Dateiname: MA101_Langer_M

Titel:
Implementierung des Network-Time-Security-Protokolls für den Unicast-Betrieb

Bearbeiter:

Martin Langer

Text der Kurzfassung:

Die technischen Entwicklungen in den letzten Jahrzehnten führten zu einem drastischen Anstieg der Vernetzungsdichte von Computersystemen. Je nach Anwendungsgebiet sind genaue und zuverlässige Zeitinformationen vonnöten, damit derartige Systeme ihre Tätigkeiten ausüben können. Die Bereitstellung dieser Daten erfolgt heutzutage durch weit verbreitete Zeitsynchronisierungsprotokolle, wie etwa das Network Time Protocol (NTP) oder das Precision Time Protocol (PTP), mit denen sich große Computernetze zeitlich synchronisieren lassen. Aufgrund der steigenden Nachfrage an Sicherheit, die auch die unverfälschte Übertragung von Zeitdaten beinhaltet, wurden im Jahr 2011 die bestehenden Sicherheitsmechanismen der Zeitprotokolle untersucht. Das Ergebnis zeigte gravierende Schwächen und setzte dadurch die Hebel zur Ausarbeitung einer neuen und zeitgemäßen Spezifikation in Gange. Fortan wurde an einem neuen Protokoll unter dem Namen Network Time Security (NTS) gearbeitet, welches sich derzeit in der Entwicklungsphase befindet und zukünftig die erforderliche Sicherheit garantieren soll.

Diese Arbeit beschäftigt sich mit Aufbau, Ablauf und Implementierung des NTS-Protokolls im Unicast-Betriebsmodus und dessen Einbettung in NTPv4. Dazu folgen eine detaillierte Beschreibung zum Softwaredesign und der konzeptionellen Vorgehensweise, die während der Umsetzung des NTS-Protokolls Anwendung fand. Die entwickelte Software und die anschließenden Tests sollen hierbei den Beweis zu korrekten Funktion der NTS-Spezifikation liefern und darüber hinaus eine Referenzimplementierung für zukünftige Entwicklungen bieten.