High Performance and Privacy for Distributed Energy Management: Introducing PrivADE$^+$ and PPPM

Daniel Brettschneider, Daniel Hölker and Ralf Tönjes
University of Applied Sciences Osnabrück, Osnabrück, Germany

Keywords: Distributed Energy Management, Smart Grid, Privacy, Communication Performance, Robustness.

Abstract: Distributed Energy Management (DEM) will play a vital role in future smart grids. An important and often overlooked factor in this concept is privacy. This paper presents two privacy-preserving DEM algorithms called PrivADE$^+$ and PPPM. PrivADE$^+$ uses a round-based energy management procedure for switchable and dynamically adaptable loads. PPPM utilises on the market-based PowerMatcher approach. Both algorithms apply homomorphic encryption to privately gather aggregated data and exchange commands. Simulations show that PrivADE$^+$ and PPPM achieve good energy management quality with low communication requirements and without negative influences on robustness.

1 INTRODUCTION

Future concepts envision the smart power grid as a distributed system of manifold stakeholders. Integrating communication technology into the former static power grid provides interconnectivity. In such a scenario, the smart grid can be understood as an Internet of Energy, where many varying devices and participants distribute and communicate their capabilities and resources. Understanding and implementing the smart grid as such a distributed system or Internet of Energy will lead to Distributed Energy Management (DEM), which will enhance and stabilise energy consumption and generation for an increasing share of renewable energy sources.

Often overlooked factors in DEM are communication performance and privacy. Despite performing high-quality energy management, a DEM algorithm might require a high data rate or extensive data volume. Thus, in DEM an additional key performance is the distributed systems aspect. Many participants work together to reach a high-quality energy management and rely on fast convergence times, minimum latencies, low computational requirements, as well as robustness.

Furthermore, privacy will play a vital role in future DEM systems. A DEM algorithm relies on extensive information flows, which might even be available to all participants in the system. Thus, everyone is capable of tracking consumption profiles or device states of others in detail. Preserving privacy resembles another key performance indicator.

In summary, the key performance indicators are energy management quality, communication performance, computation performance, robustness and privacy.

The remainder of the paper is structured as follows: section 2 shows the related work. Section 3 presents the main objectives of the paper. A detailed description of PrivADE$^+$ is given in section 4. Section 5 shows PowerMatcher and describes a new privacy preserving approach for this algorithm. Both algorithms will be evaluated in section 6. Finally, section 7 concludes the paper.

2 RELATED WORK

Energy management in smart grids resembles a well-investigated topic. However, most of them focus on energy management. This section highlights a few examples regarding the stated performance indicators.

Hinrichs et al. present COHDA (Hinrichs et al., 2013), a heuristic for distributed agents. These agents exchange consumption profiles to perform day-ahead load scheduling. The consumption profiles find their way to all participants through a small world topology and the agents adapt their loads accordingly while distributing adapted profiles. The heuristic leads to equilibrium state. The communication aspects are only described roughly and the massive information ex-

Brettschneider, D., Hölker, D. and Tönjes, R.
High Performance and Privacy for Distributed Energy Management: Introducing PrivADE$^+$ and PPPM.
In *Proceedings of the 7th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2018)*, pages 182-189
ISBN: 978-989-758-292-9

change impacts privacy.

Kok et al. describe PowerMatcher (Kok et al., 2005), a multi-agent system for market-based supply demand matching. Device agents generate bids (energy price / planned consumption) which are gathered by an auctioneer agents, who determines the equilibrium energy price. The authors evaluate communication aspects, but do not show simulations with specific technologies. Furthermore, privacy is not analysed in the publication.

In (Brettschneider et al., 2017) the authors of this paper present PrivADE, a previous version of the algorithm presented in this paper. Households are arranged in a ring overlay network and privately manage shiftable, switchable and adaptable devices based on a round-based algorithm and homomorphic encryption. However, the ring overlay network is prone to latency and robustness issues.

Mohsenian-Rad et al. introduce a DEM algorithm based on game theory in (Mohsenian-Rad et al., 2010). At random times a player optimises its own consumption schedule based on all available information and broadcasts an improved result to all other players. The authors evaluate the algorithm using a Local Area Network. However, a smart grid typically resembles a Wide Area Network.

3 OBJECTIVES

In conclusion, most papers regarding DEM miss out on one or more key performance indicators. Thus, this paper introduces PrivADE$^+$, a DEM algorithm which specifically not only focusses on energy management quality, but also communication performance, computation performance, robustness and privacy. It is compared and evaluated against the well-known PowerMatcher (Kok et al., 2005). Furthermore, the privacy scheme of PrivADE$^+$ is also applied to PowerMatcher.

4 PRIVADE$^+$

The Privacy-Preserving Algorithm for Distributed Energy Management (PrivADE$^+$) (Brettschneider, 2017) has been developed with the objective of protecting the privacy of its users without reducing energy management capabilities. Taking a look at the loads in the smart grid, four main types can be identified: First, the base load, consisting of, for example, lighting and stoves, cannot be influenced. Second, activation times of shiftable loads, for example, washing machines and driers, might be shifted to a later time. Third, switchable loads, for example, Heatpumps (HPs) and Micro Combined Heat and Power Systems (μCHPs), might be switched on or off entirely depending on their state. Fourth, adaptable loads, for example, Battery Storages (BSs) and Electric Vehicles (EVs), offer dynamic adaptation of their charge rates and might even feed into the power grid.

Thus, PrivADE$^+$ offers energy management for shiftable, switchable, and adaptable loads while additionally applying a privacy scheme, which are explained in the following sections.

4.1 Load Shifting

The algorithm for load shifting shifts the activation of a device to a later point in time. Imagine a drier being filled at 8 a.m. and turned on before going to work. A deadline is defined at 5 p.m., so that it must have finished its cycle after returning from work. The algorithm computes the optimal activation times of all devices with the stated constraints.

Taking a closer look, two problems arise. First, finding an optimal schedule for several devices is a NP-hard problem. Second, shifting an activation requires knowledge of future behaviour. Thus, in a distributed approach participants have to exchange a lot of information, for example a minute-based planned consumption of the next 24 hours. To reduce the complexity, a stochastic approach has been chosen, which achieves similar energy management quality, see (Brettschneider, 2017).

Initially, the expected future consumption $e(t)$ is distributed to all households $h \in H$. It can consist of, for example, a standard load profile. If a household h wants to shift a device $d \in D$, it defines an activation time t_a, where the device is switched on, and a deadline t_e, where it must have finished its cycle. The device runs for a duration t_d with the load $l(t,t'_a)$. A load barrier $b(t)$ represents the energy management target. All possible activation times t'_a are stored in the set

$$T_a = \{t'_a \in \mathbb{N} | t_a \leq t'_a \leq t_e - t_d\}. \tag{1}$$

To determine the cost of an activation the function

$$c(t,t'_a) = \begin{cases} e(t)+l(t,t'_a), \text{if } e(t)+l(t,t'_a) \leq b(t) \\ b(t)+f\cdot(e(t)+l(t,t'_a)-b(t)), \text{else,} \end{cases} \tag{2}$$

is defined, where exceeding the barrier $b(t)$ is penalised by a factor f. Activation times with a higher cost than the one with the lowest cost

$$c_{\min} = \arg\min_{t'_a} \sum_{t=t_a}^{t_e-t_d} c(t,t'_a) \tag{3}$$

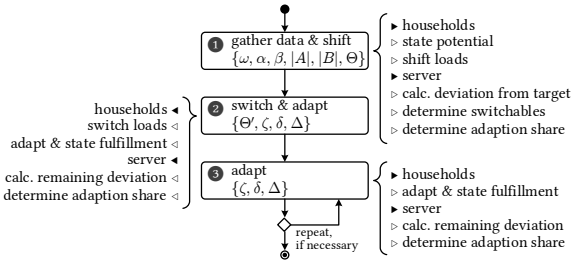

Figure 1: Visualisation of the DEM algorithm.

multiplied with a factor f are excluded, resulting in

$$T_a^* = \{t'_a \in T_a | \sum_{t=t'_a}^{t'_a+t_d} c(t,t'_a) \leq f \cdot c_{\min}\}. \quad (4)$$

Finally, an activation time is randomly chosen among T_a^*. In conclusion, the device has been shifted to a random optimal time-frame without any additional interaction.

4.2 Load Switching and Adaptation

The algorithm for load switching and adaptation combines two approaches in a distributed round-based energy management procedure, see Figure 1 for an overview. It can be applied to, for example, switchable HPs and µCHPs, as well as dynamically adaptable BSs and EVs. If, for example, the energy management target is superseded, the algorithm stimulates either HPs to switch off or µCHPs to switch on, or BSs and EVs to reduce their consumption. In a first round necessary information is gathered and used in the following rounds to fairly distribute the required changes in energy consumption and generation to reach a stated goal.

Switchable devices are arranged in categories $\lambda \in \Lambda$, for example,

$$\{\ldots, -750\,\mathrm{W}, -250\,\mathrm{W}, 250\,\mathrm{W}, 750\,\mathrm{W}, 1250\,\mathrm{W}, \ldots\}. \quad (5)$$

Thus, every category has a specific range, for example $750\,\mathrm{W} \mathrel{\widehat{=}} [500\,\mathrm{W}, 1000\,\mathrm{W})$, and acts as a counter for switchable devices within this consumption range. In combination with priorities $p \in P$ prioritised categories $\theta \in \Theta$ can be formed, where $\Theta := P \times \Lambda$. If a household owns a HP which would consume 900 watts when switched on, it increments the counter in the 750 watts category.

An adaptable device d is classified using three values: It wants to consume ω_d and has the ability to increase its consumption by α_d or to decrease it by β_d. For example, an EV wants to charge its battery using 2 kW, but might increase it by 1 kW or decrease it by 4 kW, thus possibly feeding into the power grid.

The DEM algorithm gathers the potential of households $h \in H$, which are connected the system, in the first round. Thus, a server s, which might also be called energy manager, creates a tree overlay network households as leaves, aggregators a as nodes and the server s as the root node. By using aggregators, the algorithm offers scalability and sets a first cornerstone for privacy. At the beginning of the first round every household h combines its potential in the data packet $\{\omega_h, \alpha_h, \beta_h, |A|_h, |B|_h, \Theta_h\}$, where $|A|$ counts the number of households which can increase their consumption and $|B|$ households which can decrease their consumption. The data packet is sent upwards the tree overlay network to an aggregator, which aggregates all received data packets by adding the counters and forwards the resulting data packet to the next layer in the tree. In the end the server receives the aggregated switching and adaptation potential of all households.

After the first round the server determines whether the energy management target μ is violated. First, switchable loads are managed to keep the deviation from μ in $[\mu - \alpha, \mu + \beta]$. Thus, the remaining deviation can be eliminated by adaptable loads afterwards by increasing (α) or decreasing (β) their consumption. By randomly activating positive or negative categories, depending on whether the consumption is below or above μ, the server increases or decreases the overall consumption ω until $\mu - \alpha$ or $\mu + \beta$ is reached. This results in categories

$$\Theta' \subseteq \Theta, \quad (6)$$

which have to be switched and an adapted overall consumption ω'. In this way the computational complexity is kept low, because finding the optimal solution is an NP-hard problem. The remaining deviation $\nu = \mu - \omega'$ has to be reduced by the adaptable loads. Thus, the server defines a load share

$$\zeta = \begin{cases} \frac{\nu}{|A|}, & \text{if } \nu > 0 \\ \frac{\nu}{|B|}, & \text{else,} \end{cases} \quad (7)$$

for the adaptable households A or B. By broadcasting Θ' and ζ to all households, they can perform the required energy management.

Upon receiving the data packet, a household switches its devices according to Θ'. Additionally, it tries to fulfil the load share ζ by increasing or decreasing its consumption according to the max-min fairness principle. If it can only partially fulfil the share, the residual unfulfilled share δ_h is gathered. Otherwise, remaining adaptation potential is stated by incrementing a counter Δ. All households send this information to the server using the stated procedure. Thus, after the second round, the remaining deviation δ can be further reduced depending on Δ in additional

rounds. This process continues until the consumption observes predefined limits or until no adaptable households remain.

In summary, switchable loads are managed based on categories and adaptable loads are managed fairly using the max-min fairness principle in a distributed round-based energy management algorithm.

4.3 Privacy

Considering privacy, PrivADE+ already achieves a basic level of privacy through aggregation. However, aggregators or internal attackers gain access to private data of distinct households, even if encrypted communication is a prerequisite.

Thus, PrivADE+ utilises a Homomorphic Encryption System (HES) to secure privacy of all participants. To measure the level of privacy, the k-anonymity principle is used. Reaching k-anonymity means, that the information of one household cannot be distinguished from $k-1$ others.

The HES applies the Paillier cryptosystem (Paillier, 1999), which enables homomorphic addition. Additive homomorphic encryption of two plaintexts m_1 and m_2 using an encryption function E and a decryption function D is defined as

$$\mathsf{D}(\mathsf{E}(m_1) \oplus \mathsf{E}(m_2)) = m_1 + m_2, \tag{8}$$

where $\oplus$ denotes the corresponding operation on the ciphertext. The Paillier cryptosystem is chosen because of its efficient encryption and decryption and its low message expansion factor of two. (Fontaine and Galand, 2007)

At the beginning of each round, a household encrypts the data packet with the public key of the server. To reduce the number of required encryptions, all counters are bit-shifted into a single a value before encryption. However, the Paillier cryptosystem does not allow for negative numbers, which is required by ω. Thus, ω is split into a consumption value ω^+ and a generation value ω^-. This results in

$$\begin{aligned} \varepsilon_h = \omega_h^+ \text{ or } \left(\omega_h^- \ll 32\right) \\ \text{or } (\alpha_h \ll 64) \text{ or } (A_h \ll 96) \\ \text{or } (\beta_h \ll 128) \text{ or } (B_h \ll 160) \\ \text{or } (\theta_{h,1} \ll 168) \text{ or } \ldots \\ \text{or } \left(\theta_{h,|\Theta|} \ll (160 + 8 \cdot |\Theta|)\right), \end{aligned} \tag{9}$$

when using 32 bits for consumption counters and 8 bits for switchable categories. Depending on Θ, ε has to be split into blocks, because $m \in \mathbb{Z}_n$. In this case the number of blocks is $\left\lceil \frac{6 \cdot 32 + 8 \cdot |\Theta|}{\upsilon} \right\rceil$, where υ represents the bit-size of n in the Paillier cryptosystem, e.g. 2048 bits. All households $h \in H$ encrypt

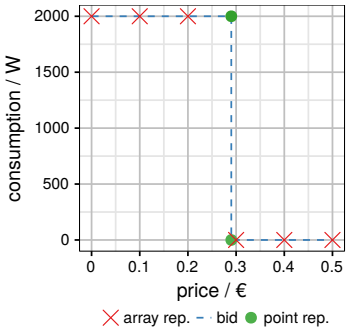

Figure 2: Array and point bid for a heatpump.

ε_h and forward it to an aggregator. The aggregators receive the encrypted data packets and perform the homomorphic aggregation, which is basically a multiplication of the ciphertexts. At the end of a round, the server receives encrypted data packets and can decrypt them using its private key. Thus,

$$\varepsilon_s = \mathsf{D}\left(\left(\mathsf{E}(\varepsilon_0) \cdot \prod_{h \in H} \mathsf{E}(\varepsilon_h)\right) \bmod n^2\right). \tag{10}$$

Because the token is split into υ blocks, υ decryptions have to be performed accordingly. Finally, the server extracts all counters using the appropriate bit-shift operations. Thus, it only gains access to aggregated information of all households.

In summary, households encrypt their data packets using the Paillier cryptosystem, aggregators aggregate the ciphertexts, and the server receives them at the end and decrypts them. In this way households and aggregators do not have access to any plaintext information of other participants. Only the server is capable of decryption and does only gain access to aggregated data. Thus, privacy is preserved. When using a tree overlay network with a single aggregator at the second layer, k-anonymity equals the number of households $|H|$.

5 POWERMATCHER

PowerMatcher (Kok et al., 2005) has been chosen as a comparative DEM algorithm, because of its well-documented behaviour and place in the state of art. It implements a multi agent approach for market-based supply demand matching. Agents form a tree structure and the energy management process can be summarised as follows: Device agents create bids for devices, concentrator agents gather and aggregate these bids, before transmitting them to an auctioneer. The auctioneer determines an optimal energy price according to the energy management target and publishes it.

A device agent represents one device, e.g. a HP or EV, and follows a predefined strategy. The agent

Table 1: Simulation Parameters.

Parameter	Value	Device	Quantity
Households	1 to 100	Basic Devices	all
DEM Function	peak clipping	Photovoltaic Systems	40 %
DEM Target	350 watts per household	Heatpumps	20 %
Simulation Time	1/5/11 to 7/5/11	Electric Vehicles	20 %
Interval	5 minutes	Battery Storages	20 %
Communication Network	Internet-like topology 5 Mbps, 20 ms latency		

creates a bid for the device depending on its current state. Such a point-based bid consists of a validity period t and a flexible list Φ_p with pairs of energy prices ϖ and consumption values ω.

$$\phi_p = \{t, \Phi_p = \{(\varpi, \omega), \dots\}\} \tag{11}$$

Figure 2 shows an exemplary point-based bid of a Heatpump, which is represented as $\Phi_p = \{(0.29€, 2\text{kW}), (0.29€, 0\text{kW})\}$. Finally, the agent sends the bid upwards the tree overlay network to a concentrator agent.

A concentrator agent manages a cluster of device agents or other concentrators. Upon receiving new bids, it aggregates them into a single bid and sends it upwards the tree.

The root node of the tree overlay network is called the auctioneer. This agent receives the aggregated bids, which represent the wishes of all device agents. Based on this knowledge, the auctioneer calculates the equilibrium energy price. The default goal of the agent is supply demand matching. Finally, the auctioneer sends the new energy price downwards the tree.

Upon receiving a new energy price, all device agents adapt their behaviour accordingly.

5.1 Privacy-preserving PowerMatcher

As privacy plays a vital role, PowerMatcher shows significant privacy issues. A concentrator agent receives bids of device agents and is thereby capable of tracking these device in detail. Thus, privacy is at risk. However, the Homomorphic Encryption System can also be applied to PowerMatcher, resulting in the Privacy-Preserving PowerMatcher (PPPM). In general, device agents encrypt their bids with the public key of the auctioneer using homomorphic encryption. Concentrators homomorphically aggregate received bids and send them to the auctioneer. Only the auctioneer is capable of decrypting the aggregated bid using its private key. Thus, PPPM reaches the same privacy-level of PrivADE$^+$.

However, the bid representation has to be adapted, because dynamic point-based bids cannot be aggregated in such a way. Thus, bids are discretised and consists of a fixed-size list Φ_a with consumption values ω. The number $|\Phi_a| \in \mathbb{N}_{\geq 2}$ of consumption values ω is called the resolution and is constant in the entire system. At the beginning, a price list Υ with the same resolution ($|\Upsilon| = |\Phi_a|$) has to be defined. This way each device agent can assign its consumption values to a corresponding price. The array based representation of the exemplary bid is defined as

$$\begin{aligned} \Upsilon &= \{0.0€, 0.1€, 0.2€, 0.3€, 0.4€, 0.5€\} \\ \Phi_a &= \{2\text{kW}, 2\text{kW}, 2\text{kW}, 0\text{kW}, 0\text{kW}, 0\text{kW}\}. \end{aligned} \tag{12}$$

5.2 Multi-stage PPPM

The energy management quality is related to the resolution $|\Phi_a|$. A low resolution might impact the quality result. In other words, a higher resolution might improve the energy management quality. However, this also results in larger bids and a higher data amount.

To reduce the data amount, while keeping the same level of energy management quality, a multi-stage approach of PPPM can be applied. During the first stage the auctioneer gathers all bids with a small bid resolution and calculates a price range where the equilibrium price is located in. Afterwards, it initiates a new round by sending the new price range to all participants. Thus, the multi-stage approach continuously increases the price resolution while decreasing the price range. Therefore, the total amount of submitted data can be reduced. Using this method, a virtual resolution of $(|\Phi_a| - 1)^\rho + 1$ can be reached by performing ρ stages. Thus, an initial bid resolution of 100, results in a virtual resolution of 9802, when two stages are executed.

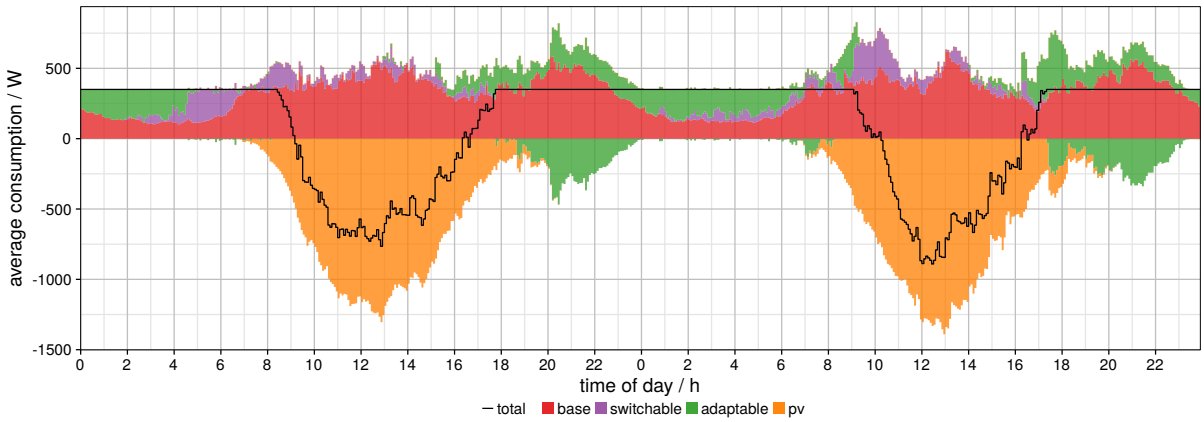

Figure 3: Exemplary consumption curve (PrivADE+, day 2).

6 EVALUATION

In this section all presented DEM algorithm are evaluated against the remaining key performance indicators energy management quality, communication performance and robustness. All simulations are executed with SiENA, which offers a realistic data basis for the smart grid, as well as communication, heat, and power network simulations. (Brettschneider et al., 2016)

6.1 Scenario

The scenario represents an urban street with up to 100 households. The households own basic appliances, as well as Photovoltaic Systems (PVs), BSs, EVs, and HPs as shown in Table 1. The energy management algorithms perform peak clipping with a target of 350 watts per household. The participants of the algorithms are connected to each other using an internet topology. Please note, that this serves as an example to show the capabilities of the algorithms. Furthermore, load shifting is not performed.

Figure 3 exemplarily shows the consumption of the second day with PrivADE+. The base load (red) cannot be influenced. PV systems (orange) offer power during the day. HPs (purple) are switched on when excess power is available. EVs return after work and require charging. Thus, the DEM target would be violated during the evening and PrivADE+ reduces the charging rate, when possible, and stimulates BSs to provide the remaining deficit. As a result, the overall consumption does not exceed the DEM target during the whole day.

The following sections evaluate the single-stage PPPM with a resolution of 100 and 1000, the two-stage PPPM with a resolution of 100 per stage, PowerMatcher, and PrivADE+.

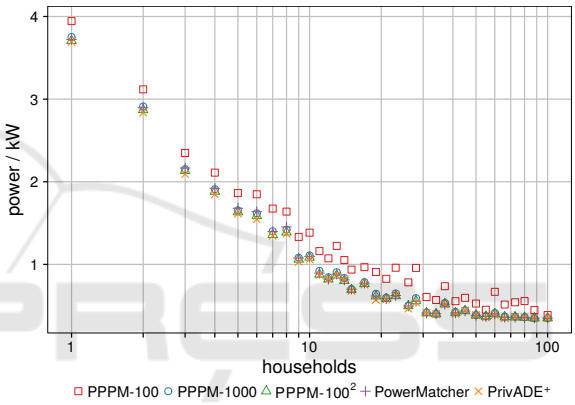

Figure 4: Comparison of average maximum power per household for all algorithms.

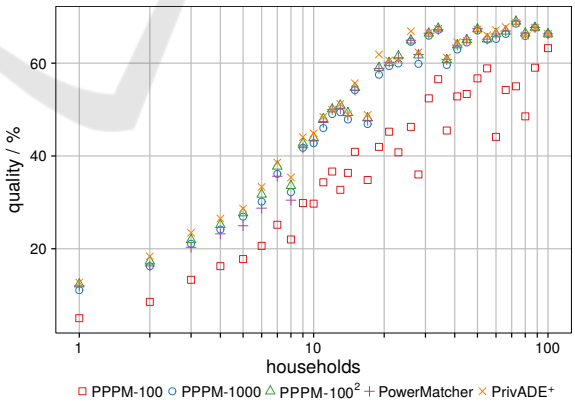

Figure 5: Comparison of average peak clipping quality for all algorithms.

6.2 Energy Management Quality

Regarding energy management quality, Figure 4 shows the average maximum power per household. All DEM algorithms are configured to perform peak clipping. They achieve similar results in all simu-

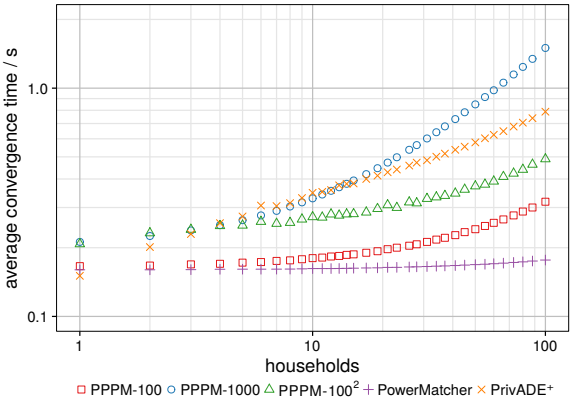

Figure 6: Scaling comparison of convergence time per interval for all algorithms.

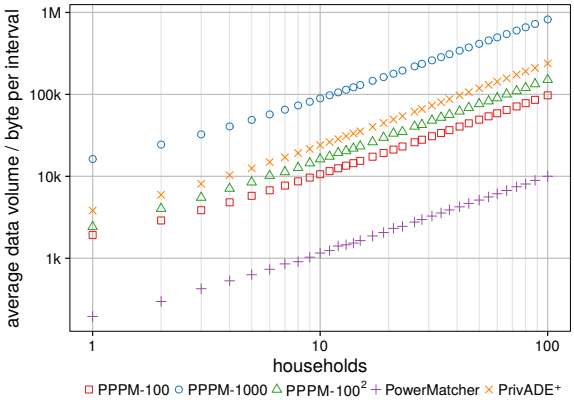

Figure 7: Scaling comparison of data volume per interval for all algorithms.

lated scenarios, ranging from 1 to 100 households. Only the PPPM algorithm with a resolution of 100 does not reduce the peaks as good as the other algorithms. Increasing the resolution to 1000 or 9802 suffices to increase the peak clipping effectiveness to a same level as PowerMatcher. In this scenario, the DEM algorithms are capable of reducing all peaks to the 350 watts target when more than 80 households participate at the energy management.

To measure the peak clipping quality a metric is used, as defined in (Hölker et al., 2016). The metric measures the reduction of the consumption peaks related to a reference simulation without energy management. It ranges from -1 (worst) to 1 (best), where 0 indicates no change. Figure 5 shows that all algorithms can decrease the peak power significantly.

In conclusion, PowerMatcher and PrivADE$^+$ achieve the same level of energy management quality. PPPM also performs well, when configured with a suitable bid resolution.

6.3 Communication Performance

Regarding the communication performance, the simulation results show more differences. Figure 6 shows the average convergence time per energy management interval and Figure 7 the corresponding data volume. PowerMatcher achieves the best results, because of its low bid size and the static energy management steps. The average convergence time is below 200 ms for 100 households and the data volume at 10 kB. PrivADE$^+$ requires more time and data volume for convergence because of its round-based procedure and larger message sizes. However, the convergence time still does not reach one second and the data volume stays well below one MB. The single-stage PPPM with reasonable resolutions need higher convergence times because of its larger messages. However, when a high bid resolution is required, the two-stage PPPM can perform better. With a resolution of 100, it reaches a 500 ms convergence time for 100 households and a data volume comparable to PrivADE$^+$.

In conclusion, PowerMatcher achieves the best results regarding communication performance. However, PrivADE$^+$ and the multi-stage PPPM also achieve good results with convergence times well below one second and a corresponding data volume below one MB. Thus, all algorithms can be deployed when using Internet-based communication technologies like in this scenario.

6.4 Robustness

PrivADE$^+$ and PowerMatcher both use a star overlay network, where each household is connected to a central unit. If a communication connection is interrupted and a household cannot transmit its information to a concentrator/aggregator or cannot receive any commands, both algorithms have to make assumptions about its energy consumption. However, existing standard load profiles and historic data counteract this lack of knowledge. Thus, the overall energy management quality is only slightly influenced. To reduce the impact on the convergence time a deadline can be defined, after which a household is considered offline. Thus, a concentrator/aggregator only has to wait until it receives data from all households or until the deadline is reached.

In conclusion, all algorithms achieve robustness from a communicational and quality point of view and the privacy mechanisms do not reduce the robustness. Robustness issues regarding false data injection can be counteracted using additional signage protocols. However, this impacts privacy and therefore has been disregarded in this paper.

7 CONCLUSIONS

This paper introduced PrivADE$^+$ and the Privacy-Preserving PowerMatcher (PPPM). Both DEM algorithms focus on preserving the privacy of all participants without reducing the energy management capabilities. They use a homomorphic encryption scheme to perform private and secure data aggregation. The PPPM extends the PowerMatcher algorithm where households aggregate bids (price/consumption) and where an auctioneer determines the best energy price. PrivADE$^+$ combines the homomorphic data aggregation with a round-based scheduling for switchable and adaptable loads. Both algorithms preserve the privacy of all participants by only publishing encrypted and aggregated information.

Regarding energy management quality PrivADE$^+$ achieves slightly better results. Considering communication performance, the multi-stage PPPM offers faster convergence times.

In conclusion, the presented DEM algorithm PrivADE$^+$ and PPPM achieve the goal of preserving the privacy of its participants without reducing energy management quality and communication performance. Thus, both algorithms fulfil all requirements for deployment.

REFERENCES

Brettschneider, D. (2017). *Preserving Privacy in Distributed Energy Management*. Shaker Verlag, Aachen.

Brettschneider, D., Hölker, D., Scheerhorn, A., and Tönjes, R. (2017). Preserving privacy in Distributed Energy Management. *Computer Science - Research and Development*, 32(1):159–171.

Brettschneider, D., Hölker, D., and Tönjes, R. (2016). SiENA: Simulator for Energy Network Applications combining Power, Heat and Communication. In *Proceedings of VDE Kongress 2016*. VDE.

Fontaine, C. and Galand, F. (2007). A Survey of Homomorphic Encryption for Nonspecialists. *EURASIP Journal on Information Security*, 2007:15:1–15:15.

Hinrichs, C., Lehnhoff, S., and Sonnenschein, M. (2013). COHDA: A Combinatorial Optimization Heuristic for Distributed Agents. In Filipe, J. and Fred, A., editors, *Agents and Artificial Intelligence*, number 449 in Communications in Computer and Information Science, pages 23–39. Springer Berlin Heidelberg.

Hölker, D., Brettschneider, D., Fischer, M., Tönjes, R., and Roer, P. (2016). Quality-functions for an uniform and comparable analysis of demand side management algorithms. *Computer Science - Research and Development*, 31(1):57–64.

Kok, J. K., Warmer, C. J., and Kamphuis, I. G. (2005). PowerMatcher: Multiagent Control in the Electricity Infrastructure. In *Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems*, AAMAS '05, pages 75–82. ACM.

Mohsenian-Rad, A.-H., Wong, V., Jatskevich, J., and Schober, R. (2010). Optimal and autonomous incentive-based energy consumption scheduling algorithm for smart grid. In *Innovative Smart Grid Technologies (ISGT), 2010*, pages 1–6.

Paillier, P. (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Stern, J., editor, *Advances in Cryptology — EUROCRYPT '99*, number 1592 in Lecture Notes in Computer Science, pages 223–238. Springer Berlin Heidelberg.