Die Sicherheit von energiesparenden 2,4-GHz-Kommunikationsprotokollen für vermaschte Netzwerke

Friedemann R. Pruß, Mara Schulke
prussf@th-brandenburg.de 20215742, schulke@th-brandenburg.de 20215853

6. Juni 2022

Die vorliegende Arbeit beleuchtet die Möglichkeiten zur sicheren Kommunikation mit energiesparenden 2,4-GHz-Protokollen im Smart-Home-Kontext. Dazu werden zwei weit verbreitete WPAN-Mesh-Protokolle – Thread und Bluetooth Mesh – hinsichtlich ihrer Sicherheit verglichen. Vermaschte Netzwerke bieten im Smart Home viele Vorteile, wie z.B. eine hohe Ausfallsicherheit und leichte Erweiterbarkeit. Gegen die Verwendung von WAN-Protokollen wie LoRa, SigFox und NB-IoT für Smart-Home-Netzwerke sprechen die hohen Kosten des initialen Aufbaus eines WAN und die häufig niedrigeren Datenraten. Außerdem ist die Anzahl möglicher Erweiterungen für das Netzwerk bei 2,4-GHz-Protokollen deutlich höher (**ThreadMeshVsOtherWirelessIEEE**).

Die Threadgroup, zu deren Mitgliedern Firmen wie Apple, Amazon und Google gehören, bezeichnet Thread als Nachfolger von Zigbee (**ThePromiseOfThread**). Des Weiteren setzt der IoT-Standard Matter für die Datenübertragung auf Thread (**Matter**). Matter wurde von der Connectivity Standards Alliance (ehem. Zigbee Alliance) entwickelt, zu deren Mitgliedern unter anderen auch die vorher genannten Firmen gehören (**Matter**).

Das Forschungsergebnis wurde erreicht, in dem im Rahmen einer Survey und Literaturanalyse die Spezifikationen der Protokolle und bereits getätigte Sicherheitsanalysen ausgewertet wurden. 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 (**ThreadApplicationIEEE**; **BluetoothMeshIntro**), oder es fand ein allgemeiner konzeptioneller Vergleich statt – zum Beispiel hinsichtlich Architektur, Protokollaufbau, Funktionsumfang etc (**ComparativeAnalysisIEEE**; **ThreadMeshVsOtherWirelessIEEE**). Des Weiteren sind die Spezifikationen für beide Protokolle öffentlich beziehungsweise kostenlos einsehbar (**BluetoothSpec**; **ThreadSpec**). Zu Bluetooth bzw. Bluetooth Mesh gibt es weitreichende Sicherheitsanalysen und gut dokumentierte Sicherheitslücken (**BluetoothLowEnergyAttackOxford**; **BluetoothIssues**). In weiteren Publikationen wurden Angriffe auf Thread durchgeführt (**ThreadEMAttack**) und mögliche Schwachstellen untersucht (**ThreadSecurityCSIAC**). Die vorliegende Arbeit grenzt sich durch einen sicherheitsbezogenen Vergleich von den oben gennanten Arbeiten ab.

In den letzten Jahren wurden mehrere, teils kritische, Sicherheitslücken in der Bluetooth Spezifikation entdeckt (**BluetoothIssues**). Diese beeinträchtigen zum Großteil die Sicherheit von Direktverbindungen - also Bluetooth BR/EDR und Bluetooth Low Energy. Zu den schwerwiegendsten Schwachstellen in der Bluetooth Core Spezifikation zählen die sogenannten “Bluetooth Impersonation Attacks”. Diese macht es möglich, dass sich ein Angreifer als bereits authentifiziertes Gerät ausgibt und somit die komplette Authentifizierung bei einem Verbindungsaufbau umgehen kann. Dies ermöglicht Man-In-The-Middle-Attacken (**BluetoothLowEnergyAttackOxford**).

Bluetooth Mesh verwendet als Übertragungsprotokoll Bluetooth Low Energy und anders als beim Bluetooth-Low-Energy-Pairing werden elliptische 256-Bit-Kurven und Out-of-Band-Authentifizierung verwendet, um das Hinzufügen von Netzwerkknoten abzusichern (**BluetoothSpec**). Allerdings wurden diesbezüglich im Jahr 2020 die Sicherheitswarnungen CVE-2020-26556, CVE–2020-26557, CVE-2020-26559, CVE-2020-26560 veröffentlicht (**BluetoothIssues**).

Thread ist im Gegensatz zu Bluetooth Mesh ein offenes Protokoll, da es kaum einen Einfluss auf die Anwendungsebene des Netzwerks hat. Im Jahr 2020 wurde eine Sicherheitsanalyse von Thread anhand der 10 relevantesten Sicherheitsbedenken dem Open Web Application Security Project (OWASP) für IoT-Netzwerke durchgeführt (**ThreadSecurityCSIAC**).

Diese Analyse zeigt, dass Thread den Fokus primär auf die Verschlüsselung und die Sicherung der Übertragung legt, aber Risiken durch die fehlende Spezifikation der Anwendungsebene entstehen könnten. Hersteller müssen selbst für die Sicherheit auf der Anwendungsebene sorgen. Ein großer Vorteil der offenen Spezifikation ist die Möglichkeit angemessene und erforschte Kryptografie einzusetzen.

Die aktuell bekannten Sicherheitslücken von Bluetooth Mesh betreffen das Hinzufügen von neuen Netzwerkknoten (**BluetoothIssues**) und vermindern somit die Integrität des Netzwerks. Bislang wurden bei Thread, trotz ausgiebiger Untersuchungen (**ThreadSecurityCSIAC**; **ThreadSecurityEmbeddedCom**) noch keine vergleichbaren Schwachstellen gefunden. Auf der anderen Seite tritt Thread die Verantwortung zu Absicherung der Anwendungsschicht an den Hersteller ab, ist somit zwar flexibler, könnte aber mögliche Sicherheitslücken durch nicht abgesicherte Geräte öffnen.

Eine eindeutige Empfehlung für oder gegen eines der beiden Protokolle nur auf Basis der Sicherheit kann

nicht klar gegeben werden, da beide Protokolle unterschiedliche Vorteile und Sicherheitsrisiken mit sich bringen. Eine Entscheidung muss vom Implementierungskontext abhängig gemacht werden.