

Kapitel 2

Begriffserklärung

Um das Verständnis der folgenden Kapitel zu erleichtern, gebe ich einen kurzen Überblick über die in den kommenden Abschnitten verwendeten Fachbegriffe und Schlüsselworte. Sie werden von mir im weiteren Text als bekannt vorausgesetzt.

2.1 Client-Mobilität

Die Mobilität der Fahrzeuge (Clients) ist grundlegender Bestandteil der CarToX-Kommunikation. Bei der ursprünglichen Konzeption der heute am weitesten verbreiteten Transportprotokolle TCP und User Datagram Protocol (UDP) wurde ein statischer Verbindungspfad zwischen Client und Server angenommen. Diese Annahme ist in der heutigen Zeit von Smartphones, Laptops und besonders im Szenario der CarToX-Kommunikation überholt. Die Fahrzeuge bewegen sich von einem Netzzugangspunkt zum nächsten fort. Dabei sind die Zeiträume, in denen eine Verbindung besteht, aufgrund der sehr hohen Geschwindigkeiten äußerst kurz. Moderne Protokolle, die diesen Sachverhalt unterstützen wollen, müssen dafür entsprechende Mechanismen zur Verfügung stellen, um dem Client eine kontinuierliche Verbindung zum Server zu gewährleisten. Bei einer klassischen stationären Verbindungen erfolgt die dauerhafte Identifikation einer einzelnen Verbindung mittels der für sie momentan verwendeten IP-Adresse. Wegen der durch die Mobilität bedingten schnellen Verbindungswechsel ist dieser Ansatz nun nicht mehr praktikabel. Gebräuchliche Lösungen dieses Problems sind u.a. eine ständige „Buchführung“ über die aktuell vergebene IP-Adresse an die jeweiligen Clients oder eine weitere Abstraktions-Ebene zur Verbindungs-identifikation, die zusätzlich zur üblicherweise verwendeten IP-Adresse aufgebaut wird.

2.2 Doppelrolle der IP-Adresse im Mobilitätsszenario

Im heutigen Internet übernimmt die IP-Adresse für jede Verbindung eine Doppelrolle. Zum einen stellt die IP-Adresse eine für die jeweilige Verbindung eindeutige Identifikations-Kennung (eng. Identifier) dar. Zum anderen wird durch sie auch der momentane Standort der jeweiligen Netzknoten lokalisiert (eng. Locator). Bei einer statischen Verbindung ist diese Doppelnutzung generell möglich. Für das Szenario der Mobilität besteht jedoch ein entscheidendes Problem (eng. Locator-Identifier-Problem). Aufgrund der ständig wechselnden Positionen der mobilen Endgeräte ist es nicht mehr möglich beide Aspekte (wie dies z.B. bei Verwendung des Transmission Control Protocols der Fall ist) sinnvoll in der IP-Adresse zu vereinigen. Ein konkretes Beispiel hierfür ist der gleichzeitige Verbindungsaufbau eines modernen Smartphones über WLAN und sein Mobilfunkmodul zu einem Server. Das Gerät bekommt vom Server dafür zwei verschiedene IP-Adressen zugewiesen, für jedes Interface entsprechend eine. Für das Smartphone sind die beiden IP-Adressen lediglich Lokatoren. Der Server dagegen verwendet die IP-Adressen zur Identifikation. Er kann somit nicht feststellen, dass es sich bei beiden IP-Adressen um ein und den selben Client handelt. Neue Konzepte und Überlegungen zur klaren Trennung von Identifier und Lokatoren einer bestehenden Internetverbindung werden somit notwendig.

2.3 Multihoming

Bei der originären Konzeption des Internets und der angebundenen Computer / Netzknoten ist man von einem einzelnen kabelgebundenen Verbindungskanal ausgegangen, über den jeder Rechner angeschlossen sein sollte. Diese Annahme ist vollkommen veraltet. Moderne Endgeräte wie z.B. Laptops und Smartphones haben mehrere Möglichkeiten sich mit dem sie versorgenden Netzwerk und darüber ins World-Wide-Web zu verbinden. Dies kann z.B. ein UMTS-Funk-Modul und eine WLAN-Karte sein. Gleiches ist auch im Bereich CarToX möglich. Diesen neuen technische Sachverhalt nennt man Multihoming.

Darunter versteht man, dass ein Endknoten (z.B. das Auto oder ein Notebook) über mehrere Kanäle (WLAN und Mobilfunk) mit dem Netz gleichzeitig verbunden sein kann. Dies dient insbesondere der Ausfallsicherung. Wenn eine der beiden Verbindungen (z.B. im Auto-Szenario durch die Fahrt von A nach B) schwächer werden sollte und möglicherweise ganz ausfällt, ist man trotzdem in der Lage den Datenstrom noch auf dem zweiten zur Verfügung stehenden Datenkanal zu übertragen. Multihoming bietet darüber hinaus die Möglichkeit die

Ressourcen aller Kanäle gleichzeitig zu nutzen. Ein Host kann somit die zur Datenübertragung zur Verfügung stehende Bandbreite wesentlich steigern, falls er die zu übertragenden Daten in mehrere Datenströme aufteilt und diese dann über die verschiedenen Kanäle gleichzeitig überträgt.

2.4 Lastverteilung (Load-Sharing)

Unter dem Begriff Lastverteilung (eng. Load-Sharing) versteht man die konkrete Anwendung des Multihomings zur Optimierung der Datenübertragung. Upper-Layer-Protokolle nutzen dabei alle zur Verfügung stehenden Verbindungskanäle gleichzeitig für ihre Aufgaben. Dadurch wird es möglich z.B. ein Kostenprofil für jede Verbindungsmöglichkeit anzulegen. So z.B. kann günstiges WLAN einer teureren Mobilfunkverbindung vorgezogen werden, sofern es verfügbar ist. Aufgaben, die eine hohe Dringlichkeit aufweisen, können durch die Anwendung von Load-Sharing priorisiert übertragen werden. Andere mit einer geringeren Dringlichkeit können dafür von den Upper-Layer-Protokollen auf einen Kanal mit höherer Latenz umgeleitet werden, um die benötigten Kapazitäten frei zu geben. Die Lastverteilung ermöglicht somit eine ausgewogene und den dynamischen Anforderungen der Upper-Layer-Protokolle angepasste Nutzung der vorhandenen Verbindungskanäle.

2.5 make-before-break-Konzept

Das sog. make-before-break-Konzept ist insbesondere für zeitkritische Anwendungen wie z.B. VoIP im Bereich der mobilen Kommunikation von hoher Relevanz. Es soll sicherstellen, dass Datenpakete aufgrund eines Übergangs von einem derzeit verwendeten Verbindungskanal auf einen neuen Kanal (der sogenannte Handover-Vorgang) möglichst unterbrechungsfrei gesendet werden können. Das am weitesten verbreitete Internetprotokoll „Transmission Control Protocol“ ist dazu aber nicht in der Lage. Klassischerweise wird immer nur eine Verbindung zwischen den Parteien gehalten und zur Datenübertragung genutzt. Wenn nun der Wechsel erfolgt, muss zunächst die alte Verbindung abgebaut und danach eine neue Verbindung aufgebaut werden. In der Zwischenzeit ist die Datenverbindung eine gewisse Zeit unterbrochen. Diese Zeit wäre bei einer VoIP-Kommunikation sehr störend und ist daher im Bereich der mobilen Kommunikation unerwünscht. Beim make-before-break-Ansatz ist deshalb das jeweils verwendete Protokoll da-

zu in der Lage, bereits vor Abbruch der derzeit genutzten Datenverbindung einen neuen Datenkanal zur Gegenstelle aufzubauen. In der Übergangsphase bestehen somit mindestens zwei Verbindungen parallel zueinander. Eine Unterbrechung der Datenübertragung wird damit vermieden.

2.6 Ingress-Filter

Ingress-Filter dienen dazu die von ihnen überwachten Subnetze vor unerwünschtem oder unerlaubtem Datenverkehr zu bewahren. Der Filter selbst ist zu diesem Zweck meist auf den Routern im Netzwerk oder einer Firewall z.B. innerhalb eines Firmennetzes implementiert und verwirft Datenpakete mit ihm unbekannten oder fehlerhaften Absenderadressen. Dadurch wird vermieden, dass unbefugte Dritte aus dem Netz heraus Daten senden oder Angriffe auf das Netz vornehmen können.

2.7 Network Address Translation

Network Address Translation (NAT)[21] ist ein Oberbegriff für alle Verfahren, die eingesetzt werden, um automatisiert bestehende IP-Adressen von Paketen durch neue zu ersetzen. Die NAT-Mechanismen werden deshalb typischerweise in Routern (NAT-Routing) verwendet, um Subnetze mit unterschiedlichen Adressbereichen untereinander zu verbinden. So können z.B. Rechner eines Firmennetzwerkes, die intern alle eine individuelle IP-Adresse zugewiesen bekommen haben, über eine einzelne öffentliche IP-Adresse an das Internet angebunden sein. Über diese können dann alle gemeinsam mit anderen Hosts im Internet kommunizieren. NAT-Routing verbirgt die firmeninternen IP-Adressen und schafft so eine erhöhte Netzwerksicherheit.

2.8 Domain Name System

Das Domain Name System (DNS) wurde ursprünglich für das sogenannte „DARPA-Internet“ [37] der „Defense Advanced Research Projects Agency“ einer Behörde des US-Verteidigungsministeriums entwickelt. Der DNS Service dient im heutigen Internet zur Namensauflösung einer Domain (einer von Menschen lesbaren und intuitiven Kennung eines Rechners - z.B. google.de), um daraus die kon-

krete IP-Adresse des Netzknotens ermitteln zu können. Das Domain Name System bildet somit einen wichtigen Schwerpunkt im Konzept des World-Wide-Web, wie es die Menschen heute kennen und nutzen.

2.9 Dynamic Host Configuration Protocol

Das Dynamic Host Configuration Protocol (DHCP) [18] bindet einen Host ohne eine manuelle Konfiguration der Netzwerkschnittstelle in ein bestehendes Netzwerk ein. Das DHCP Protokoll verteilt hierfür selbständig die benötigten Einstellungsparameter, wie z.B. die IP-Adresse und den Namen des DNS Servers an die im Netz befindlichen Rechner. Die Hosts müssen hierfür als DHCP-Clients konfiguriert sein.

2.10 Host-, netzwerk- und proxybasierte Protokollansätze

Zur praktischen Umsetzung der Funktionalität von Protokollen gibt es verschiedenen Ansätze. Hostbasierte Protokolle integrieren ihre gesamte Funktionalität in die Endknoten des Netzwerks. Für die Einführung eines solchen Protokolls müssen es somit auch sämtliche Endgeräte im Netzwerk unterstützen. Bei sich bereits im Betrieb befindlichen Legacy-Systemen ist das oft schwer umzusetzen. Das nachträgliche Hinzufügen der benötigten Eigenschaften ist schwierig und mit hohen Kosten verbunden. Viele Endgeräte lassen sich auch einfach nicht mehr entsprechend anpassen. Sie können das Protokoll dann selbst nicht nutzen.

Netzwerkbasierte Ansätze lassen aus diesem Grund die Hosts unangetastet. Die Funktionalität des Protokolls wird bei ihnen in der Netzwerk-Infrastruktur, die die Hosts untereinander verbindet, umgesetzt. Die Hosts im Netzwerk müssen dadurch nicht angepasst werden. Das Problem wird auf die Anpassung der vermittelnden Entitäten (z.B.Router) verlagert.

Proxybasierte Protokolle verwenden zur Anbindung von Legacy-Systemen einen Proxy-Server. Hosts im Netz, die das neue Protokoll unterstützen, können über ihn mit Legacy-Systemen kommunizieren, die das Protokoll selbst nicht unterstützen. Der Proxy-Server schafft somit eine Schnittstelle, um alle Hosts im Netz über das neue Protokoll direkt ohne ihn zu nutzen oder indirekt durch ihn vermittelt miteinander kommunizieren zu lassen.

Nahtloser Handover in drahtlosen
Fahrzeug-Kommunikationsnetzen
Entwicklung eines Protokollentwurfs für den Einsatz in
bestehenden Netzwerken

Jomrich, F.

2016, XX, 133 S. 40 Abb., Softcover

ISBN: 978-3-658-13300-9