Ein einfaches, sicheres IPv6 Protokoll zur kontinuierlichen Adaptierung von Sendermobilität in Multicast Verteilbäumen*

Olaf Christ[1], Thomas C. Schmidt[1], and Matthias Wählisch[1,2]

[1] HAW Hamburg, Department Informatik, Berliner Tor 7, 20099 Hamburg, Germany
[2] link-lab, Hönower Str. 35, 10318 Berlin, Germany
olaf@solutionsworks.de, {t.schmidt,waehlisch}@ieee.org

Zusammenfassung Vernetzte Systeme und verteilte Anwendungen unseres Alltags schließen zunehmend mobile Teilnehmer ein und erfordern so neue Konzepte, um Mobilitätstransparenz gewährleisten zu können. Gruppenkommunikation auf der Netzwerkschicht vereinfacht Koordination und Synchronisation verteilter Komponenten und gewinnt in einem mobilen Internet der nächsten Generation neuerlich an Bedeutung. Dennoch ist das Problem, mobilen Multicastquellen eine übergangslose Vermittlung im Netzwerk zu gewähren, weitgehend ungelöst.
In diesem Aufsatz stellen wir die Implementierung des Tree Morphing Routing Protokolls auf dem IPv6 Netzwerklayer vor. Dieser verteilte Routingalgorithmus ermöglicht die kontinuierliche Anpassung des Multicast Routings an eine Sendermobilität in quellspezifischen Verteilbäumen. Der verfolgte Ansatz bettet die erforderliche Protokollsignalisierung einfach und ohne zusätzliche Paketdefinitionen zu erfordern in das standardisierte Mobilitätsmanagement der IPv6 Netzwerkschicht ein. Auf der Basis kryptographischer Adressierung folgen alle Signalisierungen einer kryptographisch starken Authentifizierung.

Key words: Mobile IPv6, source specific multicast, SSM source mobility, secure routing, cryptographic addressing

1 Einleitung

Die Leistungsfähigkeit heutiger Standardgeräte erlaubt es, parallele Algorithmen und komplexe verteilte Anwendungen nicht mehr nur auf dedizierten Geräten auszuführen, sondern nahezu beliebige Computer in Berechnungen einzubeziehen. Verteilte Kontrollalgorithmen in Echtzeit, wie wir sie gleichermaßen in serviceorientierten Architekturen für technische Anwendungen und Spielen finden, sind prominente Beispiele hierfür. Diesem Paradigmenwechsel, von Recheninseln zu weit verstreuten 'heimischen' Clusterpunkten, sollte die unterliegende Netzinfrastruktur Rechnung tragen, indem sie Protokolle zur skalierbaren Gruppenkommunikation bereitstellt, die das ubiquitäre Computing weitreichend unterstützen.

Gruppenkommunikation findet sich auch in einer Vielzahl wohl etablierter Multimedia–Dienste und Anwendungen wieder. So sind Audio– und Videokonferenzen, verteiltes Lernen, Kollaborieren oder Spielen beispielhaft Kernthemen unserer Kommunikations-, Arbeits- und Freizeitkultur geworden. Neue Impulse und erweiterte Szenarien entstehen im Kontext der Mobilität, wenn sensitive Anwendungen in funkbasierten Netzen auf weitverteilte Datenzustellung vertrauen.

Mobile Endgeräte haben sich zu Alltagsbegleitern gewandelt. Das Internetprotokoll der nächsten Generation, IPv6 mit seinem umfangreichen Adressbereich, gestattet uns auf der Netzwerkschicht jedes Endgerät uneingeschränkt anzusprechen; seine ausgeprägte Mobilitätsunterstützung ermöglicht es, einen Subnetzwechsel gegenüber der Applikation transparent und echtzeitfähig zu verbergen. Die standardisierten Mechanismen konzentrieren sich hierbei vorangig auf Unicast–Kommunikation. Mobiles Multicast wird infolge seiner Komplexität

* Diese Arbeit wird im Projekt *Moviecast* (http://moviecast.realmv6.org) durch das Bundesministerium für Bildung und Forschung gefördert.

und gegenwärtig geringen Verbreitung nur rudimentär und für eine Echtzeitkommunikation ungeeignet unterstützt.

Effiziente Gruppenkommunikation im Internet mittels Multicast hat sich insbesondere aufgrund der benötigten komplexen Infrastruktur bisher nur zögerlich durchgesetzt, obgleich es *die* eleganteste und effizienteste Lösung vieler Koordinations- und Synchronisationsprobleme darstellt [1]. Eine stärkere Etablierung von Multicast wird durch den kürzlich verabschiedeten, leichtgewichtigen Standard Source Specific Multicast (SSM) [2,3] erwartet. Im Gegensatz zu Any Source Multicast (ASM) [4] werden in SSM (S, G)–Bäume kürzester Wege durch die Registrierung der Teilnehmer zu einer Quelle S und einer Gruppe G sofort aufgebaut, ohne das Fluten des Netzwerks zu veranlassen oder RendezVous Points zu verwenden. Die explizite Benutzung der Unicast–Quelladresse für den Aufbau von SSM Verteilbäumen reduziert zwar im Vergleich zu ASM die Routing–Komplexität, wirft aber neue Probleme im Bereich des mobilen Internets auf.

Adressen innerhalb des mobilen Internets tragen eine Doppelbedeutung: Sie sind zugleich logischer *und* topologischer Identifikator. Während Mobile IPv6 [5] diese Dualität auf den Endgeräten transparent behandelt, benötigt das Routing in SSM die Verwendung beider Adressen, für die logische Anmeldung am Multicast–Baum (Source Filtering) einerseits *und* die topologisch richtige Weiterleitung der Pakete andererseits. Ein Protokollvorschlag, der die Adressdualität bei der Errichtung von Multicast–Verteilbäumen berücksichtig und mobiles SSM unterstützt, wurde kürzlich mit dem Tree Morphing Protokoll [6,7] vorgestellt. Durch die Anwendung von Source Routing verzichtet dieses mobile Multicast Routing–Protokoll auf jegliche Tunnelmechanismen und überführt in kontinuierlichen Anpassungsschritten den alten Baum in einen neuen.

In diesem Beitrag präsentieren wir erste leichtgewichtige Implementierungsentwürfe für das bestehende algorithmische Konzept des Tree Morphings. Auf der Basis bereits standardisierter Protokollsemantiken geben wir eine konkrete Ausgestaltung der Paketköpfe an und erweitern das Protokoll um einen Sicherheitsmechanismus, der einen mobilen Multicast–Sender gegenüber dem Verteilbaum effizient authentifiziert und so vor einer ungewollten Übernahme schützt. Die vorliegende Arbeit gliedert sich wie folgt: Neben einer kurzen Einführung in Mobile IPv6 diskutieren wir in Abschnitt 2 das Problem mobiler Multicast–Quellen und reflektieren den gegenwärtigen Entwicklungsstand. In Abschnitt 3 stellen wir unseren Entwurf zur Implementierung des Tree Morphings vor, welcher im hiernachfolgenden Abschnitt 4 evaluiert und diskutiert wird. Eine Zusammenfassung und einen Ausblick geben wir in Abschnitt 5.

2 Das Problem mobiler Multicast Sender und gegenwärtige Lösungsansätze

2.1 Transparenter Netzwechsel in Mobile IPv6

Mobile IPv6 (MIPv6) sieht drei miteinander interagierende Komponenten vor: den Mobile Node (MN), seinen Home Agent (HA) und den Correspondent Node (CN). Um den MN auch außerhalb seines Heimatnetzes erreichbar werden zu lassen, teilt dieser seinem HA seinen gegenwärtigen Aufenthaltsort mit. Das geschieht durch ein Binding Update (BU) an den HA. Der HA kann nun an Stelle des MN im Heimatnetz antworten und die Pakete an diesen weiterleiten. Dabei werden die Pakete solange triangulär versendet, bis auch der CN ein solches BU erhält.

Mit einem Adresswechsel auf der Vermittlungsschicht invalidieren bestehende Socket–Verbindungen, wodurch ein Datenstrom unterbrochen und eine bestehende Kommunikation gestört würde. Mobile IPv6 umgeht dieses Problem, indem jeder mobile Knoten neben

seiner aktuellen IP–Adresse, der sog. Care–Of Adresse (CoA), eine feste ortsunabhängige Adresse, die Home Adresse (HoA), besitzt. Eine Adressveränderung kann gegenüber der Socket–Schicht effizient verborgen werden, indem Pakete vom oder zum MN beide Adressen beinhalten.

Das Mobile IPv6–Protokoll operiert wie folgt [5]: Der Kommunikationspartner des mobilen Knotens adressiert Daten an die CoA und vermerkt die HoA im *Routing Header*. Entsprechend der natürlichen Funktionsweise von (Loose) Source Routing prozessiert der MN die Pakete unter Austausch der CoA mit der HoA. Um den Subnetzwechsel wiederum für den CN transparent zu gestalten, führt MIPv6 die *Home Address Option* ein, welche die HoA in einem *Destination Option Header* signalisiert.

2.2 Problembeschreibung für mobile Multicast

Mobile Multicast–Protokolle müssen sowohl Empfänger– als auch Senderbewegungen transparent begleiten [8]. Während Empfänger nach einem Netzwechsel durch erneute, ggf. von Proxy–Agenten unterstützte Subskription ihre Gruppenkonnektivität vergleichsweise leicht wiedererlangen können, sind mobile Quellen mit dem Zusammenbruch eines etablierten *Shortest Path Trees* (SPT) konfrontiert. Source Specific Multicast bringt ein weiteres Problem mit sich: Empfänger, obgleich auf der Anwendungsschicht an eine permanente Adresse gebunden, müssen sich auf der Netzwerkschicht explizit an die topologisch richtige, temporäre Adresse der Quelle anmelden, um quellspezifische Paketfilter einzustellen. Das Routing muß demzufolge sämtliche (S_{old}, G)–Zustände in (S_{new}, G) überführen, während die Multicast–Applikation den Datenempfang mittels einer persistenten, bewegungstransparenten Quelladresse abonniert. Demnach schlagen Mechanismen wie die in MIPv6 [5] vorgesehene *Remote Subscription* fehl.

Zu bedenken ist weiterhin, dass aufgrund der generellen Entkopplung von Multicast–Sendern und Empfängern eine Quelle weder ihre Gruppenteilnehmer kennt, noch über einen Rückkanal verfügt. Adressveränderungen infolge eines Netzwechsels der SSM–Quelle müssen demnach robust und ggf. selbstheilend mitgeteilt werden. Die Quelle besitzt per se keine Möglichkeit, Zustände des Verteilbaums oder der Empfänger abzufragen.

Source Specific Multicast wurde als leichtgewichtiger Ansatz zur Gruppenkommunikation entwickelt. Mobilitätstaugliche Erweiterungen sollten die vorgegebene Schlankheit bewahren, indem sie zusätzlichen Signalisierungsaufwand minimieren.

2.3 Lösungsansätze für das mobile Multicast Problem

Gegenwärtig sind drei Konzeptansätze bekannt, um Mobilität von Sendern in SSM zu unterstützen.

Statische Verteilbäume: MIPv6 standardisiert als minimalste Multicast–Unterstützung für Sender und Emfänger das bidirektionale Tunneln über den Home Agent analog der Ideen in [9]. Jeglicher Multicast–Verkehr wird über den Home Agent zu den Empfänger verteilt. Da der Home Agent räumlich fixiert ist, wird Mobilität gegenüber dem Multicast–Routing versteckt auf Kosten von triangulären Routing und langreichweitiger Paketkapselung.

Die Autoren aus [10] empfehlen den Einsatz der RendezVous Points aus PIM–SM [11] als mobile Ankerpunkte. Mobile Sender tunneln ihre Daten zu den sogenannten „Mobility-aware Rendezvous Points“ (MRPs), wobei dies innerhalb einer Multicast–Domain als äquivalent zum bidirektionalem Tunneln angesehen werden muß. Mobiles Multicast zwischen mehreren Domainen wird durch die Verwendung einer tunnel– oder SSM–basierten Verteilung zwischen den MRPs erreicht.

Wiedererrichtung von Verteilbäumen: Mehrere Autoren schlagen die vollständige Rekonstruktion des Verteilbaumes nach dem Netzwechsel einer Quelle vor. Die Daten werden zwar hiernach entlang kürzester Wege versendet, die Empfänger sind aber vorher über die neue Quelladresse zu informieren genauso wie diese gegenüber der Klientanwendung zu verbergen ist.

Letzteres wird in [12] durch die Einführung von Binding Caches in Analogie zu MIPv6 gelöst. Informationen über die initiale Adresse sowie Adressveränderungen erhält ein Empfänger über periodisch versendete Nachrichten mithilfe eines zusätzlichen Kontrollverteilbaum, der beim Home Agent des Senders verankert ist.

Die Lösung aus [13] basiert auf der Implementierung von Ankerpunkten (AP), die dem Sender topologisch nahe sind. Während die Quelle eine Verbindung zu einem neuen AP aufbaut, sendet sie ihre Multicast–Daten zunächst so lange parallel zum alten Baum, bis dieser abgebaut werden kann. Es bleibt hierbei unklar, wann der alte Baum 'aufgegeben' wird, da die Empfänger nicht synchronisiert zur Quelle operieren können und Verfahren wie MSNIP [14] auf ASM basieren. Ferner entstehen bei einer schnellen Bewegung eine unbeschränkte Anzahl 'historisch' aktiver Verteilbäume, so dass eine Protokollkonvergenz nicht sichergestellt werden kann.

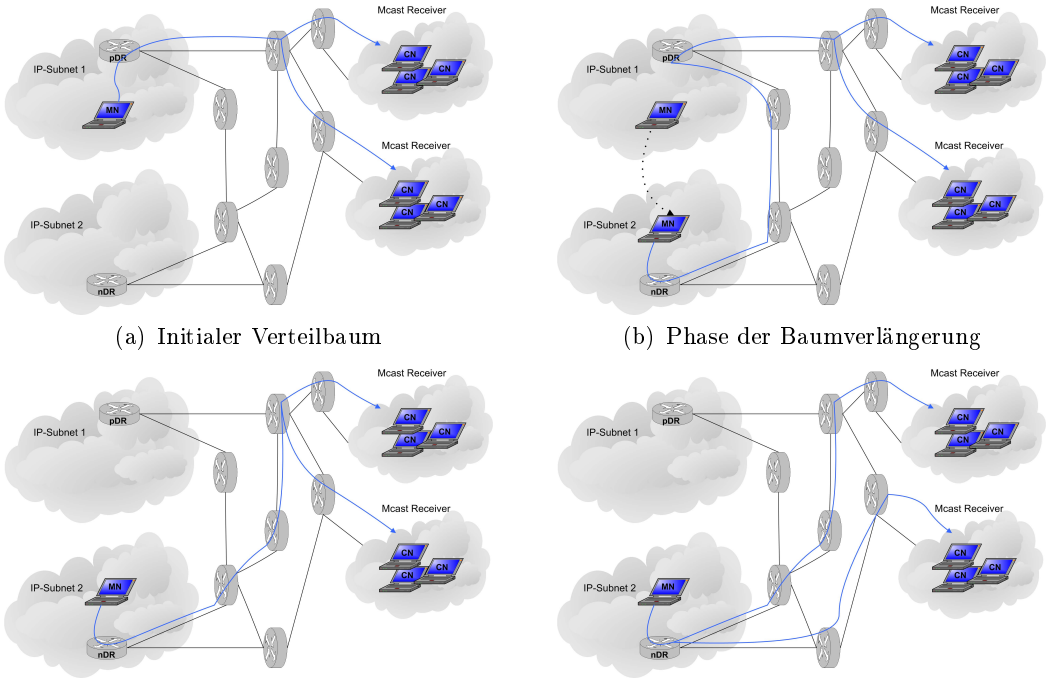
Überführung von Verteilbäumen: Wenige Vorschläge liegen bisher für Mechanismen zur Überführung eines bestehenden Verteilbaumes in einen neuen vor. Für DVMRP wird ein Algorithmus in [15] angegeben, der die Wurzel des Baumes, der Senderbewegung folgend, verlängert. Die Autoren sind auf ein komplexes Signalisierungsschema angewiesen, um die DVMRP–Zustände und den RPF–Check anzupassen. O'Neill [16] umgeht das Fehlverhalten des RPF–Checks, welcher sich durch den Wechsel der Senderadresse ergibt, indem er zusätzliche Routing–Informationen im Hop–by–Hop Paketkopf jedes Pakets kodiert.

Ein weiteres, adaptives Routing–Protokoll, das sogenannte Tree Morphing, wurde von den Autoren erstmals in [6] präsentiert und in [7] ausführlich algorithmisch evaluiert. Eine schematische Darstellung findet sich in Abbildung 1. Durch die Verwendung von Source–Routing anstelle eines Tunnels bei der Verlängerung des Baumes wird ein ineffizientes Verpacken von Paketen vermieden. Mit dieser ersten Phase (s. Abb. 1(b)) des Protokolls nach einem Wechsel werden sowohl Router, als auch Empfänger über die neue Adresse des Senders informiert: Ähnlich zu MIPv6 tragen die Pakete der Quelle eine Care–Of–Adresse (CoA) einschließlich der Home–Adresse mit sich. Schrittweise wird der alte Baum zu einem neuen migriert (s. Abb. 1(c)), indem die Router mit Hilfe des RPF–Checks topologisch korrekt Interfaces auf dem SPT identifizieren und ggf. den Aufbau noch nicht vorhandener kürzester Wege initiieren bzw. richtige mit der neuen CoA überschreiben. Unnötige Multicast–Zweige können automatisch, ohne die Verwendung fester Zeitparameter oder zusätzlicher Kontrollkanäle von den Routern abgebaut werden, sobald die Zustellung über das neue Interface erfolgt. Der alte Baum wird damit selbständig und 'rechtzeitig' in einen Baum kürzester Wege transformiert (s. Abb. 1(d)).

3 Entwurf des Tree Morphing Protocols

3.1 Anforderungen & Ansätze

Das Tree Morphing Protokoll erfordert, dass die Routerinfrastrukur nach einem Handover der Multicastquelle mithilfe der Paketverarbeitung ihre Weiterleitungszustände aktualisiert. Insbesondere muss nach einem Mobile IPv6-Handover der von der vorhergehenden Quelladresse pCoA ausgehende Multicast-Verteilbaum zur nachfolgenden nCoA übertragen werden (siehe Abbildung 1). Hierzu müssen Pakete, die von den Routern inhaltlich ausgewertet



(a) Initialer Verteilbaum

(b) Phase der Baumverlängerung

(c) Zwischenzeitlicher Morphing–Schritt

(d) Konvergierter Verteilbaum

Abbildung 1. Zustände des Tree Morphing Protokolls

werden, sowohl die kontextuellen als auch die topologischen Verteilbauminformationen enthalten. Dabei werden die kontextuellen Informationen, gegeben durch das Tupel (HoA, G), dazu verwendet, den zu überführenden Verteilbaum zu identifizieren. Die topologischen Informationen (nCoA, G) hingegen werden für das Routing benötigt. Diese drei IP-Adressen müssen unmittelbar nach dem Handover allen Routern des vorherigen und – soweit möglich – des neuen Verteilbaums gemeinsam bekannt gemacht werden.

Multicastpakete müssen dem Tree Morphing Protokoll folgend unmittelbar nach dem Netzwechsel einer mobilen Quelle vom next Designated Router (nDR) zum previous Designated Router (pDR) weitergeleitet werden. Dazu werden sie per Source Routing [17] zum pDR gesendet. Der im nächsten Abschnitt vorgestellte Protokollentwurf verwendet kryptographisch erweiterte Standardmethoden, um dieses Source Routing sicher zu realisieren.

Da die Aktualisierungspakete von den Internet Core Routern prozessiert werden, muss beim Protokollentwurf eine leichtgewichtige Lösung gefunden werden, die nur einen geringen Verarbeitungsaufwand zur Folge hat. Daher werden die Aktualisierungsinformationen mit den unmittelbar nach dem Handover fliessenden Nutzdatenpaketen verschickt. Durch diesen Mechanismus des „Piggybacking“ werden unerwünschte Komplikationen, wie z.B. Paketüberholungen vermieden. Außerdem müssen dadurch keine zusätzlichen Signalisierungspakete übertragen werden, was unerwünschten Zusatzaufwand durch die Übertragung vermeidet. Obwohl auch weiterhin Nutzdatenpakete in falscher Reihenfolge eintreffen können, enthalten zumindest die ersten Pakete die Updateinstruktionen, um robust gegenüber Störungen zu sein.

Schließlich muss beim Protokollentwurf darauf geachtet werden, das Tree Morphing Protokoll gegenüber Angreifern abzusichern. Um fehlerhafte Pakete erkennen und verwerfen zu können, wird die im Mobile IPv6 Binding Update genutzte Sequenznummer verwendet. Diese Sequenznummer wird nach jedem Handover erhöht. Das mehrfach in den ersten Multicastdatenpaketen nach dem Handover gesendete Update enthält somit dieselbe Sequenznummer. Einerseits können damit bereits verarbeitete Updates ohne weiteren Aufwand übersprun-

gen, andererseits auch Updatepakete mit gefälschten Sequenznummern leicht erkannt und verworfen werden.

Die vorzunehmenden Zustandsaktualiserungen in der Vermittlungsinfrastruktur sind ebenso anfällig für einen Identitätsdiebstahl wie z.B. Mobile IPv6 oder das Neighbor Discovery Protocol (NDP). Daher ist eine robuste, kryptographisch starke Authentifizierung der Signalisierung notwendig, welche allerdings ohne Rückkommunikation erfolgen muss. Diese Einwegauthentifizierung muss selbstkonsistent beweisen, dass die Aktualisierungspakete tatsächlich von der mobilen Multicastquelle, also der Besitzerin der Home Adresse stammen und kann analog zu [18] und [19] mithilfe kryptographisch generierter Adressen (CGAs) [20] erreicht werden. Dazu werden mit der State Update Message in demselben Paket auch die für die CGA-Authentifizierung nötigen Informationen übermittelt, die CGA Parameter und eine CGA Signature Option. Damit können Sender den Besitz der Home Address ohne weitere Infrastruktur kryptographisch stark nachweisen. Außerdem wird das Paket durch eine RSA-Signatur authentifiziert, was eine fälschungsfreie Übertragung sicherstellt. Veränderte Pakete können somit erkannt und verworfen werden.

3.2 State Update Message aus bestehenden IPv6 Headern

Ein integrativer Ansatz, das Tree Morphing Protokoll zu implementieren, liegt darin, die zum Überführen des Verteilbaums nötigen Informationen durch das Übertragen einer aus bestehenden Headern zusammengesetzten Nachricht zu übermitteln. Dabei werden minimale Erweiterungen an der bestehenden Mobilitätssignalisierung durchgeführt, um ein Höchstmaß an Einfachheit und Standardkonformität zu gewährleisten. Die nachfolgend vorgestellte Implementierung des Tree Morphings ist deshalb allein durch die zielgerichtete Kombination bestehender Protokollstrukturen und unter minimaler Ergänzung einer vorhandenen Hop-by-Hop Option realisiert. Sie kommt ohne Änderungen etablierter Header aus. Vorhandene Protokollimplementierungen wie Mobile IPv6 [5], welches für die Aktualisierung der Multicastempfänger benötigt wird, und PIM-SSM [11] können somit leicht angepasst werden, da alle Verarbeitungsfunktionen bereits vorhanden sind. Weiterhin bringt dieser leichtgewichtige Ansatz Vorteile für die Robustheit des Protokolls mit sich, da die vorhandenen, standardisierten Header und Protokolle bereits genauen Analysen und praktischen Einsatzerfahrungen unterzogen wurden.

Im Folgenden werden zunächst die neuen Headertypen der „Router Alert Option“ und des „Routing Headers“ vorgestellt, anschließend wird der Paketaufbau in den unterschiedlichen Phasen des Tree Morphings dargestellt.

Router Alert Option Die Signalisierung einer neuen Verteilbaumquelle nach dem Mobile IPv6 Handover erfolgt auf der Netzwerkschicht durch Zusatzinformationen in den Datenpaketen. Die benötigten Informationen, Gruppenadresse, Home Adresse und Care-Of Adresse sowie die Authentifizierungsnachweise, sind bereits Bestandteil der Binding Update Messages, wie sie mobile Teilnehmer – zumindest an ihre Unicast-Empfänger – nach jedem Netzwechsel verschicken. Die State Update Message kann deshalb aus verschiedenen Headern der Mobile IPv6 Netzwerkschicht zusammengesetzt werden und erfordert keine Neudefinition von Datenstrukturen. Multicast Tree Morphing Signalisierungen können so prinzipiell in transparenter Weise mit regulären, CGA-authentifizierten [18] Binding Updates prozessiert werden. Sie müssen dabei allerdings von jedem Router entlang des Paketweges interpretiert werden.

Um eine solchermaßen transparente Multicast Mobilitätssignalisierung zu ermöglichen, werden die Pakete um eine Router Alert Option im Hop-by-Hop Header [21] ergänzt. Dieses Format wird benutzt, um Routern zu signalisieren, weitere Paketverarbeitungen zu veranlassen.

Die Router Alert Option besitzt das in Abbildung 2 dargestellte Format.

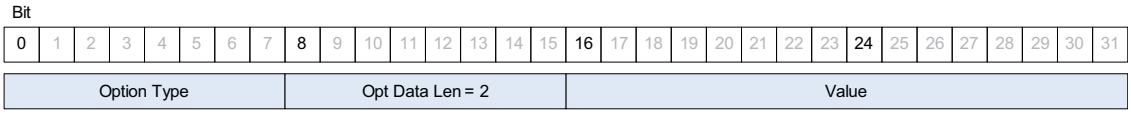


Abbildung 2. Router Alert Option

Option Type Das 8 Bit lange *Option Type*-Feld hat den Wert 0x05. Die ersten beiden Null-Bits spezifizieren laut [17], dass Router, die die Option nicht verstehen, diese überspringen und mit der Verarbeitung des Pakets fortfahren müssen. Das folgende Null-Bit definiert, dass sich die Option während der Übertragung zum Ziel nicht ändern darf.

Opt Data Len Die Datenlänge der Option in Octets ohne die Felder *Option Type* und *Opt Data Len* wird in dem 8 Bit großen Feld *Option Data Length* gespeichert. Der Wert dieses Feldes beträgt 2.

Value Dieser von der IANA zuzuweisende Wert für diesen speziellen Header spezifiziert die Semantik der State Update Message. Die weitere Paketverarbeitung der nachfolgend beschriebenen Optionsheader wird durch diesen Wert eindeutig festgelegt, so dass ihre Verarbeitung mit dem Ziel, die Forwarding States der Router zu aktualisieren, wohldefiniert erfolgen kann.

Routing Header Type 7 Für das Tree Morphing wird im Folgenden ein eigener Routing Header Typ definiert[3]. Der genaue Inhalt des Headers wird in Abschnitt 3.2 beschrieben.

Der Routing Header Type 7 besitzt das in Abbildung 3 dargestellte Format.

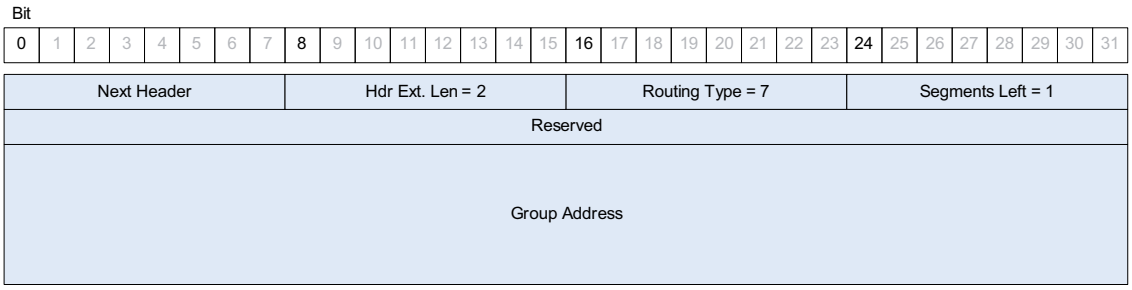


Abbildung 3. Routing Header Type 7

Next Header Das 8 Bit lange *Next Header*-Feld identifiziert den Header, der unmittelbar auf den Routing Header folgt.

Hdr Ext Len Der Wert des 8 Bit langen *Hdr Ext Len*-Feldes muss auf 2 gesetzt sein. Es beschreibt die Länge des Routing Headers in 8 Octet-Einheiten exklusiv der ersten 8 Octets.

Routing Type Der von der IANA zuzuweisende Wert für diesen speziellen Header spezifiziert den Typ des Routing Headers. Der nächste aktuell freie Wert für dieses Feld ist 7.

[3] Der in Mobile IPv6 definierte Routing Header Type 2 kann, obwohl er den gleichen Aufbau wie der vorgestellte besitzt, nicht genutzt werden, da das vorhandene IPv6-Adressfeld laut [5] nur eine Unicast-Adresse enthalten darf, hier allerdings eine Multicast-Gruppenadresse hinterlegt werden muss.

Segments Left Der Wert dieses 8 Bit langen Feldes muss auf 1 gesetzt sein.

Reserved Dieses 32 Bit lange Feld ist für zukünftige Erweiterungen reserviert und muss vom Sender mit Nullen initialisiert werden. Der Empfänger muss dieses Feld ignorieren.

Group Address Dieses 128 Bit lange Feld enthält die SSM-Gruppenadresse.

State Update Message: Paketaufbau Der vollständige Paketaufbau unterscheidet sich nach den Phasen des Tree Morphing Protokolls und wird in den folgenden Abschnitten beschrieben.

Tree Elongation Abbildung 4 zeigt den Paketaufbau in der Phase des Tree Elongation. Dabei wird das Paket vom MN mit der aktuell gültigen CoA an den Previous Designated Router (pDR) gesendet. Gemäß der Headeranordnung im IPv6 Standard [17] folgt darauf der Hop-by-Hop Option Header mit der Router Alert Option, welche im Abschnitt 3.2 erläutert wurde. Anschließend folgt der Destination Option Header, der die Home Address Option gemäß [5] enthält, mit der den Empfängern die HoA mitgeteilt wird. Im Mobility Header [5] werden die CGA Parameter Option und die CGA Signature Option hinterlegt. Sie übertragen die für die CGA-Authentifizierung nötigen Daten. Dabei ist zu beachten, dass mehrere CGA Parameter Optionen aufeinander folgen können. Als letzter Header folgt der Routing Header vom Typ 7, dessen Funktion in der Weiterleitung des Pakets an die Gruppe nach seinem Eintreffen am pDR besteht. Dazu wird die Gruppenadresse G in das erste Adress-Feld eingetragen. Schließlich folgen noch der Nutzdatenheader (Upper Layer Header) sowie die Nutzdaten. Die zum Routing benötigten Informationen werden den Headern gemäß Tabelle 1 entnommen.

IPv6 Header	**Hop-by-Hop Options Header**	**Dest. Options Header**	**Mobility Header**			**Routing Header**	**Upper Layer Header + Data**
Src: CoA Dst: pDR	Router Alert Option	Home Address Option	Binding Update Message	CGA Param. Option	CGA Signature Option	Addr[0] = G	Data

Abbildung 4. IPv6-Paketaufbau mit State Update Message aus bestehenden IPv6 Headern beim Tree Elongation vom Next Designated Router zum Previous Designated Router

IP-Adresse	**Speicherort**
HoA	Destination Options Header: Home Address Option
CoA	IPv6 Header: Source Address
G	Type 7 Routing Header

Tabelle 1. Headerposition der HoA, CoA und G IP-Adressen beim Tree Elongation (State Update Message aus bestehenden IPv6 Headern)

Reguläre Multicastübertragung Die weitere Multicastübertragung wurzelt am pDR und findet über den vor dem Handover etablierten Verteilbaum statt. Im Paketaufbau (siehe Abbildung 5) entfällt der Routing Header, nachdem der Source Routing Übergangspunkt pDR erreicht ist. Hierbei wurde entsprechend die Zieladdresse im IPv6 Header mit der Gruppenadresse G aus dem Routing Header ersetzt (siehe Tabelle 2).

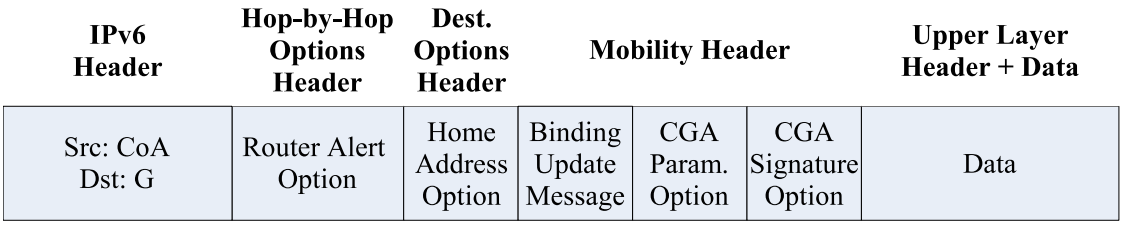


Abbildung 5. IPv6-Paketaufbau mit State Update Message aus bestehenden IPv6 Headern vom Previous Designated Router zur Multicastgruppe

IP-Adresse	**Speicherort**
HoA	Destination Options Header: Home Address Option
CoA	IPv6 Header: Source Address
G	IPv6 Header: Destination Address

Tabelle 2. Headerposition der HoA, CoA und G IP-Adressen bei der Multicastverteilung (State Update Message aus bestehenden IPv6 Headern)

3.3 Protokollablauf

Arbeitsweise der mobilen Multicastquelle Nach einem Layer 2 Handover und der darauf folgenden Adresskonfiguration sendet die mobile Multicastquelle ihre Nutzdaten per Source Routing an den Previous Designated Router (pDR). Zusätzlich werden die Home Address Option im IPv6 Destination Option Header und die State Update Message im Hop-by-Hop Option Header gesendet, um die für das (Binding-) Update nötigen Informationen zu übertragen. Außerdem werden die CGA-Optionen eingefügt (siehe Abbildung 4), um das Updatepaket zu authentifizieren.

Die mobile Multicastquelle muss die Nutzdatenpakete solange mit den Update-Headern versehen, bis sie ein Binding Acknowledgement vom pDR erhält. Dadurch ist der Baumanschluß sichergestellt. Trotzdem können noch weitere Pakete mit den zusätzlichen Headern versehen werden. Dies obliegt jedoch der Verantwortung der mobilen Multicastquelle und kann von Faktoren wie z.B. Robustheitsanforderungen und Paketaufkommen abhängen.

Parallel zu dem vorhergehend beschriebenen Verhalten führt die mobile Multicastquelle ein reguläres Binding Update mit ihrem Home Agent durch.

Arbeitsweise der Router Die Router auf dem Weg zu den Empfängern erhalten das State Update Paket und müssen laut [17] den Hop-by-Hop Option Header analysieren, dessen erste Option die in Abschnitt 3.2 definierte Router Alert Option ist. Das *Value*-Feld dieser Option spezifiziert, dass es sich um eine State Update Message handelt. Daher müssen auch die im Protokoll definierten weiteren Headerbestandteile des Pakets untersucht werden, welche ohne diese Option von Routern ignoriert werden. Bei dem darauffolgenden Header handelt es sich um den Destination Option Header. Die darin hinterlegte Option ist die Home Address Option, aus welcher der Router die HoA des Senders entnimmt.

Hiernach folgt der Mobility Header mit der Binding Update Message sowie den CGA-Optionen. Aus der Binding Update Message wird u.a. die Sequenznummer gelesen. Ist diese gültig, wird die CGA Parameter Datenstruktur den CGA Parameter Optionen entnommen. Mit dieser wird die in [20] beschriebene CGA-Überprüfung durchgeführt. Dies beinhaltet u.a. den Vergleich des in der Datenstruktur hinterlegten Subnet Prefixes mit dem der Source Address des IPv6 Header. Des weiteren wird ein SHA-1 Hash [22] über die Datenstruktur gebildet und die 64 ersten Bits des Ergebnisses mit dem Interface Identifier der Source Address verglichen. Nach erfolgreicher Überprüfung kann die aktuelle CoA des Senders eindeutig mit dem enthaltenen Public Key verbunden werden. Die folgende CGA Signature Option enthält eine kryptographische Signatur über die Home Address Option. Diese Signatur wird mithilfe

des RSA-Algorithmus überprüft. Als Eingabeparameter dient hierbei der zuvor entnommene Public Key. Ist die Signatur gültig, kann davon ausgegangen werden, dass die HoA mit der aktuellen CoA verbunden ist, der Sender also Besitzer der HoA ist. Somit ist die Aktualisierung des Verteilbaums kryptographisch stark authentifiziert. Sollte an einer beliebigen Stelle des Ablaufs eine Überprüfung fehlschlagen, so ist die Paketverarbeitung unverzüglich abzubrechen und das Paket sofort zu verwerfen.

Die weitere Paketverarbeitung hängt davon ab, ob der Router auf dem Pfad des Tree Elongation oder im regulären Multicastverteilbaum liegt. Bei ersterem entnimmt er die Gruppenadresse G dem Type 7 Routing Header (siehe Tabelle 1), implementiert den (nCoA, HoA, G) Multicast-Forwardingstate und leitet das Paket weiter. Ist der Router im regulären Multicastverteilbaum, arbeitet er wie in den *State Injection* und *Extended Forwarding* Algorithmen in [7] beschrieben.

Arbeitsweise des pDR Erreicht das Paket den pDR, wird das Paket zunächst gemäß der im vorherigen Abschnitt besprochenen Weise abgearbeitet. Danach überprüft der pDR, ob ein entsprechender (·, HoA, G) Zustand in seiner Multicast-Weiterleitungstabelle existiert und damit ein Mutlicastverteilbaum vor dem Handover vorhanden war. Ist dies der Fall, wird der Type 7 Routing Header entfernt und die Multicastadresse G als Destination Address in den IPv6 Header eingesetzt. Dann aktualisiert auch der pDR seine Multicast Forwarding States und leitet das Paket an die Multicast Gruppe weiter.

Um das Protokoll gegenüber möglichen Paketverlusten abzusichern, wird vom pDR verlangt, das erste eintreffende Updatepaket mit einem in Mobile IPv6 standardisierten Binding Acknowledgement zu bestätigen. Der pDR ist dabei der letzte sinnvolle Router, der die erfolgreiche Paketübertragung bestätigen kann, bevor es auf dem Multicastverteilbaum (möglicherweise) mulitpliziert wird.

Besteht kein (·, HoA, G)-Zustand, werden die Pakete verworfen, da es sich um gefälschte Pakete handeln könnte. Es wird dann auch kein Binding Acknowledgement Paket gesendet.

Arbeitsweise der Multicastempfänger Multicastempfänger erhalten die Pakete und analysieren sie nach dem vorgenannten Algorithmus. Ist die CGA-Überprüfung erfolgreich, interpretieren sie die Home Address Option im Destination Option Header. Daraufhin wird nicht nur der zur HoA gehörige Mobile IPv6 Binding Cache-Eintrag mit der CoA, sondern auch ebenso der Multicast Binding Cache-Eintrag aktualisiert. Schließlich werden die Daten mit der korrekten HoA und G an die Transportschicht weitergereicht, um eine störungsfreie Multicastkommunikation auf der Anwendungsschicht zu gewährleisten.

3.4 Diskussion: Data Plane, Control Plane

Das Einfügen der State Updates (Control Plane Daten) in den laufenden Nutzdatenstrom (Data Plane) birgt einige Probleme. Durch die Verwendung der Router Alert Option müssen alle Router die Header des u.U. großen Pakets untersuchen, was nicht nur die Anforderungen an die Prozessierungsgeschwindigkeit, sondern – bei gering optimierten Implementierungen – auch an den Speicherplatz erhöht. Das Einfügen und Auswerten von CGAs erhöht den Aufwand noch zusätzlich. Im Gegensatz dazu sind reine Control Plane Nachrichten kurze Datenpakete, die schnell ausgewertet werden können. Multicast-Router müssen die Update-Pakete zunächst auf der Control Plane auswerten und die Inhalte dann weiter an die Data Plane leiten. Dies kann zu unsauberen und fehleranfälligen Implementierungen führen.

Aus dem „Piggyback“-Ansatz resultieren jedoch einige Vorteile. So werden die State Updates durch die enthaltenen CGAs nicht nur selbstkonsistent authentifiziert, die Binding

Update Message enthält außerdem eine Sequenznummer, welche doppelte State Update-Verarbeitung verhindert. Außerdem können Paketduplikationen, Paketverlust und Pakete, die in falscher Reihenfolge eintreffen, erkannt werden.

4 Protokoll-Evaluierung

4.1 Protokoll-Overhead

Das Tree Morphing Protokoll ist durch das Einfügen zweier Header, den Router Alert Option und den Type 7 Routing Header, in die Binding Update Nachricht implementiert, welche mit den ersten regulären Multicast-Nutzdatenpaketen gesendet wird[4]. Daher müssen keine zusätzlichen Signalisierungspakete übertragen werden. Stattdessen werden alle nötigen Informationen in der Mobile IPv6 Binding Update Nachricht und der Home Address Option gesendet. Diese sind durch die CGA Header, ebenfalls im Mobility Header eingebettet, authentifiziert. Diese beiden Header fügen einen zusätzlichen Overhead von 256 Bit in das Paket ein.

Das Protokolldesign, welches für das Tree Morphing Protokoll eingeführt wurde, bedeutet nur minimale Veränderungen an vorhandenen Kommunikationsprotokollen. Es verwendet die Router Alert Option, um die State Update Message zu definieren, welche lediglich einen neuen Wert für das „Value"-Feld des Router Alerts benötigt, um den Typ der State Update Message darzustellen. Alle anderen Operationen basieren auf existierenden Protokollen wie z.B. IPv6 Source Routing oder Mobile IPv6. Dies schließt die Binding Update Message und die CGA Parameter und CGA Signature Optionen im Mobilitiy Header, wie in [18] definiert, ein. Durch die Wiederverwendung existierender Header und Protokolle können Implementationen auf leichte und zuverlässige Art realisiert werden.

4.2 Verarbeitungs-Overhead

Die State Update Pakete lösen eine Paketverarbeitung in jedem Router entlang des Pfades aus. Während der algorithmische Aufwand der SSM Sendermobilitätsverwaltung unter dem State-Management Aufwand für ASM in PIM-SM durch die Wiederverwendung von States ohne weitere Signalisierungen bleibt, führt die kryptographische Verifikation der CGA Home Adressen einen Berechnungsaufwand ein. Gemäß [20] werden die hereinkommenden Daten zunächst einem Sanity Check unterzogen. Dabei wird überprüft, ob die Eingabeparameter aus der CGA Parameter Option gültige Werte enthalten. Das „Collision Count"-Feld darf beispielsweise nur die Werte 0, 1 und 2 annehmen. Pakete, die diese Überprüfung nicht bestehen, müssen sofort verworfen werden. Außerdem können Pakete mit einer ungültigen Sequenznummer ebenso direkt verworfen werden.

Während diese Überprüfungen leicht durchgeführt werden können, sind die folgenden Berechnungen deutlich rechenintensiver. Zunächst wird der SHA-1 Hashwert über die gesamte CGA Parameter Option generiert und die 64 höchstwertigen Bits mit dem Interface Identifier verglichen. Da diese Generierung von der CGA Parameter Option abhängt und diese neben Feldern mit fester auch den Public Key und optionale Erweiterungsfelder mit variabler Länge enthält, hängt die für die SHA-1-Generierung nötige Zeit linear von diesen Eingabeparametern ab. Gefälschte Pakete werden wiederum verworfen. Anschließend wird ein weiterer SHA-1 Hashwert – ebenfalls über die gesamte CGA Parameter Option – generiert und abhängig vom Security-Parameter *sec* die $16 * sec$ höchstwertigen Bits mit Null verglichen. Hierbei werden jedoch das „Subnet Prefix"-, sowie das „Collision Count"-Feld auf Null gesetzt, was sich allerdings nicht auf die Berechnungsdauer des Hashwertes

[4] Zum jetzigen Zeitpunkt kann davon ausgegangen werden, dass ein Binding Update immer ein Bestandteil der zukünftigen Multicast Quellen-Mobilitätslösungen sein wird [8].

auswirkt. Sollten diese Überprüfungen erfolgreich sein, wird die CGA-Signatur des Pakets mit Hilfe des vorher überprüften Public Keys durch den RSA-Algorithmus verifiziert. Diese Berechnung ist rechenaufwändig und besitzt die komplexität $O(k^2)$, wobei k die Länge des Schlüsselmoduls ist [23].

Dennoch legt die Absicherung der Updates durch CGAs und damit die Überprüfung der RSA-Signatur einen nicht unerheblichen, zusätzlichen Berechnungsaufwand auf die Tree Morphing Router. Allerdings müssen die State Updates von jedem beteiligten Router aus den vorgenannten Gründen nur einmal pro Handover verarbeitet werden. Nimmt man eine mittlere Handoverfrequenz von einigen Wechseln pro Minute an, so liegt der Berechnungsaufwand immer noch deutlich unter dem Aufwand, den Protokolle wie z.B. SEND [19] auf die Router legen. SEND sichert die ARP-Requests eines Netzwerks ab. Diese treten in größeren Netzwerken mehrfach pro Sekunde auf.

4.3 Robustheit

Robustheit gegenüber Netzwerkfehlern In ungestörten Netzen ohne Paketverluste muss das State Update nur ein einziges Mal mit dem ersten Paket nach einem Multicast Source Handover gesendet werden, da die notwendigen Zustände in den Routern dadurch bereits etabliert werden. Um jedoch möglichem Paketverlust in unzuverlässigen oder verstopften (Funk-) Netzwerken entgegenzuwirken, muss die Übertragungsstrecke der State Update Pakete abgesichert werden. Dabei sollte nicht nur die unsichere Übertragung über (Funk-) Netzwerke, sondern auch der Weg vom nDR zum pDR abgesichert werden, damit der Baumanschluss sichergestellt ist. Der auf dem Weg zur Multicastverteilung letzte sinnvolle Knoten, der Empfangsbestätigungen auf eingehende State Update Pakete senden kann, ist der pDR. Es wird deshalb verlangt, dass der pDR auf die erste eingehende State Update Nachricht mit einer Bestätigung antwortet. Hierzu bietet sich die in Mobile IPv6 vorhandene Binding Update Acknowledgement Nachricht an. Wird diese Bestätigung von der mobilen Multicastquelle empfangen, ist der Anschluss an den Multicastverteilbaum sichergestellt. Dennoch können weitere State Updates gesendet werden, um Paketverlusten im Verteilbaum entgegenzuwirken. Somit kann sichergestellt werden, dass alle Multicastempfänger das Update erhalten.

Ein weiteres Problem, das in Netzwerken auftreten kann, sind Paketüberholungen. Dabei erhält der Empfänger der Pakete diese nicht in der Reihenfolge, in der sie vom Sender abgeschickt worden sind. Da erste aufeinanderfolgende Nutzdatenpakete gleichartige State Updates tragen, werden diese Pakete gleichermaßen Updates in den Routern auslösen. Daher ist die Reihenfolge der Pakete *eines* Handovers für die Aktualisierung der Router irrelevant. Auch hier kann wieder die Sequenznummer in den Pakete benutzt werden, um die Updates – selbst in falscher Reihenfolge – nur einmal pro Handover zu verarbeiten. Die Update-Sequenznummer ändert sich dabei lediglich bei jedem Handover.

In dem Beispielnetzwerk aus Abbildung 6 können nach dem Handover der mobilen Multicastquelle Paketverluste am nDR auftreten, da im nDR nach einem State Update kein State mehr für die Paketverteilung der aus Richtung pDR eintreffenden Pakete vorhanden ist. Obwohl es Topologien gibt, in denen dieses Worst-Case Szenario auftreten kann, tritt dieser Fehler bei üblichen Handoverzeiten (Layer 2 Handover, IPv6 Adresskonfiguration und Mobile IPv6 Binding Update) nicht auf, da nach einem Handover alle „alten“ Multicastpakete, einschließlich vorheriger Updates, bereits ausgeliefert worden sind. Beim Einsatz von Beschleuningungsprotokollen, wie z.B. Fast Handovers for Mobile IPv6 [24] oder Hierarchical Mobile IPv6 Mobility Management [25], können solche Effekte aber durchaus auftreten. Um die Auslieferung „alter“ Multicastpakete zu garantieren, sollten alle mobilen Multicastquellen sicherheitshalber eine Back-Off Zeit einhalten, in der nach einem Handover keine Multicastpakete gesendet werden dürfen.

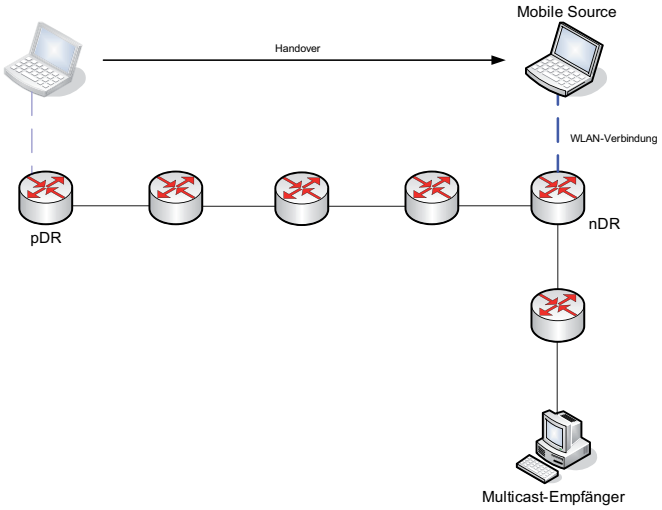


Abbildung 6. Beispiel möglicher Paketverluste am nDR

Robustheit gegenüber Angriffen Das Protokoll muss diversen bekannten Attacken standhalten. Durch das erneute Senden von mitgehörten Paketen könnte ein Angreifer der Routerinfrastruktur zusätzlichen Verarbeitungsaufwand aufzwingen. Das Ziel einer sog. „Replay Attacke“ müsste die CGA jedes Mal überprüfen, wenn ein Paket eintrifft. Das Protokoll widersteht diesen Attacken durch die Verwendung der Sequenznummer in der Binding Update Nachricht, welche durch die Paketsignatur geschützt ist. Pakete mit ungültigen Paketnummern werden bereits beim vorher erwähnten Sanity Check herausgefiltert. Das Tree Morphing Protokoll ist deshalb im Rahmen der wohlbekannten Sicherungsmechanismen lediglich so anfällig für Attacken wie das standardisierte Protokolle SEND [19] und führt keine neuen Sicherheitsprobleme ein. Daher müssen neue Nachrichten von den Routern lediglich einmal kryptographisch verarbeitet werden.

Des weiteren könnte ein Angreifer seine eigene valide Home Address benutzen, um State Updates im Netzwerk auszulösen. Da solche Pakete bei Erreichen des previous Designated Routers durch SSM Quellenfilterung verworfen werden, führt eine solche Attacke nicht dazu, dass das Netzwerk ungültige Pakete in den Multicastverteilbaum sendet, sondern lediglich dazu, dass sie entlang der initialen Unicast Source Route gesendet werden. Folglich führt die vorgestellte Tree Morphing Implementation im Gegensatz zu ASM nicht die Möglichkeit von netzwerkunterstützten verteilten Denial of Service Attacken ein.

Das Ableiten von CGAs für eine Vielzahl von Interface Identifiern ist eine zeitaufwändige Aufgabe, besonders, wenn das Angriffsziel einen hohen Security Parameter *sec* verlangt (vgl. [20]). Um die Komplexität, gültige CGAs zu erzeugen, quantitativ abschätzen zu können, wurden aufeinanderfolgende, gültige CGAs unter Veränderung des Modifiers gebildet. Der Modifier ist Teil der CGA Parameter Datenstruktur, die als Eingabe in die CGA-Berechnungsfunktion dient. Die anderen Felder der Struktur wurden bei der CGA-Generation nicht verändert. Tabelle 3 zeigt den Security Parameter *sec*, das Arithmetisches Mittel der Modifier-Schrittweite und die Standardabweichung. Die Modifier-Schrittweite bezeichnet dabei die Anzahl der Veränderungen des Modifiers, um von einer gültigen CGA zur folgenden zu gelangen.

Die Ergebnisse zeigen den erwarteten, exponentiellen Anstieg der Komplexität. Durch das Erhöhen des Security Parameters *sec* um 1 auf der Empfängerseite wird die Komplexität, zwei aufeinander folgende, gültige CGAs zu erzeugen um eine Größenordnung von 5 erhöht. Ein Knoten, der eine Attacke durch ungewöhnlich hohe Auslastung bemerkt, kann (temporär) verlangen, einen höheren Security Parameter *sec* zu benutzen. Dadurch können Angreifer zuvor generierte CGAs nicht weiter benutzen. Der Aufwand, CGAs zu generieren,

Sec	Arithmetisches Mittel der Modifier-Schrittweite	Standardabweichung
0	1	0
1	66.113	256
2	2.591.220.608	50.901

Tabelle 3. Komplexität der CGA Berechnung

ist wesentlich größer als diese zu überprüfen. Laut [23] ist der Aufwand, RSA-Signaturen zu generieren, $O(k^3)$, wobei k die Länge des Schlüsselmoduls ist. Das Verifizieren einer CGA hingegen kann durch das einfache Berechnen zweier SHA-1 Hashwerte und die RSA-Verifikation mit dem Aufwand $O(k^2)$ durchgeführt werden.

Das Generieren von CGAs ist also wesentlich komplexer als das Überprüfen - besonders wenn der Security Parameter *sec* auf einen hohen Wert gesetzt ist [20]. Daher ist es schwer für Angreifer viele CGA-signierte Nachrichten für unterschiedliche HoAs zu senden, um dadurch viele States in den Routern auf der Unicast Source Route zwischen nDR und pDR zu etablieren und damit die Ressourcen (Multicast-Routingtabelle und damit Hauptspeicher) des Routers zu verschwenden.

5 Zusammenfassung und Ausblick

Wir haben ein Realisierungskonzept für unser Tree Morphing Protokoll vorgestellt, welches allein mithilfe von Standardkomponenten der IPv6 Familie ein adaptives multicast Routing für mobile Datenquellen realisiert. In diesem kryptographisch robust authentifizierten Signalisierungsschema werden durch Einführung einer Hop-by-Hop Router Alert Option reguläre Binding Updates der Internet Mobilitätsschicht von der Vermittlungsinfrastruktur parallel zur Datenübermittlung interpretiert und bewirken die darin benötigten Aktualisierungen. Die Verarbeitung dieser State Update Messages deligiert zwar zusätzliche Verarbeitungslast in die Internet Router, doch ist zu betonen, dass pro Handover lediglich eine Aktualisierungsnachricht prozessiert werden muss. Das vorgestellte Protokoll ist durch interne Sequenzierung zudem gegen Mehrfachverarbeitung und Replay–Attacken geschützt.

Unsere gegenwärtigen Arbeiten konzentrieren sich auf eine Implementierung des Protokolls innerhalb der OMNeT++ Netzwerksimulationsplattform und auf nachfolgende Untersuchungen der Protokollperformanz und –robustheit gegenüber Netzwerkstörungen, z.B. durch Bursts und Paketüberläufe. Solchen realitätsnahen Betriebsproblemen in paketvermittelnden Netzen kann das Protokoll durch geeignete Signalisierungsredundanzen begegnen, welche lediglich im Fall von Paketverlusten zur Verarbeitung gelangen.

Multicast Mobilität ist ein an Aktualität deutlich gewinnendes, aber in zweifacher Hinsicht schwieriges Problem: Die technische Lösung einer übergangslos echtzeitfähigen Gruppenkommunikation an sich bildet eine große Herausforderung, ihre praktische Implementierung in unseren Alltagsnetzen zu bewältigen muß jedoch als beinahe größere Hürde angesehen werden. Alternative Ansätze im Overlay oder hybride Architekturen [26] mögen hier einen Übergangs- oder Ausweg bilden.

Literatur

1. Biersack, E.W.: Where is Multicast Today? Computer Communication Review **35**(5) (2005) 83–84
2. Holbrook, H., Cain, B.: Source-Specific Multicast for IP. RFC 4607, IETF (2006)
3. Bhattacharyya, S.: An Overview of Source-Specific Multicast (SSM). RFC 3569, IETF (2003)
4. Deering, S.E.: Host Extensions for IP Multicasting. RFC 1112, IETF (1989)
5. Johnson, D.B., Perkins, C., Arkko, J.: Mobility Support in IPv6. RFC 3775, IETF (2004)

6. Schmidt, T.C., Wählisch, M.: Extending SSM to MIPv6 — Problems, Solutions and Improvements. Computational Methods in Science and Technology **11**(2) (2005) 147–152 Selected Papers from TERENA Networking Conference, Poznań, May 2005.
7. Schmidt, T.C., Wählisch, M.: 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) (2006) 131–154
8. Schmidt, T.C., Wählisch, M.: Multicast Mobility in MIPv6: Problem Statement and Brief Survey. IRTF Internet Draft – work in progress 01, MobOpts (2007)
9. Xylomenos, G., Polyzos, G.C.: IP Multicast for Mobile Hosts. IEEE Comm. Mag. **35**(1) (1997) 54–58
10. Romdhani, I., Bettahar, H., Bouabdallah, A.: Transparent handover for mobile multicast sources. In Lorenz, P., Dini, P., eds.: Proceedings of the IEEE ICN'06, IEEE Press (2006)
11. Fenner, B., Handley, M., Holbrook, H., Kouvelas, I.: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised). RFC 4601, IETF (2006)
12. Thaler, D.: Supporting Mobile SSM Sources for IPv6. Proceedings of ietf meeting, individual (2001)
13. Jelger, C., Noel, T.: Supporting Mobile SSM sources for IPv6 (MSSMSv6). Internet Draft – work in progress (expired) 00, individual (2002)
14. Fenner, B., Haberman, B., Holbrook, H., Kouvelas, I.: Multicast Source Notification of Interest Protocol. Internet Draft – work in progress (expired) 05, IETF (2004)
15. Chang, R.S., Yen, Y.S.: A Multicast Routing Protocol with Dynamic Tree Adjustment for Mobile IPv6. Journ. Information Science and Engineering **20** (2004) 1109–1124
16. O'Neill, A.: Mobility Management and IP Multicast. Internet Draft – work in progress (expired) 01, IETF (2002)
17. Deering, S., Hinden, R.: Internet protocol, version 6 (IPv6) specification. RFC 2460, Internet Engineering Task Force (1998)
18. Arkko, J., Vogt, C., Haddad, W.: Enhanced Route Optimization for Mobile IPv6. RFC 4866, IETF (2007)
19. Arkko, E., Kempf, J., Zill, B., Nikander, P.: SEcure neighbor discovery (SEND). RFC 3971, Internet Engineering Task Force (2005)
20. Aura, T.: Cryptographically Generated Addresses (CGA). RFC 3972, IETF (2005)
21. Partridge, C., Jackson, A.: IPv6 router alert option. RFC 2711, Internet Engineering Task Force (1999)
22. Eastlake(3rd), D., Jones, P.: US secure hash algorithm 1 (SHA1). RFC 3174, Internet Engineering Task Force (2001)
23. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms - 2nd Edition. MIT Press (2001)
24. Koodli, R.: Fast Handovers for Mobile IPv6. RFC 4068, IETF (2005)
25. Soliman, H., Castelluccia, C., Malki, K., Bellier, L.: Hierarchical Mobile IPv6 mobility management (HMIPv6). RFC 4140, IETF (2005)
26. Wählisch, M., Schmidt, T.C.: Between Underlay and Overlay: On Deployable, Efficient, Mobility-agnostic Group Communication Services. Internet Research **17**(5) (2007)