A Light-Weight Implementation Scheme of the Tree Morphing Protocol for Mobile Multicast Sources*

Olaf Christ, Thomas C. Schmidt
HAW Hamburg, Dept. Informatik
Berliner Tor 7
D–20099 Hamburg, Germany
christ_o@informatik.haw-hamburg.de, t.schmidt@ieee.org

Matthias Wählisch
link–lab
Hönower Str. 35
D–10318 Berlin, Germany
waehlisch@ieee.org

Abstract

Multicast network services advantageously complement multimedia information and communication technologies, as they open up the realm for highly scalable multi-customer applications. Mobile environments providing shared limited bandwidth to a growing number of users will emphasize the need for multicast support even further. The traditional Internet approach of Any Source Multicast (ASM) routing, though, remains hesitant to spread beyond limited, controlled environments. It is widely believed that simpler and more selective mechanisms for group distribution in Source Specific Multicast (SSM) will globally disseminate to many users of multicast infrastructure and services. However, mobility support for Source Specific Multicast is still known to be a major open problem.

This paper presents a light-weight, secure implementation of the Tree Morphing protocol on the IPv6 network layer. This distributed routing algorithm allows for a continuous adaptation of multicast shortest path trees to source mobility. The approach introduced here is built upon standardized mobility signaling and includes strong authentication by means of cryptographically generated addresses. It neither requires definition of new protocol elements nor significant changes to the forwarding plane.

Keywords: Mobile IPv6, mobile source specific multicast, route optimization, protocol security, cryptographic identifier

1 Introduction

Mobile group communication is considered one of the major promising technologies of the near future, facilitating multimedia broadcasting and conferencing services, ubiquitous content availability as well as massive multiplayer games. The support of those and similar services is in the focus of emerging Internet Multimedia Subsystems (IMSs), which evolve not only technologically, but promise to generate major parts of provider revenues in the near future.

The virginal availability of a new, truly mobile IP enabled network layer [13] offers connectivity to nomadic users at roaming devices, while preserving communication sessions beyond IP subnet changes. It re-raises questions concerning the quality of IP services, as well: The real-time scenarios of interactive applications s.a. voice and video conferencing will appear significantly disturbed by packet loss intervals, delays or jitter exceeding 50–100 ms. IP multicasting will be of particular importance to mobile environments, where users commonly share frequency bands of limited capacities [14]. Thus, when heading towards VoIP/VCoIP or IP–TV broadcasting as a standard Internet services, important steps for global usability have to be taken with a focus on ease and quality.

In this paper we address the issue of mobile multimedia group communication, taking the perspective of Source Specific Multicast routing on the network layer. Source Specific Multicast (SSM) [4, 10], just released as an initial standard, is considered a promising improvement of group distribution techniques. In contrast to Any Source Multicast (ASM) [8], optimal (S,G) multicast source trees are constructed immediately from (S,G) subscriptions at the client side, without utilizing network flooding or Rendezvous Points. Source addresses are to be acquired by out of band channels, which a SIP [19] session initiation in conferencing scenarios may facilitate [23].

We discuss session mobility in the context of real-time multicast group communication and present a protocol implementation scheme, which adapts to sender mobility with minimal impact on service quality. Conferencing parties request seamless real–time performance of a mobility aware

*This ongoing work is supported by the German Bundesministerium für Bildung und Forschung within the project *Moviecast* (http://moviecast.realmv6.org).

group communication service, thereby attaining the simultaneous roles of mobile multicast listener and source. Intricate multicast routing procedures, though, are not easily extensible to comply with mobility requirements. Significant effort has been already invested in protocol designs for mobile multicast receivers. Only limited work has been dedicated to multicast source mobility, which poses the more delicate problem [18, 22]. The Tree Morphing protocol [20, 21], one of the few approaches to SSM source mobility management, enables immediate, unencapsulated multicast data transmission subsequent to Mobile IPv6 handovers.

As will be shown in the remaining paper, Tree Morphing can be implemented by applying minimal modifications and overheads to current standard protocols for unicast mobility management. The presented protocol design exhibits cryptographically strong authentication of message signaling, thereby complying to an enhanced security level of IPv6 mobility [2] and reaching well beyond common standards of multicast routing protocols such as PIM-SSM [9].

In this paper we first discuss the mobile multimedia group conferencing problem and related work. In section 3 we present our signaling protocol for mobile SSM sources. A first evaluation of our protocol follows in section 4. Finally, section 5 is dedicated to a conclusion and an outlook.

2 The Mobile Source Specific Multicast Problem and Related Work

2.1 Problem Statement

Multicast mobility management has to accomplish two distinct tasks, handover operations for mobile listeners and senders. While many solutions exist for roaming receivers [18], very few schemes have been detailed out for mobile multicast sources. Following a handover, multicast data reception can be fairly easily regained by a remote subscription approach in MIPv6 [13], possibly expedited by agent–based proxy schemes. In contrast, a multicast sender must not change source address while reassociating in a different network, since addresses are associated with media streams, e.g., in RTP sessions. Source Specific Multicast on the IP–layer, though, requires active subscription to contributing sources, thereby relying on topologically correct addresses. Routing at the occurrence of source movement is required to transform any (S, G) state into (S', G), while listening applications continue to receive multicast data streams admitting a persistent source address. Hence any simple mobility solution such as the remote subscription approach loses its receivers and will no longer function in this context.

With SSM an additional address problem needs consideration: A multicast listener, willing to subscribe to an (S, G) state, needs to report for the current location of the mobile source. Concurrently a multicast source submits data to a group of unknown receivers and thus operates without feedback channel. Address updates on handovers of a SSM source have to proceed without means of the mobile source to inquire on properties of the delivery tree or the receivers. As the nature of multicast routing is receiver initiated, whereas source movement is only detectable at the sender side, this leads to a somewhat obstructive interplay. All of the above severely add complexity to a robust multicast mobility solution, which should converge to optimal routes and, for the sake of efficiency, should avoid data encapsulation.

Finally, multicast mobility management inherits security risks of multicast and mobility. While the latter effectively instructs network redirects and thereby admits potential vulnerability to theft of service and resource exhaustion attacks, multicast packet replication bears the risk of network assisted distributed denial of service attacks. Any mobile multicast solution should therefore carefully secure protocol operations to comply with established IPv6 security standards.

2.2 Related Work

Three principal approaches to SSM source mobility are presently around.

2.2.1 Statically Rooted Distribution Trees

The MIPv6 standard proposes bi-directional tunneling through the home agent as a minimal multicast support for mobile senders and listeners as introduced by [25]. In this approach, the mobile multicast source (MS) always uses its Home Address (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.

Following a shared tree approach, [17] propose to employ Rendezvous Points of PIM-SM [9] as mobility anchors. Mobile senders tunnel their data to these "Mobility-aware Rendezvous Points" (MRPs), whence in restriction to a single domain this scheme is equivalent to the bi-directional tunneling. Focusing on interdomain mobile multicast, the authors design a tunnel– or SSM–based backbone distribution of packets between MRPs.

2.2.2 Reconstruction of Distribution Trees

Several authors propose to construct a completely new distribution tree after the movement of a mobile source. These schemes have to rely on client notification for initiating new router state establishment. At the same time they need to preserve address transparency to the client.

To account for the latter, Thaler [24] proposes to employ binding caches and to obtain source address transparency

analogous to MIPv6 unicast communication. Initial session announcements and changes of source addresses are to be distributed periodically to clients via an additional multicast control tree based at the home agent. Source–tree handovers are then activated on listener requests.

[11] suggest handover improvements by employing anchor points within the source network, supporting a continuous data reception during client–initiated handovers. Receiver oriented tree construction in SSM thereby remains unsynchronized with source handovers and thus will lead to an unforeseeable temporal progress. The authors henceforth are leaving the source in case of its rapid movement with an unlimited number of 'historic' delivery trees to be fed simultaneously.

2.2.3 Tree Modification Schemes

Very little attention has been given to procedures, which modify existing distribution trees to continuously serve for data transmission of mobile sources. In the case of DVMRP routing, [5] propose an algorithm to extend the root of a given delivery tree to incorporate a new source location in ASM. To fix DVMRP forwarding states and heal reverse path forwarding (RPF) check failures, the authors rely on a complex additional signaling protocol.

O'Neill [15] suggests a scheme to overcome RPF–check failures originating from multicast source address changes, by introducing an extended routing information, which accompanies data in a Hop-by-Hop option header.

An extended routing protocol adaptive to SSM source mobility, the Tree Morphing as visualized in figure 1, has been introduced by the authors in [20]. A mobile multicast source (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. fig. 1(b)). 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 short cuts. Registering nCoA as source address, those routers, which receive the state update via the topologically incorrect interface, will submit a join in the direction of a new shortest path tree 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 shortest path tree will be morphed into a next shortest path tree as shown in figure 1(c). This algorithm does not require data encapsulation at any stage.

3 An Implementation Scheme for the Tree Morphing Protocol

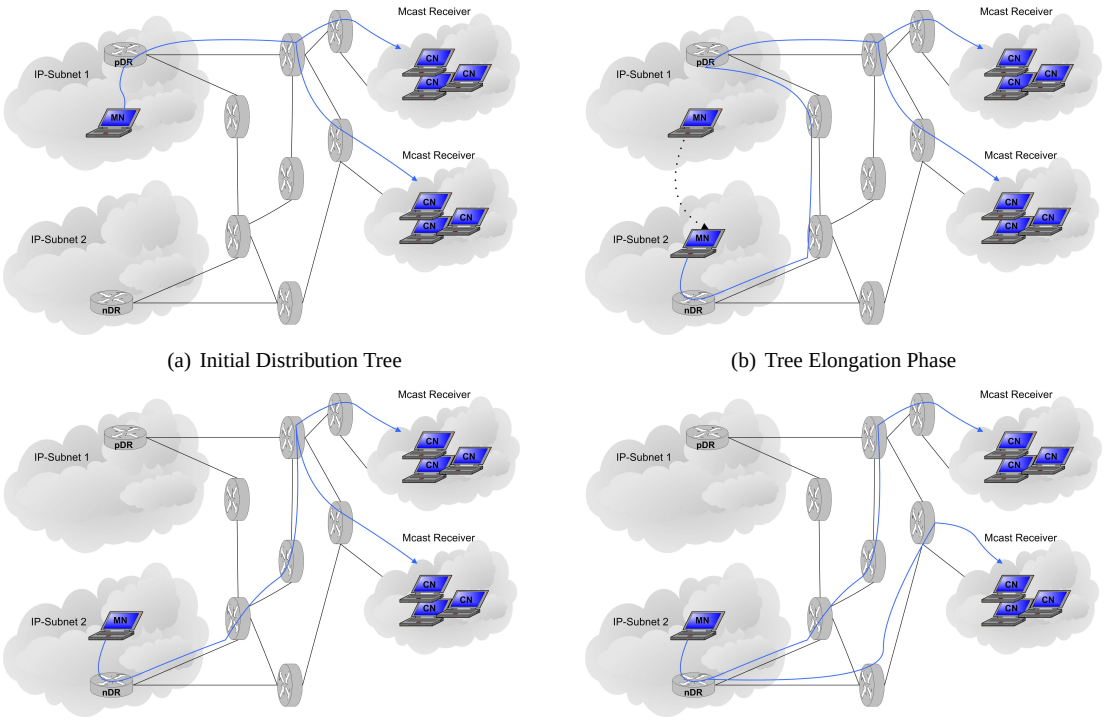
3.1 Objectives

The Tree Morphing Protocol requires a forwarding state update at the router infrastructure layer subsequent to any multicast source handover. In detail, the multicast distribution tree rooted at the pDR has to be transformed into a tree centered at nDR, as soon as Mobile IPv6 handover operations of the mobile source are completed. In order to implement this changes in tree topology, packets have to signal the update context given by (HoA, G) and the new multicast forwarding states (nCoA, G). Immediately following a handover, these three IP addresses have to be transmitted to all routers of the previous and - if possible - new distribution tree.

Regular SSM packet will invalidate from source filters at the routing layer, when transmitted at a new point of attachment of the mobile source. It is therefore important that routing states are updated prior to packet forwarding. The state update information required resemble mobility binding updates as operated by MIPv6 at unicast end nodes[1]. Since an additional signaling would add undesired overhead, a major objective lies in re-using these binding update information carried with data packets immediately following the handover. By using this 'piggy-back' mechanism, further undesired conditions, such as packet disordering, can be avoided. Even though payload packets can still arrive in an incorrect order, it should be guaranteed that the first packets contain the update instructions. The update thereby can be processed on arrival of any first packet. Additional control to improve reliability should be foreseen.

Another objective is to include the protocol operation with minimal extensions to the existing mobility signaling in order to design a simple and standard compliant protocol. The following implementation of the Tree Morphing Protocol is therefore realized by combining existing protocol structures with only few, unavoidable extensions, i.e., a

[1] Regarding the current state of knowledge [22] a Binding Update can be foreseen to be part of all future solutions for multicast source mobility.



(a) Initial Distribution Tree

(b) Tree Elongation Phase

(c) Intermediate Morphing Phase

(d) Converged Distribution Tree

Figure 1. Tree Morphing States

modified Hop-by-Hop option. Thus existing protocol implementations like PIM-SSM [9] can easily be converted, since all processing functions are already available. Furthermore this lightweight approach bears advantages for the protocol robustness, since the available, standardized headers and protocols have already been analyzed thoroughly and have been used in real life scenarios.

Special focus we devote to protocol security. The state updates that have to be performed in the Internet infrastructure are as susceptible to theft of identity as Mobile IPv6 or the Neighbor Discovery Protocol (NDP). Therefore a robust, cryptographically strong authentication of signaling is required, which has to be done without a feedback channel. By this one-way authentication the mobile source, i.e., the owner of the Home Address, has to provide proof of authenticity for the update packets self-consistently. This can be achieved analogous to [2] and [1] by using Cryptographically Generated Addresses (CGAs) [3]. Thus senders can provide cryptographically strong proof of HoA ownership within a *single*, self-consistent update packet.

3.2 Protocol Design

Signaling a new multicast source after a Mobile IPv6 handover is implemented on the network layer by inserting additional headers into the data packets. The required information, group address, home address and care-of address, as well as proof of authentication are already part of Binding Update messages sent by mobiles to correspondent end nodes subsequent to every handover. The State Update Message can therefore be composed of several Mobile IPv6 headers and there is no need to define a completely new protocol. Multicast Tree Morphing messages can thus be processed transparently with regular, CGA authenticated [2] Binding Updates. Nevertheless they need to be interpreted by every router along the packet way.

In order to enable visibility to routers of such transparent multicast mobility signaling, a Router Alert Option is inserted in a Hop-by-Hop Option Header [16]. This option is used to instruct routers to further inspect packet headers, which is normally omitted according to the IPv6 specification [7]. By placing a specific alert in the Hop-by-Hop Option Header, further instructions are processed by every router along the packet's way.

The format of a source mobility state update message reads as follows:

Option Type	Opt Data Len	Value

Figure 2. Router Alert Option

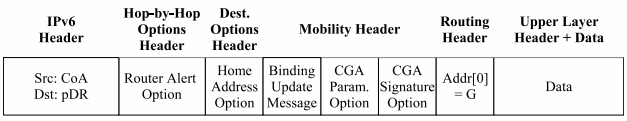


Figure 3. IPv6 header sequence including the State Update Message during Tree Elongation Phase on Path from Next to Previous Designated Router

Option Type 8-bit identifier of the type of this Hop-by-Hop Option. Its value is 0x05. The two highest order zero-bits specify [7] that nodes not understanding the option have to skip over it and continue processing the header. The third-highest-order bit defines that the data transmitted does not change en-route. The remaining bits have been assigned by IANA for the router option type.

Opt Data Len indicates an option length of two octets.

Value This value is subject to standardization by IANA for our special header. It specifies that the packet must be treated as a state update message. Further packet processing of the following option header is being defined by this value in order to update router forwarding states.

The header chain varies in different phases of the Tree Morphing Protocol and will be described in the following sections.

3.2.1 Tree Elongation

Figure 3 shows the packet's format during Tree Elongation. This packet is sent to the previous Designated Router (pDR) by the MN, using it's currently valid CoA. According to the extension header order in [7] the following header has to be the Hop-by-Hop Option header containing the Router Alert Option introduced in section 3.2. The Destination Options header follows next. It contains the Home Address Option [12] which signals the HoA to the receivers. The CGA Parameter Option and the CGA Signature Option are stored in the Mobility Header [12]. These two options are specified in [2] and contain the data necessary for CGA authentication. It should be remarked that multiple CGA Parameter Options can be stored sequentially in one Mobility Header. Since the maximum length of a single Mobility Option is 255 Bytes and the CGA Parameter structure will likely exceed this limit [2], it is divided into multiple options which can easily be concatenated and restored by the receiver. The last header consists in a Routing Header of the new type 7. This subtype of IPv6 routing headers needs specific definition like the type 2 routing header in the Mobile IPv6 standard [12]. In contrast to MIPv6, the address field may only contain one valid multicast address, allowing for application specific source routing. It allows for source routed packets with final destination of a multicast group. This is achieved by setting the type 7 Routing Header's address field to the multicast group address G. Furthermore, by defining a new type, dedicated firewall rules can be applied for state update messages. Finally, the upper layer header including data is the last part of the message.

In rigorously reliable networks without packet loss, the state update message could be sent only once in the first packet subsequent to a multicast source handover. Since real networks are error-prone, error resilient mechanisms have to be used to inform the source of successfully injecting the new states in all the routers along the path of tree elongation. As the pDR is the end point of the source routing path and can deliver confirmations reasonably, it is chosen to send a Mobile IPv6 Binding Acknowledgement Message [12] to the mobile node once a new state update message has been received successfully. It thereby secures the transmission of state updates along the tree elongation path, since source routing is used to deliver packets from the mobile node to the pDR. Once the mobile node has received the confirmation message, it may include the state update message in further packets to ensure a desired degree of redundancy for state update distribution along the multicast tree.

3.2.2 On–Tree Multicast Transmission

After the source routing, further multicast transmission originates from the pDR and re-uses the delivery tree established prior to handover. The packets sent during regular multicast transmission (see figure 4) will be stripped of the Routing Header as soon as the source routing transition point pDR has been reached. This is achieved by copying the group address G from the Routing Header into the destination address field of the IPv6 header.

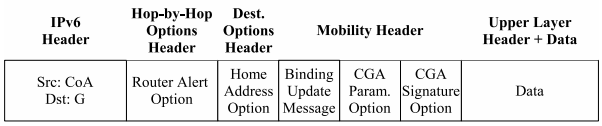


Figure 4. IPv6 header sequence including the State Update Message from Previous Designated Router to Multicast Group

3.3 Protocol Operation

3.3.1 Operations of the Mobile Source

After a Mobile IPv6 handover and successful address configuration, the MN sends its payload source routed via the previous Designated Router (pDR) to the multicast group. It

uses a Home Address Destination Option and a Binding Update Message as defined in [13] for the unicast case, which is cryptographically authenticated according to [2]. Concurrently the MN performs a regular binding update with its Home Agent. In addition to unicast operations, the MN adds the Hop-by-Hop multicast mobility router alert option as defined in section 3.2 (see figures 3 and 4) and inserts pDR into its Binding Update List.

The MN continues to source route these state update messages until it receives a Binding Acknowledgement from its previous Designated Router. Hereafter the mobile terminates source routing and switches to regular multicast packet transmission. It may decide to issue additional state updates as shown in figure 4, this choice being subject to packet frequencies or robustness requirements.

3.3.2 Operations of Routers

Routers on the delivery path receiving a State Update Packet must analyze the Hop-by-Hop Option Header according to [7]. They will identify the Router Alert Option as specified in section 3.2. The option's *value* field defines that this message is a multicast mobility State Update Message. Hence following headers as specified in section 3.2 need processing according to the Tree Morphing protocol. The router will extract the HoA of the sender from the following Destination Option Header. From the subsequent Binding Update message the sequence number is examined, leading to an immediate forwarding in case of a repeat.

For current sequence IDs the Mobility Header including CGA Options will be processed. The CGA Parameter data structure is extracted from the CGA Parameter Options. With this data structure the CGA verification of the Home Address is executed as described in [3]. This test includes a sanity check, a prefix inspection and an RSA signature verification for the HoA of the Mobile Node. If tests up to the signature turn valid, the packet can be accounted for the owner of the HoA based on cryptographically strong authentication. It can further be assumed that the current CoA is associated to a sender, who is the owner of the HoA. Consequently, the following updates of the distribution tree can proceed in a secure fashion. Conversely, a router experiencing any failure within this verification procedure will immediately discard the packet without further obligations.

Further packet processing depends on whether the router is on the path of tree elongation or on the regular multicast distribution tree. In the first case a router will extract the group address from the type 7 routing header, implement an $(nCoA, HoA, G)$ state in accordance with source route forwarding and transmit the packet towards pDR. In the second case a router will operate the STATE INJECTION and the EXTENDED FORWARDING Algorithms as described in our previous publication [21].

3.3.3 Operations of the pDR

The previous Designated Router plays the role of a prescribed intermediate forwarder of the source route. It will examine and verify packet correctness and authentication as routers on the previous tree elongation path. For any fully authenticated packet it will verify the existence of a matching $(., HoA, G)$ state in its multicast distribution table to ensure that this update arrived for a previously established multicast distribution tree. On success, the pDR will operate the source routing step, update forwarding states and transmit the packet down the corresponding tree. It furthermore issues a mobility Binding Acknowledgement towards the mobile source. Any packet not compliant with a previously established forwarding state shall be silently discarded by the pDR.

3.3.4 Operations of Listening End Nodes

Multicast receivers will analyze the state update packets analogously to the algorithms mentioned before. On successful CGA verification, the Home Address Option in the Destination Option Header is treated as a Binding Update (BU) [12] and the matching Multicast Binding Cache entry is updated. The packet's data is then passed to the transport layer with the correct HoA and G. This ensures lossless, transparent multicast communication on the application layer.

4 A First Protocol Evaluation

In this section we introduce first steps for an evaluation of the protocol implementation scheme, cf. [21] for a thorough evaluation of its algorithmic performance. The quality of the proposed realization 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 threads.

4.1 Protocol Overheads

The Tree Morphing protocol is implemented by inserting at most two headers, the Router Alert Option and a Type 7 Routing Header, into the Binding Update message included in the first regular multicast transmission payload packet. Therefore no additional signaling is required. Instead, all necessary information is sent in the Mobile IPv6 Binding Update Message and Home Address Option, including the CGA authentication parameters. These two headers jointly account for an overhead of 256 bits.

The design introduced for the Tree Morphing 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 IPv6 source routing or Mobile IPv6. This includes the Binding Update Message and CGA Parameter with CGA Signature Options in the Mobility Header as defined in [2]. By re-using well established headers and protocols, implementations can be easily realized in a lean and secure fashion.

4.2 Processing Overheads

The critical measure of protocol overheads must be seen in the operational complexity of the state update packet, which requires processing at every router along the path. On the one hand, algorithmic costs of the SSM source mobility management remain below efforts for regular ASM state management in PIM-SM, since several, persistant states are immediately re-used without further signaling requirements.

On the other hand, cryptographic verification of CGA Home Addresses 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 $O(k^2)$, where k denotes the length of the key modulus [6].

Verifying signatures of every packet - including bogus data - is undesirable. As has been foreseen in [3], 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.

Nevertheless, complexity of RSA signature verification is the drawback of our strongly secured Tree Morphing Protocol scheme. RSA execution is limited to one instance per multicast source handover at every router along the extended 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 [1] operations, where the number of required signature operations at routers is up to the order of a few dozens per second.

4.3 Robustness

4.3.1 Network Perturbance

In reliable networks without packet loss, the state update message could be sent only once in the first packet subsequent to a multicast source handover. Due to possible packet loss in real networks, our protocol requires the pDR to send a confirmation message to the MN upon arrival of a new state update message. This controls the traversal of the error-prone wireless access network and a re-connect to the previous delivery tree rooted at the pDR. After receiving this confirmation message, the MN may send further state update messages to ensure all multicast receivers are aware of the binding update.

Another problem that has to be solved in real networks is packet overrun. Considering handover times, all pre-handover multicast packets will be delivered when sending new packets including the update information. Since our protocol 'piggy-backs' the update information in the multicast data packets, only packets including the state update messages can overrun each other. In this way the first packet arriving at a router initiates the state update. Note that multiple receptions of state update messages can be identified by the routing infrastructure through its original sequence identifier within the Binding Update and thus will not lead to repeated update processing.

4.3.2 Resilience Against Common Attacks

The protocol has to withstand several common attacks. By replaying valid intercepted packets, an attacker could try to impose extra burden onto the routing 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 Binding Update message, which is protected by the packet signature. Packets with incorrect sequence numbers fail the sanity checks mentioned before. The Tree Morphing Protocol is therefore only as vulnerable as standardized well-known protocols such as SEND [1] and does not introduce new security threads. Thus new messages have to be processed cryptographically by routers only once.

Furthermore, an attacker could configure its own cryptographically valid Home Address and issue a state update to the network. As SSM source filtering would discard such packets on arrival at the previous designated router, such attack will not lead the network to forwarding bogus packets along any multicast distribution tree, but will limit transmission to the initial unicast source route. Consequently, our Tree Morphing implementation does not re-open the opportunity of network assisted distributed denial of service attacks as inherent to ASM. Additionally, generating CGAs and RSA signatures is much more complex than verifying them - especially with the security parameter *sec* set to a high value. This makes it hard for attackers to send many CGA signed messages for different HoAs.

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. [3]. To quantitatively estimate the complexity of generating CGAs, successive valid CGAs have been generated by changing the mod-

ifier field. All other input values to the function were left unchanged. Table 1 shows the security parameter *sec*, the mean number of modifier steps (the mean modifier difference between two valid CGAs) and the standard deviation.

Sec	Mean # of modifier steps	Std. Deviation
0	1	0
1	66,113	256
2	2,591,220,608	50,901

Table 1. CGA generation complexity

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 $O(k^3)$. In contrast, analyzing CGAs only requires computation of two SHA-1 hash values and an $O(k^2)$ signature verification.

5 Conclusions and Outlook

We presented an implementation scheme for our Tree Morphing Protocol, which can realize adaptive multicast routing for mobile sources solely by using standard components of the IPv6 family. In this cryptographically robust authenticated signaling scheme, regular Binding Updates on the Internet mobility layer are interpreted by the routing infrastructure concurrent to data transmission. This is achieved by introducing a Hop-by-Hop Router Alert Option. Processing these State Update Messages adds additional processing load on the Internet routers. However, it should be stressed that for every mobility handover merely one update message has to be processed. The presented protocol is protected from repeated processing and replay attacks by internal sequence numbers. It is robust against common network perturbances and withstands misuse of multicast packet replication for distributed denial of service attacks.

In further work we will continue protocol implementation and focus on analyzing protocol robustness against network disruptions from strong bursts and packet overflow, as well as against rapid movements of the mobile node.

References

[1] J. Arkko, J. Kempf, B. Zill, and P. Nikander. SEcure neighbor discovery (SEND). RFC 3971, IETF, March 2005.

[2] J. Arkko, C. Vogt, and W. Haddad. Enhanced route optimization for mobile ipv6. RFC 4866, IETF, May 2007.

[3] T. Aura. Cryptographically generated addresses (CGA). RFC 3972, Internet Engineering Task Force, Mar. 2005.

[4] S. Bhattacharyya. An Overview of Source-Specific Multicast (SSM). RFC 3569, IETF, July 2003.

[5] R.-S. Chang and Y.-S. Yen. A Multicast Routing Protocol with Dynamic Tree Adjustment for Mobile IPv6. *Journ. Information Science and Engineering*, 20:1109–1124, 2004.

[6] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms - 2nd Edition*. MIT Press, 2001.

[7] S. Deering and R. Hinden. Internet protocol, version 6 (IPv6) specification. RFC 2460, IETF, Dec. 1998.

[8] S. E. Deering. Host Extensions for IP Multicasting. RFC 1112, IETF, Aug. 1989.

[9] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Rev,). RFC 4601, IETF, Aug. 2006.

[10] H. Holbrook and B. Cain. Source-Specific Multicast for IP. RFC 4607, IETF, August 2006.

[11] C. Jelger and T. Noel. Supporting Mobile SSM sources for IPv6 (MSSMSv6). IDraft (expired) 00, indiv., Jan. 2002.

[12] D. Johnson, C. Perkins, and J. Arkko. Mobility support in IPv6. RFC 3775, IETF, June 2004.

[13] D. B. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775, IETF, June 2004.

[14] G. Kurup and Y. A. Sekercioglu. Source Specific Multicast (SSM) for MIPv6: A Survey of Current State of Standardisation and Research. In *Proc. of ATNAC 2003*, Dec. 2003.

[15] A. O'Neill. Mobility Management and IP Multicast. Internet Draft – work in progress (expired) 01, IETF, July 2002.

[16] C. Partridge and A. Jackson. IPv6 router alert option. RFC 2711, Internet Engineering Task Force, Oct. 1999.

[17] I. Romdhani, H. Bettahar, and A. Bouabdallah. Transparent handover for mobile multicast sources. In *Proceedings of the IEEE ICN'06*. IEEE Press, April 2006.

[18] I. Romdhani, M. Kellil, H.-Y. Lach, A. Bouabdallah, and H. Bettahar. IP Mobile Multicast: Challenges and Solutions. *IEEE Comm. Surveys & Tutorials*, 6(1):18–41, 2004.

[19] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261, IETF, June 2002.

[20] T. C. Schmidt and M. Wählisch. Extending SSM to MIPv6 — Problems, Solutions and Improvements. *Comp. Methods in Science and Technology*, 11(2):147–152, Nov.2005.

[21] T. C. Schmidt and M. Wählisch. Morphing Distribution Trees – On the Evolution of Multicast States under Mobility and an Adaptive Routing Scheme for Mobile SSM Sources. *Telecommunication Systems*, 33(1–3):131–154, Dec. 2006.

[22] T. C. Schmidt and M. Wählisch. Multicast Mobility in MIPv6: Problem Statement and Brief Survey. IRTF Internet Draft – work in progress 00, MobOpts, May 2007.

[23] T. C. Schmidt, M. Wählisch, H. L. Cycon, and M. Palkow. Scalable Mobile Multimedia Group Conferencing based on SIP initiated SSM. In *Proc. of ECUMN'2007*, pp. 200–209, IEEE Computer Society Press, Feb. 2007.

[24] D. Thaler. Supporting Mobile SSM Sources for IPv6. Proceedings of ietf meeting, individual, December 2001.

[25] G. Xylomenos and G. C. Polyzos. IP Multicast for Mobile Hosts. *IEEE Comm. Mag.*, 35(1):54–58, 1997.