

Hochschule RheinMain
Fachbereich ITE
Studiengang EE-CS

LabGuide

ZigBee Versuch auf Basis von zigbee2mqtt

verfasst von **Benedikt HEUSER**
Matrikelnummer 105320

am 25.04.2022

Inhaltsverzeichnis

1	Versuchsdurchführung	2
1.1	Versuchsaufbau	2
1.2	Aufgabenstellungen	4
1.2.1	Aufgabe 1 - Vorbereitungen	4
1.2.2	Aufgabe 2 - Joining einer Phillips Hue Lampe	5
1.2.3	Aufgabe 3 - Joining eines Gerätes über ein anderes Gerät	7
1.2.4	Aufgabe 4 - Binding der Fernbedienung	8
1.2.5	Aufgabe 5 - Gruppenbildung	9
1.2.6	Fragen	10

Kapitel 1

Versuchsdurchführung

1.1 Versuchsaufbau

Folgende Hardware sollte sich in Ihrer Versuchskiste befinden. Bitte überprüfen sie dies vor Beginn des Versuches.

- RaspberryPi 3 mit eingesetzter microSD-Karte
- CC2531 Sniffer Stick
- cod.m ZigBee CC2652P2 Raspberry Pi Module
- 2 x Phillips Hue White E27
- 1 x Phillips Hue Dimmer Switch
- HDMI Kabel
- Ethernet Kabel

Ein cod.m Zigbee Modul sollte bereits auf Ihrem Raspberry montiert sein.

In diesem Praktikumsversuch wird ein kleines ZigBee Netzwerk errichtet. Verschiedene Funktionen des Protokolls werden getestet und aufgezeichnet.

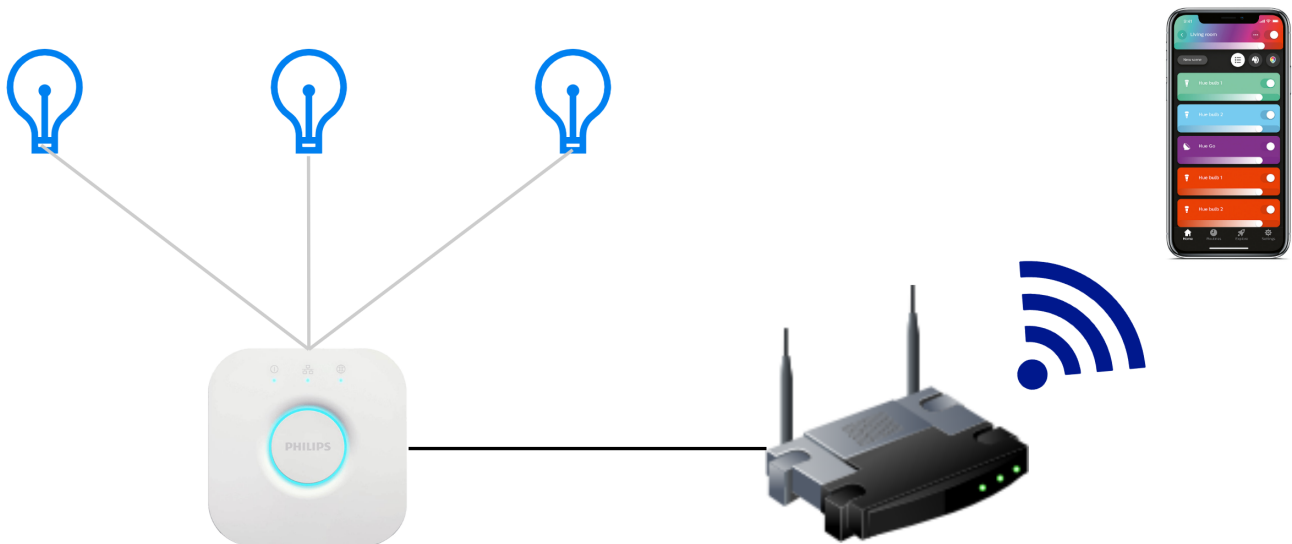


Abbildung 1.1: Philips Hue

Das ZigBee Protokoll, welches in diesem Versuch untersucht wird, kommt klassischerweise in hier gezeigtem Szenario zum Einsatz. Eine Bridge, hier von Phillips, verbindet sich per ZigBee mit Smart-home Komponenten wie Lampen. Diese Bridge fungiert als ZigBee Koordinator. Eine Smartphone App greift per REST-API auf die Bridge zu. Mit der App können nun die Lampen gesteuert werden.

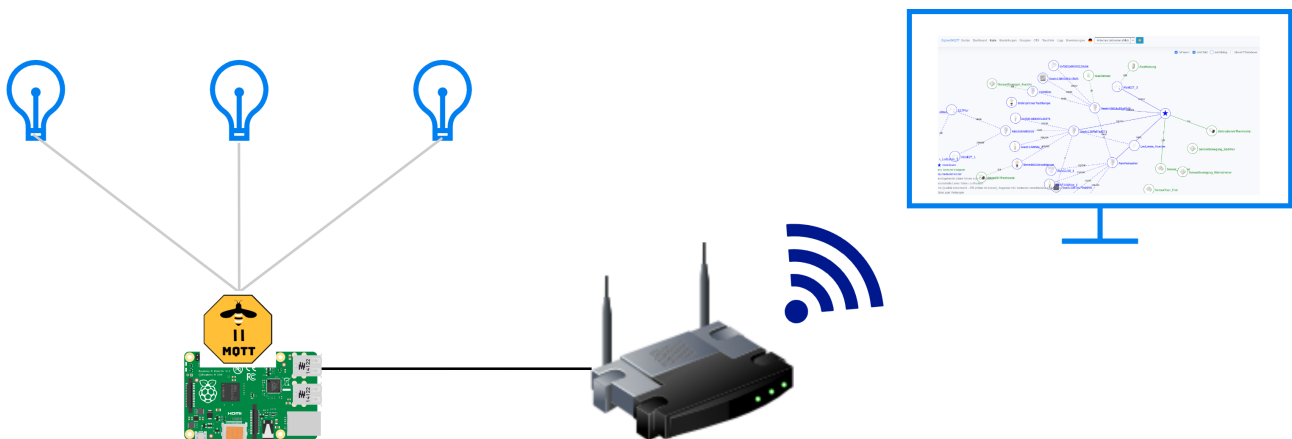


Abbildung 1.2: Versuchsaufbau

In diesem Versuch wird anstelle der Phillips Bridge ein RaspberryPi als Koordinator eingesetzt. Dieser benötigt dafür das cod.m Zigbee Modul sowie eine entsprechende Software. In dem Versuch wird Zigbee2mqtt eingesetzt. Anstelle einer App wird Zigbee2mqtt über ein Webinterface administriert. Dieses lässt sich wie in diesem Versuch gezeigt Lokal aufrufen oder aber auch nach außen verfügbar machen.

Der RaspberryPi dient in diesem Versuch als Koordinator und Versuchs-PC zugleich.

1.2 Aufgabenstellungen

Bitte arbeiten sie die folgenden Aufgabenstellungen durch. Fertigen sie im Anschluss einen Versuchsbericht an. Beantworten sie die anhängenden Fragen implizit oder explizit.

1.2.1 Aufgabe 1 - Vorbereitungen

Vorbereitung

- a) Schließen sie an den RaspberryPi Monitor, Tastatur, Maus sowie den Sniffer-Stick an. Durch Anschluss der Stromversorgung startet der RaspberryPi automatisch.
- b) Starten sie den Versuch, in dem sie ein Konsolenfenster öffnen und folgenden Befehl absetzen.

```
1 | > ansible-playbook ~/ZigbeeHSRM/playbooks/reset-lab.yaml -K -e "channel=<
    Gruppennummer>"
```

Setzen sie den gewünschten Kanal für <Gruppennummer> ein. Der Start des Labs kann einige Minuten dauern. Dieser Befehl muss nur einmal zu Beginn des Praktikums ausgeführt werden. Bei einem Neustart des RaspberryPis startet der Versuch automatisch. Sie werden nach einem Passwort gefragt. Das Passwort sollte gleich dem Benutzernamen sein. Im zweifel Fragen sie Ihren Betreuer.

- c) Starten sie ein Konsolenfenster und überprüfen mit folgendem Befehl, ob die Container ausgeführt werden:

```
1 | > docker ps
```

Es sollten 3 Container im Status "Running" sein. Sollte dies nicht der Fall sein, beispielsweise ein periodisches Neustarten des Containers "zigbee2mqtt", lesen sie die weiteren Schritte in den FAQs nach.

- d) Starten sie den Webbrowser und Navigieren zu der Seite:

```
1 | > https://z2m.local
```

- e) Starten sie Wireshark per "sudo wireshark" in einem Terminal. Bei den verfügbaren Schnittstellen sollte sich eine "TI CC2231" Schnittstelle finden. Über das vorangestellte Zahnrad-Symbol können sie den mitzuschneidenden Kanal einstellen. Stellen sie den eben gewählten Zigbee Kanal ein. (Gruppennummer)

- d) Setzen sie alle ZigBee Komponenten des Versuchs zurück. Dafür drücken sie auf der Rückseite der Fernbedienung die Reset Taste einige Sekunden, bis die LED rot leuchtet. Die Phillips Hue Lampen können ausschließlich per Touchlink zurückgesetzt werden. Drücken und halten sie dazu die äußeren Tasten der Fernbedienung während sie die Fernbedienung direkt an die Lampe halten. Warten sie bis die Lampe mehrmals aufblinkt und im Anschluss etwas gedimmt ist. Dies kann mehrere Versuche

mit verschiedenen Fernbedienungspositionen benötigen. Schalten sie im Anschluss die beiden Lampen wieder per Handschalter vollständig aus.

Alternativ bietet Zigbee2mqtt ebenfalls eine Touchlink Funktionalität. Bringen sie dafür die Lampe direkt an den Koordinator und Scannen in dem Zigbee2mqtt Webinterface nach Touchlink Geräten. Im Anschluss kann die Lampe hier zurückgesetzt werden. Auch hier wird das durch mehrmaliges blinken der Lampe signalisiert.

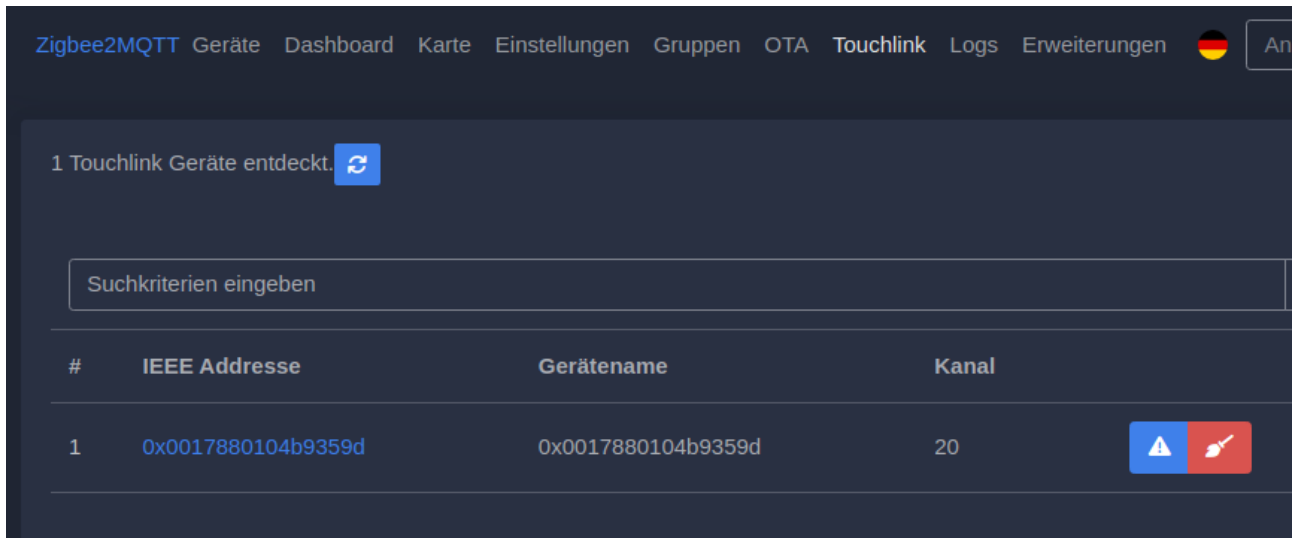


Abbildung 1.3: Touchlink - Lampen zurücksetzen

Hinweis

Alle Aufgaben sollen mit Wireshark mitgeschnitten werden. Lesen sie die Aufgabenstellung erst durch und machen sie sich den Ablauf klar. Versuchen sie das Zeitfenster des Wireshark Mitschnitts kurz halten, und in dieser Zeit nur die in der Aufgabenstellung explizit beschriebenen Aktionen durchzuführen.

1.2.2 Aufgabe 2 - Joining einer Phillips Hue Lampe

a) Schalten sie eine der beiden Lampen ein.

b) Starten sie nun ein Wireshark Mitschnitt und erlauben anschließend in Zigbee2mqtt das Anlernen von Geräten. Sobald Zigbee2mqtt ein erfolgreiches Interview gemeldet hat, beenden sie den Capture Vorgang. Die Lampe signalisiert dies durch ein kurzes blinken ein erfolgreiches Interview.

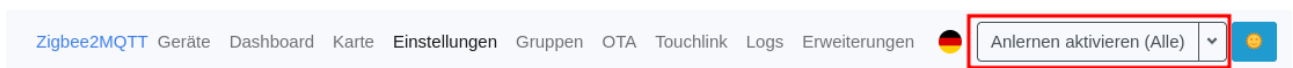


Abbildung 1.4: Zigbee Anlernen aktivieren

Aufgabe

Speichern sie den Wireshark Capture ab als “<Gruppe>-ZigbeeLab-Aufgabe2.1“.
Beantworten sie die Fragen in Ihrem Versuchsbericht.

c) Navigieren sie nun zur Übersichtsseite der Lampe. Diese sollte ähnlich wie folgende Seite aussehen:

Zigbee2MQTT Geräte Dashboard Karte Einstellungen Gruppen OTA Touchlink Logs Erweiterungen Anlernen aktivieren (Alle)

0xf0d1b8000013821d

Über Details binden Bericht Einstellungen Einstellungen (spezifisch) Status Cluster Szene Entwickler Konsole

Gerätename	0xf0d1b8000013821d
Beschreibung	N/A
Zuletzt gesehen	N/A
Verfügbarkeit	Deaktiviert
Geräte-Typ	Router
Zigbee Modell	A60 TW Z3
Zigbee Hersteller	LEDVANCE
Beschreibung	SMART+ classic E27 TW
Unterstützungsstatus	Unterstützt
IEEE Adresse	0xf0d1b8000013821d
Netzwerk Adresse	0x30FD
Firmware-Datum	Sep 29 2021
Firmware-Version	01056400
Hersteller	OSRAM
Modell	AC10787
Spannungsversorgung	
Interview erfolgreich	Wahr

Abbildung 1.5: Zigbee Device Übersicht

d) Vergeben sie in der Übersichtsseite der Lampe einen nutzerfreundlichen Namen. Dies geschieht über den blauen Button im unteren Teil der Übersicht.

e) Dimmen und schalten sie die Lampe über die Weboberfläche. Die ist unter dem Reiter “Dashboard“ möglich. Starten sie einen weiteren Capture Vorgang und schneiden einen Schaltvorgang mit.

Aufgabe

Speichern sie den Wireshark Capture ab als “<Gruppe>-ZigbeeLab-Aufgabe2.2“.
Beantworten sie die Fragen in Ihrem Versuchsbericht.

1.2.3 Aufgabe 3 - Joining eines Gerätes über ein anderes Gerät

Für diese Aufgabe sollte eine Lampe mit dem Koordinator verbunden sein. Die zweite Lampe wird nun über die Lampe dem Netzwerk hinzugefügt. Aus diesem Grund wird es nur der Lampe erlaubt ein neues Gerät in das Netzwerk aufzunehmen.

- Schalten sie die zweite Lampe ein und starten einen Wireshark Mitschnitt.
- Erlauben sie den Beitritt neuer Geräte explizit für die bereits verbundene Phillips Lampe. Ein erfolgreiches anlernen wird auch hier in der Weboberfläche und durch ein blinken der Lampe signalisiert.

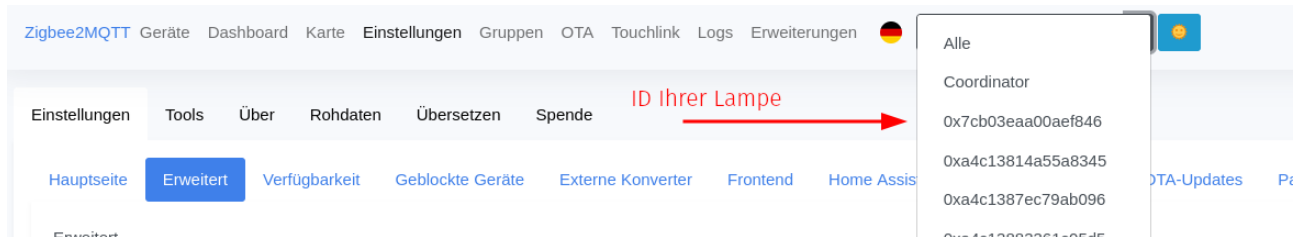


Abbildung 1.6: Zigbee Anlernen aktivieren - nur Lampe

Aufgabe

Speichern sie den Wireshark Mitschnitt ab als “<Gruppe>-ZigbeeLab-Aufgabe3”.
Beantworten sie die Fragen in Ihrem Versuchsbericht.

- Sehen sie sich die Netzwerkübersicht unter dem Reiter “Karte” an. Aktivieren sie nur den Haken “isParent”
- Fügen sie die Fernbedienung Ihrem Netzwerk hinzu. Gehen sie dabei wie bisher vor. Setzen sie die Batterie in die Fernbedienung ein und erlauben die Aufnahme neuer Geräte. Die Fernbedienung lässt sich im Zweifel durch langes drücken aller 4 Tasten in den Pairingmodus schalten. Wenn auch das nicht funktioniert, setzt man die Fernbedienung am besten erneut vollständig zurück wie in Aufgabe 1 beschrieben.

Ihre Übersichtsseite sollte wie folgt aussehen.


Suchkriterien eingeben				
#	Bild	Gerätename	IEEE Adresse	Hersteller
1		Lampe-1	0x0017880104b9359d (0x1ED6)	Philips
2		Lampe-2	0x0017880104a53274 (0xABF3)	Philips
3		Fernbedienung	0x0017880104f1ba1e (0xB9F7)	Philips

Abbildung 1.7: Zigbee2mqtt Übersichtsseite Lab

1.2.4 Aufgabe 4 - Binding der Fernbedienung

- Navigieren sie in der Weboberfläche zu der Übersicht Ihrer Lampe. Dort finden sie einen Reiter “binden”.
- Trennen sie das Binding zwischen Endpunkt 1 der Fernbedienung und dem Koordinator. Betätigen sie direkt nach dem Trennen eine Taste auf der Fernbedienung. Zum Batteriesparen “schläft” diese periodisch und kann in dieser Zeit keine Bindungsanfragen annehmen. Warten sie bis Zigbee2mqtt eine erfolgreiche Trennung des Binding meldet.
- Starten sie ein Wireshark Mitschnitt. Binden sie den Endpunkt 1 der Fernbedienung mit dem Endpunkt 11 Ihrer Lampe. Binden sie die Cluster “OnOff” und “LevelCtrl”.
- Schalten sie nun die Lampe mit der Fernbedienung ein und aus.

Hinweis

Speichern sie den Wireshark Capture ab als “<Gruppe> - ZigbeeLab - Aufgabe 4”.
Beantworten sie die Fragen in Ihrem Versuchsbericht.

Hinweis

Das Binding ist auf den Geräten mangelhaft implementiert, da Phillips selbst diese Funktion nicht nutzt. Es kann notwendig sein, die Fernbedienung ein weiteres mal vollständig zurückzusetzen und neu anzulernen. Dafür muss der Rest Knopf der Fernbedienung so lange gedrückt werden, bis die LED rot leuchtet. Vor allem wenn bei der Phillips Hue Fernbedienung mehr als ein Binding auf den Endpunkt 1 gelegt wird, scheint diese Probleme zu bekommen. Sollte es dennoch Probleme geben, kann der Wireshark Trace Aufschluss geben. Oft werden die Binding Tabellen nicht mehr aktualisiert und die Fernbedienung schickt die Kommandos an nicht mehr existierende Gruppen aus dem vorherigen Versuchsdurchgang.

d) Entfernen sie im Anschluss dieses Binding. Drücken sie auch hier eine Taste der Fernbedienung damit diese geweckt wird.

1.2.5 Aufgabe 5 - Gruppenbildung

- Navigieren sie in der Weboberfläche zu dem Reiter “Groups”.
- Legen sie eine Gruppe mit dem Namen “Hue-Lights-<Gruppe>” an.
- Starten sie einen Wireshark Mitschnitt. Editieren sie nun die Gruppe. Fügen sie die Endpunkte der beiden Lampen, die zum Steuern verwendet werden, der Gruppe hinzu.

Aufgabe

Speichern sie den Wireshark Capture ab als “<Gruppe> - ZigbeeLab - Aufgabe 5”.
Beantworten sie die Fragen in Ihrem Versuchsbericht.

d) Navigieren sie nun wieder zur Binding-Übersicht der Fernbedienung. Binden sie die Fernbedienung nun mit der soeben angelegten Gruppe. Achten sie auch hier darauf eine Taste der Fernbedienung zu betätigen.

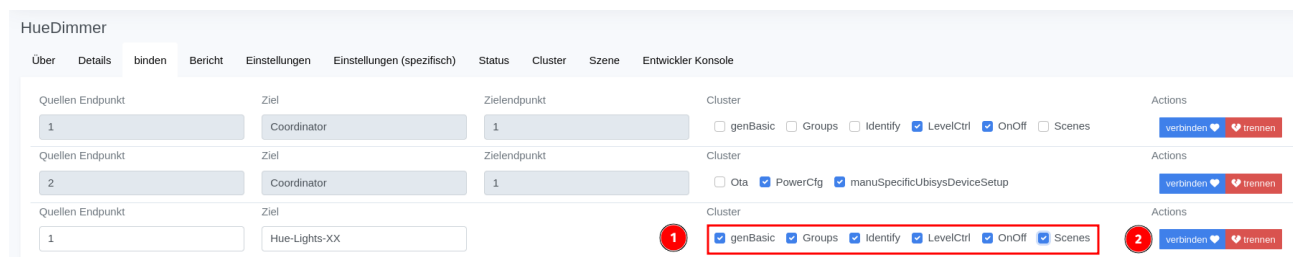


Abbildung 1.8: Zigbee2mqtt Group Binding

e) Starten sie einen Wireshark Mitschnitt. Schalten sie die Gruppe mit der Fernbedienung ein und aus.

Aufgabe

Speichern sie den Wireshark Capture ab als “<Gruppe> - ZigbeeLab - Aufgabe 5.1”.
Beantworten sie die Fragen in Ihrem Versuchsbericht.

1.2.6 Fragen

Aufgabe 2

Fragen

1. Untersuchen sie den **Beacon-Request**

- Erläutern sie den Frametype und den Command Identifier.
- Erläutern die Ziel- und Quelladresse und was sie daraus erschließen können.

Hinweis: Wireshark Filter: `frame.protocols == "wpan"`

2. Wie teilt der Koordinator den umliegenden Geräten mit, dass er dem Netzwerk den Beitritt weiterer Geräte erlaubt ?

- Zu welchem Frametype gehört der Beacon und durch welchen Wert wird er spezifiziert?
- Welche Ziel- und Quelladressen werden verwendet?

Hinweis: Wireshark Filter: `frame.protocols == "wpan:zbee_beacon"`

4. Welchen Wert hat das Feld „Association Permit“ im letzten Beacon des Koordinators und wie ist dieser Wert zu interpretieren?

5. Untersuchen Sie den **Association Request** der Lampe an den Koordinator.

- Welchen Wert hat das Feld „Allocate Address “ und wie ist dieser zu interpretieren?
- Welchen Wert hat das Feld „Device Type“ und wie ist dieser zu interpretieren?

Hinweis: Wireshark Filter: `frame.protocols == "wpan"`

7. Untersuchen die den **Data Request** von der Lampe an den Koordinator.

- Erläutern Sie die Funktion dieser Nachricht.
- Mit welchem Kommandoframe antwortet der Koordinator auf den Data-Request?
- Welche Werte besitzen die Felder „Short Address“ und „Association Status“?

Hinweis: Wireshark Filter: `frame.protocols == "wpan"`

8. Untersuchen Sie einen **IEEE802.15.4. Ack-Frame**.

Welche Adressfelder werden benutzt?

- Wie findet die Zuordnung zum Daten- oder Kommandoframe statt, der durch die Ack bestätigt wird?
- Werden grundsätzlich alle Frames bestätigt?

10. Wie lautet die letzte Nachricht, bei der 64-bit-MAC-Adressen verwendet werden?

- Wie lautet die erste Nachricht, bei der die 16-Bit-Kurzadresse der beigetretenen Lampe verwendet wird?

11. Was ist die letzte Nachricht, die auf dem NWL-Layer unverschlüsselt übertragen wird?

12. Erläutern Sie den Zweck der **Transport-Key-Nachricht**.

-Wie lautet der Frametype des 802.15.4-Frames, in dem die Transport-Key-Nachricht transportiert wird?

-Wie lautet der ZigBee-NWK Frametype des Frames?

-Treffen Sie möglichst genaue Aussagen zum in der Transport-Key übertragenen Schlüssel (Schlüsseltype).

-Erläutern Sie, wie die Transport-Key-Nachricht kryptographisch gesichert ist.

-Interpretieren Sie den Inhalt des Radius Feldes im NWK-Frame, das die TransportKeyNachricht enthält!

Hinweis: Wireshark Filter: `zbee_aps.cmd.id == 0x05`

13. Erläutern Sie, den Zweck des versendeten **Active-Endpoint-Requests** und des **SimpleDescriptor-Requests**.

-Beschreiben Sie die Information, die in den entsprechenden Response-Nachrichten enthalten ist.

-Wie stellt Zigbee2mqtt die Information dar?

-Welche Endpoints werden für den Austausch der untersuchten Request- und ResponseNachrichten verwendet? Interpretieren Sie dies!

Hinweis: Wireshark Filter: `frame.protocols == "wpan:zbee_nwk:zbee_aps:zbee_zdp"`

14. Durch welche ZigBee-Frames werden die Schaltvorgänge übertragen?

15. Beschreiben Sie möglichst genau, durch welche Headerfelder die Schaltvorgänge definiert sind!

16. Welche Endpoints werden für die Schaltvorgänge benutzt? Woher hat der Koordinator Kenntnis über die in der Lampe verwendeten Endpoints?

Aufgabe 3

Fragen

1. Erläutern Sie den Zweck der **Permit-Join-Request** Nachricht.

-An welche ZigBee-NWKZieladresse wird die Nachricht versendet?

-Erläutern Sie das wichtigste Headerfeld!

Hinweis: Wireshark Filter: `zbee_aps.profile == 0x0000`

2. Welchem Zweck dient die **Update Device** Nachricht?

-Wer ist Absender und wer ist Empfänger?

-Welche Adresse steht im Feld „Device Address“?

Hinweis: Wireshark Filter: `zbee_aps.type == 0x1`

3. Von welchem Device erhält die zweite Lampe ihre 16 Bit Kurzadresse und wie lautet sie?

4. Wie viele **Transport-Key** Nachrichten wurden ausgetauscht?

-Erläutern Sie wer jeweils der Absender und wer der Empfänger ist.

-Versuchen Sie die den Vorgang zu erklären und gehen Sie dabei auf das Kommandoframe “Tunnel“ ein. -Wie sind die Transport-Key Nachrichten kryptographisch gesichert? -Was sind die wichtigsten Headerfelder des Tunnel-Kommandoframes?

Hinweis: Wireshark Filter: `zbee_aps.type == 0x1`

5. Untersuchen Sie die **Device Announcement** Nachricht der zweiten Lampe.

-Welchen Zweck hat sie?

-Schauen Sie sich die “Capability Information “ an. Handelt es sich um ein Full-Function-Device?

-Welcher Wert steht im Feld „AC Power“ und was sagt dieser Wert aus?

Hinweis: Wireshark Filter: `zbee_aps.profile == 0x0000`

6. Untersuchen Sie die **Active-Endpoint-Request** Nachricht und ihren Weg vom Koordinator bis zur zweiten Lampe.

-Vergleichen Sie die Adressen im ZigBee-NWKLayer und im IEEE-Layer und erklären Sie den Zusammenhang.

-An welchem Headerfeld können Sie zweifelsfrei identifizieren, dass es die gleiche Nachricht ist, die nur weitergeleitet wird?

Hinweis: Wireshark Filter: `zbee_aps.profile == 0x0000`

7. Untersuchen Sie die **Simple Descriptor Response**- Nachrichten der zweiten Lampe! -Welche Informationen enthält diese Nachricht?

Hinweis: Wireshark Filter: `zbee_aps.profile == 0x0000`

8. Erklären sie die Zahlen, welche in der Kartenansicht an den Verbindungen notiert sind.

Aufgabe 4

Fragen

1. Untersuchen Sie die **Bind Request**- und die **Bind Response**-Nachricht.
-Was sind jeweils die NWK-Quell- und NWK-Zieladressen? Erläutern Sie, den Inhalt der BindRequest Nachricht.
-Was genau bewirkt die Nachricht? In der Nachricht sind nur 64-Bit Adressen enthalten. Stellt das ein Problem dar?
Hinweis: Wireshark Filter: `zbee_aps.profile == 0x0000`
2. Warum wird vom Koordinator kein Bind-Request an die Lampe gesendet?
3. Betrachten Sie die **ZCL: OnOff** Nachricht. Geben Sie die NWK-Quell- und Zieladresse an.
-Welchen Wert hat das On/OFF-Cluster und welches Kommando wird zum Schalten verwendet?
Hinweis: Wireshark Filter: `zbee_zcl.type == 0x1`
4. Interpretieren Sie die von der Fernbedienung gesendeten **Data Request** Nachrichten? -Wie groß ist der zeitliche Abstand zwischen zwei Data-Requests? -Was löst eine DataRequest-Nachricht beim Empfänger aus? Geben Sie ein Beispiel. Hinweis: Wireshark Filter: `wpan.cmd == 0x04`

Aufgabe 5

Fragen

1. Verdeutlichen Sie sich den Vorgang in dem Sie die vom Koordinator versendeten Nachricht **Add Group** untersuchen.
-Fassen Sie die wichtigsten Informationen der Nachrichten zusammen.
2. Betrachten Sie die **Add Group Response** Nachricht des Empfängers.
-Welche Information ist enthalten?
-Welcher Zielendpunkt wird im APS-Frame des AddGroup-Befehles verwendet?
-Geben Sie eine Erklärung!
3. Wie lautet die Destination Adresse im ZDP-Header der **Bind Request** Nachricht?
-Welcher Zielendpunkt ist vorhanden?
Hinweis: Wireshark Filter: `zbee_aps.profile == 0x0000`
4. Was ist die NWK-Zieladresse der **ZCL-OnOff** Nachricht?

- Um welche Art von Nachricht handelt es sich hierbei?
 - Finden Sie die von Ihnen eingestellte Gruppen-ID in der „ZCL OnOff“-Nachricht wieder?
- Hinweis: Wireshark Filter: `zbee_zcl.type == 0x1`

Weiterführende Fragen

Fragen

1. Welchem Zweck dienen die **Link Status** Nachrichten?
-Über welche Anzahl von **Hops** wird diese Nachricht übertragen? -Analysieren Sie exemplarisch einige Link-StatusNachrichten und Interpretieren Sie diese!
2. Untersuchen Sie die **Link Quality Request**- bzw. **Link Quality Response**-Nachrichten.
-Gehen Sie auf den LQI-Wert in der **Link Quality Response** Nachricht und was bedeutet dieser?
3. Interpretieren Sie **Route Request** Nachrichten und zugehörige **Route-Response**-Nachrichten.

