TECHNISCHE HOCHSCHULE DEGGENDORF

Spezielle Protokolle des IoT

Einführung und Grundlagen

Einleitung

Spezielle Protokolle des IoT

- Vermittlung einer ganzheitlichen Ansicht der Übertragung von Informationen im IoT
  - Drahtlose und drahtgebundene Übertragung
  - Übertragung über kurze und lange Distanzen
  - Effiziente Datenübertragung durch Kompression
  - Aufbau von Protokollen
  - Beispiele für Protokolle

Planung

Übersicht über die geplanten Veranstaltungen:

- Einführung, Characteristika von Protokollen, Frequenzbereiche
- Protokollstack ISO/OSI und Implementierung in TCP/IP
- Entwicklung eines eigenen Protokolls
- Informationstheoretische Grundlagen, Übertragungstechnik-Grundlagen
- Kommunikationsprotokolle des IoT: REST, MQTT und Basis HTTP/HTTPS + Proxy
- Wired Protokolle: Seriell, I2C, SPI, 1-Wire
- Wireless Protokolle im Nahbereich: Zigbee, Z-Wave, Bluetooth
- Wireless Protokolle im Fernfeld: SigFox, LoRaWan
- Routing Protokolle: Basis, Mesh

Protokolle

Aufgaben eines Protokolls im engeren Sinne sind:

- Definition des Übertragungsformats von Nutzdaten über einen Kanal
- Aufbau und/oder Überwachung der Verbindung zwischen Sender und Empfänger
- Verfahren zur Vermeidung der Monopolisierung des Kanals durch einen Beteiligten
- Fehlerkontrolle und ggf. Fehlerkorrektur
- Signalisierung von Seiteninformationen

Ein Protokoll im weiteren Sinn kann auch definieren:

- HF-Übertragung und Frequenzbereiche
- Energiebedarf der Übertragung
- ...

Charakteristika von Protokollen

Typische Charakteristika von Übertragungsprotokollen:

- Datenübertragungsrate
- Latenzzeit
- Reichweite
- Anzahl Teilnehmer
- Robustheit der Übertragung
- Datensicherheit

Charastika von Protokollen

Brainstorming (5 Minuten in Zweiergruppen):

- Erarbeiten Sie 2 möglichst unterschiedliche Übertragungsszenarien:
  Ideen: Fernsteuerung Tiefseetauchboot, Marsrover, Katastrophenhilferoboter;
  VR-Videokonferenz für Firmen; Brandmelder im Hochhaus oder im Wald;
  Notabschaltung in einem Elektronen-Synchrotron; olympischer Fackellauf
  - Welche Daten sollen übertragen werden?
  - Von wo nach wo?
  - Mit welcher Datenrate? Mit welcher Latenzzeit?
  - Wie sicher muss die Übertragung sein?
  - Wie viel darf der Aufbau kosten? Wie viel kostet die einzelne Übertragung?
  - Benötigen wir redundante Übertragung? Falls ja, wie?
  - Wie viel Energie darf verbraucht werden?
  - Welche Voraussetzungen müssen erfüllt werden? Sichtverbindung? Zwischenstationen? Stromversorgung? Automatisierung?
  - ...

Schichten

Eigenschaften und Vorteile des Schicht-Aufbaus von Protokollen

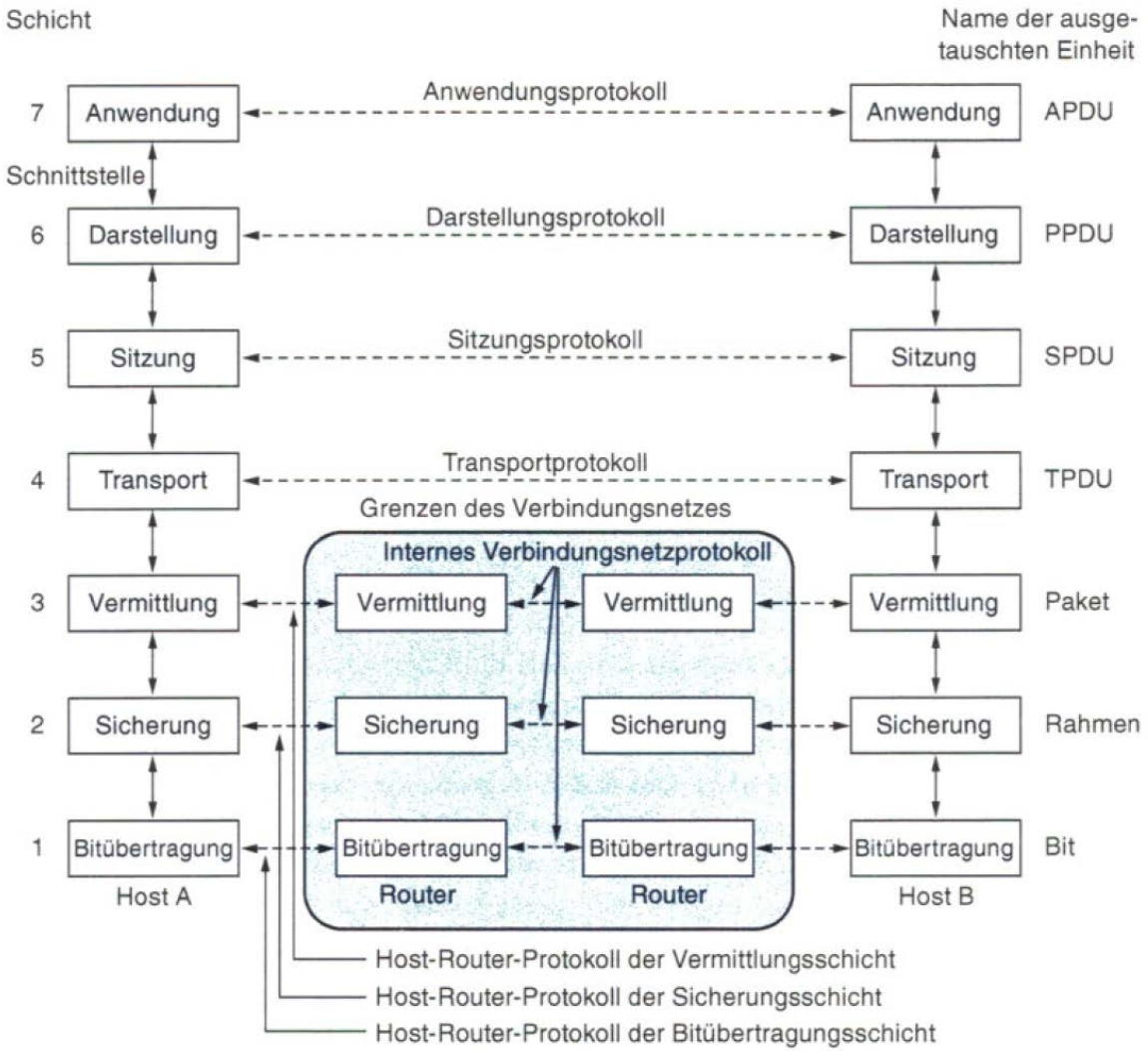
- Jede Schicht hat eine spezifische Aufgabe
- Jede Schicht kommuniziert nur mit der direkt darüber und darunterliegenden Schicht
- Jede Schicht stellt einen DIENST bereit, z.B. „Adressat finden“
- Dieser DIENST wird durch eine feste SCHNITTSTELLE definiert
- Falls für die Bereitstellung des DIENSTES eine Kommunikation mit der Gegenseite erforderlich ist, wird ein PROTOKOLL definiert, das ausschließlich im Ermessen der Schicht liegt
- Der DIENST und die SCHNITTSTELLE bleiben immer erhalten, das PROTOKOLL kann angepasst werden
- Durch Übereinandersetzen verschiedener Schichten, werden sukzessiv alle benötigten DIENSTE erstellt

Typische Schichten nach ISO/OSI Modell

Das International Standards Organization (ISO) / Open Systems Interconnection (OSI) Modell schläft vor:

- Pro Schicht sollte nur eine Funktionalität implementiert werden
- Jede Schicht sollte so viel Funktionalität enthalten, dass der Austausch zwischen den Schichten minimiert wird
- Aus den letzten beiden Kriterien ergibt sich eine Minimierungs-/Maximierungs-Strategie
- Immer wenn eine neue Abstraktionsebene eingeführt wird, sollte ihr eine Schicht zugeordnet werden
- Internationale Normen sollten bei den Schichten berücksichtigt werden, z.B. um eine Schicht gegen eine bereits normierte austauschen zu können

Typische Schichten nach ISO/OSI Modell



[Tannenbaum, Wetherall, Computernetzwerke, 5.Aufl., Pearson, 2012]

Überblick ISO/OSI Schichten

Schicht 1: Bitübertragungsschicht (Physical Layer)

- Basisschicht in der die Übertragung einzelner Bits in einem bestimmten Zeitintervall mit bestimmten elektrischen Spezifikationen (und Steckernormen) von A nach B und/oder B nach A zeitgleich oder nacheinander festgelegt wird

Schicht 2: Sicherungsschicht (Data Link Layer)

- Zusammenfassen von Bits zu größeren Einheiten (Bytes, Rahmen), deren Übertragung durch Fehlerkorrektur (meist Forward Error Correction (FEC) oder Bestätigungsrahmen (Acknowldegement frames)) und Netzwerkzugriffstechniken (Medium Access Control) gesichert wird

Schicht 3: Vermittlungsschicht (Network Layer)

- Festlegung der Routen von A nach B entweder als feste oder dynamische Strecken, Fairness und Quality of Service (Jitter, Latenz, Geschwindigkeit der einzelnen Sender)

Überblick ISO/OSI Schichten

Schicht 4: Transportschicht (Transport Layer)

- Abstraktionsebene für die Schichten 1-3 und 4-7, Kommunikation von SRC nach DST, Festlegung der Transportverbindung (Point-to-Point, Broadcast, (Nicht-) Einhaltung der Sendereihenfolge, …), Fragmentierung längerer Pakete in für das Verbindungsnetzprotokoll (1-3) geeignete kurze Pakete

Schicht 5: Sitzungsschicht (Session Layer)

- Aufbau von Datenübertragungen von einem Nutzer zu einem anderen Nutzer mit Sitzungscharakter: Einschränkung der Datenübertragung (dialog control), Nutzer-Exklusivität bei einer kritischen Operation (Token Management), Wiederaufnahme der Datenübertragung nach Abbruch der Verbindung durch Synchronisationspunkte (Synchronization)

Schicht 6: Darstellungsschicht (Presentation Layer)

- Abstraktion der übertragenen Daten für verschiedene Computersysteme durch Definition von Syntax und Semantik der Daten

Schicht 7: Anwendungsschicht (Application Layer)

- Verbindungsaufbau und Übertragung von Daten in einem für Anwender nutzbaren Service, typischerweise HTTP, FTP, SMTP, etc.

Überblick TCP/IP

TCP/IP entstand im Rahmen des ARPANET 1974 und wurde 1989 zum Standard.

ISO/OSI wurde 1983 standardisiert und 1995 überarbeitet.

TCP/IP definiert insbesondere Protokolle, die Schichten aus dem ISO/OSI Modell zugeordnet werden können.

Im Vergleich zu ISO/OSI fehlen die Schichten: Bitübertragung, Sitzung, Darstellung

TCP/IP Protokollübersicht (unvollständig)

Schicht 2: Sicherung (OSI) bzw. Netzzugang (TCP/IP)

- DSL: Digital Subscriber Line, auch ADSL (Asynchronous DSL)
- IEEE 802.11: insb. Wireless Protokolle (Wifi, Bluetooth, …), aber auch VLAN
- Ethernet

Schicht 3: Vermittlung (OSI) bzw. Internet (TCP/IP)

- IP: Internet Protocol
- ICMP: Internet Control Message Protocol

Schicht 4: Transport (OSI und TCP/IP)

- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol

Schicht 7: Anwendung (OSI und TCP/IP)

- HTTP: Hypertext Transfer Protocol
- SMTP: Simple Mail Transfer Protocol
- DNS: Domain Name System

Test von Übertragungen

Welche Angriffsszenarien kennen Sie?
(Brainstorming 5 Minuten)

Attacken auf Übertragungen

Mitlesen (Sniffing): Der Angreifer kann Nachrichtenverkehr mitprotokollieren

Man-in-the-Middle: Der Angreifer gibt sich gegenüber dem ursprünglichen Sender als Empfänger und gegenüber dem ursprünglichen Empfänger als Sender aus

Replay: Der Angreifer speichert eine (verschlüsselte) Botschaft und spielt sie später wieder ein

Denial of Service (DoS): Der Angreifer schickt so viele Anfragen, dass der angesprochene Service zusammenbricht

Distributed Denial of Service: Wie DoS, nur dass die Anfragen von vielen Sendern ausgehen

Attacken auf Implementierungen: Pufferüberlauf, Rootkit, Virus, Trojaner, ...

Projekt 1: Entwurf eines Netzwerkprotokolls

Entwerfen Sie ein Netzwerkprotokoll!

- 3 Blöcke Zeit (+3 Blöcke Hausarbeit), jeweils der 2. Block der Vorlesung
- Arbeit als Zweiergruppe
- Abgabe in Form einer schriftlichen Dokumentation
  - Protokollaufbau – Schichten und logischer Aufbau
  - PROTOKOLL-Informationen (im Sinne von ISO/OSI, Header-Information)
  - DIENST- und SCHNITTSTELLEN-Informationen (im Sinne von ISO/OSI, API Dokumentation)
  - Analyse der Latenz und Geschwindigkeit
  - Analyse der Energieeffizienz
  - Analyse der Zuverlässigkeit
  - Analyse der Robustheit gegen Attacken

Projekt - Szenario

Szenario: Messung von Umgebungsdaten im Bayrischen Wald

- Sensorknoten werden in unregelmäßigen Abständen im Wald platziert
- Sensorknoten kennen ihre eigene GPS Position
- Sensorknoten müssen energieeffizient arbeiten (Batteriebetrieb)
- Sensorknoten verfügen über LoRa-Sende- und Empfangseinrichtung
- Gatewayknoten verfügen über LoRa und Mobilfunk (LTE) Sende- und Empfangsmöglichkeiten zur Übertragung an einen zentralen Server
- Gatewayknoten müssen nicht energieeffizient arbeiten (Netzbetrieb)
- Jeder Sensorknoten soll mindestens einen anderen Sensorknoten erreichen, dazu muss die maximale LoRa-Entfernung ausgeschöpft werden
- Jeder Sensorknoten kann 0, 1 oder mehrere Gatewayknoten erreichen
- Jeder Gatewayknoten kann 0, 1 oder mehrere Sensorknoten erreichen
- Der Erfolg der Übertragung von Paketen im LoRa-Netz hat eine statistische Verteilung je nach Entfernung und Konfiguration der Schnittstelle
- Die Konfiguration der Schnittstelle kann geändert werden (siehe nächste Seiten)

Projekt - Szenario

Szenario: Messung von Umgebungsdaten im Bayrischen Wald

- Die Sensorstationen können 1-4 Parameter messen: Temperatur, Luftfeuchtigkeit, Schneehöhe, Sonneneinstrahlung
- Zur Speicherung auf dem Server muss die GPS Position zusammen mit dem jeweiligen Wert gespeichert werden
- Die Sensoren verändern ihre GPS Position nach der Installation nicht mehr
- Die Messung der Schneehöhe an einer beliebigen Stelle muss innerhalb von 1 Stunde an die Zentrale via Mobilfunkverbindung geschickt werden
- Die Sonneneinstrahlung wird auf Anfrage via Mobilfunknetz innerhalb von maximal 30 Minuten an die Zentrale zurückgesendet
- Temperatur und Luftfeuchtigkeit wird ein Mal pro Stunde gemessen und soll spätestens nach 24 Stunden am Server verfügbar sein

Projekt - Szenario

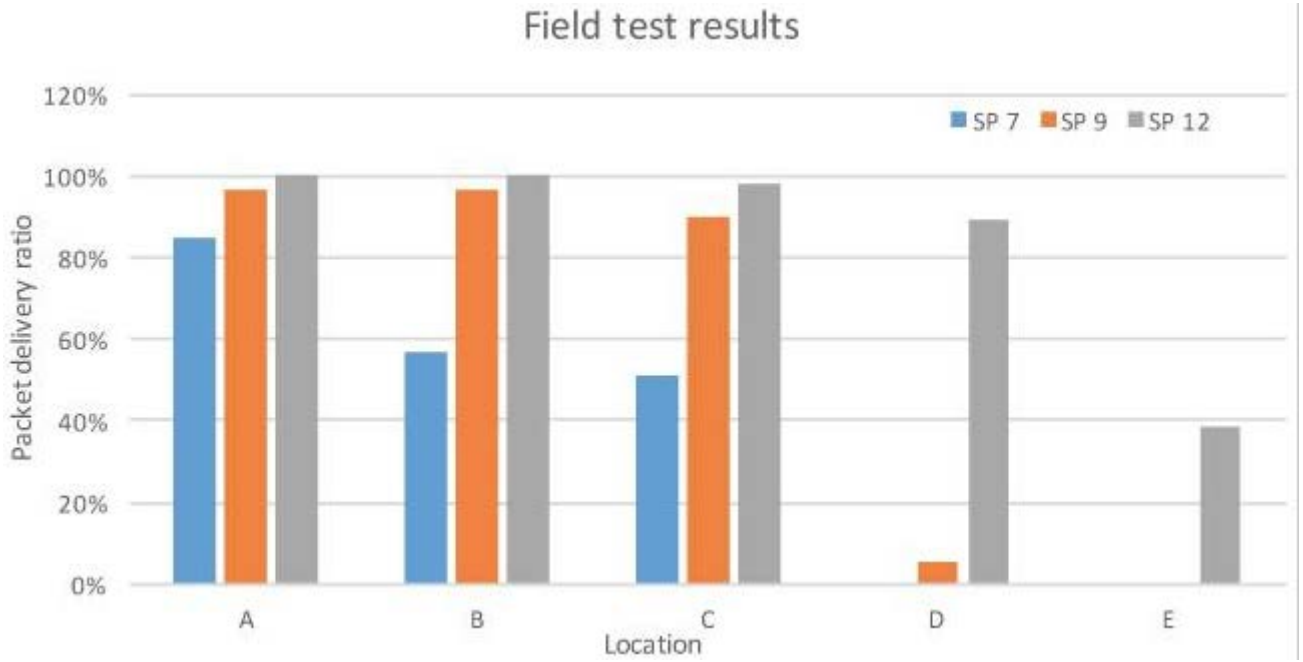
Energieverbrauch:

- Aufwecken eines Knoten bis zur Sendebereitschaft: 3 Energie-Einheiten (EE)
- Stromverbrauch während Betrieb: 10EE pro Minute
- Stromverbrauch während Deep-Sleep-Standby: 0.1EE pro Minute
- Betrieb der LoRa Sendeeinheit: 1EE pro Sekunde

Projekt - Szenario

LORA Einstellungen

- Jeder Knoten (Gateway und Sensor) kann verschiedene Parameter für die Übertragung wählen, die Energie, Übertragungsrate und Reichweite beeinflussen
- Einfluss des Spreading Factors (SF) aus [Augustin A, Yi J, Clausen T, Townsley WM. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors (Basel)*. 2016;16(9):1466. Published 2016 Sep 9. doi:10.3390/s16091466]



Distanz:
A: 650m
B: 1400m
C: 2300m
D: 2800m
E: 3400m

Projekt Szenario

LORA-Einstellungen

- Mit dem Spreizfaktor (Spreading Factor SF),
  der Anzahl im Payload zu übertragender Bytes PL= 1..255),
  der Bandbreite (Bandwidth BW=125kHz),
  und der Coderate (CR=4/8),
  einer impliziten Konfiguration ohne Header (Erklärung später im Kurs),

  ergibt sich die Übertragungszeit für ein Paket in Sekunden wie folgt:

$$T_{Packet} = \left(12 + 4.25 + 8 + \frac{8PL - 4SF + 28 - 20}{4 \cdot SF} \cdot 8 \right) \cdot \frac{2^{SF}}{125000}$$

- Daraus ergibt sich für die vorigen Spreizfaktoren bei jeweils einer Payload von 1, 10 und 100 bytes:
  SF=7 : 0.02s, 0.035s, 0.186s
  SF=9 : 0.08s, 0.14s, 0.743s
  SF=12 : 0.64s, 1.12s, 5.94s

- Beachten Sie, dass die Payload-Länge hier die Länge des Pakets ist, die Sie in Ihrer untersten Schicht erstellen.

Projekt Szenario

Erstellen Sie nun Ihr Netzwerkprotokoll!

- Welche Funktionalitäten möchten Sie implementieren?
- Wie gehen Sie mit dem Energieverbrauch um?
- Senden Sie im Broadcast oder nutzen Sie die GPS Daten für das Routing?
- Wer sendet wann?
- Was geschieht, wenn ein Datenpaket nicht am Sender ankommt?
- Was geschieht, wenn ein Knoten ausfällt?
- Wie schätzen Sie die Latenzzeiten ab?

- Falls Sie weitere Daten benötigen, schätzen Sie diese ab und dokumentieren Sie Ihre Schätzung
- Falls Sie das Szenario erweitern oder einschränken möchten, dokumentieren Sie Ihre Erweiterung!
  Beispiele: „Jeder Knoten soll ab Werk über eine eindeutige 8bit Kennung verfügen“, „Das System ist erst nach 3 Tagen vollständig operativ“

TECHNISCHE HOCHSCHULE DEGGENDORF

Danke für Ihre Aufmerksamkeit!