Mit dem OCG-Förderpreis 2012 ausgezeichnete Dilpmarbeit

**Secure Stack for Clocks Synchronized by IEEE 1588**

**DI Bernd Hirschler, TU Wien, Inst. f. Computertechnik**

Diese Diplomarbeit analysiert die Auswirkungen von verschiedenen Sicherheitsprotokollen auf Systeme, die das IEEE 1588v2 Uhrensynchronisationsprotokoll verwenden.

In heutigen Automatisierungsnetzwerken spielt die Zeit eine immer größere Rolle. Ein prominentes Beispiel dafür ist der Large Hadron Collider (LHC) des CERN. Einerseits müssen die einzelnen magnetischen Komponenten, die den Protonenstrahl lenken, exakt angesteuert werden um das Experiment zu ermöglichen, und andererseits werden bei den Messungen exakte Informationen darüber benötigt, zu welchem Zeitpunkt ein Detektor die Messgröße erfasst. In beiden Fällen wird vorausgesetzt, dass alle Komponenten Zugriff auf die aktuelle Uhrzeit haben. Für diese Einsatzzwecke müssen die Uhren synchronisiert sein.

Es wird jedoch nicht verhindert, dass z.B. die Uhrzeit manipuliert werden kann. Dies kann unabsichtlich z.B. durch einen Wartungstechniker oder absichtlich durch einen Angreifer geschehen. Deshalb müssen Security Mechanismen eingesetzt werden, um dies zu verhindern.

Der Schwerpunkt dieser Arbeit liegt dabei auf der hochgenauen Uhrensynchronisation und wie diese durch die Verwendung von Security Protokollen beeinflusst wird. Im Zuge dieser Arbeit wurden verschiedene Protokolle analysiert, die für die Sicherung der Pakete genutzt werden können.

Neben der nativen Lösung (Annex K) für das Precision Time Protocol (PTP) wird auch untersucht, welchen Einfluss ein Standardprotokoll auf die Uhrensynchronisation hat. Für diesen Vergleich wird das weit verbreitete und standardisierte Protokoll IPsec (Internet Protocol security) verwendet. IPsec erlaubt die gesicherte Kommunikation auf IP (Internet Protocol) Ebene. IPsec sowie die native Lösung werden herangezogen, um die Faktoren zu identifizieren, die die Uhrensynchronisation beeinflussen.

Während der Analyse der neuen Security Erweiterung (Annex K) des IEEE 1588v2 Standards wurde ein fundamentaler Fehler im Protokoll gefunden. Dieser macht die Security Erweiterung des Precision Time Protocol (PTP) anfällig für Man-in-the-Middle und Replay Attacken.

Die durchgeführten Messungen zeigen, dass die verschiedenen Sicherheitsprotokolle einen deutlichen Einfluss auf die Verzögerungen der einzelnen Pakete haben. Die Schwankungen dieser Verzögerung bewegen sich jedoch in einem kleinen Bereich und können durch Regelalgorithmen kompensiert werden. Bei den abschließenden Messungen wird gezeigt, dass die Packet Delay Variation (PDV), die durch die Sicherheitsprotokolle hervorgerufen wird, nur geringe Auswirkungen auf die Qualität der hochgenauen auf Software basierenden Uhrensynchronisation hat.