Technical Report: Privacy-Enhanced Bi-Directional Communication in the Smart Grid

Andrew Paverd
Department of Computer Science
University of Oxford
andrew.paverd@cs.ox.ac.uk

Andrew Martin
Department of Computer Science
University of Oxford
andrew.martin@cs.ox.ac.uk

Ian Brown
Oxford Internet Institute
University of Oxford
ian.brown@oii.ox.ac.uk

***Abstract*—Although privacy concerns in smart metering have been widely studied, relatively little attention has been given to privacy in bi-directional communication between consumers and service providers. Full bi-directional communication is necessary for incentive-based demand response (DR) protocols, such as demand bidding, in which consumers bid to reduce their energy consumption. However, this can reveal private information about consumers. Existing proposals for privacy-enhancing protocols do not support bi-directional communication. To address this challenge, we present a privacy-enhancing communication architecture that incorporates all three major information flows (network monitoring, billing and bi-directional DR) using a combination of spatial and temporal aggregation and differential privacy. The key element of our architecture is the Trustworthy Remote Entity (TRE), a node that is singularly trusted by mutually distrusting entities. The TRE differs from a trusted third party in that it uses Trusted Computing approaches and techniques to provide a technical foundation for its trustworthiness. A automated formal analysis of our communication architecture shows that it achieves its security and privacy objectives with respect to a previously-defined adversary model. This is therefore the first application of privacy-enhancing techniques to bi-directional smart grid communication between mutually distrusting agents.**

I. Introduction

It is widely acknowledged that there are privacy concerns associated with smart energy meters. Various privacy-enhancing protocols and systems have been proposed to mitigate the risk of private information being inferred from frequent energy consumption measurements. Experience has shown that consumers do not always trust service providers such as the energy supplier or distribution network operator (DNO) with these fine-grained consumption measurements [1]. Even if service providers follow the defined protocols, they might still be perceived as honest-but-curious (HBC) adversaries attempting to learn private information about consumers [2]. In addition to these privacy concerns, there are numerous security threats that must also be taken into account in smart grid communication protocols. Most privacy-enhancing protocols that have been proposed focus on two main information flows: monitoring and billing. In the monitoring flow, consumers send frequent consumption measurements to the DNO to allow fine-grained monitoring of the distribution network. In the billing flow, these frequent measurements are sent to the energy supplier to facilitate price-based demand response schemes such as dynamic pricing. The communication of energy price information is not included in these information flows as it is usually sent via a broadcast channel. Both monitoring and billing are therefore uni-directional information flows.

Demand response (DR) is defined as: *"Changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized"* [3]. As shown in this definition and confirmed in the categorization by Albadi et al. [4], there are two types of DR approaches: price-based and incentive-based DR. An example of an incentive-based approach is *demand bidding* [4] in which consumers interact with the Demand Side Manager (DSM) as follows: When a shortage in supply is expected, the DSM creates a DR event and notifies all consumers. Consumers send *bids* to the DSM stating the amount of consumption they are willing to reduce and the desired incentive price for this reduction. The DSM selects the winning bids and communicates its decision to individual consumers. After the event, the respective incentives are credited to the successful bidders. Demand bidding requires full bi-directional communication between consumers and the DSM so that consumers can submit bids and the DSM can respond to individual consumers to accept or reject their bids. This bi-directional communication provides a closed feedback loop allowing the DSM to monitor and control the DR process and also constitutes a third primary information flow. Standards such as Open Automated Demand Response (OpenADR) version 1.0 [5] and the subsequent OASIS Energy Interoperation (Ei) standard [6] specify data models for demand bidding. Although initially targeted at large industrial consumers, demand bidding can also be applied to residential consumers. In a residential setting, a home energy management system or feature-rich smart meter would place bids and control energy-consuming systems according to a user-defined policy.

However, it has been shown that these bids can be used to infer private information about consumers [7][8][2]. The magnitude and timing of a particular bid could reveal the use of a particular type of system (e.g. charging a plug-in electric vehicle after arriving home). If multiple bids can be linked to a specific consumer, these can be used to infer behavioural patterns. Any deviation from these patterns could also reveal private information [2]. The challenge is that

existing proposals for privacy-enhanced smart metering do not support bi-directional communication.

In order to address this challenge, we present a unified communication architecture incorporating all three primary information flows. The key element of our architecture is the Trustworthy Remote Entity (TRE), a communication node that is singularly trusted by mutually distrusting entities. The TRE is an intermediary in the communication path between consumers and service providers. The TRE enhances consumers' privacy using a combination of spatial and temporal aggregation techniques and facilitates privacy-preserving bi-directional communication for demand bidding protocols.

Although the TRE performs a similar role to a trusted third party, the fundamental difference is that the TRE provides a technical mechanism for proving its trustworthiness to the relying parties. As our second contribution, we present a technical approach for establishing trust in the TRE using approaches and technologies from the field of Trusted Computing (TC). Due to the unique characteristics of the smart grid application domain, we propose that existing TC components and approaches, such as the Trusted Platform Module (TPM) and remote attestation, can be leveraged to provide meaningful security guarantees.

Previous work has shown how some communication protocols that have been proposed for the smart grid have failed to meet their security and privacy requirements [9]. As our third contribution, we have formally analysed the security and privacy properties of our proposed protocols using an enhanced version of the Casper/FDR protocol analysis tool [10]. Our key contributions are:

- A privacy-enhancing communication architecture incorporating all three smart grid information flows, utilizing Trustworthy Remote Entities (TREs).
- An approach for establishing trust in the TRE using tools and approaches from the field of Trusted Computing.
- An automated formal analysis showing that our communication architecture improves upon existing protocols, particularly with respect to bi-directional communication.

II. Related Work

A. Privacy in Smart Metering

For purposes of network monitoring, consumption measurements do not need to be attributable to individual consumers. It is sufficient for the DNO to receive aggregated consumption data from a group of smart meters. One class of proposals involves anonymizing or pseudonymizing individual measurements [11][12][13][14]. However, it has been shown that in some cases these can be de-pseudonymized [9]. Furthermore, anonymization is not directly suitable for DR bidding protocols because the relevant incentives cannot be credited to anonymous bidders. Another class of proposals use *spatial aggregation* in which measurements from a group of consumers are added together such that the recipient cannot determine each individual's contribution to the total. Various mechanisms for performing spatial aggregation have been proposed including homomorphic encryption schemes [15][16], data perturbation [17][18] and secret sharing [19]. However, these cannot be used for demand bidding protocols because the service provider is unable to select and notify individual bidders.

For billing purposes, measurements must be attributable to individual, named consumers. Some privacy-preserving billing protocols make use of *temporal aggregation* in which measurements from a single consumer are aggregated over time. The energy supplier has a significant financial interest at stake and so must be convinced that this aggregation has been performed honestly. It has been proposed that this can be achieved using verifiable computation techniques [20][21]. However, temporal aggregation cannot be used for demand bidding protocols because the bidding interactions must take place in real time. An improved form of temporal aggregation for billing has been proposed by Danezis et al [22]. Building on the success of differential privacy [23], they have shown that data perturbation can be used to enhance consumers' privacy whilst still providing some real time feedback to the supplier [22]. Although the data is attributable to named consumers and approximate individual measurements are available at each point in time, this approach is still not ideal for demand bidding because the perturbation of each individual bid could result in an unacceptably large overall error. Furthermore, the DSM requires accurate data in order to select successful bidders, ensure that they have fulfilled their obligations and credit them with the relevant incentives. Some proposals for monitoring or billing have included trusted third parties [17][24][25] but none of these have addressed the challenge of bi-directional communication.

B. Privacy in Demand Response

Early research efforts have begun to investigate privacy-enhancing techniques for DR applications. Rottondi and Verticale [8] have proposed the use of multi-party computation to facilitate privacy-friendly appliance load-scheduling. Although it addresses a similar problem, their architecture is designed for collaborative scheduling rather than incentive-based DR. The most similar work to ours is that by Karwe and Strüker [7] who investigated a demand bidding protocol based on the Open Automated Demand Response (OpenADR) specification [5]. They showed that an untrusted intermediary between the consumers and the DSM could compromise consumers' privacy and they proposed enhancements to prevent this intermediary from inferring private information [7]. As explained in the next section, we focus on the complementary threat scenario in which the third party is provably trustworthy whilst all other agents are mutually distrusting. We have previously analysed the privacy issues in bi-directional DR communication using different types of adversary models and suggested that these issues could be mitigated using a trustworthy third party [2]. This paper is the fulfilment of that suggestion and, to the best of our knowledge, is the first work to address privacy concerns in bi-directional DR communication between mutually distrusting agents.

III. Communication Architecture

We first describe the baseline system model and the current security and privacy threats. We then present our privacy-enhancing communication architecture in terms of the three main information flows and discuss some implementation considerations.

A. Baseline System Model

In the set of all consumers $\mathcal{C}$, each consumer $c \in \mathcal{C}$ has a feature-rich smart meter or home energy management system capable of bi-directional communication. At time $t \in \mathbb{N}$, c produces a consumption measurement m_t^c and sends this to the DNO (monitoring) and to the supplier (billing). For dynamic pricing, the supplier periodically broadcasts the prevailing price per unit p_t to all consumers but this is not included in the billing information flow because it is a broadcast message. When incentive-based DR is required, the DSM notifies consumers and invites bids. At time t, each consumer c may generate a DR bid $(bid\text{-}q_t^c, bid\text{-}p_t^c)$ consisting of the bid quantity and the bid price per unit and send this to the DSM. The DSM replies to individual consumers indicating acceptance of the bid. We refer to this bi-directional communication between the consumer and DSM as the DR information flow.

In this baseline model, there are various threats to consumers' privacy as well as the overall security of the system. We focus on the threat model defined in [2]. In this model, it is assumed that a limited number of consumers are adversarial and will submit false measurements (a type of false data injection attack). It is also assumed that all service providers could be honest-but-curious (HBC) adversaries who will follow the defined protocol but will attempt to learn private information about consumers from any received messages [2].

B. Enhanced System Model

In our privacy-enhancing communication architecture architecture, all communication between consumers and service providers passes through a TRE. For each information flow, the TRE performs specific information processing tasks as described in the following subsections. In all cases, communication with the TRE takes place over a secure authenticated channel providing confidentiality and integrity protection with respect to external adversaries as well as strong mutual authentication. For example, this could be achieved using Transport Layer Security (TLS) with mutual authentication or an equivalent protocol. Although we describe the functionality of a single TRE, we envisage that there will be a network of TREs distributed throughout the grid, each providing identical functionality.

C. Network Monitoring

In the network monitoring information flow, the TRE performs spatial aggregation over a group of consumers and applies data perturbation to the result to achieve differential privacy [23]. Consumers are divided into aggregation groups $g \subset \mathcal{C}$ where $\mathcal{G}$ is the set of all groups on a particular TRE. The aggregation groups are dynamically defined by the DNO such that each group $g \in \mathcal{G}$ represents a sector within the distribution network.

Every 15 or 30 minutes, at time t, consumers send individual measurements m_t^c to the TRE. The TRE first performs bounds checking to mitigate against false data injection attacks. Measurements that exceed a consumer's installed capacity will be excluded from the aggregation and an alert will be raised. For each aggregation group, the TRE computes the sum of the measurements and adds random noise according to the Laplace distribution, Lap(λ), which has the density function $h(y) \propto exp(-|y|/\lambda)$ (zero mean and standard deviation λ) [26]. The result is sent to the DNO:

$$\text{TRE} \rightarrow \text{DNO:} \quad \left(\sum_{c \in g} m_t^c\right) + Y \; ; \quad \text{where: } Y \sim \text{Lap}(1/\epsilon)$$

This mechanism is therefore ϵ-indistinguishable [26]. The addition of random noise necessary to mitigate against a variant of the *set-difference* attack [27] in which the DNO creates two overlapping aggregation groups that differ by a single consumer in order to learn that individual's consumption. The *sensitivity* of the added noise is calibrated to mask the presence of absence of any single consumer in the aggregate [26]. All consumers in a particular group must connect to the same TRE. Consumers' privacy is technically preserved if $|g| \geq 2$ but in practice, larger aggregation groups would be used. As $|g|$ increases, the percentage error introduced by the random noise decreases. In all practical implementations, this error will be less than other errors such as those caused by electrical losses in the distribution network. The maximum $|g|$ depends on implementation details such as the bandwidth and computational capacity of the TRE. This approach achieves the same outcome as other spatial aggregation techniques [15][16][17][18][19] without requiring any modification to the smart meters and only minimal configuration changes at the DNO. Specifically, this approach does not increase the number of messages sent by the consumers.

D. Billing

In the billing information flow, temporal aggregation is used to preserve the level of privacy available before smart meters. At time t the supplier notifies the TRE of the current energy price p_t which the TRE then broadcasts to consumers. By verifying that p_t was sent by the TRE, consumers are assured that this is the price that will be applied. Consumers send measurements m_t^c to the TRE which performs bounds checking and adds them to the consumer's running total:

$$bill_t^c \; = \; bill_{t-1}^c + (m_t^c \times p_t)$$

At the end of the billing period ($t = t\text{-}end$), the TRE sends each consumer's aggregated total to the energy supplier and resets the running total:

$$\text{TRE} \rightarrow \text{Supplier:} \quad bill_{t\text{-}end}^c \; ; \quad bill_{t\text{-}end}^c = 0$$

The temporal aggregation period is dynamically defined by the supplier but must exceed the minimum value specified

by the regulator and enforced by the TRE to protect privacy (e.g. weeks or months). It is not necessary to apply differential privacy in this case because the supplier cannot define overlapping time periods and thus cannot learn anything other than the temporal aggregate. The maximum temporal aggregation period is again implementation-dependent. This achieves the same result as other privacy-preserving billing methods [22][20][21] without requiring modifications to the smart meters or increasing the number of messages sent by consumers. The TRE can combine the temporal aggregation for billing purposes with the spatial aggregation for monitoring since both use the same individual measurements as inputs.

E. Demand Response

Due to the requirement for full bi-directional communication in the DR information flow, techniques such as spatial or temporal aggregation cannot be used directly. For example, in demand bidding, the bids cannot be spatially aggregated over multiple consumers because each bid contains both quantity and price information. Furthermore, residential consumers may only have the ability to reduce demand by a specific amount (e.g. disconnecting a particular load) so bids cannot be partially accepted. In our architecture, the TRE combines the functionality of a privacy proxy with temporal aggregation techniques as shown in Figure 1. When the DSM creates a new DR event, the TRE notifies the consumers and participating consumers submit bids to the TRE:

$$\forall c \in \mathcal{C}: \quad c \rightarrow \text{TRE:} \quad (bid\text{-}q_t^c, bid\text{-}p_t^c)$$

To mitigate against false bid injection, consumers must authenticate themselves to the TRE and the TRE performs bounds checking on all bids. The TRE sends the DSM a set of *pseudo-bids* corresponding to the consumers' bids:

$$\forall c \in \mathcal{C}: \quad \text{TRE} \rightarrow \text{DSM:} \ (pseudo\text{-}q_t^c, pseudo\text{-}p_t^c)$$

Each pseudo-bid includes a single-use anonymous identifier that can only be linked to the original bid by the TRE. This differs from pseudonymization in which the same pseudonym would be used for all bids from a particular consumer, thus allowing linkability between bids. From the DSM's perspective, the TRE appears to be a large aggregated load that submits multiple bids for each DR event. The DSM can therefore use its existing processes and algorithms to select a set of accepted specific pseudo-bids, $\mathcal{A}$ and notify the TRE which in turn notifies the individual consumers. If this information flow were viewed in isolation, the TRE would still not enable full demand bidding because the incentives could not be credited to individual consumers. However, since our architecture incorporates all three information flows, the TRE can credit the consumers' internal aggregated bills:

$$\forall\, c \in \mathcal{A} \ : \ bill_t^c \ = \ bill_{t-1}^c - (bid\text{-}q_t^c \times bid\text{-}p_t^c)$$

These incentives are therefore included in the temporal aggregation of the billing data thus preventing them from being used to link bids to individual consumers. If required, the TRE could also verify that successful bidders have complied with their bid obligations based on their consumption measurements. This protocol ensures that the DSM is unable to link bids to individual consumers and is therefore unable to detect if specific consumers have placed bids.

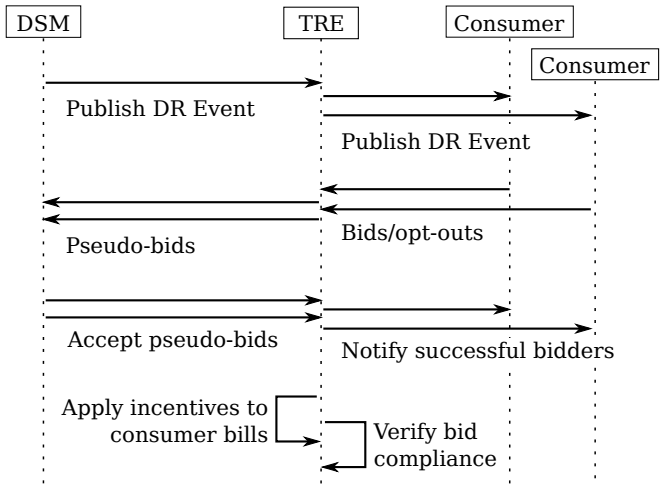

Fig. 1. Hybrid spatial and temporal aggregation for privacy-preserving DR.

F. Implementation Considerations

In the United Kingdom, the Data Communication Company (DCC) is a licensed entity mandated to provide communication services for all smart meters. Such an entity is ideally positioned to operate the network of TREs. To ensure availability, it is expected that there would be a significant number of TREs (in the order of thousands) geographically distributed throughout the grid. If a TRE fails, the affected consumers would re-connect to a different TRE since the aggregation groups are dynamically defined. The maximum number of consumers per TRE depends on implementation factors such as the computational capacity and network bandwidth of the TRE node. Given the simplicity of the information processing it performs, the TRE is not expected to add significant communication latency. Since our architecture does not increase the number of messages sent by consumers compared to the baseline system, it would impact the performance of the communication network. This architecture could be deployed incrementally in parallel with the roll-out of smart meters since no modifications are required on the consumer side.

IV. Establishing Trust

In the most extreme case, consumers and service providers could be mutually distrusting. Consumers do not necessarily trust service providers with their fine-grained energy measurements [1] and service providers do not trust consumers to aggregate their own measurements or calculate their own bills honestly. The key feature of our communication architecture is that the TRE is singularly trusted by these mutually distrusting entities. Although the TRE provides the functionality of a trusted third party, the fundamental difference is that a trusted

third party is typically trusted without proof whilst the TRE uses Trusted Computing (TC) technologies and approaches to provide a technical basis for this trust.

A. Trusted Computing Background

We focus on TC technologies standardized by the Trusted Computing Group (TCG). These make use of the Trusted Platform Module (TPM), a cryptographic co-processor securely integrated into the platform that provides isolated storage for cryptographic keys and a special set of Platform Configuration Registers (PCRs). Each PCR stores an integrity measurement in the form of cryptographic hash which cannot be directly written but can be *extended* by supplying a new hash which is concatenated with the existing value and the hash of the result stored in the PCR. The PCRs provide integrity-protection for the log of all software that has been executed on the platform. Before any software is executed, the preceding software takes a hash of the new binary, adds it to the log and extends it into the PCRs. If the measurement log has been tampered with, its sequence of hashes will not match the PCR values. This forms a chain of trust extending back to either the platform reset or to a point at which the platform transitioned into a secure state. The TPM can *seal* data by encrypting the data such that it can only be decrypted when the PCRs have the correct value. The platform can perform a *secure boot* in which software binaries are only executed if their hashes are on a pre-defined whitelist. *Remote attestation* can then be used to prove the state of the platform to a remote verifier by sending a TPM-signed *quote* of the PCR values to the verifier.

Although TPMs are readily available in server platforms, the use of remote attestation has been very limited due to the size and complexity of modern general-purpose systems. Studies have shown that remote attestation of a typical web service involves approximately 300 integrity measurements with about 35 new measurements added each month due to software updates [28]. Furthermore, a general-purpose system usually includes an operating system (OS) kernel consisting of millions of lines of code. Even if the software can be unambiguously identified, its complexity makes it infeasible for a remote party to make informed trust decisions.

B. Trusted Computing in the TRE

In our architecture, the TRE avoids these scalability issues since it is a highly specialized system with a single well-defined unchanging purpose. The TRE has a minimal Trusted Computing Base (TCB) consisting of a purpose-built network stack, a limited number of cryptographic primitives and the simple information processing procedures described above. The TCB could be further reduced by partitioning the TRE into its trusted and untrusted components using a similar approach to that proposed by Lyle and Martin [28]. As a single-purpose system, the TRE requires neither an OS nor the ability to execute any other software. This makes it feasible to use TCG *secure boot* so software binaries are only executed if their hashes are on a pre-defined white-list. During normal operation, the PCRs will therefore always reach the same value thus allowing sensitive information, such as cryptographic keys, to be *sealed* to this state. Most importantly, the TRE can use remote attestation to prove its state to all relying parties and due to its minimal TCB, this attestation can be used to make informed trust decisions. Since the TRE must be unambiguously identified, there is no need to use privacy-preserving attestation protocols. Each TRE uses a consistent Attestation Identity Key (AIK), endorsed by a regulatory authority, and a simple challenge-response attestation protocol:

$$\text{Verifier} \rightarrow \text{TRE:} \quad attestation\ request,\ n_t^v$$
$$\text{Verifier} \leftarrow \text{TRE:} \quad ML_t^{TRE},\ TS_t,\ \left\{n_t^v,\ PCR_t^{TRE}\right\}_{Sig(AIK)}$$

At time t, the verifier supplies nonce n_t^v. The TPM generates a signature over n_t^v and the current PCR values PCR_t^{TRE} using its AIK and sends this to the verifier with the current measurement list ML_t and a timestamp TS_t. The most significant performance constraint is the TPM's quote operation since current generation TPMs (version 1.2) are not usually designed to provide high throughput. To quantify this, we have performed micro-benchmarks on an Infineon TPM 1.2. The time taken by the TPM to perform one quote operation is approximately 731 milliseconds with a standard deviation of 0.7 ms over 3000 samples. Even with over 1000 consumers per TRE, this still allows every consumer to run the attestation protocol at least once every 15 minutes. It is anticipated that the TPM 2.0 will improve this performance.

V. Formal Analysis

The trust establishment procedure described above provides a technical basis for checking the exact system state of the TRE. However, in order to make a well-founded trusted decision, they must also be able to decide if this state provides the required security and privacy properties. Practically, these decisions are usually based on consistent experience of good behaviour but in some cases, formal methods can be used to analyse certain security and privacy properties resulting in much higher levels of assurance. Arguably the most critical aspects of the system are the communication protocols since a protocol flaw could have catastrophic effects. To mitigate against this risk, we have conducted an automated formal analysis of all the communication protocols in our architecture.

A. Enhanced Casper/FDR Tool

The analysis was conducted using an enhanced version of the Casper/FDR security protocol analysis tool [10]. The original Casper/FDR tool developed by Lowe [29] takes an abstract description of a security protocol and compiles it into a formal model in the process algebra of Communicating Sequential Processes (CSP) [30]. The tool then uses the FDR model checker to perform trace refinement on the model to verify the security properties of secrecy and authentication. For this research, we augmented Casper/FDR to model and automatically analyse the privacy properties of undetectability and unlinkability in addition to the security properties of secrecy and authentication [10]. These privacy properties are analysed

with respect to an honest-but-curious (HBC) adversary who is a legitimate participant in the protocol.

Since the security properties are verified using a reachability-based approach, the same type of approach must be used for analysing the privacy properties. Ideally, an indistinguishability-based approach would be used to analyse these properties because such an approach can be used to prove unlinkability and undetectability in the absolute sense. In contrast, a reachability-based approach is limited to a particular adversary model and set of adversary capabilities which must be specified in advance. In our analysis, we use the adversary model defined in [2] and the adversary capabilities defined for the enhanced Casper/FDR tool [10]. However, the advantage of the reachability-based approach is that the same formal model can be used for both the analysis of the security properties and the analysis of the privacy properties. This is particularly useful in cases where there is tension between the security goals and the privacy goals. For example, in the baseline system model for the smart grid, a relaxation in the authentication requirements between consumers and service providers could be beneficial from a privacy perspective. If consumption measurements were reported anonymously, it would be more difficult to link these measurements to individual consumers as explained in the protocols presented by Borges et al. [12]. However, as shown by the enhanced Casper/FDR tool, this could lead to a false data injection attack since an external adversary could masquerade as one or more legitimate consumers and submit falsified measurements. It is therefore critical to analyse both the security and privacy properties and to ensure that the analysis method used can capture the inter-dependence between these properties. This enhanced tool was used to analyse the various communication protocols that constitute our architecture as described in the following subsections. The analysis tool and all input scripts are available online[1].

B. Network Monitoring

Our model for the network monitoring information flow consists of two consumers, a TRE and a distribution network operator (DNO). At each of two consecutive time periods ($t \in \{1, 2\}$) both consumers send consumption measurements to the TRE. The TRE aggregates these measurements and sends the result to the DNO. Since any aggregation group must contain at least two consumers, the DNO cannot perform a set-difference attack [27] in this model. Therefore, the model does not need to include the random noise that would be added to achieve differential privacy and thus mitigate against the set-difference attack in a real implementation. All communication is assumed to take place over secure channels that provide confidentiality and integrity protection with respect to an external adversary. In this protocol, the following security properties are analysed:

- **Secrecy:** Individual consumption measurements must only be known to the TRE and the respective consumers. This protects consumers' privacy with respect to external adversaries.
- **Authentication:** The consumers and the TRE must agree on the individual measurement values that have been sent and the TRE and DNO must agree on the aggregated measurement values. This mitigates against false data injection attacks caused by falsified measurements sent from an external adversary.

The following privacy properties are analysed:

- **Unlinkability:** The DNO must not be able to link individual measurements to specific consumers and the DNO must not be able to link multiple measurements from the same consumer. The DNO knows that the aggregated measurement is the sum of individual measurements. This enhances consumers' privacy with respect to the DNO in the monitoring information flow.

The analysis has shown that all the above properties are achieved with respect to the defined adversary model.

C. Billing

Our model of the billing information flow consists of a consumer, a TRE and an energy supplier. At each of two consecutive time periods ($t \in \{1, 2\}$) the supplier sends price information to the TRE which then forwards this to the consumer. The consumer submits an individual consumption measurement for that period to the TRE which multiplies the consumption by the prevailing price and adds this to the consumer's running total. At the end of the billing period ($t = 2$), the TRE sends the consumer's aggregated total to the supplier. As before, all communication is assumed to take place over secure channels that provide confidentiality and integrity protection with respect to an external adversary. In this protocol, the following security properties are analysed:

- **Secrecy:** Individual consumption measurements must only be known to the TRE and the respective consumers. This protects consumers' privacy with respect to external adversaries.
- **Authentication:** The consumer and the TRE must agree on the prices and individual measurement values and the TRE and DNO must agree on the aggregated measurement values. This mitigates against the possibility of an external adversary manipulating this billing information. It should be noted that this protocol does not mitigate against malicious consumers who might send falsified measurements as this is an orthogonal problem.

The following privacy properties are analysed:

- **Unlinkability:** The supplier must not be able to link individual measurements to the consumer and the must not be able to link multiple measurements from the same consumer. The supplier knows that the aggregated measurement is the sum of individual measurements weighted by the prevailing price at each point in time. This enhances consumers' privacy with respect to the energy supplier in the billing information flow.

The analysis has shown that all the above properties are achieved with respect to the defined adversary model.

[1] https://www.cs.ox.ac.uk/people/andrew.paverd/casper/

D. Demand Response

Our model for the DR information flow consists of two consumers, a TRE and a demand side manager (DSM). At a specific time, the DSM notifies the TRE of a DR event and the TRE in turn notifies the consumers. This first message exchange is not critical to the protocol and so is not included in the model. At this point each of the consumers may submit bids to the TRE. For each bid it receives, the TRE creates a pseudo-bid containing the same bid quantity and bid price and sends these to the DSM. The DSM uses its usual processes to select the winning bids and notifies the TRE which then passes on the notifications to the individual consumers. At this point, the TRE would add the incentives to the running bills of the successful bidders and optionally verify their compliance with their bids, however these steps are also not crucial to the analysis and so are not included in the model. As before, all communication is assumed to take place over secure channels that provide confidentiality and integrity protection with respect to an external adversary. In this protocol, the following security properties are analysed:

- **Secrecy:** Individual bids must only be known to the TRE and the respective consumers. This protects consumers' privacy with respect to external adversaries.
- **Authentication:** The consumer and the TRE must agree on the individual bids and bid notifications. The TRE and DSM must agree on all pseudo-bids and notifications. This mitigates against the possibility of an external adversary placing false bids or manipulating the bidding process.

The following privacy properties are analysed:

- **Undetectability:** The DSM is unable to detect if a specific consumer has placed a bid. This ensures that the DSM cannot infer any private information about consumers based on the presence or absence of bids.
- **Unlinkability:** The DSM must not be able to link pseudo-bids to consumers or to consumer bids.
  The supplier knows that each pseudo-bid corresponds to a real bid and that the notification for the pseudo-bid will be forwarded to the specific consumer. This enhances consumers' privacy with respect to the DSM in the bi-directional demand response information flow.

The analysis has shown that all the above properties are achieved with respect to the defined adversary model.

VI. Conclusion

Due to the requirement of full bi-directional communication between service providers and individual consumers, current techniques for enhancing privacy in smart metering cannot be used address the privacy concerns arising from incentive-based DR protocols such as demand bidding. To address this challenge, we have proposed a unified communication architecture combining all three major information flows and making use of a Trustworthy Remote Entity (TRE). We have shown how the TRE facilitates demand bidding whilst preserving consumers' privacy using a combination of spatial and temporal aggregation and differential privacy. The TRE differs from a typical trusted third party in that it uses Trusted Computing technologies (secure boot and remote attestation) to provide the technical foundation for establishing its trustworthiness. Preliminary micro-benchmarks on a current generation TPM confirm the feasibility of this approach from a performance perspective. We have also conducted a systematic formal analysis of the communication protocols in our architecture using an automated analysis tool. This has shown that our architecture achieves its security and privacy objectives with respect to the defined adversary model.

References

[1] C. Cuijpers and B.-J. Koops, "Smart Metering and Privacy in Europe: Lessons from the Dutch Case," Feb. 2013.

[2] A. Paverd, A. Martin, and I. Brown, "Security and Privacy in Smart Grid Demand Response Systems," in *Second Open EIT ICT Labs Workshop on Smart Grid Security - SmartGridSec14*, 2014.

[3] United States Department of Energy, "Benefits of Demand Reponse in Electricity Markets and Recommendations for Achieving Them," Tech. Rep. February, 2006. [Online]. Available: http://energy.gov/oe/downloads/benefits-demand-response-electricity-markets-and-recommendations-achieving-them-report

[4] M. Albadi and E. El-Saadany, "A summary of demand response in electricity markets," *Electric Power Systems Research*, vol. 78, no. 11, Nov. 2008.

[5] M. A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, "Open Automated Demand Response Communications Specification (Version 1.0)," California Energy Commission, PIER Program, Tech. Rep. April, 2009.

[6] OASIS, "Energy Interoperation Version 1.0," T. Considine, Ed., 2013.

[7] M. Karwe and J. Strüker, "Maintaining Privacy in Data Rich Demand Response Applications," in *First Open EIT ICT Labs Workshop on Smart Grid Security - SmartGridSec12*, 2013.

[8] C. Rottondi and G. Verticale, "Privacy-friendly appliance load scheduling in smart grids," in *Fourth IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2013.

[9] M. Jawurek, M. Johns, and K. Rieck, "Smart metering de-pseudonymization," in *Proc. Computer Security Applications Conference - ACSAC '11*, 2011.

[10] A. J. Paverd, A. Martin, and I. Brown, "Modelling and Automatically Analysing Privacy Properties for Honest-but-Curious Adversaries," Tech. Rep., 2014. [Online]. Available: https://www.cs.ox.ac.uk/people/andrew.paverd/casper/casper-privacy-report.pdf

[11] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010.

[12] F. Borges, L. A. Martucci, and M. Muhlhauser, "Analysis of privacy-enhancing protocols based on anonymity networks," in *Third IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Nov. 2012.

[13] C. Rottondi, G. Mauri, and G. Verticale, "A data pseudonymization protocol for Smart Grids," in *2012 IEEE Online Conference on Green Communications (GreenCom)*, Sep. 2012.

[14] M. Stegelmann and D. Kesdogan, "GridPriv: A Smart Metering Architecture Offering k-Anonymity," in *Proc. IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Jun. 2012.

[15] F. D. Garcia and B. Jacobs, "Privacy-Friendly Energy-Metering via Homomorphic Encryption," in *Proceedings of the 6th international conference on Security and trust management*, 2011.

[16] F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010.

[17] J.-M. Bohli, C. Sorge, and O. Ugus, "A Privacy Model for Smart Metering," in *2010 IEEE International Conference on Communications Workshops*, May 2010.

[18] G. Ács and C. Castelluccia, "I have a DREAM!: differentially private smart metering," in *Proceedings of the 13th international conference on Information hiding - IH'11*, 2011.
[19] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Proceedings of the 11th international conference on Privacy enhancing technologies - PETS'11*, 2011.
[20] M. Jawurek, M. Johns, and F. Kerschbaum, "Plug-in privacy for smart metering billing," in *Proceedings of the 11th international conference on Privacy enhancing technologies - PETS'11*, 2011.
[21] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society - WPES '11*, Oct. 2011.
[22] G. Danezis, M. Kohlweiss, and A. Rial, "Differentially private billing with rebates," in *Proceedings of the 13th international conference on Information hiding - IH'11*, 2011.
[23] C. Dwork, "Differential Privacy," in *Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds., 2006, vol. 4052.
[24] A. Bartoli, J. Herna andndez Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure Lossless Aggregation for Smart Grid M2M Networks," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010.
[25] R. Petrlic, "A privacy-preserving Concept for Smart Grids," in *Sicherheit in vernetzten Systemen: 18. DFN Workshop*, 2010.
[26] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating Noise to Sensitivity in Private Data Analysis," in *Theory of Cryptography*, ser. Lecture Notes in Computer Science, S. Halevi and T. Rabin, Eds. Springer Berlin Heidelberg, 2006, vol. 3876.
[27] T. de Souza, J. Wright, P. O'Hanlon, and I. Brown, "Set Difference Attacks in Wireless Sensor Networks," in *Security and Privacy in Communication Networks*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, A. Keromytis and R. Pietro, Eds., 2013, vol. 106.
[28] J. Lyle and A. Martin, "Engineering attestable services," in *Proceedings of the 3rd international conference on Trust and trustworthy computing - TRUST '10*, Jun. 2010.
[29] G. Lowe, "Casper : A Compiler for the Analysis of Security Protocols," Oxford University Computing Laboratory, Tech. Rep., 2009. [Online]. Available: http://www.cs.ox.ac.uk/gavin.lowe/Security/Casper/
[30] C. A. R. Hoare and J. Davies, *Communicating Sequential Processes*, 2004.