Zeitsynchronisation des Smart Meter Gateways

Dieter Sibold*

1 Einleitung

Das Smart Meter Gateway (SMGW) verfügt über eine Reihe von Funktionen, die einen Bezug zur gesetzlichen Zeit verlangen. Ein Beispiel hierfür ist die vom SMGW durchzuführende Zeitstempelung und Tarifierung der zu erfassenden Messwerte. Die Technische Richtlinie BSI TR-03109-1 (TR) schreibt vor, dass die Zeit des SMGW durch eine vertrauenswürdige Zeitquelle zu synchronisieren ist [1], damit sie sich innerhalb der eichrechtlich vorgegebenen Unsicherheiten mit der gesetzlichen Zeit deckt. Die TR beschreibt hierzu eine hierarchische Zeitsynchronisationsstruktur, in der das SMGW durch den Zeitserver beim SMGW-Administrator (GW-Admin) und dieser wiederum von den Zeitservern der PTB zu synchronisieren ist (siehe Bild 1). In beiden Hierarchieebenen wird die Zeitsynchronisation durch das weit verbreitete *Network Time Protocol* [2, 3] realisiert. Die Anforderungen an die Zeitsynchronisation zwischen SMGW und GW-Admin beschreibt die TR. Die Anforderungen für die Verbindung zwischen GW-Admin und der PTB sind in den PTB-Anforderungen 50.8 [4] beschrieben.

2 Funktionsweise der Zeitsynchronisation

Das *Network Time Protocol* (NTP) ermöglicht den Aufbau einer hierarchisch gegliederten Zeitsynchronisationsstruktur, mit deren Hilfe eine einheitliche Zeit in verteilten Infrastrukturen etabliert und kontinuierlich aufrechterhalten wird. Der Verbreitungsgrad des NTP ist hoch, sodass nationale Metrologie-Institute häufig öffentliche NTP-Server zur Weitergabe der koordinierten Weltzeit Universal Time Coordinated (UTC) bereitstellen.

Das NTP verwendet ein Zweiwege-Zeitübertragungsverfahren, wie in Bild 2 dargestellt. Dieses Verfahren setzt voraus, dass beide Kommunikationspartner Nachrichten empfangen und versenden können. Ein Client bestimmt seine Zeitdifferenz zu einem Zeitserver (im Folgenden kurz Server bezeichnet), indem er zu einem Zeitpunkt

* Dr. Dieter Sibold, Arbeitsgruppe Q.42 "Serversysteme und Datenhaltung", E-Mail: dieter.sibold@ptb.de

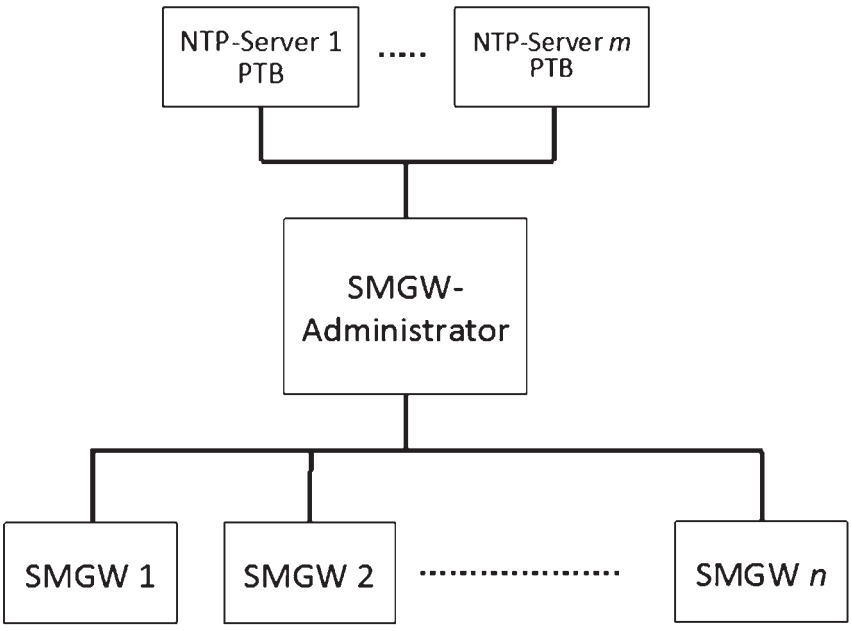

Bild 1:
Zeitsynchronisationshierarchie für das Smart Meter Gateway

t_1 eine Zeitanfrage an den Server verschickt, der diese zum Zeitpunkt t_2 erhält. Client und Server fügen diese Zeiten jeweils in die Nachricht ein. Der Server sendet die Antwort zum Zeitpunkt t_3 an den Client, der sie zum Zeitpunkt t_4 erhält. Diese Zeiten werden beim Versand und Empfang ebenfalls in die Nachricht eingetragen. Die Zeiten t_1 und t_4 werden relativ zur Systemzeit des Clients, die Zeiten t_2 und t_3 relativ zur Systemzeit des Servers gemessen. Anhand dieser vier Zeitstempel kann der Client unter der Annahme, dass die Paketlaufzeiten für die Anfrage und Antwort gleich lang sind (symmetrischer Fall, d. h. $\xi = 0{,}5$; siehe Bild 2) die Zeitdifferenz Δ zum Server aus $\Delta = \frac{1}{2}((t_2-t_1) + (t_3-t_4))$ berechnen [5]. In IP-Netzwerken ist diese Annahme häufig nicht zutreffend, sodass die Bestimmung von Δ mit einem Fehler ε behaftet ist. Der Fehler ist begrenzt durch $|\varepsilon| \leq \frac{1}{2}\,\delta$, wobei δ die gesamte Paketlaufzeit aus Anfrage und Antwort darstellt. Die gesamte Paketlaufzeit δ kann aus den vier Zeitstempeln mit $\delta = ((t_4-t_1) - (t_3-t_2))$ berechnet werden. Die gemessene Zeitdifferenz Δ verwendet der Client, um den Zeit- und Frequenzfehler seiner Systemuhr zu minimieren [6].

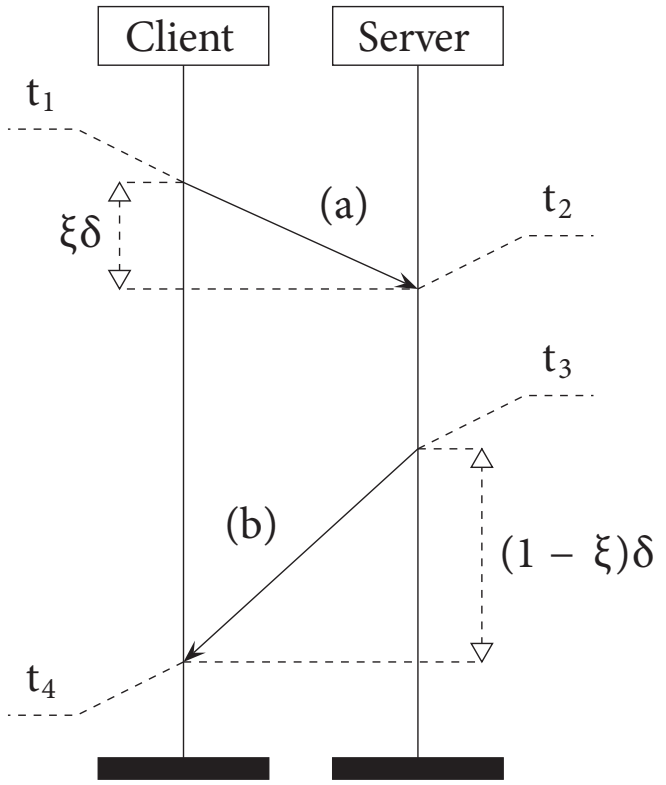

Bild 2:
Schematische Darstellung der Zeitanfrage (a) und -antwort (b) zwischen Client und Server. Der Parameter ξ, $0<\xi<1$, quantifiziert die Asymmetrie zwischen den Laufzeiten für die Zeitanfrage und -antwort. Für den symmetrischen Fall, $\xi = \frac{1}{2}$, sind die Paketlaufzeiten für die Anfrage und Abfrage gleich. Die gesamte Paketlaufzeit ist durch $\delta = ((t_4-t_1) - (t_3-t_2))$ gegeben. Der Fehler in der Berechnung der Zeitdifferenz Δ zwischen Client und Server beträgt $(\xi-\frac{1}{2})\delta$.

3 Synchronisationshierarchie

In der aktuellen Version der TR des BSI wurde festgelegt, dass sich die SMGWs nicht direkt mit den Servern der PTB synchronisieren, sondern stattdessen ihre Zeit vom Zeitserver des Gateway-Administrator (GW-Admin) beziehen sollen. Der GW-Admin wiederum hat seine Zeitserver mit den Zeitservern der PTB zu synchronisieren, siehe Bild 1.

3.1 Zeitsynchronisation des GW-Admin

Der GW-Admin hat aus eichrechtlichen Gründen die Rückführung der Zeit der SMGW zur gesetzlichen Zeit sicherzustellen. Er muss daher seine Zeitserver-Infrastruktur mit der PTB synchronisieren, um die Rückführbarkeit seines Zeitdienstes auf die gesetzliche Zeit zu sichern. Die PTB stellt für solche Zwecke eine Zeitserver-Infrastruktur zur Verfügung. Die Vertrauenswürdigkeit der Zeitserver-Infrastruktur wird durch das im NTP integrierte symmetrische Authentifizierungsverfahren sichergestellt.

3.2 Zeitsynchronisation des SMGW

Für die Zeitsynchronisation des SMGW durch den GW-Admin legt die TR fest, dass die Inhalte der NTP-Pakete entgegen des NTP-Standards über einen Webservice (ntp-over-http) oder alternativ über einen gesicherten TLS-Kanal (ntp-over-TLS) transportiert werden müssen. Diese Festlegung gewährleistet die Konformität mit den Anforderungen des Schutzprofiles für das SMGW [7]. Sie erhöht allerdings auch den Kommunikationsaufwand und das auszutauschende Datenvolumen und führt damit zwangsläufig zu einem höheren Ressourcenbedarf bei den Kommunikationspartnern und des Netzwerks. Die Güte der Zeitsynchronisation wird durch diese Festlegung zwar reduziert, ist aber aufgrund der moderaten Genauigkeitsanforderungen an die Zeitsynchronisation vertretbar.

4 Genauigkeitsanforderungen

Die Zeitabweichung des SMWG gegenüber der gesetzlichen Zeit darf laut TR 3 % der kleinsten zu unterstützenden Abrechnungsperiode nicht überschreiten. Die TR legt als kleinste vom SMGW zu unterstützende Abrechnungsperiode fünf Minuten fest. Das entspricht einer zulässigen Abweichung von 9 Sekunden zur gesetzlichen Zeit. Das SMGW berechnet daher regelmäßig die Zeitabweichung Δ und die Paketlaufzeit δ. Dann wird geprüft, ob der Betrag $|\Delta|+\frac{1}{2}\delta$ kleiner ist, als die durch die kleinste Abrechnungsperiode vorgegebene maximal zulässige Zeitabweichung.

Ist die Bedingung nicht erfüllt, muss das SMGW dies durch einen Log-Eintrag dem GW-Admin bekannt machen.

Damit die Unsicherheit des Zeitdienstes beim GW-Admin in der Überwachung des SMGW vernachlässigt werden kann, legen die PTB-A 50.8 fest, dass die Zeitserver des GW-Admin nicht mehr als 1 % (d. h. 0,03 % der kleinsten Abrechnungsperiode) von den Zeitservern der PTB abweichen dürfen. Für die oben genannte Abrechnungsperiode ergibt sich damit eine Fehlergrenze von 90 ms, die vom Zeitserver des GW-Admin einzuhalten sind. Die Unsicherheit der PTB-Zeitserver ist kleiner als 10 µs [8] und kann daher bei der Unsicherheitsbetrachtung des Zeitservers beim GW-Admin vernachlässigt werden.

5 Sicherheitsbetrachtungen

Aus eichrechtlichen Gründen muss die Authentizität der in der Synchronisationshierarchie verwendeten Zeitserver und außerdem die Authentizität und Integrität der ausgetauschten NTP-Pakete sichergestellt werden. Da die NTP-Pakete keine vertraulichen Informationen enthalten, besteht keine Notwendigkeit, diese zu verschlüsseln. Zwischen PTB und GW-Admin werden die Sicherheitsanforderungen durch das native Authentifizierungsverfahren vom NTP erfüllt. Zwischen GW-Admin und SMGW wird der Schutz der Synchronisationspakete durch die oben beschriebene Kapselung in einen TLS-Kanal sichergestellt, der die NTP-Pakete zusätzlich verschlüsselt.

Neben den Angriffen auf Authentizität und Integrität gibt es weitere Angriffsmöglichkeiten auf Zeitsynchronisationsprotokolle [9]. Ein besonders effektives Beispiel stellt der Delay-Angriff dar. Hierbei verzögert ein Angreifer systematisch die Abfrage- oder Antwortpakete zwischen Client und Zeitserver. Die hierdurch verursachte Modifikation des Asymmetrie-Parameters ξ führt zu einem systematischen Fehler in der Berechnung der Zeitdifferenz Δ (siehe Bildunterschrift zu Bild 2). Da die NTP-Pakete dabei nicht modifiziert werden, sind kryptographische Sicherungsmaßnahmen zum Erkennen und Abwehren dieses Angriffs ungeeignet. Eine charakteristische Eigenschaft dieses Angriffs ist jedoch die Erhöhung der gesamten Paketlaufzeit δ der NTP-Pakete. Eine geeignete Methode zur Erkennung des Angriffs besteht demnach darin, δ kontinuierlich zu überwachen und bei signifikanten Abweichungen zu warnen. In der TR wird daher festgelegt, dass bei Überschreiten eines Schwellwerts für δ der GW-Admin informiert werden muss.

6 Zukünftige Entwicklungen

Die TR weist darauf hin, dass die vorgegebene Zeitsynchronisationshierarchie vorläufig ist. Die zwischen SMGW und GW-Admin spezifizierte Kapselung der NTP-Paketinhalte in TLS oder HTTPS war notwendig, um die Anforderungen des SMGW-Schutzprofils zu erfüllen. Derzeit wird im Rahmen der Internet Engineering Task Force (IETF) an der Spezifikation eines neuen nativen Authentifizierungsverfahrens für NTP gearbeitet [10]. Es ist beabsichtigt, dieses Verfahren für die Zeitsynchronisation zwischen PTB und GW-Admin und nach einer Neufassung der TR ggfs. auch für das SMGW zu verwenden. Es ist ebenfalls vorstellbar, eine direkte Synchronisierung der SMGW mit PTB-Zeitservern zu ermöglichen.

7 Literatur

[1] BSI, Technische Richtlinie TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, 2013, Bundesamt für Sicherheit in der Informationstechnik, Bonn

[2] Mills, D., J. Burbank, and W. Kasch, Network Time Protocol Version 4: Protocol and Algorithms Specification. 2010, RFC Editor. DOI: 10.17487/rfc5905

[3] Mills, D., Computer network time synchronization: the Network Time Protocol, 2006, CRC Press. 304

[4] PTB, PTB-Anforderungen PTB-A 50.8 Smart Meter Gateway, 2014, Physikalisch-Technische Bundesanstalt

[5] Levine, J., A review of time and frequency transfer methods, Metrologia, 2008, 45(6), S. S162–S174, DOI: 10.1088/0026-1394/45/6/S22

[6] Mills, D.L., Adaptive hybrid clock discipline algorithm for the network time protocol, Ieee-Acm Transactions on Networking, 1998, 6(5), S. 505–514, DOI: 10.1109/90.731182

[7] BSI, Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073, 2014, Bundesamt für Sicherheit in der Informationstechnik, Bonn

[8] Piester, D., et al., PTB´s time and frequency services 2010–2014, in Precise Time and Time Interval Systems and Applications Meeting, 2014, Boston, Mass., USA

[9] Mizrahi, T., Security Requirements of Time Protocols in Packet Switched Networks, 2014, RFC Editor, DOI: 10.17487/rfc7384

[10] Sibold, D., Röttger, S., Teichel, K., Network Time Security Internet Draft, in Vorbereitung, Oktober 2015, https://datatracker.ietf.org/doc/draft-ietf-ntp-network-time-security/ (letzter Aufruf 21. Oktober 2015)