htw saar
Hochschule für
Technik und Wirtschaft
des Saarlandes
University of
Applied Sciences

Mobile IPv4 vs. Mobile IPv6

Fatemeh Zarsaz

CONTENTS

KAPITEL I: EINELEITUNG

Einführung

Vor einigen Jahrzehnten war es nur möglich, über Festnetztelefone oder öffentliche Telefonzellen fernzukommunizieren. Die Fähigkeit, jederzeit und überall zu telefonieren oder online zu gehen, war undenkbar. Jedoch haben die rasante Entwicklung der Kommunikationstechnologien und die Entstehung des Mobilfunks diese Einschränkungen beseitigt. Heute können wir über unsere Mobiltelefone telefonieren, uns ins Internet einwählen und den Standort wechseln, ohne dabei die Verbindung zu verlieren. Diese nahtlose Übertragung wird durch Mobile Internet Protocols ermöglicht, die im Hintergrund arbeiten und sicherstellen, dass eine stabile Verbindung aufrechterhalten bleibt. Mobile Telefone sind heutzutage ein unverzichtbarer Teil unseres Alltags und bieten vielfältige Nutzungsmöglichkeiten wie den Zugang zum Internet, E-Mail-Kommunikation, Videokonferenzen und mobiles Arbeiten.

Definition

Mobile IP (MIP) ist ein Netzwerkprotokoll, das von der Internet Engineering Task Force (IETF) entwickelt wurde, um mobilen Geräten zu ermöglichen, ihre IP-Adresse bei Bewegung zwischen Netzwerken beizubehalten. Durch die Trennung der IP-Adresse des Geräts von seiner physischen Position nutzt das Protokoll temporäre "Besucheradressen", wenn das Gerät sich in einem neuen Netzwerk anmeldet. Die Heimatadresse des Geräts wird in einem zentralen Verzeichnis namens "Home Agent" hinterlegt, um sicherzustellen, dass das Gerät trotz Änderung der IP-Adresse erreichbar bleibt. MIP verbessert die Konnektivität von Mobilgeräten durch nahtlose Übertragungen zwischen Netzwerken.
Mobile IP ist in der Lage, aktuelle Internetprotokolle sowohl in kabelgebundenen als auch in drahtlosen Netzwerken zu unterstützen, ohne dass andere Knoten geändert werden müssen, um mit den Knoten mit Mobile-IP-Funktionalität kommunizieren zu können. Das Protokoll ist für eine große Anzahl von Benutzern skalierbar und bietet eine sichere Übertragung, bei der die Benutzer darauf vertrauen können, dass ihre Nachrichten nicht abgehört und ihre Ressourcen nicht unbefugt genutzt werden.

Überblick über MIPv4 Und MIPv6

MIPv4 und MIPv6 repräsentieren signifikante Fortschritte in den Protokollen für mobile Netzwerke. Während MIPv4 den Weg für MIPv6 bereitete, hat letzteres noch größere Fortschritte bei der Verbesserung der Stabilität von Verbindungen, Sicherheit und Benutzerfreundlichkeit gemacht. Obwohl es immer Spielraum für Verbesserungen gibt, hat MIPv6 viele Fortschritte und Lösungen eingeführt, um die in MIPv4 aufgetretenen Probleme zu lösen.
Während wir uns auf weitere Entwicklungen in den Protokollen für mobile Netzwerke freuen, die weiterhin die Art und Weise verbessern werden, wie wir uns in der digitalen Welt verbinden und miteinander interagieren, müssen wir auch verstehen, wie wir bisher gekommen sind. In dieser Ausarbeitung werden wir sowohl diese Technologien als auch ihre Entwicklung im Laufe der Zeit untersuchen.

Hintergrund Von MIPv4

Die Idee von Mobile IP (MIP) entstand in den frühen 1990er Jahren, als die Notwendigkeit aufkam, eine mobile Geräteverbindung aufrechtzuerhalten, während sich die Geräte in verschiedenen Netzwerkumgebungen bewegen. Im Jahr 1994 wurde eine erste MIP-Version von Charles Perkins[1] entwickelt und in der Internet Engineering Task Force (IETF) diskutiert. Eine endgültige Version wurde jedoch erst 1996 fertiggestellt [17].

In diesem Jahr wurden auch RFCs (Request for Comments) veröffentlicht, um das MIP-Protokoll zu standardisieren und es anderen Entwicklern zur Verfügung zu stellen. Das RFC 2002 [17], das im Jahr 1996 veröffentlicht wurde, beschreibt das erste formelle MIPv4-Protokoll. Das Protokoll ermöglichte es mobilen Geräten, sich nahtlos zwischen verschiedenen IP-Netzwerken zu bewegen, ohne ihre Verbindung zu unterbrechen.

In den folgenden Jahren wurde das MIPv4-Protokoll weiterentwickelt und verbessert, um seine Leistung und Funktionalität zu optimieren. Im Jahr 1998 wurde das RFC 2290 veröffentlicht, das die Verwendung von MIP in Verbindung mit „Network Address Translation“ (NAT) unterstützt und das "Mobile IP Protocol" wird von der Internet Engineering Task Force (IETF) als offizieller Standard anerkannt

Im Jahr 1999 wurden zusätzliche RFCs veröffentlicht, darunter das RFC 2356, das MIP-Implementierungen auf verschiedenen Plattformen beschreibt, und das RFC 2486, das die Verwendung von MIP in Verbindung mit IPv6-Netzwerken unterstützt.

Im Jahr 2000 wurde das RFC 3024 veröffentlicht, das die Verwendung von MIP in Verbindung mit IP-Sicherheit (IPSec) beschreibt. Das Protokoll wurde weiterhin verbessert, um die Unterstützung für verschiedene Netzwerkszenarien und die Interoperabilität mit anderen Protokollen wie IPv6 zu verbessern. RFC 5944 gilt als die letzte Version der Kette von RFC-Updates für MIPv4 und ist eine der Hauptquellen, die wir für diesen Abschnitt verwendet haben.

Funktionen Und Komponenten Von MIPv4 [1] [7]

Die Funktionen und Komponenten von MIPv4 umfassen Mechanismen zur Unterstützung der Mobilität von Endgeräten in IP-Netzwerken. Dazu gehören die Möglichkeit für ein Endgerät, seine IP-Adresse beizubehalten, während es von einem Netzwerk in ein anderes wechselt, sowie die Übertragung von Datenpaketen von der alten zur neuen Adresse .

MIPv4 besteht aus verschiedenen Komponenten wie dem „Mobile Node“ (MN), dem „Correspondent Node“ (CN), dem „Home Agent“ (HA) und dem „Foreign Agent“ (FA), usw.

Nun möchten wir mehr über diese Elemente erfahren und wie sie zusammenwirken, um die Mobilität über IP im MIPv4 zu ermöglichen.

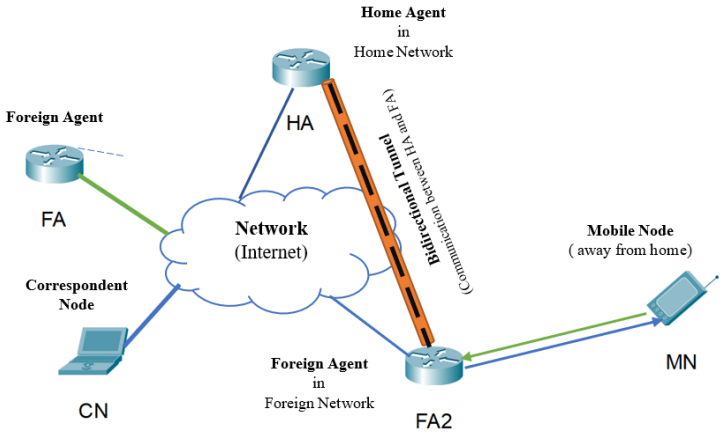

Figure 1.Verbindung über Foreign Agent in MIPv4

[1] als Hauptredakteur von RFC 2002, dem ersten Entwurf von MIP

- Home Address (HA): Die Home Address wird für alle Verbindungen innerhalb des Heimnetzes des mobilen Knotens verwendet, also dem ersten Netzwerk, in dem sich das Gerät registriert. Die HA bleibt immer unverändert, auch wenn sich der Standort des mobilen Knotens ändert. Alle Anwendungen innerhalb des mobilen Knotens verwenden diese IP-Adresse (alle höheren OSI-Schichten kennen nur den HA). Die Heimadresse ist eine permanente IP-Adresse, die einem mobilen Knoten zugewiesen wird und das Heimnetzwerk des Knotens identifiziert. Durch diese permanente Zuweisung bleibt der mobile Knoten unter seiner HA im Heimnetzwerk erreichbar, auch wenn er sich außerhalb des Heimnetzwerks befindet.
- Home Subnet Prefix: Das IP-Subnetzpräfix, das der HA des MN entspricht. Dieses Präfix ist ein wichtiger Bestandteil des MIPv4-Protokolls, da es dem MN ermöglicht, seine Verbindung aufrechtzuerhalten, indem es seine Home Address verwendet, wenn es in seinem Home-Netzwerk ist, und das „Temporary CoA“ verwendet, wenn es sich außerhalb des Home-Netzwerks befindet.
- Home Link: Der Link, an dem das Home Subnet Prefix definiert ist. Dieser Link verbindet den mobilen Knoten mit dem Home-Netzwerk.
- Mobile Node (MN): Ein Mobile Node ist ein Knoten, der sein Netzwerk und damit auch seine aktuelle IP-Adresse wechseln kann. Ein MN ist aber immer über seine Home Address erreichbar. Der MN kann von einem Netzwerk zum anderen wechseln, während er eine Verbindung aufrechterhält. Um dies zu erreichen, muss der MN das Protokoll von MIPv4 nutzen. Mithilfe von MIPv4 kann der MN seine Verbindung beibehalten, indem er das Home Network Prefix verwendet und einen „Temporary Care of Address“ (CoA) registriert.
- Correspondent Node (CN): Ein Knoten, der mit einem MN (Mobile Node) Daten austauscht und kommuniziert. Der CN kann selbst ein MN oder auch ein festes Gerät in einem Netzwerk sein. Der CN kann entweder mit der HA oder mit der CoA des MN kommunizieren, je nachdem, wo sich der mobile Knoten im Moment befindet. Durch die Verwendung von MIPv4 kann der CN in Echtzeit den Standort des mobilen Knotens mit Hilfe von HA verfolgen und die Verbindung entsprechend herstellen.
- Care of Address (CoA): Die Care of Address ist die momentane IP-Adresse, die vom mobilen Knoten verwendet wird, während er sich von seinem Home-Netzwerk entfernt hat (Away from Home). CoA ist eine globale Unicast-Adresse für den Mobil Knoten. Ein MN kann mehrere CoA haben, aber nur einer davon ist beim Home Agent (HA) des MN als primäre CoA registriert. Die CoA ist temporär und ändert sich bei jedem Standortwechsel des mobilen Knotens aus seinem Home Network. Eine CoA gilt nur, wenn das Mobile End Device in einem bestimmten Gast netz verbleibt.
- Tunneling Verfahren: Das Tunneling-Verfahren wird in MIPv4 eingesetzt, um Datenpakete zwischen dem mobilen Gerät (über sein Foreign Agent) und dem Heimnetzwerk des Geräts (HA) zu übertragen, wenn das Gerät sich in einem fremden Netzwerk befindet. Es ist notwendig, da das fremde Netzwerk möglicherweise keine Unterstützung für das Routing von Paketen an eine mobile Adresse bietet und es daher notwendig ist, einen Tunnel zu erstellen, um Pakete an das Gerät zu übertragen. Das Tunneling-Verfahren bietet auch eine Möglichkeit, um das Mobile Node (MN) während seiner Bewegung erreichbar zu halten, da es ständig mit seinem Heimnetzwerk verbunden bleibt.

- Binding Update (BU)
  Ein Befehl, den der MN an den HA sendet, um ihn darüber zu informieren, dass er eine neue CoA hat. Dies ist notwendig, damit der HA die Pakete an den MN weiterleiten kann, wenn dieser sich an einem neuen Ort befindet. Das BU enthält die neue CoA des MN sowie weitere Informationen wie z.B. den Security Association Identifier (SAI).

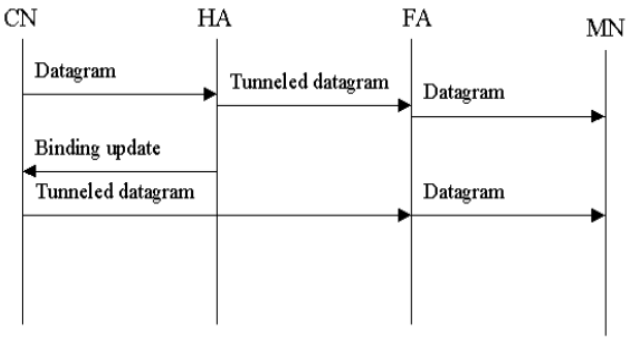

Figure 2. Binding Update zwischen CN und HA [11]

- Binding Acknowledgement (BA)
  Die Bestätigung des HAs, dass es das Binding Update des MN erhalten und akzeptiert hat. Der BA enthält die Informationen aus dem BU und kann auch eine Lifetime-Feld enthalten, das angibt, wie lange das Binding gültig ist.
- Smooth Handover: Handover-Prozess mit minimiertem Paketverlust.
- Fast Handover: Ein Handover-Prozess, bei dem die Handover-Verzögerung nicht kritisch ist.
- Seamless Handover: Ein Handover ohne Änderung der Qualität, Sicherheit oder Fähigkeiten des Dienstes (mehr zum MIPv6-Konzept).
- Roaming: Wenn sich MN außerhalb seiner erlaubten Region befindet und FA die Zulassung der Konnektivität zu MN auf der Grundlage vorheriger Vereinbarungen zwischen FA und HA gewähren muss.
- Reverse Tunneling (RT)
  Ein Mechanismus, der verwendet wird, wenn der FA den Datenverkehr an den HA weiterleitet. Der FA erstellt einen Tunnel zum HA und leitet dann den Datenverkehr durch diesen Tunnel weiter. Der Tunnel wird als " Reverse " bezeichnet, weil der Datenverkehr vom FA zum HA und dann zurück zum FA geleitet wird.

Betrieb von MIPv4

Der Begriff "Betrieb von MIPv4" umfasst die technischen Anforderungen und Einstellungen, die für die Implementierung und Nutzung von MIPv4 in einem Netz erforderlich sind. Dazu gehören z. B. die Konfiguration mobiler Geräte, die Verwaltung von IP-Adressen und Routing-Tabellen, die Bereitstellung von Sicherheitsfunktionen und die Überwachung der Netzaktivitäten, um ein reibungsloses Funktionieren von MIPv4 zu gewährleisten.
Die Implementierung von MIPv4 erfordert die Konfiguration spezieller MIPv4-Entitäten im Netz, einschließlich MN, HA, FA und anderer im letzten Abschnitt erwähnter Einheiten.
Mobile Geräte müssen außerdem speziell für die Verwendung von MIPv4 konfiguriert werden.
Während des Betriebs können verschiedene Herausforderungen auftreten, z. B. Latenz- und Sicherheitsprobleme, die durch geeignete Maßnahmen wie die Verwendung von Dienstqualitäts-Merkmalen und Sicherheitsprotokollen wie ESP gelöst werden können.
Um einen Überblick darüber zu gewinnen, wie MIPv4 tatsächlich funktioniert und wie diese Komponenten zusammenarbeiten, um eine reibungslose und stabile Verbindung zu gewährleisten, müssen wir uns zwei Hauptszenarien ansehen.

Entweder befindet sich der MN noch in seinem Heimatnetz (unter Verwendung der Heimatadresse) oder er ist "Away from Home" und wird zu einem Gast in einem anderen fremden Netz.

1. Wenn das mobile Gerät (MN) sich in seinem Heimnetzwerk befindet und sich innerhalb dieses Netzwerks bewegt:
   MN behält seine Heimadresse bei, unabhängig davon, wo es sich innerhalb des Heimnetzwerks befindet. Also erfolgt die Kommunikation direkt zwischen CN und MN, da sie sich beide im gleichen Netzwerk befinden.
   Die Bewegung innerhalb des Heimnetzwerks hat keinen Einfluss auf die Konnektivität, da MN weiterhin seine Heimadresse verwendet.
2. Wenn das mobile Gerät " weg von seinem Heimnetzwerk" ist:
   Wenn sich der MN außerhalb seines Heimatnetzes befindet, erhält er eine Care-of-Adresse (CoA) im fremden Netz. Die CoA identifiziert den aktuellen Standort des MN im fremden Netz. Der MN registriert dann seine CoA bei seinem Home Agent (HA), der ein Router in seinem Heimatnetz und für die Weiterleitung von Paketen an den MN verantwortlich ist. Der Registrierungsprozess umfasst das Senden einer Registrierungsanforderung an den HA, die den CoA des MN und andere Informationen enthält.
   Wenn der HA die Registrierungsanforderung erhält, erstellt er eine Mobilität Bindung zwischen der Heimatadresse des MN und der CoA. Der HA fängt dann Pakete ab, die für die Heimatadresse des MN bestimmt sind und kapselt sie in einen Tunnel zur CoA ein. Die eingekapselten Pakete werden dann an das fremde Netz weitergeleitet, wo sie entkapselt und an den MN zugestellt werden.
   Wenn der MN ein Paket an einen CN sendet, verwendet er seine Heimatadresse als Quelladresse und fügt seine CoA in das Optionsfeld des Pakets ein. Das Paket wird an den HA im Heimatnetz des MN weitergeleitet, der das Paket abfängt und es in einen Tunnel zum CoA einkapselt. Das eingekapselte Paket wird dann an das Fremdnetz weitergeleitet und an den CN zugestellt.

In beiden Szenarien behält MN seine Heimadresse bei, während es sich innerhalb oder außerhalb des Heimnetzwerks bewegt. Durch die Verwendung von temporären Adressen und Tunneling-Verfahren ist es möglich, die Konnektivität des mobilen Geräts aufrechtzuerhalten, auch wenn es sich in einem anderen Netzwerk befindet.

Triangle Routing

Triangle Routing ist eine Situation in MIPv4, bei der Datenpakete zwischen einem Communication Node (CN) und einem Mobile Node (MN) über den Home Agent (HA) umgeleitet werden, was zu einem längeren Pfad und möglicherweise höherer Latenz führt. Das kommt vor, wenn sich der MN nicht in seinem Heimnetzwerk befindet und sich der Datenverkehr zwischen dem CN und dem MN über den HA leiten muss, um die Mobilität des MN zu verwalten. Diese zusätzliche Umleitung über den HA kann zu einer ineffizienten Netzwerkperformance führen, da der Datenverkehr unnötig lange umgeleitet wird.

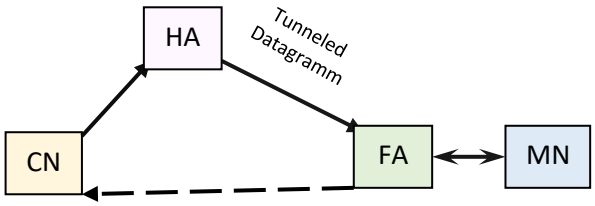

Figure 3.Triangle Routing mit CoA von FA [11]

Route Optimization [11] [7]

Wenn sich ein mobiler Knoten (MN) im fremden Netzwerk bewegt, kann er über seinen lokalen Router (Foreign Agent, FA) eine direkte Verbindung zu seinem Korrespondenzknoten (Correspondent Node, CN) aufbauen, ohne dass der gesamte Datenverkehr über seine Home Agent (HA) gehen muss und das Problem des Triangle Routing so weit wie möglich vermeiden. Dieser Prozess wird als Route-Optimierung bezeichnet und kann die Latenzzeit reduzieren und die Netzwerkbandbreite sparen. Es ist jedoch wichtig zu beachten, dass die Route-Optimierung in MIPv4 optional und nur eine Ergänzung der Mobile IPv4 ist und von den mobilen Knoten und dem Korrespondenzknoten unterstützt werden muss, um genutzt werden zu können.
In diesem Konzept, Die Route-Optimierung in MIPv4 nutzt die Technik des „Reverse Tunneling“, um eine direkte Verbindung zwischen dem MN und dem CN aufzubauen. Ein konzeptioneller Datenstruktur namens "Binding Cache" wird verwendet, um Bindungen für die Home-Adresse des MN und dessen aktuelle CoA zu speichern, die es dem CN ermöglicht, Datagramme direkt an die CoA des MN zu tunneln, ohne dass der Datenverkehr durch den HA geroutet werden muss. Wenn sich ein MN an einen anderen Standort (CoA) bewegt, sendet er eine "Binding update" an den Home Agent.
Eine "Binding " ist eine Zuordnung von HA plus der CoA, die ein Home Agent für alle seine mobilen Knoten unterhält.
Es ist aber wichtig zu merken, dass "Binding Updates" wirklich sensible Informationen in Bezug auf die Sicherheit sind und sie es einem Angreifer ermöglichen können, den gesamten Datenverkehr zum mobilen Knoten umzuleiten, wenn sie gefälscht werden können!
Um sie vor Fälschung zu schützen, verlangen die Standards daher, dass alle verbindlichen Updates mit IPsec ESP (IP-Security Encapsulating Security Payload) verschlüsselt warden.

Bei der Route Optimization gibt es zwei Arten von Verbindungen:

- Direct Routing: Wenn der MN und der CN im gleichen Subnetz sind, kann eine direkte Verbindung zwischen den beiden aufgebaut werden, ohne dass der HA involviert wird (HA wird nur einmal verwendet, um die foreign Adresse vom MN an den CN weiterzuleiten.). Dies wird als "Direct Routing" bezeichnet.

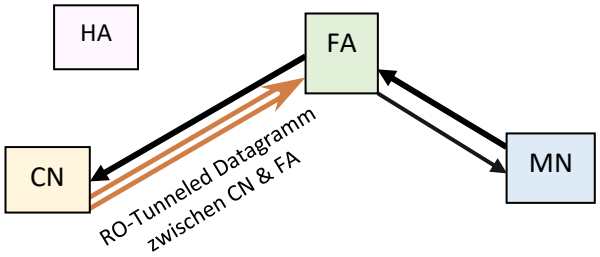

Figure 4.Direkte Verbindung mit RO und Binding Updates

- Indirect Routing: Wenn der MN und der CN sich in verschiedenen Subnetzen befinden, wird der Reverse Tunnel verwendet, um den Datenverkehr zwischen ihnen zu leiten. Hierbei wird der Datenverkehr vom CN zum HA geleitet, der ihn dann über den Reverse Tunnel an den MN weiterleitet. Dies wird als "Indirect Routing" bezeichnet.

Durch die Verwendung der Route Optimization wird die Leistung von MIPv4 verbessert und die Kommunikation zwischen MN und CN effizienter gestaltet. In Abwesenheit von Route

Optimization wird von MIPv4 Triangle Routing für das Routing verwendet. Während Route Optimization einen effizienteren und direkteren Routing-Pfad zwischen einem mobilen Knoten und seinem Korrespondenzknoten bietet, wird RO als optionales Feature von MIPv4 nicht genutzt, wenn beide Seiten der Verbindung diese Funktion nicht unterstützen."

Sicherheit in MIPv4 [7][13]

Sicherheit in MIPv4 bezieht sich auf die Maßnahmen, die ergriffen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Daten in einem MIPv4-Netzwerk zu gewährleisten. Dazu gehören verschiedene Sicherheitsprotokolle, die entwickelt wurden, um Bedrohungen wie unbefugten Zugriff, Datenmanipulation und Dienstausfälle zu verhindern. Eine effektive Sicherheitsstrategie erfordert die kontinuierliche Überwachung und Aktualisierung dieser Maßnahmen, um auf sich ständig ändernde Bedrohungen und Angriffstechniken reagieren zu können.
Während der Entwicklung von MIPv4 wurden mehrere Sicherheitsprobleme identifiziert, wie z.B. die Offenlegung von Informationen durch die Übertragung von IP-Adressen im Klartext, die Möglichkeit von „Man-in-the-Middle-Attacks“, „Bombing Attack“, „Redirection Attack“, “Reply Attack“ und „Denial-of-Service-Attacks“ auf den Home Agent oder den Mobile Node.[18]
Um diese und andere Sicherheitsprobleme zu lösen, wurden verschiedene Sicherheitsprotokolle wie das Mobile IPv4 Authentication Protocol (MIAP) und das Mobile IPv4 Message Authentication Code (MIMAC) und auch Unterstützung für „Quality of Service“ (QoS) entwickelt. MIAP bietet einen Mechanismus zur Authentifizierung des mobilen Knotens beim Home Agent oder Foreign Agent, während MIMAC die Nachrichtenauthentifizierung für mobile IP-Registrierung und Bindungsaktualisierungen bereitstellt.

Ein weiteres wichtiges Sicherheitsprotokoll, das in MIPv4 verwendet wird, ist IPsec (Internet Protocol Security). IPsec ist ein Protokoll, das zur Absicherung von IP-Kommunikationen eingesetzt wird und Vertraulichkeit, Datenintegrität und Datenursprungsauthentizität bietet. Es kann zur Absicherung der mobilen Knotenkommunikation in einem MIPv4-Netzwerk verwendet werden, indem es Verschlüsselung und Authentifizierung für die IP-Pakete bereitstellt.

Neben MIAP, MIMAC und IPsec können MIPv4-Netzwerke auch AAA- (Authentication, Authorization and Accounting) Protokolle wie RADIUS(Remote Authentication Dial-In User Service) und TACACS+ (Terminal Access Controller Access-Control System) für die Authentifizierung und Autorisierung des mobilen Knotens einsetzen. RADIUS ist ein beliebtes AAA-Protokoll, das zur Authentifizierung von Benutzern und Geräten und zur Verwaltung ihres Netzwerkverbrauchs eingesetzt wird. TACACS+ ist ein sichereres AAA-Protokoll, das separate Kanäle für Authentifizierung und Autorisierung verwendet.
Um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten in einem MIPv4-Netzwerk zu gewährleisten, ist es unerlässlich, geeignete Sicherheitsmaßnahmen zu implementieren. Die Vertraulichkeit kann durch Verwendung von Verschlüsselung und Zugriffskontrollmechanismen gewährleistet werden, um unbefugten Zugriff auf Daten zu verhindern. Die Datenintegrität kann durch Verwendung von kryptografischen Mechanismen wie digitalen Signaturen und Nachrichtenauthentifizierungscodes aufrechterhalten werden, um unbefugte Änderungen zu erkennen und zu verhindern. Die Verfügbarkeit kann durch Verwendung von Redundanz- und

Ausfallsicherheitsmechanismen sichergestellt werden, um Netzwerkkontinuität im Falle eines Ausfalls zu gewährleisten.
Es ist wichtig zu beachten, dass diese Sicherheitsprotokolle zwar einen gewissen Schutz für MIPv4-Netzwerke bieten, aber nicht narrensicher sind. Da neue Schwachstellen und Angriffsvektoren entdeckt werden, ist es entscheidend, sich über die neuesten Sicherheitsbest Practices auf dem Laufenden zu halten und die eingesetzten Sicherheitsmaßnahmen kontinuierlich zu bewerten und zu aktualisieren, um die Sicherheit des Netzwerks und seiner Benutzer zu gewährleisten.[2]

MIPv4: Vorzüge und Limitierungen

Bisher haben wir die Definition und die Funktionen von IPv4 kennengelernt.
Obwohl MIPv6 als Erweiterung von MIPv4 viele der Einschränkungen von MIPv4 überwindet, wird MIPv4 in einigen Netzwerken immer noch verwendet und hat seine eigenen Vor- und Nachteile.
In diesem Abschnitt betrachten wir einige dieser Eigenschaften.

Vorteilen

In den vorherigen Abschnitten haben wir bereits einige der wichtigsten Vorteile von MIPv4 erläutert, die für die Existenz dieser Technologie entscheidend waren. Zusammenfassend lässt sich sagen, dass MIPv4 die Bewegung von mobilen Geräten ohne die Notwendigkeit, die Netzwerkverbindung zu unterbrechen oder neu zu konfigurieren, ermöglicht. Die Implementierung von MIPv4 ist vergleichsweise einfach und kann auf einer Vielzahl von Geräten und Plattformen genutzt werden. Obwohl die Latenz bei der Verwendung von MIPv4 im Vergleich zu herkömmlichen statischen IP-Adressen höher sein kann, ist sie im Vergleich zu anderen mobilen IP-Protokollen geringer.
Ein weiterer wichtiger Vorteil von MIPv4 ist die breite Unterstützung. Es wird von vielen Betriebssystemen und mobilen Geräten unterstützt, was zu einer hohen Kompatibilität und Interoperabilität führt. MIPv4 bietet auch Unterstützung für Quality-of-Service (QoS)-Funktionen, die eine differenzierte Behandlung von Datenverkehr auf Netzwerkebene ermöglichen.
Darüber hinaus hatte MIPv4, wie im Abschnitt Sicherheit erläutert, einen großen Einfluss auf die Entwicklung und Verbesserung von Sicherheitsprotokollen und die Erhöhung des Sicherheitsniveaus.

Nachteilen

Insgesamt können wir die Nachteile von IPv4 in vier Kategorien einteilen:

- Sicherheitsprobleme
- Physische Einschränkungen
- Netzwerkleistung
- Einschränkung bei der Nutzung

[2] Mehr über MIPv4-Sicherheit im nächsten Abschnitt.

- **Sicherheitsprobleme**

Eine potenzielle Einschränkung der in MIPv4 verwendeten Sicherheitsmaßnahmen besteht darin, dass die Authentifizierungs- und Autorisierungsmechanismen in beträchtlichem Umfang auf die Verwendung von Pre-Shared Keys angewiesen sind. Das bedeutet, dass ein Angreifer, der den Pre-Shared Keys erlangen kann, sich einfach als legitimer Benutzer ausgeben und Zugriff auf das Netzwerk erhalten kann. Dies ist eine erhebliche Schwachstelle, da Pre-Shared Keys für Brute-Force-Angriffe anfällig sind und sich nur sehr schlecht schützen und verwalten lassen.
Eine weitere Schwäche, der bei MIPv4 verwendeten Sicherheitsmaßnahmen ist, das Fehlen einer Verschlüsselung für Daten, die über das Netzwerk übertragen werden. Dies bedeutet, dass alle über das Netzwerk gesendeten Daten, einschließlich sensibler Informationen wie Anmelde-informationen und Finanzinformationen, potenziell von einem Angreifer abgefangen und gelesen werden können. Dies könnte insbesondere für Benutzer, die das Netzwerk von öffentlichen Wi-Fi-Hotspots oder anderen ungesicherten Netzwerken ausnutzen, alarmierend sein.
Schließlich kann die Verwendung von MIPv4 für Netzwerkadministratoren auch eine Herausforderung darstellen, wenn es darum geht, Sicherheitsrichtlinien zu verwalten und durchzusetzen. Da Benutzer zwischen Netzwerken und Geräten wechseln, kann es schwierig sein sicherzustellen, dass alle Geräte mit den neuesten Sicherheitspatches und Konfigurationen auf dem neuesten Stand sind. Dies könnte das Netzwerk anfällig für Angriffe lassen, selbst wenn einzelne Geräte gesichert sind.
Insgesamt bieten die bei MIPv4 verwendeten Sicherheitsmaßnahmen zwar einige Schutz-maßnahmen gegen unbefugten Zugriff, es gibt jedoch mehrere potenzielle Einschränkungen und Schwächen, die berücksichtigt werden sollten. Um diesen Bedenken entgegenzuwirken, sollten Netzwerkadministratoren möglicherweise zusätzliche Sicherheitsmaßnahmen wie sicherere Authentifizierungsmethoden und die Verwendung von Verschlüsselung für über das Netzwerk übertragene Daten in Betracht ziehen.

- **Netzwerkleistung- und Physische Einschränkungen**

Physische Einschränkungen bezieht sich auf die Nachteile von MIPv4, die mit den physischen Aspekten des Netzwerks und der Netzwerkinfrastruktur zusammenhängen. Ein Beispiel hierfür ist die begrenzte Reichweite von WLAN-Netzwerken, die die Mobilität von Benutzern einschränken kann, die zwischen verschiedenen WLAN-Netzwerken wechseln. Ein weiteres Beispiel sind die Kosten und logistischen Herausforderungen, die mit dem Aufbau und Betrieb eines umfangreichen Netzwerks von Home Agents verbunden sind, die erforderlich sind, um MIPv4 zu unterstützen. Ein weiteres Beispiel ist die Abhängigkeit von der Verfügbarkeit von geeigneten Netzwerkverbindungen, um eine reibungslose Mobilität zu gewährleisten, was zu Problemen führen kann, wenn Netzwerkverbindungen instabil oder unzuverlässig sind.
In diesem Kontext bezieht sich "geeignete Netzwerkverbindungen" auf Netzwerkverbindungen, die in der Lage sind, eine nahtlose und unterbrechungsfreie Übertragung von Daten zu gewährleisten, wenn sich ein mobiler Knoten zwischen verschiedenen Netzwerken bewegt. Das bedeutet, dass die Netzwerkverbindungen eine ausreichend hohe Qualität und Bandbreite haben sollten, um den Anforderungen der mobilen Anwendungen und Geräte gerecht zu werden und einen reibungslosen Übergang zwischen den Netzwerken zu ermöglichen

Noch dazu, MIPv4 kann sich negativ auf die Netzwerkperformance auswirken, da es zu einem erhöhten Datenaufwand führen kann. Insbesondere kann die begrenzte Anzahl von verfügbaren Adressen in MIPv4 (2^{32} -IP-Adresse, ungefähr 4,3 Milliarden) zu Problemen führen, da sich viele mobile Geräte um eine begrenzte Anzahl von Adressen "streiten" müssen. Dies kann zu längeren Latenzzeiten und erhöhtem Paketverlust führen, was wiederum die Netzwerkperformance beeinträchtigen kann. Da MIPv4 die simultane Nutzung mehrerer Netzwerkschnittstellen nicht unterstützt, kann es auch zu einer eingeschränkten Mobilität führen, da mobile Geräte gezwungen sind, zwischen verschiedenen Netzwerken umzuschalten, um eine Verbindung aufrechtzuerhalten. Triangle Routing: Triangle Routing ist weder ein Vorteil noch ein Nachteil von Mobile IPv4 an sich, sondern eine von mehreren möglichen Tunneling-Methoden von MIPv4. Es wird aber als Nachteil von MIPv4 angesehen, wenn es zu einem unnötigen Anstieg des Netzwerkverkehrs führt. Das liegt daran, dass bei Triangle Routing der Datenverkehr zwischen dem mobilen Knoten und dem entfernten Knoten über den Home Agent umgeleitet wird, anstatt eine direkte Verbindung zu ermöglichen. Dieser Umweg kann zu Verzögerungen und erhöhtem Netzwerkverkehr führen, insbesondere in großen Netzwerken mit vielen mobilen Knoten. Außerdem kann die erhöhte Latenzzeit durch die zusätzliche Umleitung des Datenverkehrs die Qualität der Übertragung beeinträchtigen, insbesondere bei anwendungsintensiven Anwendungen wie Video-Streaming oder Sprachkommunikation.

- **Einschränkungen bei Nutzung**

Nutzungsbeschränkungen in MIPv4 verweisen auf bestimmte Szenarien, in denen die Mobilität der Benutzer begrenzt sein kann. So kann MIPv4 beispielsweise nur eine Verbindung pro Endgerät unterstützen, was die Nutzung mehrerer Netzverbindungen erheblich erschweren kann. Darüber hinaus kann die MIPv4-Signalisierung einen zusätzlichen Overhead und eine Verzögerung verursachen, was die Netzleistung beeinträchtigt.

Darüber hinaus kann die Verwendung von MIPv4 auf mobilen Geräten zu einem erhöhten Stromverbrauch führen, da häufige "Handoffs" zwischen verschiedenen Netzen erforderlich sind und eine ständige Kommunikation mit mehreren Netzeinheiten stattfinden muss. Dies kann dazu führen, dass mobile Geräte schneller entladen werden, was vor allem in Umgebungen mit begrenzter Stromversorgung, z. B. im Außeneinsatz, problematisch sein kann. Daher kann die Verwendung von MIPv4 die Energieeffizienz von Mobilgeräten in bestimmten Anwendungsfällen einschränken.

Hintergrund von MIPv6 [1]

Mobile IPv6 (MIPv6) ist ein Nachfolger von Mobile IPv4 (MIPv4) und wurde im Jahr 2004 von der Internet Engineering Task Force (IETF) spezifiziert, um die Mobilität von IPv6-Geräten zu unterstützen. Im Gegensatz zu MIPv4, das auf optionaler Route-Optimierung und Reverse Tunneling basiert, ist MIPv6 darauf ausgelegt, die Mobilität auf eine transparentere und effizientere Weise zu bewältigen, die eine nahtlose Weiterleitung von Verbindungen zwischen verschiedenen Netzwerken ermöglicht. Mobile IPv6 ist in RFC 6275 „Mobility Support in IPv6" definiert .

Funktionen und Komponenten von MIPv6 [1][2]

Im Vergleich zu MIPv4 werden im MIPv6 mehrere neue Komponenten, einschließlich der Home Agents (HAs), der Correspondent Nodes (CNs), der Mobile Nodes (MNs) und einige der anderen Komponenten, die im letzten Abschnitt vorgestellt wurden, definiert, die alle spezifischen Rollen im Protokoll spielen. Zudem werden im MIPv6 einige neue Komponenten und Verfahren eingeführt, die nun erläutert werden sollen.

- Da MIPv6 einige Optionen wie MIPv6-RO als seine fundamentalen Funktionen anbietet, gibt es keinen Bedarf für einen Foreign Agent in MIPv6. Stattdessen führt MIPv6 neue Destination-Optionen in das IPv6-Protokoll ein, um einige Aufgaben des FA zu übernehmen. Die neuen Optionen sind Binding Update, Binding Acknowledgement, Binding Request und Home Address Option (wird als Source Address in Binding Messages verwendet - Source Routing).
- Mobility Agents (MAs): MAs sind Router, die Mobilitätsmanagement-Funktionen in einem Netzwerk bereitstellen und zwischen Home Agents (HAs) und Mobile Nodes (MNs) vermitteln. Es gibt zwei Arten von MAs: **Local Mobility Anchors (LMAs)** und **Mobile Access Gateways (MAGs)**. LMAs bilden den zentralen Punkt für Mobilitätsmanagement-Operationen (Network-Based Mobility Management -NBMM) in einem Netzwerk und verwalten die Zustellung von Daten an MNs, während sich diese in fremden Netzwerken aufhalten. MAGs sind Router, die sich in Fremdnetzwerken befinden und die Verbindung zwischen MNs und LMAs aufrechterhalten.
- Binding Update List (BUL): Die BUL ist eine Liste, die die Zuordnung zwischen der IP-Adresse des MNs und seiner aktuellen Netzwerklokation enthält und regelmäßig von den MAs aktualisiert wird. Wenn ein MN seine Netzwerklokation ändert, informiert es die beteiligten MAs durch Senden von Binding Update (BU) Nachrichten. Die MAs aktualisieren daraufhin die BUL, um sicherzustellen, dass sie den Standort des MNs korrekt verfolgen.
- Binding Cache Entry: Ein Eintrag im Binding Cache, der den Standort des MNs und andere Parameter wie die Lebensdauer des Eintrags speichert. Wenn ein CN eine Datenübertragung an einen MN startet, überprüft es zunächst den Binding Cache, um die aktuelle

Netzwerklokation des MNs zu finden. Wenn ein Eintrag im Binding Cache vorhanden ist, leitet der CN die Daten direkt an die aktuelle Netzwerkadresse des MNs weiter.

- IPv6 Neighbor Discovery for Mobile IPv6: Eine Erweiterung des Neighbor Discovery Protokolls (NDP), das MAs und MNs bei der dynamischen Konfiguration von Routen und Adressen unterstützt, während das Gerät sich zwischen verschiedenen Netzwerken bewegt. ND-MIPv6 bietet zusätzliche Nachrichten und Optionen, um MNs zu unterstützen, die eine neue IP-Adresse erhalten, eine vorhandene IP-Adresse beibehalten oder den Standort ändern. ND-MIPv6 bietet auch Unterstützung für Route Optimization und das Senden von BU-Nachrichten an Mas.

Betrieb von MIPv6 [6]

MIPv6 setzt auf dem IPv6-Protokoll auf, um die Mobilität von Hosts in einem Netzwerk zu ermöglichen. Es ergänzt den IPv6-Header um zusätzliche optionaler Felder, um Informationen zur Mobilität zu transportieren.
Zum Beispiel kann MIPv6 eine zusätzliche Mobility Header-Information in den IPv6-Header einfügen, die die aktuellen Standort- oder Bewegungsinformationen eines mobilen Hosts enthält. Auch kann es eine Binding Update Nachricht senden, um seinen neuen Standort an den Home Agent und andere Netzwerkknoten zu melden.

Das MIPv6-Mobility Header (MH) ist durch einen Next Header-Wert von 135 im "immediately preceding"-Header gekennzeichnet und hat das folgende Format:

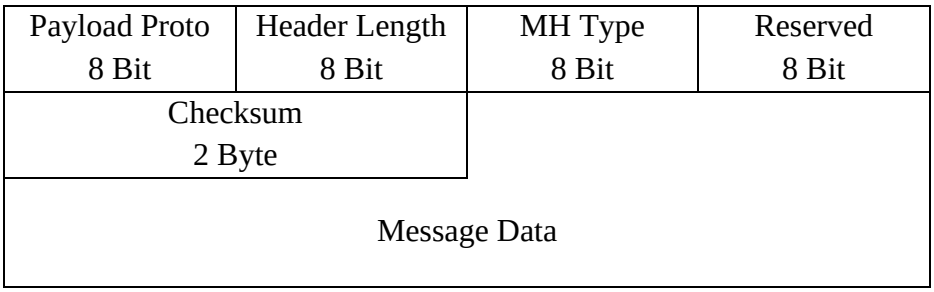

Figure 5.Mobilitäts-Header gemäß RFC 3775[6]

Payload Proto (8 Bit): Gibt den Typ des Headers an, der unmittelbar dem Mobility Header folgt.

Es verwendet die gleichen Werte wie das IPv6 Next Header Feld.

Länge (: gibt die Länge des Mobility Header in 8-Byte-Blöcken an.

MH Typ : gibt den Typ des Mobility Header an.

Reserved: Für zukünftige Verwendung reserviert.

Checksum: Eine optionale Prüfsumme zur Überprüfung der Integrität des Mobility-Headers.

Ein mobiler Knoten (MN) verbindet sich über das Access-Netzwerk (z. B. Wi-Fi) mit dem Internet und erhält vom Router des Access-Netzwerks eine temporäre IP-Adresse, die von einem lokalen Netzwerk zugewiesen wird. Der MN hat in der Regel eine primäre IP-Adresse (Home Address),

die von seinem Home Network Prefix (HNP) abgeleitet wird. Wenn der MN in ein anderes Netzwerk wechselt, erhält er eine sekundäre IP-Adresse (CoA), die von dem Netzwerkpräfix des aktuellen Netzwerks abgeleitet wird. Der MN nutzt die primäre IP-Adresse, um mit seinem Heimatnetzwerk und HA zu kommunizieren, während die sekundäre IP-Adresse verwendet wird, um mit dem aktuellen Netzwerk und dem LMA zu kommunizieren.
Wenn sich der MN nochmal in ein anderes Netzwerk bewegt, wird er eine neue IP-Adresse (aktuelle CoA) von einem anderen Router erhalten. Um die Verbindung aufrechtzuerhalten, nutzt MIPv6 ein Binding Update-Verfahren, bei dem der MN seinen neuen Standort dem HA meldet, der die Home Address des MN verwaltet. Der HA erstellt daraufhin einen Binding-Cache-Eintrag (Binding Update List, MIPv6-BUL), der die neue Care-of-Address (CoA) des MN enthält. Der Binding-Cache-Eintrag wird auch an den Correspondent Node (CN) gesendet, mit dem der MN kommuniziert. Der CN nutzt dann den Eintrag, um direkt an die neue CoA des MN zu senden. Wenn der MN einen anderen Standortwechsel durchführt, wird er erneut einen Binding Update senden und einen neuen Eintrag im Binding Cache erstellen.
Das MIPv6-Protokoll verwendet auch Mobility Agents (MA), darunter den Home Agent (HA) und den Local Mobility Anchor (LMA). Der HA fungiert als Gateway zwischen dem Heimatnetzwerk und dem aktuellen Netzwerk und leitet den Datenverkehr zwischen ihnen weiter. Der LMA dient als Ankerpunkt für den mobilen Knoten, um sicherzustellen, dass er erreichbar bleibt, wenn er in ein anderes Netzwerk wechselt.
Der Mobility Agent (wie HA) spielt eine wichtige Rolle bei der Verwaltung der Bewegung von MNs im Netzwerk. Seine Aufgaben umfassen die Registrierung und Verwaltung von MNs, die Überwachung ihrer Bewegung und die Aktualisierung von Routingtabellen, um sicherzustellen, dass der Datenverkehr an den richtigen Ort geleitet wird. Der MA ist auch für die Umleitung von Datenverkehr an Mobile Nodes, die ihre Position geändert haben, verantwortlich. Sie spielt eine bedeutende Rolle bei der Beibehaltung der Konnektivität mobiler Knoten und der Optimierung der Netzleistung in mobilen Umgebungen.

Sicherheit in MIPv6 [4][13][14]

Mobile IPv6 (MIPv6) ist so konzipiert, dass es in einer sicheren Art und Weise funktioniert, indem es Schutz gegen unbefugten Zugriff, "Paket Interception" und andere Sicherheitsgefährdungen bietet.
Das GWS (Generic Warning Service) ist ein Sicherheitsprotokoll in MIPv6, das verwendet wird, um verschiedene Arten von Bedrohungen zu erkennen und darauf zu reagieren. Es basiert auf dem PMIPv6-Protokoll (Proxy Mobile IPv6), das eine Netzwerkarchitektur verwendet, in der mobile Knoten ihre Kommunikation über einen oder mehrere Mobility Service Provider (MSPs) leiten, die als Proxies fungieren und die Verbindung zum Heimnetzwerk des mobilen Knotens aufrechterhalten.
Besonders im Vergleich zu MIPv4 und allen Sicherheitsproblemen, mit denen es konfrontiert war, wird die MIPv6-Security als ein großer Schritt in Richtung sicherer Verbindungen angesehen.
Hier sind einige wichtige Sicherheitsmechanismen und -protokolle, die in MIPv6 verwendet werden:

- **IPsec**
  MIPv4 und MIPv6 beide verlassen sich auf Internet Protocol Security (IPsec), um eine sichere Kommunikation zwischen dem mobilen Knoten und dem Korrespondenzknoten zu gewährleisten. IPsec bietet Datenintegrität, Vertraulichkeit und Authentifizierung (CIA-Triad). MIPv6 enthält integrierte Unterstützung für IPsec und verwendet es als obligatorischen Teil seiner Sicherheitsmechanismen, während MIPv4 nicht über eine solche integrierte Unterstützung verfügt und möglicherweise eine zusätzliche Konfiguration erfordert, damit IPsec verwendet werden kann.

- **Cryptographically Generated Addresses (CGA)**
  CGAs werden verwendet, um die IPv6-Adressen von mobilen Knoten zu sichern. CGA ist eine Technik, die es einem Knoten ermöglicht, eine eindeutige IPv6-Adresse mithilfe eines öffentlichen Schlüssels zu erstellen.
  CGA ist ein Bestandteil des „Enhanced Route Optimization“ in Mobile IPv6.

- **Return Routability (RR):**
  Return Routability ist ein Prozess, der zur Authentifizierung der vom mobilen Knoten gesendeten Binding Update Message verwendet wird. Dieser Prozess beinhaltet den Austausch einer Reihe von Nachrichten zwischen dem mobilen Knoten und seinem Home Agent, die dazu helfen, die Authentizität des mobilen Knotens festzustellen. RR gibt dem CN die Möglichkeit, zu überprüfen, ob der mobile Knoten tatsächlich über seine CoA und seine Home Address verfügbar ist. Auf diese Weise wird sichergestellt, dass der mobile Knoten wirklich beide IP-Adressen besitzt und somit die Aktualisierung der Bindung legitim ist.
  Erst wenn dies bestätigt ist, akzeptiert der CN die Binding Updates des MN und sendet ab diesem Zeitpunkt weitere Daten direkt an die CoA des MN.

  Diese vier Nachrichten werden verwendet, um das Verfahren der Return Routability vom mobilen Knoten zu einem Correspondent node durchzuführen.

. Die **Binding Update (BU)** informiert den CN oder den FA über den neuen Standort des mobilen Knotens.
. Die **Binding Acknowledgement(BA)** wird vom CN oder FA als Antwort auf die Aktualisierung der Bindung gesendet. Sie enthält die Heimatadresse des mobilen Knotens und einen Statuscode. Außerdem enthält sie eine Identifikationsnummer, falls eine solche in der entsprechenden BU enthalten war.
. Der **Binding Request (BR)** wird vom CN an den HA gesendet, um ein Binding Update (BU) anzufordern. Sie enthält die Heimatadresse des angefragten mobilen Knotens und eventuell eine Identifikationsnummer.
. Das **Binding Warning (BW)** wird vom vorherigen Foreign Agent als Antwort auf den Empfang eines getunnelten Datagramms für einen mobilen Knoten gesendet, für den er eine Bindung hat und für den er nicht als aktueller Foreign Agent tätig ist. Die Bindungswarnung wird an den HA gesendet. Sie enthält die Heimatadresse des MN und die Adresse des CN, der nicht über aktuelle Informationen über die aktuelle Care-of-Adresse des mobilen Knotens informiert ist . Mit diesen Informationen kann der HA eine BU an den CN senden.

- **Authentication Header (AH) und Encapsulating Security Payload (ESP)**
  AH, und ESP sind zwei IPsec-Sicherheitsprotokolle, die verwendet werden, um Datenintegrität, Vertraulichkeit und Authentifizierung (the CIA Triad) für IP-Pakete bereitzustellen.

- **MIPv6- Threat Analysis**
  Die MIPv6-Bedrohungsanalyse ist ein Prozess, der zur Identifizierung potenzieller Sicherheitsbedrohungen für das MIPv6-Netzwerk verwendet wird. Dieser Prozess beinhaltet die Identifizierung von Schwachstellen im MIPv6-Netzwerk und die Entwicklung von Sicherheitsmechanismen zur Minderung dieser Schwachstellen.

- **MIPv6- Security Association**
  Ein Sicherheit Assoziation ist eine Gruppe von Sicherheitsparametern, die zur Sicherung der Kommunikation zwischen dem mobilen Knoten und dem Korrespondenzknoten verwendet werden. Der Sicherheit Assoziation enthält Informationen wie das verwendete Sicherheitsprotokoll, den Verschlüsselungsalgorithmus und den Sicherheitsschlüssel.

- **Mobile IPv6-Route-Optimierung [11]**
  Route Optimization ist eine integrierte Funktion von MIPv6, die den Kommunikationsweg zwischen MNs und Correspondent Nodes (CNs) optimiert, indem der Datenverkehr direkt zwischen den beiden Parteien geroutet wird, ohne dass die Daten durch den Heimagenten gesendet werden müssen.
  RO basiert auf dem Neighbor Discovery Protocol (NDP) von IPv6 und verwendet die sogenannte "Care-of-Address Destination Option" (COD) in den IPv6-Header.
  CODs ermöglichen es einem CN, den Standort eines MN direkt zu erfahren, ohne den Verkehr über einen HA leiten zu müssen. CNs besitzen "Binding Caches", die die aktuell gültigen Bindungen enthalten, die dem Knoten bekannt sind. Jedes Mal, wenn ein CN ein Datagramm senden will, prüft er zunächst, ob er eine Bindung für das Ziel hat. Ist die Bindung vorhanden, fügt der Knoten dem Datagramm einen Routing-Header mit einem einzelnen Routensegment hinzu, setzt die IPv6-Zieladresse auf die in der Bindung angegebene CoA und die ursprüngliche Destination Address auf das Routensegment im Routing-Header.
  Durch die Verwendung von Source-Routing und Binding-Caches kann der CN bei mobilem IPv6 direkt mit dem MN kommunizieren und so die zuvor beschriebene Anomalie des Triangle-Routings vermeiden.
  Dieser Mechanismus gewährleistet eine End-to-End-Sicherheit, indem sichergestellt wird, dass alle zwischen dem mobilen Knoten und seinem Korrespondenzknoten gesendeten Pakete mit IPsec verschlüsselt sind.

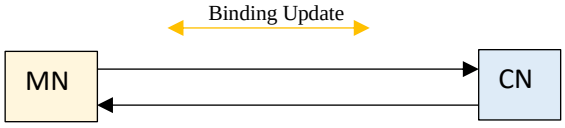

Figure 6.Mobile IPv6 Route Optimization

- **Enhanced Route Optimization (ERO)**
  ERO ist eine verbesserte Version der Route Optimization (RO)-Funktion in Mobile IPv6 (MIPv6). ERO nutzt die Sicherheitsfunktionen von CGA, um sicherzustellen, dass die vom mobilen Knoten verwendete CoA-Adresse tatsächlich von diesem Knoten generiert wurde und

nicht gefälscht ist. Durch die Verwendung von CGA kann ERO auch Angriffe auf das MIPv6-Netzwerk verhindern, die auf gefälschte CoA-Adressen abzielen. [3]

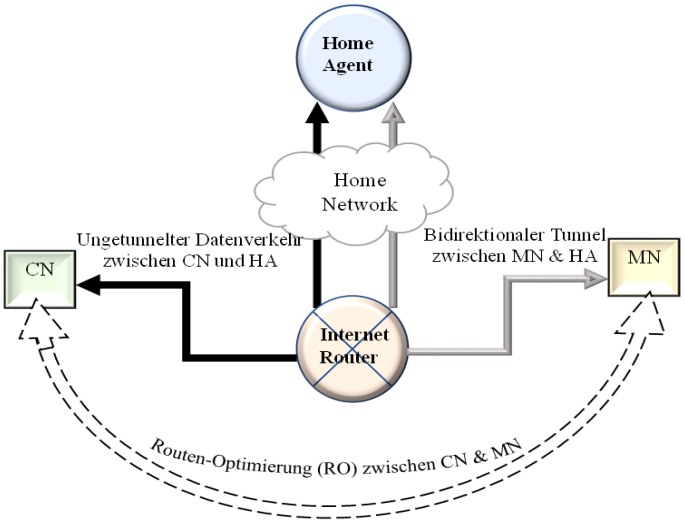

Figure 7. Bidirectional Tunneling vs. Route Optimization

Vor- und Nachteilen von MIPv6

Wenn über alle Vorteile von MIP gesprochen wird, gibt es viele, von denen einige bereits im Kapitel über MIPv4 erwähnt wurden. Dank neuer Protokolle und Dienstverbesserungen verfügt MIPv6 jedoch über eigene Vorteile. Die meisten von denen wurden bereits in den vorherigen Abschnitten erwähnt. Hier wird aber als Zusammenfassung ein kurzer Überblick über einige von ihnen gegeben.

- Direkte globale Adressierung: MIPv6 ermöglicht es mobilen Knoten, global eindeutige IP-Adressen zu haben, was bedeutet, dass sie von überall auf der Welt direkt angesprochen werden können. Dies ermöglicht eine effizientere Routenführung und beseitigt die Notwendigkeit komplexer Adressübersetzung.

- Verbesserte Routeneffizienz: MIPv6 verwendet ein hierarchisches Adressierungsschema, das eine effizientere Routenführung ermöglicht und die Anzahl der Routingtabelleneinträge reduziert, die auf Routern benötigt werden. Dies erleichtert das Weiterleiten von Paketen durch Router und verbessert die Netzwerkperformance.

- Flexible Adresskonfiguration: MIPv6 unterstützt mehrere Methoden der Adresskonfiguration, einschließlich Stateless Address Autoconfiguration (SLAAC) und Dynamic Host Configuration Protocol Version 6 (DHCPv6). Dies bietet mehr Flexibilität in der Netzwerkgestaltung und -verwaltung.

- Effizientes Handover: MIPv6 ermöglicht schnellere und effizientere Handover (wie Seamless Handover) zwischen verschiedenen Zugangspunkten. Dies wird durch die Verwendung von proaktiver Nachbarerkennung und Routenoptimierungstechniken erreicht.

[3] Mehr über MIPv6-Sicherheit im nächsten Abschnitt

- Sicherheit: MIPv6 enthält integrierte Sicherheitsfunktionen wie IPsec und Cryptographically Generated Addresses (CGAs), um vor unbefugtem Zugriff und anderen Sicherheitsbedrohungen zu schützen.

Obwohl MIPv6 ein signifikanter Fortschritt in der Drahtlostechnologie darstellt, sind immer noch einige Nachteile und Herausforderungen vorhanden, die in Zukunft gelöst werden können. Hier sind einige von denen:

- Handover-Latenz: Der Handover-Prozess kann einige Zeit in Anspruch nehmen, was zu einer vorübergehenden Unterbrechung der Kommunikation führen kann.
- Handover-Ausfall: In einigen Fällen kann der Handover-Prozess fehlschlagen, was zu einer Unterbrechung der Kommunikation führen kann.
- Komplexität: Die Implementierung von MIPv6 ist komplexer als die von IPv4 und erfordert zusätzliche Ressourcen, insbesondere in Bezug auf Sicherheitsaspekte.
- Overhead: MIPv6 führt zu zusätzlichem Overhead für das Netzwerk, einschließlich der Notwendigkeit für zusätzliche Nachrichtenübertragung und Verarbeitung, was die Netzwerkleistung und Effizienz beeinträchtigen kann.
- Sicherheit: MIPv6 birgt immer noch einige Sicherheitsherausforderungen, einschließlich des Potenzials für Man-in-the-Middle-Angriffe und andere Sicherheitslücken, da das Protokoll auf die Authentifizierung und Integrität von Signalisierungsnachrichten angewiesen ist.
- Interoperabilität: MIPv6 ist nicht rückwärtskompatibel mit MIPv4 und es kann Probleme mit der Interoperabilität zwischen verschiedenen MIPv6-Implementierungen geben, insbesondere zwischen Netzwerken mit unterschiedlichen Konfigurationen und unterschiedlichen Funktionen.
- Deployment: MIPv6 erfordert die Deployment neuer Netzwerkkomponenten und Infrastruktur, was teuer und zeitaufwändig sein kann, insbesondere für große Netzwerke.

Es sollte nicht vernachlässigt werden, dass MIPv6 trotz dieser Schwierigkeiten eine Reihe von Vorteilen hat, wie z. B. eine bessere Skalierbarkeit und Effizienz für die mobile Kommunikation über IPv6-Netze, die nicht übersehen werden dürfen. Die Nutzung von MIPv6 wird voraussichtlich steigen, wenn mehr Netzwerke und Geräte IPv6 übernehmen und die Lösungen für die genannten Herausforderungen weiterentwickelt werden.
Zwar gibt es bereits mehrere Lösungen für einige dieser Probleme (z. B. verschiedene Tunneling-Verfahren für die Verbindung zwischen IPv4 und IPv6, wie z. B. 6over4 und 4in6), jedoch arbeiten die Entwickler kontinuierlich daran, diese Lösungen weiterhin zu optimieren und MIPv6 noch effektiver zu gestalten.

Vergleich von Merkmalen und Komponenten

MIPv4 und MIPv6 sind zwei Protokolle, die in der mobilen Kommunikation verwendet werden. Obwohl sie ähnliche Ziele verfolgen, weisen sie signifikante Unterschiede in Bezug auf ihre Merkmale und Komponenten auf.
Wir können diese Unterschiede in folgende Kriterien einteilen:

- Skalierbarkeit
- Adressumsetzung
- Handover-Prozess
- Art der Konfiguration für jeden MN
- Unterstützung für QoS

MIPv4 hat aufgrund des begrenzten Adressraums von IPv4 (2^{32}-Adressen) eine begrenzte Skalierbarkeit. Es erfordert auch die Adressumsetzung (NAT), um mobilen Knoten eine Internetverbindung bereitzustellen. Im Gegensatz dazu bietet MIPv6 einen erweiterten Adressraum (2^{128}-Adressen), der Skalierbarkeit ermöglicht und die Notwendigkeit von Adressumsetzung verringert.
Der Handover-Prozess kann bei MIPv4 unzuverlässig sein und zu Verbindungsunterbrechungen führen, aber bei MIPv6 Handover ist effizienter und zuverlässiger.
MIPv4 ist auf eine manuelle Konfiguration für jeden mobilen Knoten angewiesen und bietet nur begrenzte Unterstützung für Quality-of-Service (QoS).
Im Gegensatz dazu, MIPv6 ermöglicht eine automatische Konfiguration, wodurch die Konfiguration von mobilen Knoten erleichtert wird, und bietet verbesserte Unterstützung für QoS. Noch dazu gibt es noch einige spezifische Komponenten von MIPv6, die in MIPv4 nicht vorhanden sind. Umfassen das Neighbor Discovery Protocol (NDP)[4] und die Route Optimization, die die Verzögerung bei der Übertragung von Paketen reduziert, indem unnötige Umwege vermieden werden.

Zusammenfassend bietet MIPv6 eine verbesserte Skalierbarkeit, effizientere Handover-Verfahren, automatische Konfiguration und verbesserte QoS-Unterstützung im Vergleich zu MIPv4.

[4] In Funktionen und Komponenten von MIPv6 erklärt.

Betrieb Vergleich

Der haupt betriebliche Unterschied zwischen MIPv4 und MIPv6 besteht in der Art und Weise, wie sie die Bewegung eines mobilen Knotens von einem Netz zu einem anderen unter Beibehaltung der Kontinuität der Kommunikation handhaben. Ein wichtiger und wesentlicher Trennungspunkt zwischen MIPv4 und MIPv6 sind die "Routing-Mechanismen". Sowohl MIPv4 als auch MIPv6 verwenden verschiedene Routen-optimierungsprotokolle, um die Effizienz und Leistung der mobilen Kommunikation zu verbessern. Wir haben in vorherigen Abschnitten bereits über die Arbeitsweise beide dieser Technologien gesprochen.

Um es zusammenzufassen, können wir kurz die Hauptunterschiede zwischen "MIPv4-Triangle Routing“, „Reverse Tunneling“ und "MIPv6-Route Optimization" erwähnen.

- Für MIPv4 gibt es keine offizielle Route-Optimierungsprotokolle, jedoch können die Techniken des "Triangle Routing" und des Reverse-Tunnelings verwendet werden, um die Route zu optimieren. Wie im Abschnitt MIPv4 erläutert, haben diese Protokolle jedoch ihre eigenen Einschränkungen.

-Triangle Routing in MIPv4 kann aufgrund des zusätzlichen Hop zum Home Agent zu längeren Paketverzögerungen und höherer Netzüberlastung führen.

-Reverse Tunneling in MIPv4 kann zu ineffizientem Routing und erhöhter Verzögerung aufgrund des Tunnelaufbaus und des Overheads für die Wartung führen.

-RO in MIPv4 ist eine optionale Funktion, die nicht unbedingt von allen Knoten im Netz unterstützt wird, und ihre Verwendung erfordert zusätzlichen Signalisierungs-Overhead, der die Latenzzeit und die Netzüberlastung erhöhen kann.

- Mobile IPv4 Foreign Agents bieten die Funktion eines lokalen Mobilitäts-Agenten (MA) für einen mobilen Knoten, der sich in ein fremdes Netz begeben hat. Für Mobile IPv6 ist aber kein lokaler Mobility Anchor erforderlich, daher gibt es keinen Foreign Agent in einem Mobile IPv6 Netzwerk und da es keinen fremden Agenten gibt, sind Routenoptimierung und Reverse-Tunneling-Optionen für Mobile IPv6 nicht erforderlich. Die Mobile IPv6-Routenoptimierungsfunktion ermöglicht dem Mobile IPv6-Protokoll die Koexistenz mit Ingress-Filter[5]-Geräten, die sich an Border-Gateways befinden.

- MIPv6 hingegen bietet ein spezielles Route-Optimierungsprotokoll namens "MIPv6-Route Optimization" (im letzten Abschnitt weiter erklärt), das unnötige Verzögerungen bei der Übertragung von Paketen vermeidet, indem es unnötige Umwege vermeidet. Route Optimization nutzt den Neighbor Discovery Protocol (NDP) von IPv6, um die optimale Route zu bestimmen und sicherzustellen, dass Daten direkt an das Ziel geleitet werden, ohne Umwege über den Home Agent. Als weitere Verbesserung wurde ERO von MIPv6 eingeführt, das kryptografische Techniken verwendet, um eine sichere und effiziente Kommunikation zwischen dem mobilen Knoten und dem entsprechenden Knoten zu ermöglichen, ohne dass ein Home Agent erforderlich ist, und das die Verzögerung und den Overhead im Zusammenhang mit dem Routenoptimierungsprozess reduziert, was zu einer besseren Leistung und Effizienz des gesamten Netzes führt.

[5] Ingress-Filter in MIP ist eine Sicherheitsmaßnahme, bei der der eingehende Datenverkehr anhand bestimmter Kriterien überprüft und unerwünschte Pakete verworfen werden.

Es gibt jedoch auch alternative Route-Optimierungsprotokolle, die von MIPv6 verwendet werden können, wie beispielsweise "Hierarchical Mobile IPv6" (HMIPv6) und "Fast Handovers for Mobile IPv6" (FMIPv6). HMIPv6 nutzt eine hierarchische Struktur, um die Routing-Entscheidungen zu optimieren und die Verzögerung bei der Übertragung von Paketen zu reduzieren. FMIPv6 hingegen nutzt eine schnelle Handover-Technik, um den Verlust von Daten während eines Handover-Prozesses zu minimieren.

Vergleich der Sicherheit

Mobile IPv6 und Mobile IPv4 haben unterschiedliche Sicherheitsmerkmale und Protokolle, die sie unterstützen. Einige der Sicherheitsprotokolle, die in beiden Versionen von Mobile IP verwendet werden können, sind IPsec (Internet Protocol Security), IKEv2 (Internet Key Exchange Version 2) und AAA (Authentication, Authorization, and Accounting) Protokolle.
Mobile IPv6 bietet jedoch zusätzliche Sicherheitsfunktionen wie die Unterstützung von Cryptographically Generated Addresses (CGA) und Return Routability (RR) für die Bindungsaktualisierung. MIPv6 verwendet auch die Secure Neighbor Discovery (SEND)-Protokolle für die Adressauflösung und Authentifizierung von Nachbarn.
Im Gegensatz dazu bietet MIPv4 keine spezifischen Sicherheitsfunktionen und es müssen zusätzliche Protokolle wie IPsec implementiert werden, um die Sicherheit zu gewährleisten.

zusammengefasst, lassen sich die Unterschiede zwischen den Sicherheitsaspekten von MIPv4 und MIPv6 durch die Verwendung von Protokollen in folgende Kategorien einteilen:

-Authentifizierung (Authentication)
-Verschlüsselung (Encryption)
-Routenoptimierung (Route Optimization)

- Authentifizierung:

MIPv4 verwendet keine integrierte Authentifizierung, was bedeutet, dass es anfällig für Angriffe durch gefälschte oder modifizierte Nachrichten ist (bspw. Man-in-the-Middle Attack). In MIPv6 wird hingegen das IPsec-Protokoll als integrierte Protokoll verwendet, das eine starke Authentifizierung und Integritätssicherung bietet.

- Verschlüsselung:

In MIPv4 ist die Verschlüsselung optional und nicht standardmäßig aktiviert, was bedeutet, dass die Daten, die über die Netzwerke übertragen werden, anfällig für „Interception Attacks“ sind. In MIPv6 ist die Verschlüsselung standardmäßig aktiviert(RRP, IKEv2usw.), was bedeutet, dass die Daten, die über das Netzwerk übertragen werden, verschlüsselt und dadurch sicherer sind.

- Routing-Optimierung:

Wie oben erklärt, MIPv4 verwendet Reverse-Tunnelings und Triangle-Routings als optionale RO Techniken. Aber leider bieten diese Techniken keine zusätzliche Sicherheit.

MIPv6 hingegen verwendet standardisierte Route-Optimierungsprotokolle wie den Binding Update (BU) und den Binding Acknowledgement (BA), um eine direkte und sichere Route zwischen dem mobilen Knoten und dem korrespondierenden Knoten zu etablieren.

In einer Übersicht können wir die Hauptunterschiede von MIPv4 und MIPv4 wie folgt anschaulichen.

	Mobile IPv4	**Mobile IPv6**
Komponenten & Funktionen	MN, Home Agent, Foreign Link, Home Link	Das gleiche
	MN home Adresse	Globally Routable HA and Link Local Address
	Foreign Agent	Ein "einfacher" IPv6-Router auf der ausländischen Verbindung (Foreign Agent existiert nicht mehr)
	Collected Care of Address	
	CoA erhalten über Agent Discovery, DHCP oder manuell	CoA erhalten über SLAAC, DHCP or manuell
Security & Performance	Authentifizierte Registrierung über den Home Agent	Authentifizierte Benachrichtigung über HA und andere CNs
	Routing über Tunnelling ("Triangle" oder "Bidirectional")	Routing über Tunnelling und Source Routing
	Routenoptimierung als Ergänzung über eine separate Protokollspezifikation	Integrierte Unterstützung für die Routenoptimierung

Figure 8.MIPv4 VS MIPv6

Die Erfindung des Internet Protokolls (IP) in den 1970er Jahren war eine revolutionäre Idee, die die Schaffung des modernen Internets ermöglichte. Mobile IP (MIP) hingegen kann als Evolution des Internet Protokolls (IP) betrachtet werden, da es die Fähigkeiten von IP erweitert, um die Mobilität von Netzwerkknoten zu unterstützen.
Mobile IPv4 und Mobile IPv6 werden beide weit verwendet, aber die genaue Verwendung jedes Protokolls variiert je nach Region und Netzwerk.
In den letzten Jahren hat die Verwendung von IPv6 zugenommen, und viele Netze und Geräte haben auf die neuere Version des Internetprotokolls aktualisiert. Daher wird MIPv6 immer häufiger als Mittel zur Unterstützung mobiler Kommunikation über IPv6-Netze eingesetzt.
MIPv4 wird jedoch weiterhin in vielen Teilen der Welt weit verwendet, insbesondere in Regionen, in denen die Bereitstellung von IPv6 noch in den Anfängen ist.
Allgemein hängt die Verwendung von MIPv4 und MIPv6 von einer Reihe von Faktoren ab, wie die Verfügbarkeit von IPv6-Verbindungen, dem Vorhandensein von Mobilfunkbetreibern, die MIPv6 unterstützen, und dem in einer bestimmten Region verwendeten Gerätetyp. Es kann jedoch schwierig sein, die genaue Verwendung jedes Protokolls zu bestimmen, da verschiedene Netze und Geräte unterschiedliche Kombinationen von Mobile IP-Technologien verwenden können, um mobile Kommunikationen zu unterstützen.
Es gibt keine spezifischen Informationen darüber, wie weit MIPv6 in Deutschland verwendet wird. Allgemein gilt aber, dass MIPv6 in der Welt noch nicht so weit verbreitet ist wie MIPv4, aber es wird ständig weiter entwickelt und verwendet.
Mobile IP spielt eine wichtige Rolle in der Mobilität von Geräten und der Fähigkeit, die Konnektivität beim Wechsel zwischen Netzwerken aufrechtzuerhalten. Es wird in einer Vielzahl von Anwendungen wie Mobile Computing, VoIP und standortbasierten Diensten eingesetzt. Mit der zunehmenden Verwendung von mobilen Geräten und der wachsenden Nachfrage nach nahtloser Mobilität und Konnektivität bleibt MIP eine wichtige Technologie sowohl für Einzelpersonen als auch für Organisationen. Die neue Normalität in unserem Alltag ist die Verflechtung unseres Lebens mit IoT-Geräten und anderen Technologien, die ein umfangreiches Netz von Verbindungen herstellen.
Online zu bleiben bedeutet, erreichbar zu sein, und in unserer Welt mit all den neuen Normen, die entweder dank der unvorhersehbaren Geschwindigkeit der Technologieentwicklung oder aufgrund von Situationen wie Covid definiert werden, wird die Erreichbarkeit nicht mehr als persönliche Entscheidung angesehen. In unserer Gesellschaft ist die Erreichbarkeit eine der wichtigsten Pflichten, die wir als Mitglieder dieser Gesellschaft zu erfüllen haben!
Und das ist noch nicht alles. Tag für Tag steigt das Bedürfnis, von überall aus verbunden zu sein, und verlangt nach immer besseren Technologien, um uns in Verbindung zu halten!
Mobile IP ist eine dieser Schlüsseltechnologien. Seine Entwicklung wurde verlangt, und seine Weiterentwicklung von MIpv4 zu Mobile IPv6 war auch aufgrund all der wichtigen Bedürfnisse wie bessere, schnellere und sicherere Verbindungen notwendig. Wir verlangen immer noch nach mehr und entwickeln uns deshalb immer weiter.
Nach dem Erscheinen von Wifi-5 stellt sich für MIP-Protokolle die Frage, wie diese drahtlose Verbindung am besten genutzt werden kann. Oder wie wir MIP für IoT-Geräte nutzen können, um sowohl Konnektivität als auch Sicherheit für diese Geräte zu gewährleisten.

Hier konnten wir nur die Spitze des Eisbergs berühren. Es gibt noch viele weitere interessante Protokolle und Informationen über MIPv4 und MIPv6, über die wir nicht sprechen konnten.
Aber wenn man sich diese beiden Protokolle ansieht, kann man erkennen, dass etwas so Einfaches wie die Aufrechterhaltung der Internetverbindung während eines Telefonats dank all der komplizierten Protokolle und Funktionen im Hintergrund abläuft. und das alles in einem einzigen Augenblick!
Daraus wird deutlich, wie wichtig das Verständnis der Konzepte und Technologien im Zusammenhang mit MIP ist, insbesondere für Fachleute in der Technologiebranche. So können wir den Weg der Entwicklung sehen und lernen und vielleicht die nächsten Schritte auf diesem Weg unternehmen, um noch größere Verbesserungen zu erzielen.

KAPITEL VI : REFERENZEN

[1] Hagen, Silvia. IPV6: Grundlagen-Funktionalität-Integration. Sunny Edition CH-8124 Maur.

[2] Fichtner, Klaus; Hemmling, Daniel; et al. Netzwerke: IPv6-Internet Protocol Version 6. HERDT-Digitaldruck; Am Kümmerling 21-25, 55294 Bodenheim.

[3] Choi, Sunghyun; Associate Professor. Mobile IP. School of Electrical Engineering, Seoul National University.

[4] Jing, Li & Po, Zhang & Srinivas, Sampalli. (2008). Improved Security Mechanism for Mobile IPv6. International Journal of Network Security. 6.

[5] Nada, Fayza. (2007). Performance Analysis of Mobile IPv4 and Mobile IPv6.. Int. Arab J. Inf. Technol.. 4. 153-160.

[6] D. Johnson, et al. RFC 3775. Mobility Support in IPv6. Section 5 and Section 6. Network Working Group. https://www.rfc-editor.org/rfc/rfc3775#section-5

[7] C. Perkins, Ed. Wichorus Inc. RFC 5499. IP Mobility Support for IPv4, Revised. Section 2, 3 and 4. Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/rfc5944.html.

[8] C. Perkins, Ed. IP Mobility Support. Network Working Group. https://datatracker.ietf.org/doc/html/rfc2002#section-1.1

[9] Mobile Internet basics: Mobile IPv6 technology overview. https://tinyurl.com/mr2bhbhd

[10] IPv6 Mobility Overview. https://panenka.sk/ipv6-mobility-overview/

[11] Petander Henrik. Mobile IP Route Optimization. Department of Electrical and Communications Engineering. Helsinki University of Technology. https://tinyurl.com/yadccdxh

[12] Mobile IP. Binary Terms. https://binaryterms.com/mobile-ip.html.

[13] F. Gont, W. Liu. RFC 7123: Security Implications of IPv6 on IPv4 Networks. Intern Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/pdfrfc/rfc7123.txt.pdf

[14] J. Korhonon, Ed; et al. RFC 6618 : Mobile IPv6 Security Framework Using Transport Layer Security for Communication between the Mobile Node and Home Agent. Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/pdfrfc/rfc6618.txt.pdf.

[15] Perkins, Charles. (2003). Mobile IPv6 and Seamless Mobility. 16.

[16] Raj Jain, Professor of Computer Science and Engineering. Mobile IPv6. Washington University in Saint Loui

[17] C. Perkins, Ed. RFC2002: IP Mobility support. https://www.rfc-editor.org/rfc/rfc2002

[18] Sajedul Talukder, Md. Iftekharul Islam Sakib, et al. Attacks and Defenses in Mobile IP: Modeling with Stochastic Game Petri Net. International Conference on Current Trends in Computer, Electrical, Electronics and Communication (ICCTCEEC-2017).

[19] Professor Raj Jain. Mobile IPv4-part 1 and part2. https://www.youtube.com/watch?v=a9uRfSNXmgk https://www.youtube.com/watch?v=xU29yrTh0DY

[20] Professor Raj Jain. Mobile IPv6. https://www.youtube.com/watch?v=swWRM8NIhr4