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 29. Oktober 2021

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

Inhaltsverzeichnis

1 Thematische Fokussierung **1**

2 Motivation & Abgrenzung **1**

3 Recherchebericht **2**

4 Zeitplan **3**

5 Vorläufige Literaturliste **3**

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 (Vangimalla & El-Sharkawy, 2018a; Woolley, 2020), oder es fand ein allgemeiner konzeptioneller Vergleich statt – zum Beispiel hinsichtlich Architektur, Protkoll-Aufbau, Funktionsumfang etc. (Dvoynikov et al., 2021; Gregersen, 2021; Rzepecki & Ryba, 2019). Desweiteren sind die Protokollspezifikationen für beide Protokolle öffentlich einsehbar (Group, n. d.; ThreadGroup, n. d.).

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

In verschiedensten Arbeiten werden diverse Anwendungsszenarien erläutert und die Vorteile der jeweiligen Architektur für die betrachtete Problemstellung herausgestellt. (Lan, 2016; Vangimalla & El-Sharkawy, 2018b)

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. (Pallavi & Narayanan, 2019; Strayeri, 2020) Zu typischen Angriffen zählen beispielsweise Man-In-The-Middle-Attacken. (Malliak, 2018)

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 Antonioli et al. (2020) oder Rzepecki und Ryba (2019). 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

Antonioli, D., Tippenhauer, N. & Rasmussen, K. (2020). Key Negotiation Downgrade Attacks on Bluetooth und Bluetooth Low Energy. *ACM Trans. Priv. Secur.*, *23*(3). https://doi.org/10.1145/3394497

Ayers, H., Crews, P., Teo, H., McAvity, C., Levy, A. & Levis, P. (2020). Design Considerations for Low Power Internet Protocols. *2 020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 103–111. https://doi.org/10.1109/DCOSS49796.2020.00027

Dvoynikov, V., Smirnov, V. & Burilov, D. (2021). Comparative Analysis of Mesh und Thread Networks und their Application Possibility in the "Smart Home' Systems. *2021 IEEE Conference of Russian Young Researchers in Electrical und Electronic Engineering (ElConRus)*, 8–11. https://doi.org/10.1109/ElConRus51938.2021.9396680

Elshimi, A. (2020). Thread protocol simplifies IoT security - Embedded.com [(Accessed on 10/17/2021)].

Gregersen, C. (2021). Thread vs Bluetooth: The IoT battle of low-power protocols (Reader Forum) [(Accessed on 10/17/2021)].

Group, B. S. I. (n. d.). Bluetooth Kernspezifikation Version 5.2 Funktionsübersicht [(Accessed on 10/28/2021)].

Inc., G. (2021). What is Thread? | OpenThread [(Accessed on 10/17/2021)].

Kennis, J. (2021). Thread, Matter, und CHIP – This Glossary Will Quickly Bring You Up To Speed > Thread Group [(Accessed on 10/17/2021)].

Kennis, J. & Bruins, J. (2021). Thread in Commercial Network Topology Explained [[Online; accessed 22. Oct. 2021]]. https://www.threadgroup.org/news-events/blog/ID/185/Thread-in-Commercial-Network-Topology-Explained#.YXMFKSWxW0p

Klein, U. (2021). Bluetooth LE Smart Home Funkstandard – Wissen, Geräte, Bedeutung [(Accessed on 10/17/2021)].

Lan, D. (2016). *Experimental Study of Thread Mesh Network for Wireless Building Automation Systems*. DIVA. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1040491&dswid=-8223

Lan, D., Pang, Z., Fischione, C., Liu, Y., Taherkordi, A. & Eliassen, F. (2018). Latency Analysis of Wireless Networks for Proximity Services in Smart Home und Building Automation: The Case of Thread. *IEEE Access*, *7*, 4856–4867. https://doi.org/10.1109/ACCESS.2018.2888939

Mainetti, L., Patrono, L. & Vilei, A. (2011). Evolution of wireless sensor networks towards the Internet of Things: A survey. *SoftCOM 2011, 19th International Conference on Software, Telecommunications und Computer Networks* (S. 1–6). IEEE. https://ieeexplore.ieee.org/document/6064380

Malliak, A. (2018). Man-In-The-Middle-Attack: Understanding In Simple Words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*, 109–134. https://doi.org/http://dx.doi.org/10.22373/cj.v2i2.3453

Miethe, S. & Krug, S. (2021). Evaluation of Interoperability Between Various Implementations of the Thread Protocol Stack. In R. H. Reussner, A. Koziolek & R. Heinrich (Hrsg.), *INFORMATIK 2020* (S. 1185–1194). Gesellschaft für Informatik, Bonn. https://doi.org/10.18420/inf2020_110

Pallavi, S. & Narayanan, V. (2019). An Overview of Practical Attacks on BLE Based IOT Devices und Their Security. *2019 5th International Conference on Advanced Computing Communication Systems (ICACCS)*, 694–698. https://doi.org/10.1109/ICACCS.2019.8728448

Pannell, T. (2018). Funktechniken für Netzwerke: Zigbee, Thread und Bluetooth Mesh im Vergleich – Kommunikation/Wireless – Elektroniknet [(Accessed on 10/17/2021)].

Prajapati, D. (n. d.). Zigbee, Z-Wave, BLE 5.0 und Thread Protocol und their applications [(Accessed on 10/17/2021)].

Ritesh, K., Manolova, A. & Nenova, M. (2017). Abridgment of bluetooth low energy (BLE) standard und its numerous susceptibilities for Internet of Things und its applications. *2017 IEEE International Conference on Microwaves, Antennas, Communications und Electronic Systems (COMCAS)*, 1–5. https://doi.org/10.1109/COMCAS.2017.8244814

Ryan, M. (2013). Bluetooth: With Low Energy Comes Low Security. *7th USENIX Workshop on Offensive Technologies (WOOT 13)*. https://www.usenix.org/conference/woot13/workshop-program/presentation/ryan

Rzepecki, W. & Ryba, P. (2019). IoTSP: Thread Mesh vs Other Widely used Wireless Protocols – Comparison und use Cases Study. *2019 7th International Conference on Future Internet of Things und Cloud (FiCloud)*, 291–295. https://doi.org/10.1109/FiCloud.2019.00048

Sandhya, S. & Devi, K. (2012). Analysis of Bluetooth threats und v4.0 security features. *2012 International Conference on Computing, Communication und Applications*, 1–4. https://doi.org/10.1109/ICCCA.2012.6179149

Santos, A., Filho, J., Silva, A., Nigami, V. & Fonseca, I. (2019). BLE injection-free attack: a novel attack on bluetooth low energy devices. *Journal of Ambient Intelligence und Humanized Computing*. https://doi.org/https://doi.org/10.1007/s12652-019-01502-z

Silicon Laboratories, I. (n. d. a). Bluetooth Mesh, Thread, und Zigbee Network Performance Benchmarking - Silicon Labs [(Accessed on 10/17/2021)].

Silicon Laboratories, I. (n. d. b). UG103.11: Thread Fundamentals [(Accessed on 10/17/2021)].

Strayeri, K. (2020). Can the "Gorilla" Deliver? Assessing the Security of Google's New "Thread" Internet of Things (IoT) Protocol - CSIAC [(Accessed on 10/17/2021)].

ThreadGroup. (n. d.). Thread 1.1 Specification [(Accessed on 10/28/2021)].

Vangimalla, S. R. & El-Sharkawy, M. (2018a). Interoperability Enhancement in Health Care at Remote Locations using Thread Protocol in UAVs. *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society* (S. 2821–2826). IEEE. https://doi.org/10.1109/IECON.2018.8592759

Vangimalla, S. R. & El-Sharkawy, M. (2018b). Remote Wireless Sensor Network Range Extension Using UAVs with Thread Protocol. *2018 International Conference on Computational Science und Computational Intelligence (CSCI)* (S. 902–906). IEEE. https://doi.org/10.1109/CSCI46756.2018.00178

Woolley, M. (2020). Bluetooth Mesh Networking - An Introduction for Developers [[Online; accessed 17. Oct. 2021]]. https://www.bluetooth.com/bluetooth-resources/bluetooth-mesh-networking-an-introduction-for-developers