Privacy and Smart Meters / Smart Grid

Thomas Oberwallner
Betreuer: Dr. Heiko Niedermayer
Hauptseminar - Innovative Internettechnologien und Mobilkommunikation WS 2011/2012
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: thomas.oberwallner@mytum.de

KURZFASSUNG

Durch die zunehmende dezentrale Stromversorgung durch erneuerbare Energien muss das Stromnetz den Strom über weitere Strecken transportieren. Um eine zuverlässige Versorgung zu erreichen, ist es daher notwendig, dass die Betreiber die Auslastung zuverlässig messen können. In dieser Ausarbeitung wird beschrieben, welche Probleme im Bereich Datenschutz bei der Einführung des Smart Grids (intelligenten Stromnetzes) und Smart Meter (intelligenter Stromzähler) auf die Verbraucher zukommen. Es werden zwei Protokolltypen (grundlegendes Protokoll und No-Leakage Protokoll) dargestellt, die sowohl eine Lastüberwachung des Stromnetzes, als auch eine regelmäßige Rechnungsstellung der Stromverbraucher ermöglichen, ohne die Privatsphäre der Nutzer zu gefährden. Bislang sind diese Protokolle jedoch noch nicht in den Geräten implementiert.

Schlüsselworte

Smart Meter, Smart Grid, Privacy, Protocol, No-Leakage, Datenschutz

1. EINLEITUNG

1.1 Begriffe Smart Grid/ Smart Meter

Der Begriff Smart Grid kommt aus dem Englischen und wird meist mit intelligentem Stromnetz oder Energieinformationsnetz übersetzt. Er bezeichnet die Vernetzung zwischen Stromerzeuger, Stromverbraucher, Stromspeicher und Stromübertrager. Dieser Vernetzung kommt eine hohe Bedeutung zu, da aktuell ein Übergang von zentraler Stromerzeugung durch Großkraftwerke wie Kohle-, Gas- oder Atomkraftwerke hin zu dezentraler Versorgung durch erneuerbare Energien stattfindet. Wenn im südlichen Teil Deutschlands wenig Sonne scheint, muss beispielsweise der aus Windkraft erzeugte Strom von der Nordsee nach Bayern transportiert werden, da die Grundlastkraftwerke im südlichen Teil von Deutschland den Strombedarf eventuell nicht decken können. In Deutschland war im Jahr 2010 eine Photovoltaik-Nennleistung von 17370 Megawatt-Peak installiert [6], was in etwa der Gesamtleistung aller Atomkraftwerke in Deutschland entspricht. Insgesamt wurden jedoch nur etwa 12000 Gigawattstunden Strom [6] produziert, was in etwa der Jahresstromproduktion des Kernkraftwerks Isar 2 entspricht [4]. Also ist die durch Photovoltaik erzeugte Energiemenge stark schwankend und sollte, wenn bei sonnigem Wetter Stromüberfluss vorhanden ist, zum Beispiel in Pumpspeicherkraftwerken gespeichert werden.

Smart Meter bezeichnet intelligente Zähler, die den aktuellen Verbrauch an Strom, Wasser, Gas oder Fernwärme kontinuierlich ermitteln und anzeigen. Zusätzlich wird wie in [8] davon ausgegangen, dass sie zu einer Zwei-Wege-Kommunikation fähig sind, also den Stromverbrauch auch an den Versorger weiterleiten können. In dieser Ausarbeitung beschränke ich mich auf das Einsatzgebiet im Stromnetz, allerdings lässt sich ein Großteil der Schlussfolgerungen auch auf andere Verbraucher übertragen. Ziel dieses Messgeräts ist es, den Stromverbrauch häufiger an den Versorger zu übermitteln, um die Rechnungsstellung anhand des aktuellen Verbrauchs in kürzeren Intervallen zu ermöglichen und damit einerseits tageszeitabhängige Stromtarife anzubieten und andererseits den Kunden für den eigenen Stromverbrauch zu sensibilisieren und somit den Energieverbrauch zu senken. Damit können Kunden zum Beispiel erkennen, wie hoch der Stromverbrauch der nachts auf Standby laufenden Geräte ist. Ebenfalls können Anreize geschaffen werden, damit Kunden den Strom dann beziehen, wenn gerade ausreichende Mengen davon im Netz sind und somit Lastspitzen im Netz des Netzbetreibers zu senken. Für den Kunden haben intelligente Zähler jedoch einige Nachteile: So kosten diese Zähler deutlich mehr als normale Drehstromzähler (der einzelne Nutzer muss jedoch nicht die Anschaffung zahlen, sondern diese wird auf alle Kunden in Form einer Grundgebühr umgelegt) und haben möglicherweise einen nicht zu vernachlässigenden Eigenverbrauch. Ebenfalls werden durch tageszeitabhängige Tarife unflexible Kunden benachteiligt, die nicht die Zeit haben, zu günstigen Tarifen Strom zu verbrauchen und somit mit deutlich höheren Stromkosten rechnen müssen. Zusätzlich ist für die Übermittlung der Verbrauchsdaten eine Internetverbindung nötig, die - falls nicht bereits vorhanden - weitere Kosten verursacht. Eine weitere Gefahr besteht auch darin, dass der Stromversorger nun die Möglichkeit erhalten könnte, die Stromversorgung des Nutzer abzuschalten, falls dieser seine Rechnungen nicht bezahlt.

Das aus Sicht der Informatik interessanteste Problem ist jedoch, dass die Privatsphäre der Kunden in Gefahr ist, wenn die Datenübertragung ungesichert oder in zu kurzen Abständen erfolgt und Stromanbieter somit Details über Lebensgewohnheiten ihrer Kunden erfahren, die nicht öffentlich werden sollten. Diese Gefahren werden im folgenden Kapitel erörtert. Kapitel 2 beschreibt, wie Smart Meter mit den Stromverbrauchern im Haushalt und mit dem Internet verbunden sind. Anschließend wird auf die internationale Umsetzung von Smart Metern eingegangen. In Kapitel 4 werden zuerst die Anforderungen an Übertragungsprotokolle definiert und anschließend Protokolle vorgestellt, die sowohl eine regelmäßige Rechnungsstellung als auch eine Lastermittlung ermöglichen, ohne die Privatsphäre der Kunden

doi: 10.2313/NET-2012-04-1_4

zu gefährden.

1.2 Mögliche Gefahren für die Privatsphäre

Wenn von einer unverschlüsselten Übertragung des aktuellen Stands des Stromzählers ausgegangen wird, hängen die Inferenzmöglichkeiten von der Häufigkeit der Übertragung ab: Wird der Zählerstand täglich übertragen, so kann der Energieversorger (oder mögliche Einbrecher, die die Datenübertragung des Smart Meters abfangen) erkennen, ob der Nutzer an diesem Tag zu Hause war. Falls der Nutzer eventuell mehrere Tage abwesend war, könnte ein Einbrecher darauf schließen, dass das potentielle Opfer im Urlaub ist und wahrscheinlich auch am folgenden Tag nicht zu Hause sein wird. Wenn die Messungen häufiger, also zum Beispiel stündlich oder sogar viertelstündlich erfolgen, kann man die Lebensgewohnheiten der Kunden erkennen. Beispielsweise ist anhand der Verbrauchsdaten ersichtlich, wann ein Nutzer aufsteht, wann er in die Arbeit fährt und wann er wieder nach Hause kommt, oder auch wie viele Personen im Haushalt leben. Letzteres ist insbesondere dann möglich, wenn nicht nur der Strom-, sondern auch Wasser- und Gas-/Fernwärmeverbrauch übertragen wird. Bei sekündlicher Messung können Details über die aktuelle Tätigkeit des Kunden ermittelt werden. So lässt sich beispielsweise durch die unterschiedliche Leistungsaufnahme des Fernsehers in Abhängigkeit der Bildschirmhelligkeit sogar der aktuelle Fernsehsender des Kunden ermitteln [11]. Unabhängig von der genauen Übertragungshäufigkeit (so lange die Übermittlung zumindest täglich stattfindet), sind auch langfristige Analysen des Stromverbrauchs des Kunden möglich [7]. So kann beispielsweise gezielte Werbung geschaltet werden, wenn der Kühlschrank des Kunden älter wird und somit zunehmend ineffizient arbeitet, oder wenn ein Haushalt einen hohen Standby-Verbrauch besitzt.

2. INFRASTRUKTUR IM HAUSHALT

In diesem Kapitel wird kurz auf die Infrastruktur des Smart-Meters im Haushalt eingegangen (siehe Abbildung 1) [3]: Das Gateway stellt die zentrale Kommunikationseinheit der Infrastruktur dar. Es verbindet ein oder mehrere Smart Meter im Lokalen Metrologischen Netz (LMN) mit dem Internet (WAN). Ebenfalls sind Energieverbraucher aus dem Haushaltsnetzwerk (Home Area Network, HAN) angeschlossen. In Mehrfamilienhäusern stellen Gateways Knoten dar, die die Verbrauchdaten der einzelnen Smart Meter regelmäßig verschlüsselt übermittelt bekommen und diese signiert im eigenen Speicher ablegen. Anschließend werden diese Daten vom Gateway an den Stromversorger übermittelt. Zusätzlich muss das Gateway sicherstellen, dass nur berechtigte Zugriffe von außen auf Daten des/der Smart Meters zugelassen werden. Diese Darstellung stellt nur die logische Sicht dar, in Einfamilienhäusern können Smart Meter durchaus auch direkt in das Gateway eingebaut werden. Deswegen wird im Weiteren nicht mehr zwischen den Aufgaben des Gateways und des Smart Meters unterschieden, sondern es wird davon ausgegangen, dass ein Gerät, das „Smart Meter“, die genannten Funktionen beinhaltet.
Zusätzlich ist denkbar, dass wichtige oder sicherheitskritische Stromverbraucher, wie Außenbeleuchtung, Rollos, Herd oder Backofen mit dem Gateway verbunden sind, so dass der Stromkunde diese von der Ferne aus steuern kann. Diese Vernetzung wird als Smart Living oder intelligentes Wohnen bezeichnet. Es wird allerdings in dieser Arbeit nicht genauer darauf eingegangen, da die Steuerung der Hausgeräte im Allgemeinen nicht zu Smart Metering gezählt wird.

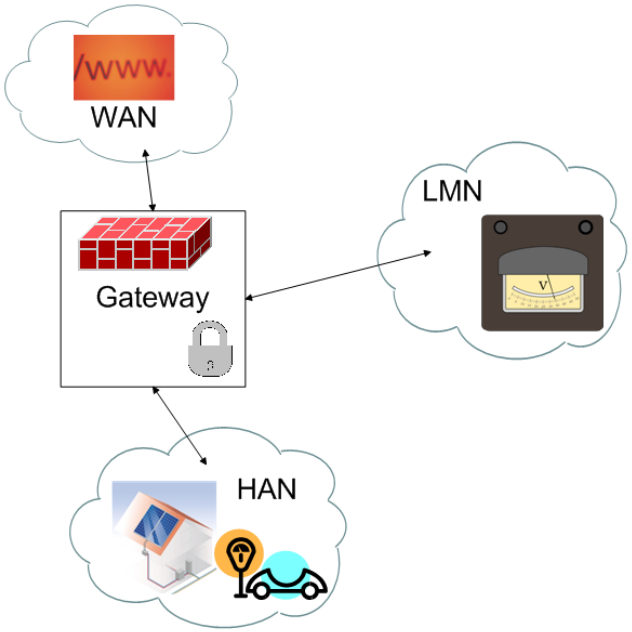

Abbildung 1: Infrastruktur der Smart Meter (LWN), des Gateways, der Verbraucher (HAN) im Haushalt nach [3]

3. INTERNATIONALE UMSETZUNG

3.1 Gesetzliche Vorgaben in der EU/Deutschland

Die Rahmenbedingungen für den Einsatz von intelligenten Stromnetzen beziehungsweise intelligenten Stromzählern sind in der EU-Richtlinie 2006/32/EG festgelegt. Ziel dieser Richtline war es, Anreize zu schaffen, um den Energieverbrauch der Mitgliedsstaaten mittelfristig um 20% zu senken. In Bezug auf intelligente Stromzähler enthält sie folgenden Abschnitt:
„Soweit es technisch machbar, finanziell vertretbar und im Vergleich zu den potenziellen Energieeinsparungen angemessen ist, stellen die Mitgliedstaaten sicher, dass, alle Endkunden in den Bereichen Strom, Erdgas, Fernheizung und/oder -kühlung und Warmbrauchwasser individuelle Zähler zu wettbewerbsorientierten Preisen erhalten, die den tatsächlichen Energieverbrauch des Endkunden und die tatsächliche Nutzungszeit widerspiegeln.“[1]
Ebenfalls ist vorgegeben, dass intelligente Stromzähler für Neubauten und Totalsanierungen verpflichtend sind. Dies wurde in Deutschland im Energiewirtschaftsgesetz (EnWG) umgesetzt. So ist der Netzbetreiber hierzulande seit Anfang 2010 für den Einbau einer „Mindestlösung“ zuständig, in der keine Funktion der Fernübertragung des aktuellen Stromverbrauchs eingebaut ist. Dieses Messgerät kann somit nur den Stromverbrauch aufzeichnen und ermöglicht dem Stromkunden einen Überblick über den eigenen Stromverbrauch. Der Entwurf der Europäischen Kommission für eine neue

[1]RICHTLINIE 2006/32/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 5. April 2006 über Endenergieeffizienz und Energiedienstleistungen und zur Aufhebung der Richtlinie 93/76/EWG des Rates

doi: 10.2313/NET-2012-04-1_4

Energieeffizienzrichtlinie sieht vor, dass spätestens bis zum 01.01.2015 der Stromverbrauch monatlich nach tatsächlichem Verbrauch abgerechnet wird[2].
Für den Datenschutz ist die EG-Datenschutzrichtlinie 95/46/EG anwendbar, die Vorgaben hinsichtlich der Verarbeitung personenbezogener Daten festlegt. Genauere Vorgaben in Bezug auf die Nutzung personenbezogener Daten im intelligenten Stromnetz sind im Energiewirtschaftsgesetz vorhanden[3]: So dürfen unter anderem nur personenbezogene Daten von berechtigten Stellen erhoben, verarbeitet und genutzt werden, um beispielsweise den Energieverbrauch und die Einspeisemenge zu messen und abzurechnen, oder um variable Tarife umzusetzen. Diese Stellen müssen Anforderungen aus §4a des Bundesdatenschutzgesetzes genügen.

3.2 Verlauf in den Niederlanden

In den Niederlanden schlug die Regierung im Jahr 2007 vor, dass alle Haushalte bis 2013 einen intelligenten Stromzähler erhalten müssen. Die niederländische Wirtschaftsministerin plante sogar, alle Hausbesitzer, die keinen solchen Zähler einbauen wollen, mit einer Geldstrafe von 17.000 Euro oder einer sechsmonatigen Gefängnisstrafe zu belegen [2]. Im weiteren Verlauf traten Verzögerungen auf, weil diese Messgeräte zum damaligen Zeitpunkt keine ausreichenden Möglichkeiten boten, eigene Stromproduktion (zum Beispiel durch Photovoltaik) abzurechnen. Im Jahr 2009 wurde - hauptsächlich wegen möglicher Gefahren für die Privatsphäre - die Einführung von intelligenten Stromzählern nur noch auf freiwilliger Basis beschlossen.

3.3 Aktuelle Smart-Metering-Tarife in Deutschland

In Deutschland bieten aktuell mehrere Energieversorger Tarife mit Smart-Metern an. In diesem Kapitel wird auf den aktuellen Stand der drei größten Energieversorger E.ON, RWE und EnBW eingegangen: Bei E.ON wird derzeit der Tarif E.ON EnergieNavi beworben, bei dem Nacht- und Tagstrom zu unterschiedlichen Preisen verkauft wird. Ebenfalls erhalten Kunden die Möglichkeit, den eigenen Stromverbrauch über ein Webportal in einer Auflösung von bis zu fünfzehn Minuten zu betrachten [5]. Bei RWE wird aktuell kein solcher Tarif angeboten, aber die Möglichkeiten von Smart Metering im Rahmen eines Pilotprojekts erforscht, bei dem eine Fernabfrage des Zählerstands durch den Versorger vorgesehen ist [12]. EnBW bietet ebenfalls einen intelligenten Stromzähler in Verbindung mit einem Tarif an, der nachts und am Wochenende vergünstigte Preise für verbrauchten Strom bietet. Die Kunden können sich den eigenen Stromverbrauch ebenso über ein Webportal ansehen [1]. Somit besteht bei allen drei Versorgern grundsätzlich das Risiko, dass mögliche Angreifer den Stromverbrauch des Kunden detailliert erfahren. Weniger komfortabel, aber deutlich sicherer wäre es, wenn nur der für Abrechnungszwecke benötigte Energieverbrauch an den Versorger übermittelt wird und die Analyse des eigenen Stromverbrauchs nur aus dem eigenen Netzwerk heraus möglich ist. Daten zur Lastermittlung des Stromnetzes sollten nur in anonymisierter Form durch sichere Protokolle übertragen werden. Die Anforderungen an derartige Übertragungsprotokolle werden im folgenden Kapitel erläutert.

[2]RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Energieeffizienz vom 22.06.2011
[3]Energiewirtschaftsgesetz (EnWG) vom 7. Juli 2005, §21g

Tabelle 1: Notation der Protokolle

Notation	Bedeutung
$A \rightarrow B : m$	Nachricht von A an B mit Inhalt m
$\{m\}_A$	Nachricht m von A verschlüsselt
$[m]_A$	Nachricht m von A signiert

4. PROTOKOLLE

4.1 Anforderungen an den Datenschutz

Die Anforderungen an den Datenschutz bei der Erhebung von Smart Meter Daten zu Lastüberwachungszwecken sind in [9] zusammengefasst: Bei der Übertragung der Daten an Energieversorger oder Netzbetreiber muss die Anonymität des einzelnen Kunden gewahrt bleiben, so dass keine Aussagen über die Lebensgewohnheiten des Verbrauchers möglich sind, jedoch müssen Abrechnungsdaten eindeutig einem Smart Meter zugeordnet werden können. Ebenfalls soll die Unverknüpfbarkeit von Datenpaketen gewährleistet sein, damit Pakete des gleichen Smart Meter, die zu unterschiedlichen Zeitpunkten gesendet werden, nicht miteinander verknüpft werden können. Es soll somit bei der Datenübertragung zur Lastübermittlung nicht möglich sein, auf den Verbrauch des einzelnen Kunden zu schließen. Die Daten müssen zusätzlich authentisch sein. Der Netzbetreiber muss erkennen, ob Verbrauchsdaten von nicht-registrierten Smart Metern stammen. Das Entfernen von Smart Metern (und damit das Abweisen von zukünftigen Datenpaketen) muss einfach möglich sein. Spamming- und Replay-Angriffe[4] sind zu verhindern und die Daten müssen weitgehend verzögerungsfrei (beziehungsweise im Zeitraum von wenigen Minuten) übertragen werden können. Wenn möglich, soll auf keine dritte Partei (Trusted Third Party) zurückgegriffen werden, da dies einen höheren Aufwand erfordern würde und eventuell negative Auswirkungen auf die Sicherheit hätte.
Für Abrechnungszwecke sollten grundsätzlich nur die Daten übertragen werden, die der Energieversorger für die Rechnungsstellung benötigt. Wenn das Abrechnungsintervall groß genug (also zum Beispiel monatlich) gewählt ist, bestehen - bei verschlüsselter und signierter Datenübertragung - keine Gefahren für die Privatsphäre.
Im Anschluss werden zwei Protokolle in Anlehnung an [7] vorgestellt, die die Übertragung von Informationen zu Abrechnungs-, aber auch zu Laststeuerungszwecken ermöglichen, jedoch beide noch nicht in aktuellen Messgeräten verwendet werden. Das grundlegende Protokoll berücksichtigt dabei nicht den Datenschutz gegenüber dem Versorger, sondern nur die Authentizität der übermittelten Daten und ist damit ausschließlich zu Abrechnungszwecken geeignet. Die Notation der Protokolle ist in Tabelle 1 dargestellt.

4.2 Grundlegendes Protokoll

Am grundlegenden Protokoll sind drei Parteien beteiligt:

- Netzbetreiber GO

[4]Bei einem Replay-Angriff spielt ein Angreifer einmal abgefangene Daten zu einem späteren Zeitpunkt erneut ein, um somit eine fremde Identität vorzutäuschen.

doi: 10.2313/NET-2012-04-1_4

- Versorger S
- Smart-Meter M

Vor Beginn des eigentlichen Protokolls besitzt das Smart-Meter bereits den öffentlichen Schlüssel des Netzbetreibers (GO) und den öffentlichen Schlüssel der Zertifizierungsstelle. Der Netzbetreiber besitzt den öffentlichen Schlüssel des Smart-Meters. Das grundlegende Protokoll besteht insgesamt aus drei Unterprotokollen. In set_supplier wird dem Smart Meter der zuständige Versorger mitgeteilt, switch_power ermöglicht dem Netzbetreiber die Stromversorgung des Kunden einzuschränken und meter_report sendet den aktuellen Zählerstand des Smart Meters an den Stromversorger. In set_supplier wird dem Smart-Meter vom Netzbetreiber mitgeteilt, wer der zuständige Versorger (S) ist. Zusätzlich wird dem Smart-Meter der öffentliche Schlüssel des Versorgers übermittelt (pk_S), der Zeitpunkt (ts) festgelegt, zu dem der neue Versorger aktiv wird und das Abrechnungsintervall mitgesendet (P):

1. GO → M: hi, init set_supplier
2. M → GO: nonce n
3. GO → M: $\{[\text{set\_supplier, M, n, S, } pk_S\text{, ts, P}]_{GO}\}_M$

Das Smart-Meter kann nun die Nachricht mit dem eigenen privaten Schlüssel entschlüsseln und die Signatur der Nachricht mit dem öffentlichen Schlüssel des Netzbetreibers und die Zufallszahl n verifizieren. Falls dies erfolgreich ist, wird der neue Versorger eingetragen.

Wenn der Netzbetreiber (GO) Wartungsarbeiten am Netz durchführt oder der Kunde seine Rechnungen nicht bezahlt, wird das switch_power Protokoll ausgeführt, das es dem Netzbetreiber ermöglicht, einen Kunden teilweise oder vollständig vom Netz zu trennen. power liegt im Intervall zwischen 0 und 1 steht für den Anteil der maximalen Stromaufnahme, die das Smart-Meter dem Netz entnehmen darf, wobei 0 eine vollständige Netztrennung darstellt und 1 den normalen Modus repräsentiert. ts repräsentiert den Zeitpunkt, zu dem die Stromverbrauchsvorgabe aktiv wird. Die Vorgehensweise ist identisch zum vorhergehenden Protokoll:

1. GO → M: hi, init switch_power
2. M → GO: nonce n
3. GO → M: $\{[\text{switch\_power, M, n, ts, power}]_{GO}\}_M$

Wiederum entschlüsselt das Smart-Meter die Nachricht und überprüft die Signatur und die Zufallszahl n. Bei erfolgreicher Verifikation wird die Änderung umgesetzt.

Der letzte Nachrichtentyp stellt die Übertragung der Verbrauchsdaten an den Versorger (S) dar (meter_report). Meter readings entspricht dem aktuellen Zählerstand des Smart Meters, time der aktuellen Uhrzeit.

1. M → S: $\{[\text{M,time, meter readings}]_M\}_S$

Dieses grundlegende Protokoll stellt die Integrität und Verbindlichkeit der übertragenen Daten sicher, da durch Verwendung von digitalen Signaturen mögliche Veränderungen an den Daten erkannt werden und die Nachrichten an jedes Smart-Meter gebunden sind. Ebenfalls ist die Vertraulichkeit sichergestellt, da alle relevanten Informationen verschlüsselt werden und somit nur vom Empfänger entschlüsselt werden können. Ein Schutz vor Replay-Attacken ist zusätzlich gegeben, da durch die Zufallszahl (nonce) n jeweils unterschiedliche Nachrichten übermittelt werden. Der Datenschutz ist allerdings nicht sichergestellt, da der Versorger (bei zu gering gewählten Update-Intervallen) die in Kapitel 1.2 vorgestellten Rückschlüsse auf das Verhalten des Nutzers ziehen kann. Bei einheitlichen Tarifen und ausreichend groß gewählten Abrechnungszeiträumen (zum Beispiel monatlicher Rechnungsstellung) ist das Protokoll allerdings ausreichend. Falls jedoch tageszeitabhängige Tarife angeboten werden, so darf nicht der Verbrauch jeder einzelnen Tarifeinheit übermittelt werden, da dadurch wiederum Rückschlüsse auf das individuelle Verhalten des Nutzers möglich sind. So kann beispielsweise ermittelt werden, dass ein Nutzer zur Mittagszeit sehr wenig Strom benötigt und daraus geschlossen werden, dass er berufstätig ist und zu dieser Zeit das Haus verlassen ist. Das Protokoll sollte deshalb um weitere Nachrichten ergänzt werden, so dass der Energieversorger dem Smart Meter die aktuellen Preise pro Kilowattstunde (abhängig von der Tageszeit) mitteilen kann und das Smart Meter am Ende des Abrechnungszeitraums (zum Beispiel monatlich) die Gesamtkosten des Haushalts übermittelt.
Im folgenden Kapitel wird eine Erweiterung des Protokolls eingeführt, so dass auch die Abrechnung des Verbrauchs bei tageszeitabhängigen Stromtarifen möglich ist.

4.3 Grundlegendes Protokoll (erweitert)

Das grundlegende Protokoll wird um einen weiteren Protokollschritt (set_tariff) erweitert, in dem der aktuelle Energieversorger (S) dem Smart Meter (M) die aktuelle Tarifstruktur (tariff) und den Beginn der Gültigkeit (ts) mitteilt, damit nach Ablauf des Abrechnungsintervalls (P) die Kosten vom Smart Meter übermittelt werden können:

1. S → M: hi, init set_tariff
2. M → S: nonce n
3. S → M: $\{[\text{set\_tariff, M, n, S, tariff, ts, P}]_S\}_M$

Beim Empfang dieser Nachricht muss wiederum das Smart Meter überprüfen, ob die Signatur korrekt ist. Nur bei erfolgreicher Prüfung wird der neue Tarif angenommen und

doi: 10.2313/NET-2012-04-1_4

der Stromverbrauch des Haushalts entsprechend überwacht. Zusätzlich die wird die Übertragung des Verbrauchs (meter_report) angepasst, so dass nun nicht der Zählerstand übertragen wird, sondern die Kosten des angefallenen Stromverbrauchs (priced_meter_readings):

1. M $\rightarrow$ S: $\{$[M,time, priced_meter_readings]$_{\mathrm{M}}\}_{\mathrm{S}}$

Somit erfüllt das Protokoll alle Anforderungen für Abrechnungszwecke. Sämtliche Nachrichten sind digital signiert und verschlüsselt, somit ist sowohl die Integrität als auch die Authentizität sichergestellt und die Daten sind ohne Kenntnis des Schlüssels nicht zu entschlüsseln. Für die Lastermittlung ist ein solches Protokoll aber nicht geeignet, da alle Nachrichten des Smart Meters direkt dem Haushalt zuordenbar sind. Um eine Lastermittlung des Netzes bei gleichzeitigem Schutz der Privatsphäre zu ermöglichen, wird im folgenden Kapitel das No-Leakage Protokoll vorgestellt.

4.4 No-Leakage Protokoll

Das No-Leakage Protokoll ist nur zur Überwachung der Netzlast geeignet und geht davon aus, dass N (üblicherweise circa 100) Haushalte an einer Zwischenstation (SST) angeschlossen sind, die den Gesamtverbrauch dieser Haushalte erfasst (siehe Abbildung 2) und an den Netzbetreiber weiterleitet. Im Gegensatz zu einer ausschließlichen direkten Messung bei der Zwischenstation bietet es den Vorteil, dass dadurch erkannt werden kann, ob dem Stromnetz unbemerkt Strom entnommen wird. Falls der Netzbetreiber darauf verzichtet, wäre es auch denkbar, dass der Netzbetreiber spezielle Smart Meter bei jedem N-ten Kunden einbaut, die dann die Funktion der Zwischenstation übernehmen. Somit müsste der Netzbetreiber keine eigene Messstellen mehr betreiben. Damit könnte jedoch eine unbemerkte Stromentnahme nicht mehr entdeckt beziehungsweise lokalisiert werden.
Im No-Leakage Protokoll melden die Smart-Meter aller Haushalte ihren Verbrauch ($\mathrm{m_i}$) gleichzeitig in regelmäßigen Abständen an diese Zwischenstation. Zur Verschlüsselung der Daten wird ein additiv-homomorphes Kryptosystem verwendet, das eine asymmetrische Verschlüsselung verwendet. Somit gilt Folgendes:

$$\{\mathrm{m_1}\}_{\mathrm{k}} * \{\mathrm{m_2}\}_{\mathrm{k}} = \{\mathrm{m_1} + \mathrm{m_2}\}_{\mathrm{k}}$$

Die Multiplikation zweier mit dem gleichen öffentlichen Schlüssel verschlüsselter Nachrichten entspricht also der Addition der beiden Klartexte (in dem Fall Stromverbräuche) und der anschließenden Verschlüsselung der Nachrichten. Das Paillier Kryptosystem besitzt beispielsweise diese Eigenschaften [10]. Zu Beginn des No-Leakage Protokolls verschickt die Zwischenstation die Zertifikate aller teilnehmenden Meter an alle Meter (1). Anschließend werden von jedem Meter N Zufallszahlen so gewählt, dass die Summe der Zufallszahlen (Modulo n, wobei n groß genug gewählt wird) dem eigenen Verbrauch in diesem Zeitraum entspricht. N-1 Zufallszahlen werden mit den N-1 öffentlichen Schlüsseln der restlichen beteiligten Smart-Metern verschlüsselt und an die Zwischenstation geschickt (2). Die Zwischenstation multipliziert die Nachrichten mit identischen Schlüsseln und versendet das Ergebnis an diejenige Station, die den privaten Schlüssel für die jeweilige Nachricht besitzt (3). Nun entschlüsselt jede Station die Nachricht und addiert die noch nicht versendete Zufallszahl auf die Nachricht und sendet das Ergebnis in Klartext an die Zwischenstation (4), die nun überprüfen kann, ob der übermittelte Gesamtverbrauch dem selbst gemessen Gesamtverbrauch entspricht. Der Ablauf des Protokolls ist im Folgenden dargestellt:

1. SST $\rightarrow$ $\mathrm{M_i}$: no-leakage, $\mathrm{cert_{M_1}}$,...,$\mathrm{cert_{M_N}}$
2. $\mathrm{M_i}$ $\rightarrow$ SST: $\mathrm{y_{i1}}$,...,$\mathrm{y_{ii-1}}$,$\mathrm{y_{ii+1}}$,...,$\mathrm{y_{iN}}$
   wobei $\mathrm{M_i}$ Zufallszahlen $\mathrm{a_{i1}}$,...,$\mathrm{a_{iN}}$ wählt,
   so dass $\mathrm{m_i} = \sum_{\mathrm{j=1}}^{\mathrm{N}} \mathrm{a_{ij}} \bmod n$
   mit $\mathrm{y_{ij}} := \{\mathrm{a_{ij}}\}_{\mathrm{pk_j}}$ und $\mathrm{j} \in \{\ \mathrm{j} \in [\mathrm{N}] \mid \mathrm{j} \neq \mathrm{i}\ \}$
3. SST $\rightarrow$ $\mathrm{M_i}$: $\prod_{j \in \{j \in [N] | j \neq i\}} y_{ji} = \left\{ \sum_{j \in \{j \in [N] | j \neq i\}} a_{ji} \right\}_{pk_i}$
4. $\mathrm{M_i}$ $\rightarrow$ SST:
   $$\sum_{j \in \{j \in [N] | j \neq i\}} a_{ji} + a_{ii} = \sum_{j} a_{ji} \bmod n$$

Insgesamt werden dabei 4N Nachrichten verschickt (in jedem Schritt N Nachrichten). Die Zwischenstation kann nicht auf den Verbrauch einzelner Haushalte schließen, da sie nur Summen des Verbrauchs aller beteiligten Haushalte unverschlüsselt übermittelt bekommt. Es kann sogar gezeigt werden, dass ein Angreifer nicht einmal die Vertauschung des Stromverbrauchs zweier beliebiger Haushalte erkennen kann. Somit kann mit Sicherheit auch nicht auf den Verbrauch einzelner Haushalte geschlossen werden. Das Protokoll ist dann sicher, wenn sich zumindest zwei Haushalte nach der Protokollspezifikation verhalten. Wenn ein Angreifer beispielsweise den Gesamtverbrauch und den Verbrauch von allen bis auf einen Haushalt kennt, kann er trivialerweise den Verbrauch des verbleibenden Haushalts ermitteln, in dem er die Verbräuche der bekannten Haushalte vom Gesamtverbrauch subtrahiert. Da N jedoch in der Größenordnung von 100 liegen sollte, stellt dies keine größere Gefahr dar. Ebenfalls geht das Protokoll davon aus, dass kein Angreifer eine große Anzahl an privaten Schlüsseln der verwendeten Zertifikate ermitteln kann. Diese Annahme wird jedoch bei allen Protokollen getroffen, die auf asymmetrischer Verschlüsselung in Form von Zertifikaten basieren und stellt somit keine Einschränkung dar, so lange in der Implementierung darauf geachtet wird, dass ausreichend lange Schlüssel (>2048 Bit) verwendet werden und/oder die Schlüssel regelmäßig erneuert werden.

5. ZUSAMMENFASSUNG

Insgesamt existieren, wie in Kapitel 4 gezeigt, Möglichkeiten, um den Privatsphäre von Nutzern zu schützen. Die Energieversorger können damit sowohl flexible Tarifstrukturen anbieten und haben bei gleichzeitigem Schutz der Privatsphäre der Nutzer die Möglichkeit, die Netzlast zu messen. In aktuellen Geräten sind diese Funktionen bislang noch nicht implementiert. So übertragen die in [11] verwendeten Messgeräte die Verbrauchswerte unverschlüsselt und mit Geräte-ID und ermöglichen so einerseits eine Aggregation der Daten für einzelne Benutzer, als auch möglicherweise eine Identifikation der Nutzer und sind damit absolut nicht geeignet, um die Privatsphäre der Verbraucher zu schützen. Auch die

doi: 10.2313/NET-2012-04-1_4

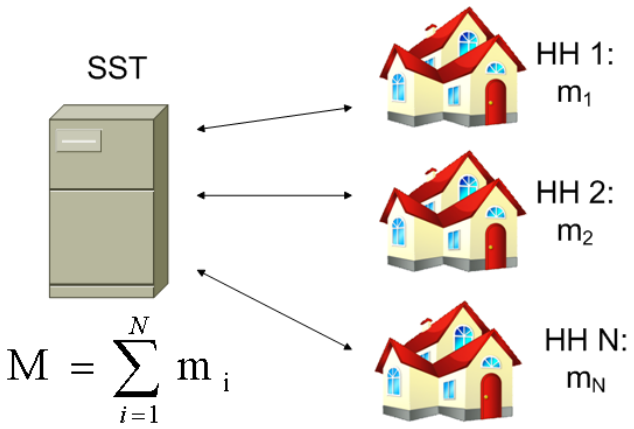

Abbildung 2: Haushalte (HH) melden Stromverbrauch (m_i) an Zwischenstation (SST)

aktuell von den Energieversorgern angebotenen Tarife beinhalten das Risiko, dass detaillierte Verbrauchsdaten durch Angreifer ermittelt werden können, da die Verbrauchsdaten ins Internet übertragen werden, um den Nutzern einen mobilen Zugriff zu ermöglichen. Für besseren Datenschutz wäre es jedoch wünschenswert, wenn eine Abfrage nur innerhalb des eigenen lokalen Netzwerks möglich ist, und somit nicht das Risiko besteht, dass Verbrauchsdaten in fremde Hände geraten. Einen mobilen Abruf könnte man dennoch beispielsweise per VPN realisieren.
Somit spricht aus Sicht des Datenschutzes bei Verwendung sinnvoller Kommunikationsprotokolle zwischen Smart Meter und Netzbetreiber beziehungsweise Stromversorger nichts gegen die Einführung von intelligenten Stromzählern, die den Stromverbrauch (für Abrechnungszwecke und zur Lastermittlung) selbstständig übertragen. Besonders aufgrund der Möglichkeiten, den Zustand des Stromnetzes zu überwachen, ist zu erwarten, dass diese Geräte in naher Zukunft verpflichtend eingeführt werden. Auch bei der ab 2015 vorgeschriebenen monatlichen Abrechnung des Stromverbrauchs auf Grundlage des tatsächlichen Verbrauchs bieten sie für Kunden einen deutlich größeren Komfort, da die Verbrauchsdaten nicht manuell an den Stromversorger übermittelt werden müssen.

6. LITERATUR

[1] Privatkunden - intelligenter stromzähler - faq. Website. http://www.enbw.com/content/de/privatkunden/produkte/zusatzinformationen/isz_faq/index.jsp.

[2] R. Anderson and S. Fuloria. On the Security Economics of Electricity Metering. In *Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS)*, June 2010.

[3] N. T. A. A. Dr. Helge Kreutzmann, Stefan Vollmer. Protection profile for the gateway of a smart metering system. Technical report, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011.

[4] E. Energie. Ex-post daten archiv 2010. http://www.eon-schafft-transparenz.de/download/expost, 2011.

[5] EON. E.on energienavi. Website. https://www.eon.de/de/eonde/pk/produkteUndPreise/Strom/E.ON_Energienavi/index.htm.

[6] O. (France). *Photovoltaic Barometer*. EurObserv'ER, 2011.

[7] F. D. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption. In J. C. et al., editor, *6th Workshop on Security and Trust Management (STM 2010)*, volume 6710 of *Lecture Notes in Computer Science*, pages 226–238. Springer Verlag, 2010.

[8] J. Hladjk. Smart metering und eu-datenschutzrecht. *Datenschutz und Datensicherheit - DuD*, 35:552–557, 2011. 10.1007/s11623-011-0136-5.

[9] T. Jeske. Datenschutzfreundliches smart metering. *Datenschutz und Datensicherheit - DuD*, 35:530–534, 2011. 10.1007/s11623-011-0132-9.

[10] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT*, pages 223–238, 1999.

[11] D. L. M. Prof. Dr.-Ing U. Greveler, Dr. B. Justus. Hintergrund und experimentelle ergebnisse zum thema smart meter und datenschutz. Technical report, Labor für IT-Sicherheit der FH Münster, 2011.

[12] RWE. Smart meter - inteligente mess- und zähltechnik von morgen. Website. http://www.rwe.com/web/cms/de/238130/rwe/innovationen/energieanwendung/smart-meter/.

doi: 10.2313/NET-2012-04-1_4