Die Internet-Protokollwelt

6. MOBILITÄTSUNTERSTÜTZUNG IM INTERNET

Vielen Dank an Prof. Jochen Schiller (FU Berlin) für diese Folien und das dazugehörige Buch

196

Übersicht

197

Motivation für Mobile IP

Wegwahl
- gemäß IP-Zieladresse, Netzwerk-Präfix (z.B. 129.13.42) identifiziert physikalisches Subnetz
- Wechsel des Subnetzes → passender Wechsel der IP-Adresse (normales IP) oder spezieller Routing-Eintrag

Spezifische Routen zum Endgerät?
- Anpassen aller Routing-Einträge, damit Pakete umgeleitet werden
- Skalierungsproblem bei großer Anzahl mobiler Geräte und u.U. häufig wechselnden Aufenthaltsorten
- Sicherheitsprobleme

Wechseln der IP-Adresse?
- Wahl der passenden IP-Adresse je nach Aufenthaltsort
- Auffinden des Endsystems schwierig – langwierige DNS-Aktualisierung
- Abbruch von laufenden TCP-Verbindungen, Sicherheitsprobleme

Anforderungen an Mobile IP

[RFC 5944]

Transparenz
- mobile Endgeräte behalten ihre IP-Adresse
- Wiederaufnahme der Kommunikation nach Abtrennung möglich
- Anschlusspunkt an das Netz kann gewechselt werden

Kompatibilität
- Unterstützung der gleichen Rechnernetzanschluss-Protokolle wie IP
- keine Änderungen an bisherigen Rechnern und Routern
- mobile Endgeräte können mit festen kommunizieren

Sicherheit
- alle Registrierungsnachrichten müssen authentifiziert werden

Effizienz und Skalierbarkeit
- möglichst wenige zusätzliche Daten zum mobilen Endgerät (dieses ist ja evtl. über eine schmalbandige Funkstrecke angebunden)
- Internet-weite Unterstützung einer großen Anzahl mobiler Endgeräte

Terminologie

Mobile Node (MN)
- Knoten, der den Ort des Netzanschlusses wechseln kann, ohne seine IP-Adresse ändern zu müssen

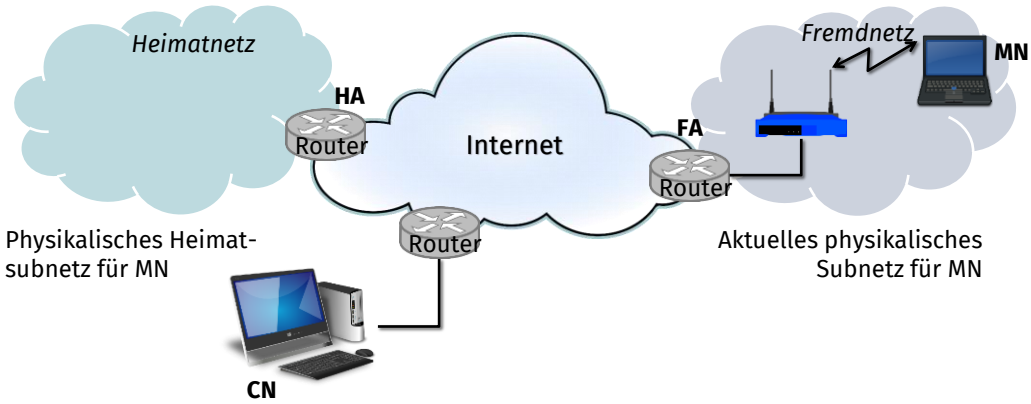
Home Agent (HA)
- Einheit im „Heimatnetz" des MN, typischerweise Router
- verwaltet Aufenthaltsort des MN, tunnelt IP-Datagramme zur COA

Foreign Agent (FA)
- Einheit im momentanen „Fremdnetz" des MN, typischerweise Router
- Weiterleiten der getunnelten Datagramme zum MN, default-Router für MN, stellt COA zur Verfügung

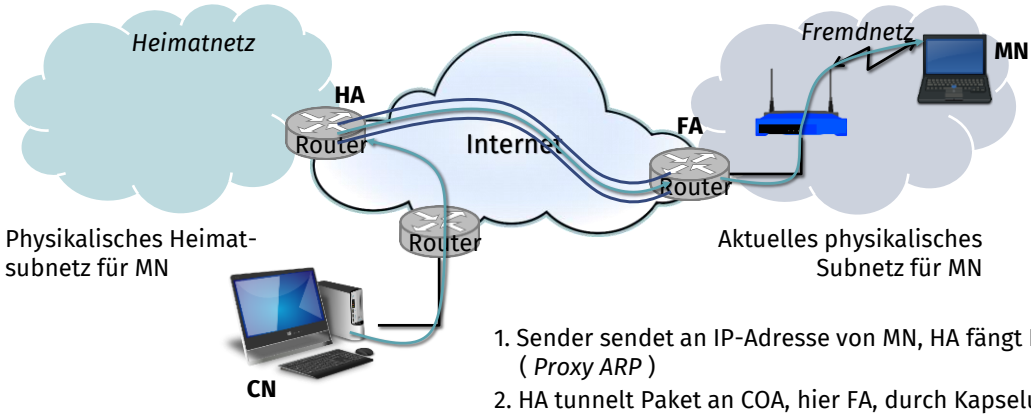
Care of Address (COA)
- Adresse des für den MN aktuell gültigen Tunnelendpunkts
- aktueller Aufenthaltsort des MN aus Sicht von IP
- kann z. B. via DHCP vergeben werden

Correspondent Node (CN)
- Kommunikationspartner

Beispielnetz

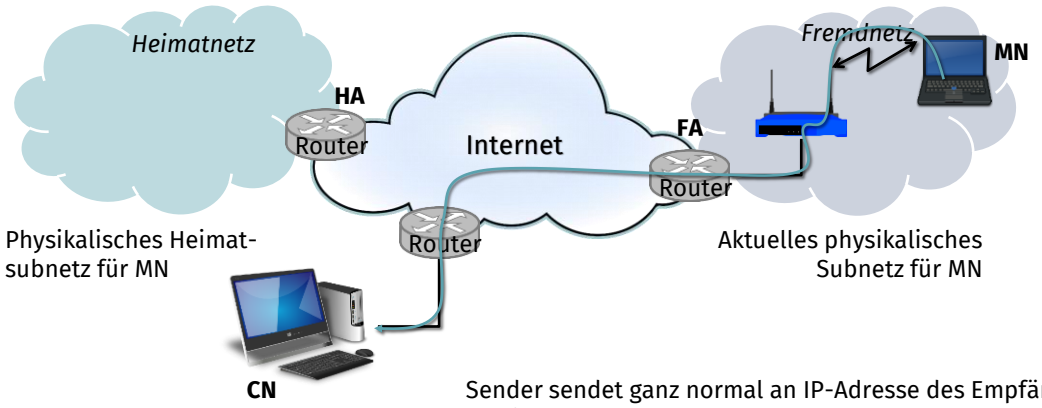


Datentransfer zum Mobilrechner



1. Sender sendet an IP-Adresse von MN, HA fängt Paket ab (*Proxy ARP*)
2. HA tunnelt Paket an COA, hier FA, durch Kapselung
3. FA leitet das Paket an MN weiter

Datentransfer vom Mobilrechner



Sender sendet ganz normal an IP-Adresse des Empfängers, FA dient als Standard-Router

Netzintegration

Agent Advertisement
- HA und FA senden periodisch spezielle Nachrichten über ihr Vorhandensein in die jeweiligen physikalischen Subnetze
- MN hört diese Nachrichten und erkennt, ob er sich im Heimat- oder einem Fremdnetz befindet
- MN kann eine COA aus den Nachrichten des FA ablesen

Registrierung (stets begrenzte Lebensdauer)
- MN meldet via FA seinem HA die COA, dieser bestätigt via FA an MN
- diese Aktionen sollten durch Authentifikation abgesichert werden

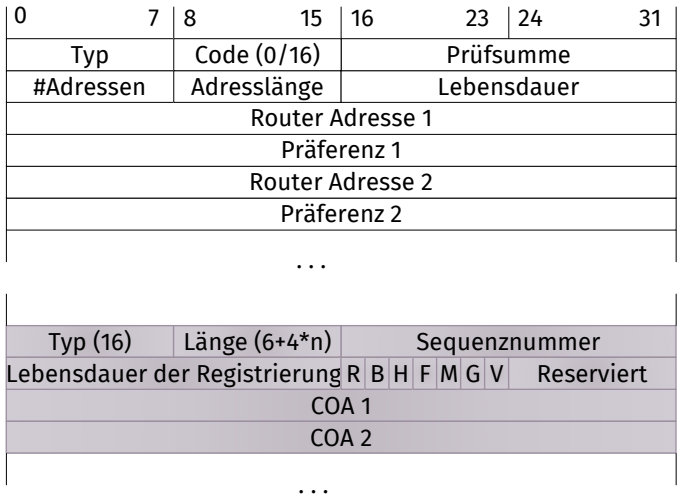
Bekanntmachung
- typischerweise macht nun der HA die IP-Adresse des MN bekannt, d. h. benachrichtigt andere Router, dass MN über ihn erreichbar ist
- Router setzen entsprechend ihre Einträge, diese bleiben relativ stabil, da HA nun für längere Zeit für MN zuständig ist
- Pakete an MN werden nun an HA gesendet, Änderungen an COA und FA haben darauf keinen Einfluss

204

Agent Advertisement

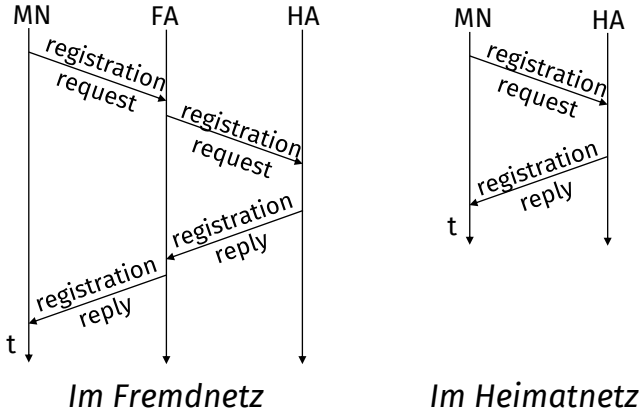
Erweiterung zum ICMP Router Discovery

(RFC 1256)



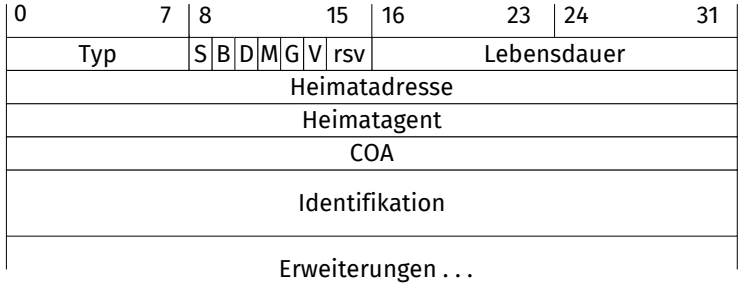
205

Registrierung



206

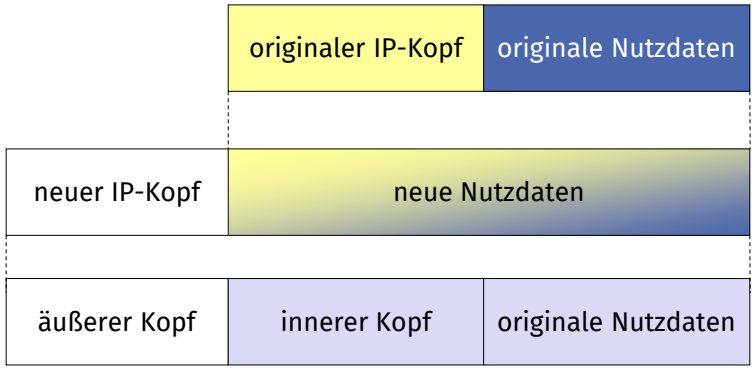
Mobile IP Registrierungs -anforderung



- Basiert auf UDP, Zielport 434
- S: Simultaneous Bindings
- B: Broadcast Datagrams
- D: Decapsulation by Mobile Node
- M: Minimal Encapsulation
- G: GRE Encapsulation
- V: Van Jacobson Header Compression
- Lebensdauer: Gültigkeit der Registrierung in Sekunden (0=Deregistrierung)

207

Kapselung



Kapselung I

Einkapseln eines Paketes in ein anderes als Nutzlast

- z. B. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
- hier z. B. IP-in-IP-Kapselung, minimale Kapselung oder *Generic Routing Encapsulation*, GRE (RFC 1701)

IP-in-IP-Kapselung (verpflichtend im Standard, RFC 2003)

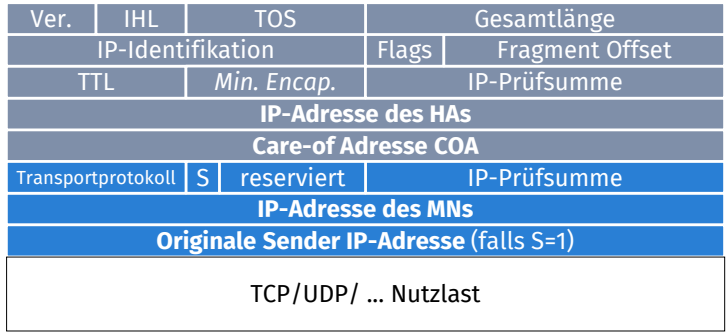
- Tunnel zwischen HA und COA

Ver.	IHL	TOS	Gesamtlänge
IP-Identifikation		Flags	Fragment Offset
TTL	*IP-in-IP*	IP-Prüfsumme	
IP-Adresse des HAs			
Care-of Adresse COA			
Ver.	IHL	TOS	Gesamtlänge
IP-Identifikation		Flags	Fragment Offset
TTL	Transportprotokoll	IP-Prüfsumme	
Originale Sender IP-Adresse des CNs			
IP-Adresse des MNs			
TCP/UDP/ ... Nutzlast			

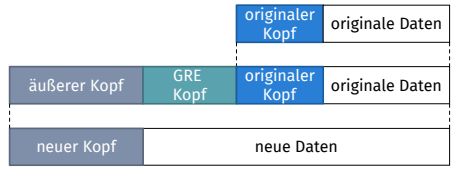
Kapselung II

Minimale Kapselung (optional)

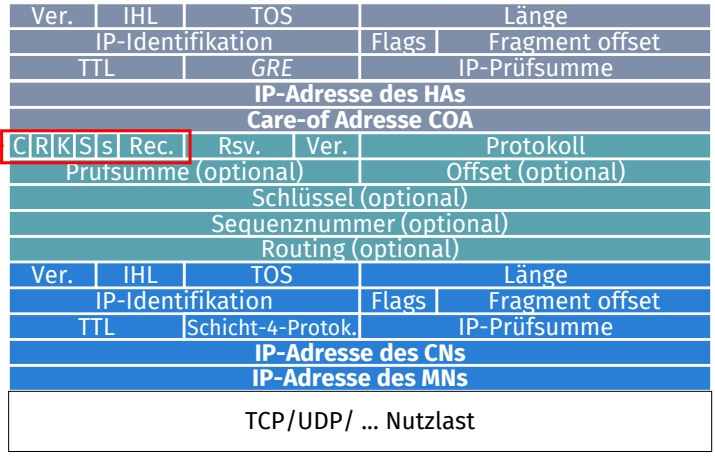
- vermeidet die Wiederholung gleicher Felder
- z.B. TTL, IHL, Version, TOS
- kann nur bei unfragmentierten Paketen eingesetzt werden, da nun kein Platz mehr für eine Fragmentkennung vorgesehen ist



Generic Routing Encapsulation (RFC 1701)



- Checksum Present
- Route Present
- Key Present
- Sequence Number Present
- Strict Source Routing
- Recursion Control



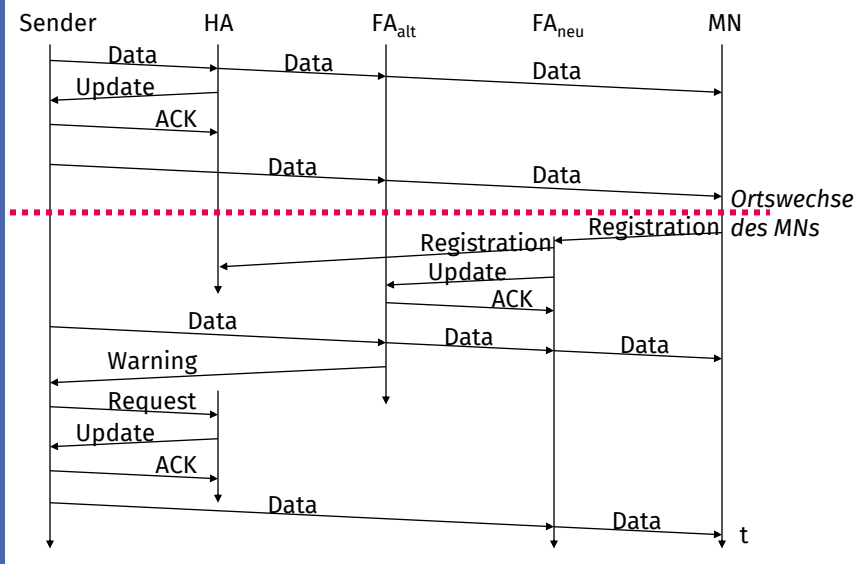
Optimierung des Datenpfades

Triangular Routing
- Sender sendet alle Pakete via HA zum MN
- unnötige Verzögerung und Netzlast

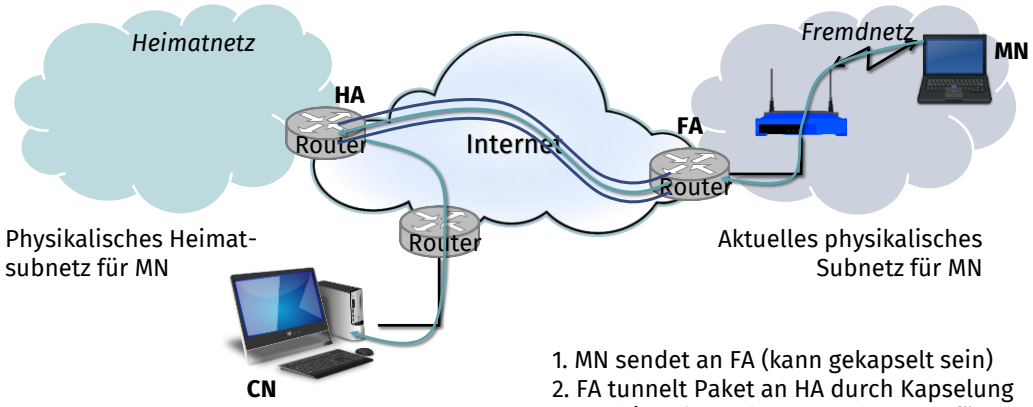
Lösungsansätze
- Lernen des aktuellen Aufenthaltsorts von MN durch einen Sender
- direktes Tunneln zu diesem Ort
- HA kann einen Sender über den Ort von MN benachrichtigen
- große Sicherheitsprobleme

Wechsel des FA
- Pakete „im Flug" während des Wechsels gehen verloren
- zur Vermeidung kann der neue FA den alten FA benachrichtigen, der alte FA kann nun die noch ankommenden Pakete an den neuen FA weiterleiten
- diese Benachrichtigung hilft evtl. dem alten FA auch, Ressourcen für den MN wieder freizugeben

Wechsel des Foreign Agent



Reverse Tunneling (RFC 3024)



1. MN sendet an FA (kann gekapselt sein)
2. FA tunnelt Paket an HA durch Kapselung
3. HA leitet das Paket normal an Empfänger weiter

Eigenschaften von Mobile IP mit Reverse Tunneling

Router akzeptieren oft nur „topologisch korrekte" Adressen
- ein durch den FA gekapseltes Paket des MN ist nun topologisch korrekt
- weiterhin Multicast und TTL-Problematik nun gelöst
  (TTL im Heimatnetz richtig, nun aber u.U. zu weit vom Ziel)

Reverse Tunneling löst nicht
- Problematik der Firewalls, hier könnte dann der umgekehrte Tunnel zur Umgehung der Schutzmechanismen missbraucht werden (*Tunnel Hijacking*)
- Optimierung der Wege, d. h. Pakete werden normalerweise über den Tunnel zum HA geleitet, falls Tunneln nicht ausgeschaltet ist (u.U. doppeltes Triangular-Routing)

Der neue Standard ist rückwärtskompatibel
- Erweiterungen können einfach integriert werden und kooperieren mit Implementierungen ohne die Erweiterung

Einige Probleme mit Mobile IP

Sicherheit
- Authentifikation mit FA problematisch, da u.U. nicht unter eigener Kontrolle (fremde Organisation)
- kein Protokoll für die Schlüsselverwaltung und -verteilung im Internet standardisiert
- Patent- und Exportproblematik

Firewalls
- verhindern typischerweise den Einsatz von Mobile IP, spezielle Konfigurationen sind nötig (z. B. Reverse Tunneling)

QoS
- häufige erneute Reservierungen im Fall von RSVP
- Tunneln verhindert das Erkennen eines gesondert zu behandelten Datenstroms

➔ *Sicherheit, Firewalls, QoS etc. sind aktueller Gegenstand vieler Arbeiten und Diskussionen!*

Sicherheit in Mobile IP

Sicherheitsanforderungen (*Security Architecture for the Internet Protocol*, RFC 4301)
- **Integrität** (*Integrity*)
  Daten können auf dem Weg vom Sender zum Empfänger nicht verändert werden, ohne dass der Empfänger es bemerkt
- **Authentizität** (*Authentication*)
  Absender = Sender und empfangene = gesendete Daten
- **Vertraulichkeit** (*Confidentiality*)
  Nur Sender und Empfänger können die Daten lesen
- **Nicht-Zurückweisbarkeit** (*Non-Repudiation*)
  Sender von Daten kann nicht abstreiten, diese gesendet zu haben
- **Verkehrsflussanalyse** (*Traffic Analysis*)
  Erstellung von Bewegungsprofilen sollte nicht möglich sein
- **Wiedereinspielsicherung** (*Replay Protection*)
  Abgefangene gültige Registrierung, die erneut gesendet wird, wird als ungültig erkannt

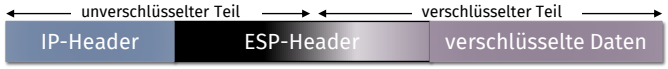
Sicherheitsarchitektur bei IP

Abstimmung der Sicherheitsmechanismen zwischen zwei oder mehreren kommunizierenden Partnern → Verwendung der gleichen Verfahren und Parameter (*Security Association*)

Zwei verschiedene Header für die Sicherung von IP-Nachrichten:

- *Authentication Header*
  - Sicherung der Integrität und der Authentizität von IP-Datagrammen
  - Nicht-Zurückweisbarkeit bei Verwendung von asymmetrischen Verschlüsselungsverfahren

- *Encapsulation Security Payload*
  - Schützt die Vertraulichkeit zwischen zwei Kommunikationspartnern

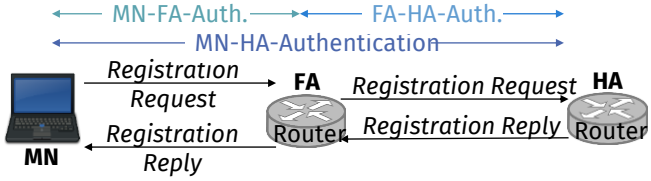


Sicherheitsarchitektur bei Mobile IP

„*Mobile Security Association*" für die Sicherung von Registrierungen für die Vereinbarungen zwischen dem mobilen Knoten, dem Home Agent und dem Foreign Agent

Erweiterungen der IP-Sicherheitsarchitektur

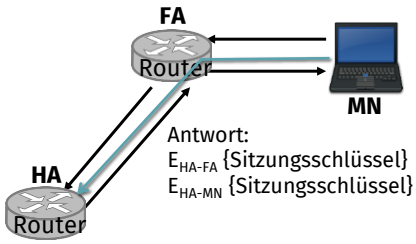
- Authentication-Erweiterung der Registrierung



- Verhindern des wiederholten Rücksendens von Registrierungen
  - Zeitstempel: 32 bit Zeitstempel + 32 bit Zufallszahl
  - Einmalwerte („*nonces*"): 32 bit Zufallszahl (MN) + 32 bit Zufallszahl (HA)

Schlüsselvergabe durch den Home Agent

Home Agent als „Schlüsselverteilzentrale”



- Foreign Agent ←→ Home Agent: *Security Association*
  - Registrierung des mobilen Knotens mit dem Home Agent
  - Antwort des Home Agents mit neuem Sitzungsschlüssel für Foreign Agent und mobilen Knoten

Motivation für die Änderung von Transportprotokollen

Transportprotokolle bisher entworfen für
- Stationäre Endgeräte
- Festnetze

Forschungsschwerpunkte
- Leistungsfähigkeit
- Staukontrolle
- Effiziente Übertragungswiederholung

TCP-Staukontrolle
- Paketverluste in Festnetzen i. Allg. durch Überlast
- Verwerfen von Paketen in Routern, sobald Puffer voll
- Konzept von TCP:
  - indirekter Hinweis auf Stau durch ausbleibende Quittungen
  - Verschlimmerung der Stausituation durch Übertragungswiederholungen
  - Slow-Start Algorithmus

Motivation II

TCP Slow-Start Algorithmus

- Bestimmung eines Staufensters
- Start mit Fenstergröße gleich 1 Segment
- Exponentielles Wachstum des Fensters bis zu einem Schwellwert, danach lineares Wachstum
- Nach Ausbleiben einer Bestätigung
  - Halbierung des aktuellen Schwellwerts
  - Rücksetzen des Staufensters auf ein Segment

TCP Fast Retransmit/Fast Recovery

- Versendung einer kumulativen Bestätigung nur nach Empfang eines Pakets
- Empfang mehrerer Bestätigungen für das gleiche Paket → Lücke in den empfangenen Paketen
  - Erfolgreiche Übertragung aller Pakete bis zur Lücke
  - Erfolgreiche Übertragung weiterer Pakete nach der Lücke
- Kein Stau, sondern Verlust eines einzelnen Pakets
  - Kein Slow-Start
  - Wiederholung des verlorengegangenen Pakets
  - Weitersenden mit dem aktuellen Staufenster

Auswirkung der Mobilität auf TCP-Mechanismen

Für TCP: Paketverlust = Stau, aber

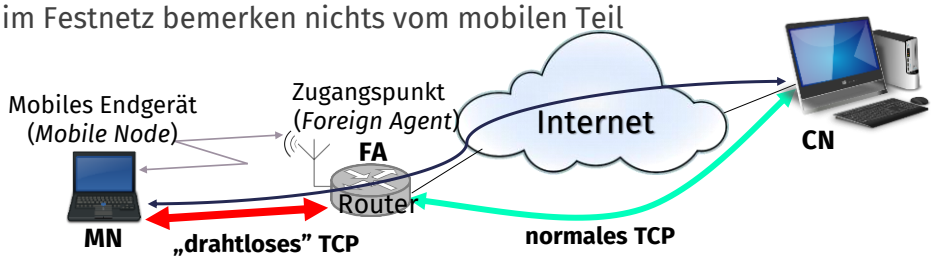
- in drahtlosen Netzen häufig Paketverluste durch Übertragungsfehler
- Paketverluste durch Mobilität der Knoten:
  Wechsel des MN von einem Zugangspunkt (FA) zu einem anderen, während Pakete noch zum ehemaligen Zugangspunkt unterwegs sind

→ Katastrophaler Einbruch der Leistung des unveränderten TCP

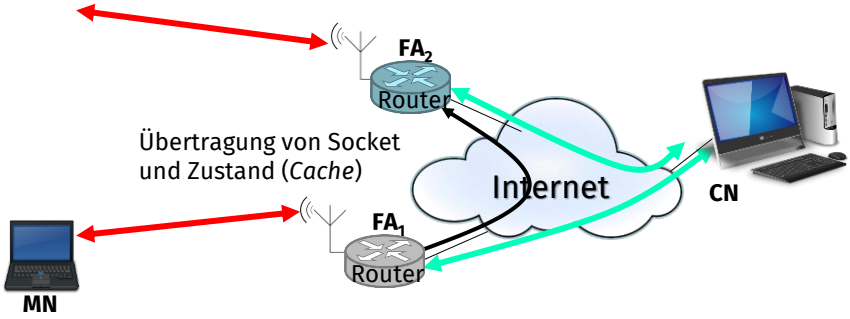
- Grundsätzliche Veränderung von TCP nicht möglich zur Wahrung der Interoperabilität mit Festnetzrechnern
- TCP-Mechanismen vorteilhaft im Festnetz des Internets

Indirektes TCP (I)

Indirektes TCP, I-TCP: Segmentierung der TCP-Verbindung
- keine Änderung am TCP-Protokoll für Rechner im Festnetz
- optimiertes TCP-Protokoll für mobiles Endgerät
- Auftrennung der TCP-Verbindung z. B. am Foreign Agent in zwei TCP-Verbindungen
- keine „echte" Ende-zu-Ende-Semantik mehr
- Rechner im Festnetz bemerken nichts vom mobilen Teil



I-TCP Zustandsübertragung



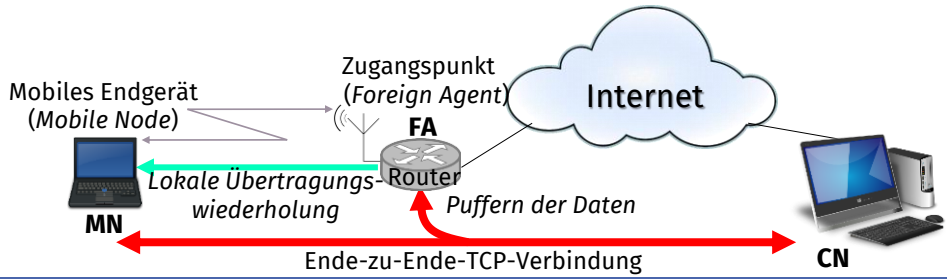
Indirektes TCP (II)

Vorteile
- keine Änderungen im Festnetzbereich, alle Optimierungsmaßnahmen helfen hier weiterhin
- Fehler auf der drahtlosen Strecke pflanzen sich nicht ins Festnetz fort
- relativ einfach beherrschbar, da mobile TCP-Varianten nur die kurze Strecke (ein „hop") zwischen Foreign Agent und mobilem Endgerät betreffen
- dadurch sehr schnelle Übertragungswiederholung, da Verzögerungszeit auf der drahtlosen Strecke bekannt

Nachteile
- Verlust der Ende-zu-Ende-Semantik: ACK an Sender heißt nun nicht mehr, dass der Empfänger wirklich die Daten erhalten hat
  - Was passiert, wenn der Foreign Agent abstürzt?
  - Konsistenz der Sichten?
- vergrößerte Latenzzeiten durch Pufferung der Daten im Foreign Agent und evtl. Übertragung an den neuen Foreign Agent

Snooping TCP I

„Transparente" Erweiterung von TCP im Foreign Agent
- Puffern der zum mobilen Endgerät gesendeten Daten
- bei Datenverlust auf der drahtlosen Strecke (beide Richtungen) direkte Übertragungswiederholung zwischen Foreign Agent und mobilem Endgerät („lokale" Übertragungswiederholung)
- dazu Abhören des Datenverkehrs und Erkennung von Bestätigungen in beide Richtungen (Filtern der ACKs)
- Änderung von TCP nur im Foreign Agent



Snooping TCP II

Datentransfer zum mobilen Endgerät
- FA puffert die Daten bis zum ACK des MN, erkennt Paketverluste durch duplizierte ACKs oder Time-out
- schnelle Übertragungswiederholung, unbemerkt vom Festnetz

Datentransfer vom mobilen Endgerät
- FA erkennt Paketverluste auf dem Weg vom MN anhand der Sequenznummern, sendet daraufhin NACK zum MN
- MN kann nun sehr schnell erneut übertragen

Integration der N2H-Schicht
- N2H-Schicht hat oft ähnliche Mechanismen wie TCP
- Erkennung von Paketduplikaten durch Übertragungswiederholungen bereits in der N2H-Schicht

Probleme
- Snooping TCP isoliert die drahtlose Verbindung nicht so gut
- je nach Verschlüsselungsverfahren ist Snooping nutzlos

Mobile TCP

Spezielle Handhabung längerer und/oder häufiger Unterbrechungen

Aufteilung der Verbindung ähnlich wie bei I-TCP:
- normales TCP im Festnetz bis zum *Supervisory Host*, SH
- optimiertes TCP zwischen SH und MN

Supervisory Host
- keine Pufferung der Daten, keine Übertragungswiederholung
- Überwachung aller Pakete, sobald eine Unterbrechung festgestellt wird:
  - setze Sendefenster auf 0
  - der Sender kann keine weiteren Pakete mehr senden
- der alte oder neue SH öffnet das Fenster wieder

Vorteile
- erhält Semantik
- unterstützt Unterbrechungen
- keine Zustandsübertragung notwendig bei Wechsel des Zugangspunktes

Nachteile
- Verluste auf der drahtlosen Strecke wirken sich auf das Festnetz aus
- verwendet spezielles TCP auf der drahtlosen Strecke

Fast Retransmit/Fast Recovery

Gefahr des Paketverlusts beim Wechseln des Foreign Agents
- TCP Slow-Start, obwohl kein Stau vorliegt

Lösung: Erzwingen des *Fast Retransmit*-Modus
- Bewusstes Versenden duplizierter Bestätigungspakete, sobald sich das mobile Endgerät bei einem neuen Foreign Agent registriert hat
- Wechsel des Kommunikationspartners im Festnetz in den *Fast Retransmit*-Modus
- Schnelles Senden des mobilen Endgeräts, sobald die Registrierung mit dem neuen Foreign Agent abgeschlossen ist

Vorteil
- einfache Änderungen für große Leistungssteigerung

Nachteile
- weitere Vermischung von IP und TCP
- Transparenz des Verfahrens problematisch

Transmission/Timeout Freezing

Lang anhaltende Abkopplung des mobilen Endgeräts
- keinerlei Datenaustausch möglich z. B. im Tunnel, Funkloch
- Abbrechen der TCP-Verbindung

Lösung: „Einfrieren" von TCP
- Erkennung eines bevorstehenden Verbindungsabbruches durch die N2H-Schicht
- Signalisierung an TCP über dieses bevorstehende Ereignis
- Einstellen des Sendens in TCP
- Kein Verdacht auf Stau
- erneute Signalisierung bei Wiederaufnahme des Kontakts

Vorteil
- Schema unabhängig von Verschlüsselung und Dateninhalten

Nachteil
- Anpassung von TCP und N2H-Schicht auf dem mobilen Endgerät

Selektive Übertragungswiederholung

TCP-Quittungen üblicherweise kumulativ
- ACK *n* bestätigt korrekten und reihefolgerichtigen Empfang bis Byte *n-1*
- Bei ausbleibender Quittung Wiederholung aller Bytes ab dem letzten unbestätigten Byte (*Go-back-N*)
- Bei einer Lücke im Datenstrom unnötige Wiederholung von Paketen

Lösung: selektive Übertragungswiederholung
- RFC 2018: Quittung aller empfangenen Pakete, nicht nur der reihefolgetreuen und lückenlosen

Vorteile
- weitaus effizienter
- wird schon häufig im Festnetz genutzt

Nachteile
- etwas komplexere Empfängersoftware
- mehr Speicher benötigt

Transaktionsorientiertes TCP

TCP-Phasen:
- Verbindungsaufbau, Datenübertragung, Verbindungsabbau
- Aufbau und Abbau gemäß 3-Wege-Handshake durch je 3 Pakete
- selbst für kurze Nachrichten mindestens 7 Pakete notwendig

Lösung: *Transaktionsorientiertes TCP*, T/TCP
- Nach RFC 1644
- Zusammenfassung von Verbindungsaufbau-, Daten- und Verbindungsabbaupaketen
- Übertragung kurzer Nachrichten inclusive Verbindungsmanagement in 2 oder 3 Paketen

Vorteil
- Effizienz

Nachteile
- geänderte TCP-Version
- Mobilität nicht mehr transparent
- RFC 1644 wurde im Mai 2011 als historisch deklariert

Vergleich der vorgestellten Verfahren

Siehe auch J. Schiller (2003)

Verfahren	Mechanismus	Vorteile	Nachteile
Indirektes TCP	Auftrennen in zwei TCP-Verbindungen	Isolation der drahtlosen Strecke, einfach	Verlust der Ende-zu-Ende-Semantik, erhöhte Latenz
Snooping TCP	Mithören von Daten und Quittungen, lokale Wiederholung	Transparent für Ende-zu-Ende, Integration von N2H-Schicht	Problematisch bei Verschlüsselung, schlechtere Isolation
M-TCP	Auftrennen in zwei TCP-Verbindungen, Drosseln des Senders über die Sendefenstergröße	Erhalt der Ende-zu-Ende-Semantik, kommt mit langen/ häufigen Unterbrechungen klar	Schlechte Isolation, höherer Berechnungsaufwand durch Bandbreitenmanagement
Fast Retransmit/ Fast Recovery	Vermeidung von Slow-Start nach Verbindungswechsel	Einfach, effizient	Vermischung der Schichten, nicht transparent
Transmission/ Timeout Freezing	Einfrieren des TCP-Zustands bei Unterbrechung	Unabhängig von Dateninhalten und Verschlüsselung	Geändertes TCP, N2H-abhängig
Selektive Übertragungswiederholung	Wiederholung nur der echt verlorengegangenen Daten	Sehr effizient	Etwas komplexere Empfängersoftware, mehr Speicher
Transaktionsorientiertes TCP	Zusammenfassung von Verbindungsauf-/ -abbau und Datenpaketen	Effizient	Geändertes TCP, nicht transparent

234

Literatur

GRAYSON, Mark; SHATZKAMER, Kevin; WAINNER, Scott (2009): *IP Design for Mobile Networks. Revolutionizing the Architecture and Implementation of Mobile Networks*. Indianapolis: Cisco Press.

GRAYSON, Mark; SHATZKAMER, Kevin; WIERENGA, Klaas (2011): *Building the Mobile Internet. Pervasive; Ubiquitous Computing Technologies and Protocols that are Shaping the Future of Our Mobile Experience*. Indianapolis: Cisco Press.

KAMEL, Sherif (2014): *Route Optimization in Mobile IP*. 1. Auflage. Saarbrücken: LAP LAMBERT Academic Publishing.

RAAB, Stefan; CHANDRA, Madhavi W. (2005): Mobile *IP Technology and Applications. Real-world Solutions for Mobile IP Configuration and Management*. Indianapolis: Cisco Press.

SCHILLER, Jochen (2003): *Mobilkommunikation*. 2., überarbeitete Auflage. München: Pearson-Studium (Pearson Studium Informatik).

235

Requests for Comments

Deering, Stephen E. (1991): *ICMP Router Discovery Messages*. Internet Engineering Task Force (IETF) (Request for Comments, 1256).

Braden, Robert (1994): *T/TCP -- TCP Extensions for Transactions Functional Specification*. Internet Engineering Task Force (IETF) (Request for Comments, 1644).

Hanks, Stan; Li, Tony; Farinacci, Dino; Traina, Paul (1994): *Generic Routing Encapsulation (GRE)*. Internet Engineering Task Force (IETF) (Request for Comments, 1701).

Perkins, Charles E. (1996): *IP Encapsulation within IP*. Internet Engineering Task Force (IETF) (Request for Comments, 2003).

Mathis, Matt; Mahdavi, Jamshid; Floyd, Sally; Romanow, Allyn (1996): *TCP Selective Acknowledgment Options*. Internet Engineering Task Force (IETF) (Request for Comments, 2018).

Glass, Steven M.; Hiller, Tom; Jacobs, Stuart; Perkins, Charles E. (2000): *Mobile IP Authentication, Authorization, and Accounting Requirements*. Internet Engineering Task Force (IETF) (Request for Comments, 2977).

Montenegro, Gabriel E. (2001): *Reverse Tunneling for Mobile IP, revised*. Internet Engineering Task Force (IETF) (Request for Comments, 3024).

Kent, Stephen; Seo, Karen (2005): *Security Architecture for the Internet Protocol*. Internet Engineering Task Force (IETF) (Request for Comments, 4301).

Perkins, Charles E. (2010): *IP Mobility Support for IPv4, Revised*. Internet Engineering Task Force (IETF) (Request for Comments, 5944).

Perkins, Charles E.; Johnson, David B.; Arkko, Jari (2011): *Mobility Support in IPv6*. Internet Engineering Task Force (IETF) (Request for Comments, 6275).

Zhu, Zhenkai; Wakikawa, Ryuji; Zhang, Lixia (2011): *A Survey of Mobility Support in the Internet*. Internet Engineering Task Force (IETF) (Request for Comments, 6301).