Technische Hochschule Brandenburg
Online Studiengang Medieninformatik
Fachbereich Informatik und Medien
Einführung in die wissenschaftliche Projekarbeit
Prof. Dr. rer. nat. Martin Christof Kindsmüller

Konzept:

Drahtlose Low Power Kommunikationsprotokolle und ihre Sicherheit

Wintersemester 2021
Abgabetermin 6. Juni 2022

Friedemann Richard Pruß (Matrikel-Nr. 20215742)
Mara Schulke (Matrikel-Nr. 20215853)

Inhaltsverzeichnis

1 Thematische Fokussierung

In einer vernetzten Welt mit unzähligen IoT-Geräten wird sichere Kommunikation mit sogenannten Low-Power-Protokollen immer wichtiger. Smart-Devices wie zum Beispiel Sicherheitskameras, Smart-Lampen oder allgemeiner – jegliche Embedded-Hardware, lässt sich mittlerweile so gut wie überall wiederfinden.

Diese Geräte zeichnen sich dadurch aus, dass sie oft stark begrenzte Ressourcen haben. In der Regel ist ein niedriger Stromverbrauch gewünscht, da viele Geräte mit Akku- oder Batterie betrieben werden. Bei diesen ist folglich die Rechenleistung eingeschränkt, da mit einer leistungsstarken CPU die Batterielaufzeit enorm verkürzt würde.

Da Kommunikation dennoch meist eine elementare Aufgabe dieser Geräte ist, gibt es zahlreiche Entwicklungen, um die Problematik energieeffizient zu lösen. Low-Power-Protokolle benötigen weniger Strom als vergleichbare Protokolle aus dem Desktop-Umfeld. Weiterhin ist die Vertraulichkeit & Sicherheit der kommunizierten Daten unabdinglich, da gerade im Smart-Home-Bereich ein Angriff fatale Folgen haben könnte.

Die entstehende Arbeit soll in dem oben genannten Kontext das Thema der sicheren Kommunikation genauer beleuchten. Dazu werden zwei der am weitesten verbreiteten Protokolle, namentlich Thread und Bluetooth-Low-Energy (kurz *BLE*) hinsichtlich ihrer Sicherheit verglichen. Insbesondere ist die Frage interessant, ob das jüngere Thread-Protokoll die bekannten sicherheitsrelevanten Problematiken von Bluetooth-Low-Energy behebt.

2 Motivation & Abgrenzung

Auch nach ausführlicher Recherche ließ sich, trotz der bereits großen und immer weiter zunehmenden Bekanntheit der beiden Protokolle, keine Publikation finden, in der ein detaillierter Sicherheitsvergleich stattgefunden hat. In der Regel wurde eines der beiden Protokolle alleinstehend betrachtet (**ThreadInteroperabilityIEEE**; **BluetoothMeshIntroBLTW:online**), oder es fand ein allgemeiner konzeptioneller Vergleich statt – zum Beispiel hinsichtlich Architektur, Protkoll-Aufbau, Funktionsumfang etc. (**ThreadMeshVsOtherWirelessIEEE**; **ComparativeAnalysisIEEE**; **ThreadVsBluetoothEnterpriseIotInsights:online**). Desweiteren sind die Protokollspezifikationen für beide Protokolle öffentlich einsehbar (**ThreadSpec:online**; **BluetoothSpec:online**).

Antonioli, Tippenhauer und Rasmussen haben im Jahr 2020 bereits eine sehr detaillierte Arbeit über die Sicherheitsprobleme und Angriffsmöglichkeiten auf Bluetooth-Low-Energy veröffentlicht. (**BluetoothLowEnergyAttackOxford**)

In verschiedensten Arbeiten werden diverse Anwendungsszenarien erläutert und die Vorteile der jeweiligen Architektur für die betrachtete Problemstellung herausgestellt. (**ThreadApplicationIEEE**; **ThreadApplicationSmartBuildingsIEEE**)

Die geplante Arbeit grenzt sich durch die Fokussierung auf den Sicherheitsaspekt von den oben genannten Arbeiten ab. Im besten Fall soll diese eine konkrete Empfehlung für oder gegen die Benutzung eines der Protokolle geben – eventuell auch einen Ausblick über eine mögliche zukünftige Entwicklung. Dafür werden mögliche Sicherheitslücken und -mechanismen von Thread und Bluetooth-Low-Energy untersucht. Insbesondere werden sich diese Untersuchungen auf mögliche Angriffe und die Mechanismen der Protokolle, um sich vor eben diesen zu schützen, beziehen. (**BluetoothPracticalAttacksICACCS**; **ThreadSecurityCSIAC:online**) Zu typischen Angriffen zählen beispielsweise Man-In-The-Middle-Attacken. (**GeneralManInTheMiddle**)

Andere Arbeiten stellen Eigenschaften und Problematiken, teils durch größer angelegte Feldversuche, heraus. Anhand dieser experimentellen Untersuchungen kann man Chancen und Risiken der verglichenen Protokolle gegeneinander abwägen. Daraus soll die angestrebte Empfehlung abgeleitet werden.

3 Recherchebericht

Um einen Einstieg in das Thema zu finden, wurde graue und nicht-zitierfähige Literatur gesichtet, wie zum Beispiel Blogposts, Videos und Wikipedia-Artikel. Dadurch konnte ein grober Überblick über die zu bearbeitende Thematik – *Sicherheit im Smart-Home* – gewonnen werden.

Es wurde deutlich, dass momentan ein Umbruch der Kommunikationsprotokolle im IoT-Bereich stattfindet. Da dies große Relevanz für die Zukunft der Branche hat, lag es nahe, das Thema Sicherheit mit den am weitest verbreiteten Kommunikationsprotokollen zu verbinden. Dies führte letztendlich zu dem Thema der Arbeit: *Drahtlose Low Power Kommunikationsprotokolle und ihre Sicherheit.*

Nachdem die Themenfindung abgeschlossen war, begann die fokussierte Recherche bei den großen wissenschaftlichen Datenbanken. Dabei zeigten sich die Datenbanken der IEEE, ACM und die Gesellschaft für Informatik besonders ergiebig für das gewählte Thema. Zuerst wurden die Publikationen nach Schlagwörtern, Titeln und Aktualität vorgefiltert. Nachdem eine grobe Vorauswahl bestand, hat sich das Überfliegen des Abstracts und der Zusammenfassung als effiziente Möglichkeit zur Überprüfung der Relevanz einer Arbeit erwiesen.

Dadurch fanden sich besonders interessante und relevante Quellen wie zum Beispiel **BluetoothLowEnergyAttac**
oder **ThreadMeshVsOtherWirelessIEEE**. Diese und weitere sehr vielversprechende Arbeiten boten einen guten Anhaltspunkt um über deren Literaturliste weitere themennahe Publikationen zu finden. Nach der ersten Kollektion von Quellen, war es ein sinnvoller Schritt diese nach Kategorie (zum Beispiel *Bluetooth*, *Thread* und *Vergleiche*) und Relevanz zu sortieren. Priorisiert wurde nach Aktualität, thematischer Nähe und wissenschaftlicher Wertigkeit.

Jede relevante Publikation wurde in BibTeX erfasst. Nachdem eine erste Liste vorhanden war, lag es nahe, diese erneut auf Vollständigkeit und Verfügbarkeit – insbesondere bei online Quellen – zu überprüfen. Dieses Vorgehen wurde so lange wiederholt, bis sich für den Umfang der zu erstellenden Arbeit genügend hochwertige Quellen ergeben haben.

4 Zeitplan

KW43 – Recherche & mediale vorbereitung Präsentation

KW44 – Recherche & Präsentation

KW45-48 – Inhaltliche Ausarbeitung

KW49 – Schreiben des Extended Abstract

KW50-02 – Entwicklung des wissenschaftlichen Posters

5 Vorläufige Literaturliste