereafter it will identify the Router Alert option as specified in Section 4.3. The option *value* field defines that this message is a multicast mobility State Update message. Hence, the appended headers as specified in Section 4.3 require processing according to the AuthoCast protocol. The router will extract the HoA of the sender from the following Destination Option header. The sequence number of the subsequent BU message is examined, leading to a skip of authentication and update in case of a repeat.

For valid sequence IDs, the mobility header including CGA Options will be processed. The CGA parameter data structure is extracted from the CGA options. With this data structure, the CGA verification of the HoA is executed as described in Reference [14]. This test includes a sanity check, a prefix inspection and an RSA signature verification for the HoA of the Mobile Node. If tests arrive at a valid signature, the packet can be accounted to the owner of the HoA based on its cryptographically strong authentication. As signed with mobility data, it can further be concluded that the current CoA is associated to a sender, who is the owner of the HoA. Consequently, the following updates of the binding cache and forwarding states can proceed in an authorized fashion. Conversely, a router experiencing any failure within this verification procedure will immediately discard the packet without further obligations.

After the authentication and state update have been successfully completed, further treatment of the packet will proceed according to the mobility scheme in use. In all cases, where binding states at routers are limited to the multicast agent, the Hop-by-Hop Router Alert header will be removed and the packet natively passed on to the receivers. Whenever on-tree routers maintain binding states, the packet will be forwarded without header changes, i.e., including the Router Alert option, and processed as described in the following section.

4.4.3. Operations of on-tree routers

Routers on the delivery path receiving a packet with BU and CGA headers will take notice only if the Router Alert Hop-by-Hop option is included. This will happen, whenever on-tree state updates are required for the multicast mobility management protocol in use.

In the case where on-tree routers receive an update packet with router alert, they will apply ingress filters, perform parameter examination, sanity checking and signature verification exactly as the multicast agent beforehand and will equally discard any improper packet. After the verification, a router will perform binding state updates as specified by its mobility protocol.

4.4.4. Operations of ASM receivers

Any source multicast receivers will analyze the state update packets analogously to the algorithms

DOI: 10.1002/sec

mentioned before. On successful CGA verification, the HoA Option in the Destination Option Header is treated as a BU [1] and the matching Multicast Binding Cache entry is updated. The packet payload is then passed to the transport layer with the correct addressing, i.e., source HoA and destination G. This ensures lossless, transparent multicast communication on the application layer.

4.4.5. Operations of SSM receivers

SSM receivers will execute authentication, BU and data delivery exactly as ASM listeners. In addition they will need to update multicast channel subscription, i.e., to issue a source specific join to (*nCoA*, *G*), where *nCoA* is the new source address received within the BU.

5. Evaluation

In this section we evaluate key aspects of the protocol. The quality of the proposed implementation can be judged from overheads introduced by signaling load, operational processing and implementation complexity, as well as from its robustness against perturbed network conditions or security threats. While the convergence of the mobile multicast routing protocol remains unaffected by authentication, state update costs at the routing infrastructure differ.

5.1. Protocol Overheads

The AuthoCast protocol is implemented by inserting a single header, the Router Alert Option, into the BU message required for client updates and included in the first regular multicast transmission payload packet(s). Therefore, no additional signaling is required. Instead, all necessary information is contained in the Mobile IPv6 BU Message and HoA Option, including the CGA authentication parameters. The alert header accounts for an overhead of 32 bits. It should be noted that headers are composed at the mobile source and may be only partially removed along the packet's path. Thus no MTU-size issues occur, as are common for intermediate tunneling or header adjoining.

The design introduced for the AuthoCast approach implies only minimal changes to existing communication protocols, as well. It re-uses the Router Alert Option for defining the State Update Message, which only requires a new value for the Routing Alert *value* field as to indicate our new State Update Message type. All other operations are based on existing protocols such as Mobile IPv6. This includes the BU Message and CGA Parameter with CGA Signature Options in the Mobility Header as defined in Reference [15]. By re-using well established headers and protocols, implementations can be easily realized in a lean and secure fashion.

5.2. Processing Overheads

The critical measure of protocol overheads must be seen in the operational complexity of the State Update packet, which requires processing at routers along the path. Ingress filters restrict updates to originate from local networks, only.

On the one hand, algorithmic costs of source mobility management remain comparable to efforts for regular multicast state management, e.g., in PIM-SM register messages. On the other hand, cryptographic verification of CGA HoAes imposes computational labor. At first, a SHA-1 hash value is generated and checked against the interface identifier. An RSA signature verification follows, which is a computationally expensive operation of complexity $\mathcal{O}(k^2)$, where k denotes the length of the key modulus [18].

Verifying signatures of every packet—including bogus data—is undesirable. As has been foreseen in header design, a sanity check is therefore executed on the input data first. Packets failing this check must be discarded immediately. Subsequently, bogus packets are ruled out by testing on the interface identifier integrity, as well.

To quantify the processing overhead of the CGA verification, we have implemented the scheme on a standard Linux platform using the OpenSSL [19] cryptographic library. We compare RSA and DSA for typical ranges of key lengths (512–2048 bits) with ECC of corresponding strength (secp160r1/secp192r1/secp224r1). Absolute processing times were measured for packet sizes from 500 to 1500 bytes. Averages were taken over 100 randomly generated keys, each of which employed to verify 10 000 packets. Results obtained on a single core of a standard PC with 2.4 GHz AMD Athlon X2 processor are displayed in Figure 8.

Strikingly, signature *verification* using RSA on the current level of key strength is fastest by almost one order of magnitude. Processing costs remain independent of data packet sizes, since the overhead of evaluating SHA-1 hashes is negligible as compared to signature verification. 10 μs are needed by RSA to perform the validation process for a typical current key strength of 1024 bits.

DOI: 10.1002/sec

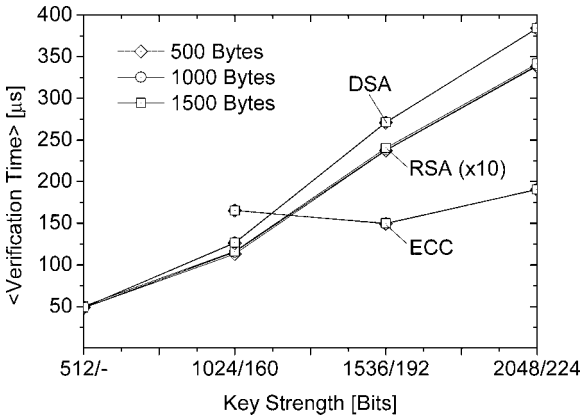

Fig. 8. Processing times for CGA signature verification for RSA/DSA-512 . . . 2048 and ECC-160 . . . 224 with varying packet sizes.

If performed on a standard software router platform, the AuthoCast packet authentication will lead to an increase of processing cost by about a factor of 10. This additional packet delay of $\sim$10 µs caused by the security protocol operations will not result in a noticeable end-to-end performance degradation, as this timescale is still in the range of regular fluctuations for packet network transmission. When performed in software on the main processor of a wirespeed router platform, though, packet authentication will degrade forwarding performance by three to four orders of magnitude. Consequently, hardware-accelerated routers will require cryptoprocessing extensions to prevent performance flaws. Since the verification procedure is solely based on individual packets, cryptoprocessing can be implemented on linecards, sustaining full scalability and preventing bogus packets from affecting the central processing unit of the router.

Nevertheless, complexity of RSA signature verification is the drawback of the AuthoCast scheme. Alternate asymmetric authentication methods could be employed to replace RSA, e.g., elliptic curve cryptography. ECC signature *verification*, though, did not appear at reduced calculation costs in our emulation applied to realistic keys of medium strength. RSA execution is limited to one instance per MS handover at selected routers of the distribution tree. In medium mobility regimes of moderate sender densities, requirements may not be expected to exceed a frequency of a few updates per minute. Thus cryptographic verification challenges are likely to remain significantly below SEND [20] operations, where the number of required signature operations at routers is up to the order of a few dozens per second.

5.3. Robustness

5.3.1. Network perturbance

In reliable networks without packet loss and reordering, the state update message could be sent only once in the first packet subsequent to a MS handover. AuthoCast objects possible loss of update messages by a confirmation message sent from the mobility agent to the MS. This acknowledgement controls the traversal of the error-prone wireless access network and a reconnect to the previous delivery or control tree rooted at this agent. State updates may be retransmitted according to adaptive timers until this acknowledgement arrives.

As another problem, packet re-ordering needs addressing in real networks. Considering disconnection times at layer 2 handovers, all buffered multicast packets will be delivered after the reconnect as new packets including the update information.[‡] Since our protocol 'piggy-backs' the update information in the multicast data packets, state update signaling cannot be overrun by data. In this way, the first packet arriving at a router initiates the state update. Note that repeated packet receptions are a priory identified through sequence numbers and thus will not lead to iterated update processing.

5.3.2. Resilience against common attacks

The protocol has to withstand several common attacks. Threats to routers performing multicast mobility management may derive from the costs of processing unwanted packets. Commonly, current routers examine an IP datagram in the 'slow path' when it carries the Router Alert option, and an excess of such datagrams may cause route performance degradation. To mitigate the threat of resource exhaustion from suchlike and further denial of service attacks, ingress filters are applied at AuthoCast routers. Recent discussions of Router Alert handling [21] further suggest a change in router design such that the alert option is examined prior to entering the slow path. As cryptographic verifications of state update packets can be performed on appropriate line cards, a router recognizing the Router Alert option in 'normal path' could avoid to switch to the slow.

By replaying valid, intercepted packets, an attacker could try to impose extra burden onto the routing

[‡]At this point the multicast-extended mobile IPv6 stack is probably required to fragment buffered packets. Fragmentation at end nodes has been foreseen in IPv6 and does not cause problems.

DOI: 10.1002/sec

infrastructure. A victim of a replay attack would have to verify the CGA every time a packet arrives. The protocol withstands these attacks by using the sequence number in the BU message, which is protected by the packet signature. Packets with incorrect sequence numbers fail the sanity checks described above. The AuthoCast protocol is therefore only as vulnerable as standardized well-known protocols such as SEND [20] and does not introduce new security threats. Thus new messages have to be processed cryptographically by routers only once.

An attacker could configure its own cryptographically valid HoA and issue a state update to the network. As a mobile multicast agent could identify such packet according to its source filters, it would be discarded on arrival at the first designated agent router. Such attack will not lead the network into forwarding bogus packets along any multicast distribution tree, but will limit transmission to the initial multicast agent. Consequently, the AuthoCast implementation does not reopen the opportunity of network assisted, distributed denial of service attacks as inherent to unprotected ASM. Additionally, generating CGAs and RSA signatures is much more complex than verifying them. The derivation of CGAs for a number of interface identifiers is a time consuming task, especially if the victim requires a high security parameter *sec*, cf. Reference [14]. To quantitatively estimate the complexity of generating CGAs, successive valid CGAs have been generated by changing the modifier field. All other input values to the function were left unchanged. Table I shows the security parameter *sec*, the mean number of modifier steps (the mean modifier difference between two valid CGAs) and the standard deviation.

The results reflect the expected strong exponential increase in complexity. Incrementing the required *sec* value on the receiver's side by one results in a rise of computational complexity by at least five orders of magnitude until a valid CGA is found. A node facing an attack could therefore require remote stations to (temporarily) use higher *sec* values if unusual high load occurs. Precomputed CGAs would then no longer be usable by attackers. Additionally, RSA signature generation is of complexity $\mathcal{O}(k^3)$. In contrast, analyzing CGAs only requires computation of two SHA-1 hash values and an $\mathcal{O}(k^2)$ signature verification.

Table I. CGA generation complexity.

Sec	Mean no. of modifier steps	Std. deviation
0	1	0
1	66 113	256
2	2 591 220 608	50 901

6. Related Work on Multicast Sender Authentication

Significant work has been dedicated to secure multicast group management. This has been reviewed in Reference [22] and re-examined from a mobility perspective in Reference [23]. Very little attention has been committed to securing mobile sources that operate in a regime where the legitimacy of a source address cannot be controlled by conventional means.

An early analysis of multicast security threats, as well as counter measures for multicast group access control and sender authentication have been presented in Reference [24] for the Core Based Trees (CBT) protocol . In presence of appropriate certification authorities, the authors propose to employ an authorization server that asynchronically verifies packets in transit. At the creation time of a multicast group, a certificate is issued and administered by this authorization server. Based thereon and in presence of a PKI, a security association identifier is created for each sender and included in multicast packets. After the authorization server has convicted a source of emitting invalid packets, source filters are activated to block further forwarding. As already apparent in the static case, this scheme is too slow to perform a synchronous access control for senders. In the mobility regime, a rapidly moving node could continuously issue malicious packets without blocking source filters being active in time.

The efficiency of authenticating multicast packet flows could be increased in TESLA [25,26] by using one-way key chains to generate message authentication code (MAC) keys valid within limited time intervals. Receivers buffer packets until the sender discloses the secret MAC key at the end of each time interval and enables authentication. Subsequent publications introduced further improvements, e.g., resistance to packet loss, reordering and data injection in Lysyanskaya *et al.* [27], or reductions of signature verifications in PRABS [28], or the joined minimization of packet overhead, signature processing costs in combination with loss resilience in Reference [29]. However, these protocols do not address the mobility problem of initial sender access authorization. Even though packets originating from an illegal source can be discarded by the receivers, an attacker can still inject traffic into a mobility-tolerant multicast distribution infrastructure.

DOI: 10.1002/sec

Several further developments have advanced the early, centralized key management scheme of Ballardie and Crowcroft [23]. A scalable infrastructure for multicast key management (SIM-KM) has been designed by Mukherjee and Atwood [30,31], which divides a secure distribution tree into a hierarchy of subgroups. Distributed subgroups are served by distinct group controllers that provide a proxy encryption function to convert cipher messages for one key into cipher text for another without revealing secret encryption keys. A central group manager initiates the creation or annihilation of subgroups and distributes a symmetric key to all group members and controllers. This key is used for source-specific packet authentication at intermediate proxy controllers and receivers, limiting overheads in message data and computation due to symmetric cryptography. In a static environment, this robust scheme admits favorable performance properties by segregating group-external packets based on lightweight symmetric MACs, while performing (group-internal) decryption and source authentication with the help of asymmetric cryptography. The mobile environment, though, requests a service to operate in changing multicast distribution topologies. Using SIM-KM (or another hierarchical key management) handovers will lead to a reorganization of controllers which is complex and far too slow to remain seamless.

Some approaches concentrate on sender access control with respect to the routing infrastructure. A simple admission scheme is proposed in Reference [32] as a complement to multicast listener discovery (MLD) [33]: Prior to data dissemination, a new source issues an empty packet to the multicast group, which triggers an admission procedure between the access router and an authentication, authorization and accounting (AAA) server. In a mobile regime, such AAA third party admission will be required on each handover, thus placing a significant signaling burden as well as delay onto mobile multicast protocols. For the special case of BIDIR-PIM multicast routing [34], Wang and Pavlou [35] devise an admission control function to reside on the rendezvous point (RP). After the reception of register packets from a new sender, the RP activates sender access control lists at on-tree routers to regulate packet distribution within the multicast tree. For a mobile source, these access controls will invalidate on handover as topological addresses change.

Cryptographically derived addresses have been used to secure multicast group membership management [36]. The authors propose to apply the CGA concept to group addresses in order to secure MLD Report messages. For each group, authorized group members receive a public-private key pair from a group controller in a secure manner, which corresponds to the cryptographic group address. When a node wishes to join or leave the group, it includes the public key in its listener report and signs the message. On reception of the MLD packet, a router can verify a proof-of-group membership by evaluating the corresponding group address hash along with the signature of the packet.

Mobility BUs based on CGA authentication have been standardized recently in Reference [15]. To the best of our knowledge, neither MS address authentication has been foreseen by CGAs yet, nor have been solutions worked out for a secure and autonomously verifiable MS handover management.

7. Conclusions, Discussions and Outlook

In this paper we presented a protocol for the authentication of mobile multicast senders, which jointly applies to the network infrastructure and to receivers. This cryptographically strong, one-way signaling scheme bears two major advantages. At first, it conforms to all multicast mobility management schemes presently proposed and allows for a uniform signaling of the mobile source. Hence a mobile sender can operate independent of mobile multicast routing details, as is compliant with the common paradigm of multicast. At second, this authentication protocol has been designed by minimal extensions of standard mobility protocols. Regular BUs on the Internet mobility layer are interpreted by the routing infrastructure concurrent to data transmission. Its realization minimizes signaling overhead, additional implementation requirements, and thereby deployment complexity.

Receiving AuthoCast messages adds additional processing load on mobility managing devices, which is the major drawback of this approach. However, it should be stressed that for every mobility handover only one update message is required. Authentication may be performed by any asymmetric cryptographic algorithm. Our evaluations revealed that RSA standard cryptography in combination with software routing or cryptoprocessing linecards does attain acceptable performance, while ECC and DSA in the current key regime remain too slow. The presented protocol is protected from resource exhaustion and replay attacks by internal sequence numbers and ingress filters. It is

DOI: 10.1002/sec

robust against common network perturbances and withstands misuse of multicast packet replication disposed for distributed denial of service attacks.

This work can be extended to incorporate a general source admission control at the multicast routing layer. In a single source scenario or SSM case, the multicast group address can simply be created as a cryptographic identifier by the sender derived from its identical public-private key pair used for its CGA. Any router receiving packets for this group will then be able to prove legitimacy of the sender without further knowledge or configuration. In a multi-source environment, an appropriate key management will be required to achieve an autonomous source admission for predefined group, which is subject to future work. The AuthoCast protocol can be adapted to overlay multicast by appropriate extensions, as well.

Acknowledgement

This work has been supported by the German Bundesministerium für Bildung und Forschung within the project *Moviecast* (http://moviecast.realmv6.org). We thank the referees for their thorough advices which helped significantly in improving this article.

References

1. Johnson DB, Perkins C, Arkko J. Mobility support in IPv6. *RFC 3775*, IETF, June 2004.
2. Schmidt TC, Wählisch M, Fairhurst G. Multicast mobility in MIPv6: problem statement and brief survey. IRTF Internet Draft—work in progress 04, MobOpts, July 2008.
3. Deering SE. Host extensions for IP multicasting. *RFC 1112*, IETF, August 1989.
4. Holbrook H, Cain B. Source-specific multicast for IP. *RFC 4607*, IETF, August 2006.
5. Fenner B, Handley M, Holbrook H, Kouvelas I. Protocol independent multicast - sparse mode (PIM-SM): protocol specification (revised). *RFC 4601*, IETF, August 2006.
6. Xylomenos G, Polyzos GC. IP multicast for mobile hosts. *IEEE Communications Magazine* 1997; **35**(1): 54–58.
7. Romdhani I, Bettahar H, Bouabdallah A. Transparent handover for mobile multicast sources. In *Proceedings of the IEEE ICN'06*, Lorenz P, Dini P (eds). IEEE Press, NJ, USA, April 2006.
8. Lin CR, Wang K-M. Scalable multicast protocol in IP-based mobile networks. *Wireless Networks* 2002; **8**(1): 27–36.
9. Soliman H, Castelluccia C, Malki K, Bellier L. Hierarchical mobile IPv6 (HMIPv6) mobility management. *RFC 5380*, IETF, October 2008.
10. Schmidt TC, Wählisch M. Seamless multicast handover in a hierarchical mobile IPv6 environment (M-HMIPv6). Internet Draft—work in progress (expired) 04, individual, December 2005.
11. Thaler D. Supporting mobile SSM sources for IPv6. *Proceedings of IETF Meeting*, individual, December 2001.
12. Jelger C, Noel T. Supporting mobile SSM sources for IPv6 (MSSMSv6). Internet Draft—work in progress (expired) 00, individual, January 2002.
13. Schmidt TC, Wählisch M. Morphing distribution trees—on the evolution of multicast states under mobility and an adaptive routing scheme for mobile SSM sources. *Telecommunication Systems* 2006; **33**(1–3): 131–154.
14. Aura T. Cryptographically generated addresses (CGA). *RFC 3972*, IETF, March 2005.
15. Arkko J, Vogt C, Haddad W. Enhanced route optimization for mobile IPv6. *RFC 4866*, IETF, May 2007.
16. Partridge C, Jackson A. IPv6 router alert option. *RFC 2711*, IETF, October 1999.
17. Deering S, Hinden R. Internet protocol, version 6 (IPv6) specification. *RFC 2460*, IETF, December 1998.
18. Cormen TH, Leiserson CE, Rivest RL, Stein C. *Introduction to Algorithms* (2nd edn). MIT Press, MA, USA, 2001.
19. Cox M, Engelschall R, Henson S, Laurie B, *et al*. Openssl. http://www.openssl.org, 2008.
20. Arkko J, Kempf J, Zill B, Nikander P. Secure neighbor discovery (SEND). RFC 3971, Internet Engineering Task Force, March 2005.
21. Rahman R, Ward D. Use of IP router alert considered dangerous. Internet Draft—work in progress 00, individual, October 2008.
22. Challal Y, Bettahar H, Bouabdallah A. A taxonomy of multicast data origin authentication: issues and solutions. *IEEE Communications Surveys & Tutorials* 2004; **6**(3): 34–57.
23. Kellil M, Romdhani I, Lach H-Y, Bouabdallah A, Bettahar H. Multicast receiver and sender access control and its applicability to mobile IP environments: a survey. *IEEE Communications Surveys & Tutorials* 2005; **7**(2): 46–70.
24. Ballardie T, Crowcroft J. Multicast-Specific Security Threats and Counter-Measures. In *SNDSS'95: Proceedings of the 1995 Symposium on Network and Distributed System Security (SNDSS'95)*, Washington, DC, USA, 1995; 2–16. IEEE Computer Society.
25. Perrig A, Canetti R, Song D, Tygar JD. Efficient and secure source authentication for multicast. In *8th Annual Internet Society Network and Distributed System Security Symposium, NDSS'01*, 2001; 35–46.
26. Perrig A, Canetti R, Tygar JD, Song D. The TESLA broadcast authentication protocol. *RSA CryptoBytes* 2002; **5**(2): 2–13.
27. Lysyanskaya A, Tamassia R, Triandopoulos N. Multicast authentication in fully adversarial networks. In *IEEE Symposium on Security and Privacy*, 2004; 241–253. IEEE Computer Society.
28. Karlof C, Sastry N, Li Y, Perrig A, Tygar JD. Distillation codes and applications to DoS resistant multicast authentication. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, USA, 2004.
29. Tartary C, Wang H, Pieprzyk J. A coding approach to the multicast stream authentication problem. *International Journal of Information Security* 2008; **7**(4): 265–283.
30. Mukherjee R, Atwood JW. SIM-KM: scalable infrastructure for multicast key management. In *LCN'04: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, Washington, DC, USA, 2004; 335–342. IEEE Computer Society.
31. Mukherjee R, Atwood JW. Scalable Solutions for Secure Group Communications. *Computer Networks* 2007; **51**(12): 3525–3548.
32. Islam S, Atwood JW. Sender access control in IP multicast. In *LCN'07: Proceedings of the 32nd IEEE Conference on Local Computer Networks*, Washington, DC, USA, 2007; 79–86. IEEE Computer Society.
33. Vida R, Costa LHMK. Multicast listener discovery version 2 (MLDv2) for IPv6. *RFC 3810*, IETF, June 2004.

DOI: 10.1002/sec

34. Handley M, Kouvelas I, Speakman T, Vicisano L. Bidirectional protocol independent multicast (BIDIR-PIM). *RFC 5015*, IETF, October 2007.
35. Wang N, Pavlou G. Scalable IP multicast sender access control for bi-directional trees. In *NGC'01: Proceedings of the 3rd International COST264 Workshop on Networked Group Communication*, London, UK, 2001; 141–158. Springer-Verlag.
36. Castelluccia C, Montenegro G. Securing group management in IPv6 with cryptographically based addresses. In *Proceedings of 8th IEEE International Symposium on Computers and Communication*, Turkey, July 2003; 588–593.

DOI: 10.1002/sec