Um Mecanismo de Preservação de Privacidade para Medição Inteligente contra Empresa Curiosa

Tiago B. Castro[1], **Helio N. Cunha Neto**[2], **Natalia C. Fernandes**[1]

[1]MídiaCom - PPGEET/TET/UFF
Universidade Federal Fluminense (UFF)

[2]Laboratório de Ciência da Computação (LCC) - PEL/FEN/IME/UERJ
Universidade do Estado do Rio de Janeiro (UERJ)

Resumo. *As redes elétricas inteligentes permitem a comunicação entre clientes e a empresa de energia; entretanto, os dados de medição podem comprometer a privacidade dos usuários. A literatura propõe soluções para lidar com atacantes externos, mas não resolve o problema de ataques internos. Este artigo propõe um mecanismo de medição inteligente para proteger a privacidade contra empresas curiosas, utilizando assinaturas às cegas e agregação descentralizada. Na avaliação de desempenho, a solução apresentou uma redução de 44% no uso de CPU em comparação ao modelo parcialmente homomórfico e 46% em relação ao modelo com Shamir's Secret Sharing, demonstrando um melhor equilíbrio entre privacidade e desempenho.*

Abstract. *Smart grids enable communication between customers and the utility; however, the measurement data may compromise user privacy. The literature proposes solutions to address external attackers but does not solve the issue of internal attacks. This paper proposes a smart metering mechanism to protect privacy against curious utility, using blind signatures and decentralized aggregation. In the performance evaluation, the solution showed a 44% reduction in CPU usage compared to the partially homomorphic model and 46% compared to Shamir's Secret Sharing model, demonstrating a better balance between privacy and performance.*

1. Introdução

Nas redes elétricas inteligentes há integração de redes de telecomunicações com as redes elétricas, proporcionando maior automação e agilidade na correção de falhas no sistema elétrico [Finster and Baumgart 2015]. A instalação de medidores inteligentes possibilita a comunicação entre a empresa de energia e as unidades consumidoras. A empresa obtém mais informações sobre o comportamento dos usuários, e o usuário tem informação mais detalhada sobre o seu próprio consumo. Assim, a empresa pode monitorar a qualidade da energia da rede [Junior et al. 2019], oferecer programas de gerenciamento de energia pelo lado da demanda [Ahir and Chakraborty 2022] ou até mesmo melhorar a previsão de demanda de energia elétrica [Lazzari et al. 2022]. Os dados de medição podem ser classificados em três tipos: dados de faturamento, dados de operação e dados de serviços [Asghar et al. 2017]. Cada tipo de dado de medição possui uma frequência de coleta diferente. Por exemplo, a frequência de coleta dos dados de faturamento pode ser a cada 15 dias ou em uma base mensal. Os dados de prestação de serviço dependem do requisito de tempo necessário para determinado serviço. Já os dados de operação,

utilizados para monitorar qualidade da rede, apresentam frequência amostral de 15 minutos [Van Aubel and Poll 2019].

Apesar dos muitos benefícios, a instalação dos medidores inteligentes também traz um grande risco. A privacidade dos usuários pode ser exposta se os dados de operação forem interceptados por um agente malicioso, ou se forem usados de forma indevida pela própria empresa de energia elétrica. A análise dos dados de consumo coletados com uma frequência alta pode fornecer informações significativas sobre o comportamento e estilo de vida do usuário [Devlin and Hayes 2019], revelando seus eletrodomésticos, horários de uso e momentos em que a casa está vazia. Essa exposição é diretamente proporcional à frequência da coleta de dados [Eibl and Engel 2014]. Reportar os dados em um intervalo maior de tempo ajuda a camuflar os hábitos do usuário monitorado; entretanto, não protege integralmente a privacidade do usuário. O envio dos dados em uma baixa frequência prejudica serviços necessários para a manutenção da qualidade da rede elétrica, como a estimação de estados e o monitoramento da tensão do sistema elétrico.

Diante desse cenário, surge o desafio de estabelecer uma comunicação segura que preserve a privacidade dos usuários. Outros trabalhos já foram propostos para proteger a privacidades dos usuários durante medições inteligentes [Asghar et al. 2017, Finster and Baumgart 2015, Sultan 2019, Kua et al. 2023]. Entretanto, os trabalhos da literatura partem da premissa que a empresa de energia é confiável, e apenas protegem o usuário contra terceiros externos maliciosos. Logo, não protegem a privacidade do usuário contra uma empresa curiosa. Empresa curiosa é um tipo de ataque em que a empresa não deseja modificar os dados, mas deseja monitorá-los em um nível que comprometa a privacidade dos clientes [Joshi et al. 2022].

Os trabalhos relacionados frequentemente usam agregação de dados para tentar solucionar o problema de privacidade. Na agregação de dados, as medições de diferentes clientes são agregadas localmente, protegendo a privacidade dos usuários durante medições com menor granularidade. O uso de pseudônimos é outra prática comum, dificultando a associação deliberada de dados de medição a um cliente específico. Ao autenticar no gerenciador de chaves, o medidor recebe um pseudônimo. Desta maneira, se um agente malicioso interceptar os dados de medição, não identificará o usuário de origem do dado.

Entre as principais contribuições deste trabalho está a análise de desempenho dos modelos de preservação de privacidade para medições inteligentes, verificando a viabilidade do uso de assinatura às cegas; e o desenvolvimento de um mecanismo de preservação de privacidade contra empresa curiosa, integrando assinatura às cegas e agregação de dados. Neste mecanismo, os pseudônimos são assinados às cegas. Assim, nenhuma elemento da rede conhece o mapeamento entre um pseudônimo e seu medidor inteligente. Em seguida, os medidores se revezam agregando os dados, evitando que um único nó da rede ou da concessionária tenha acesso às medições subsequentes. Para preservar a privacidade através das informações de rede, os medidores usam dois endereços de IP (e MAC). Um IP para os dados de faturamento e outro IP para os dados de operações.

Na análise de resultados foi verificada a viabilidade do uso de assinatura às cegas. O modelo de assinatura às cegas foi comparado com outros modelos apresentando uso de CPU 44% menor que o modelo parcialmente homomórfico e 46% menor que o modelo com *Shamir's secret sharing*. Nas análises de segurança, o mecanismo proposto mostrou-

se o mais seguro contra ataques de privacidade, protegendo os usuários contra agentes maliciosos externos e contra empresas curiosas.

O restante do artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A proposta é descrita na Seção 3. A Seção 4 descreve as análises, comparações e resultados. A Seção 5 conclui o artigo.

2. Trabalhos Relacionados

A maior parte das soluções aplicadas à privacidade dos dados de operações das medições inteligentes se dividem em mecanismos com criptografia homomórfica e baseado em terceiro confiável [Sultan 2019].

Li et al. apresentam um esquema de proteção de privacidade utilizando armazenamento em nuvem privada [Li et al. 2021]. O medidor autentica-se em uma autoridade confiável utilizando suas credenciais e recebe um par de chaves criptográficas. As medições são criptografadas e encaminhadas para o agregador, que encaminha os dados para o centro de controle através de uma nuvem privada. O centro de controle descriptografa os dados e acessa as informações dos medidores. Esses dados são usados para faturamento ou outro serviço. Os autores partem do pressuposto de que a empresa é confiável. O centro de controle tem acesso aos dados detalhados de consumo dos usuários. Além disso, a autenticação e geração de chaves dos medidores são realizadas por um terceiro confiável.

Zhang et al. apresentam um esquema descentralizado de preservação de privacidade baseado em blockchain de consórcio [Zhang et al. 2023]. Os autores também utilizam a autenticação através de um terceiro confiável, o gerenciador de chaves. A solução busca proteger a privacidade dos usuários dividindo o faturamento em duas entidades da rede. O fornecedor de energia conhece a identidade associada a cada pseudônimo, mas não tem acesso ao consumo detalhado do usuário. O centro de controle conhece o pseudônimo e seu consumo respectivo, mas não sabe a identidade real do pseudônimo. Entretanto, não é possível garantir que não haverá comunicação entre as duas entidades, expondo assim a privacidade do usuário.

Singh et al. propõem um modelo de agregação de dados e preservação de privacidade baseado em criptografia homomórfica para redes elétricas inteligentes [Singh et al. 2021]. O centro de controle é responsável por autenticar os medidores que entram na rede. Os medidores criptografam os dados com a chave homomórfica e enviam as medições para um agregador local. O agregador verifica a mensagem, realiza a agregação com a propriedade homomórfica e encaminha o resultado para o centro de controle da empresa de distribuição. O centro de controle usa a chave homomórfica para descriptografar os dados e obter a agregação. A privacidade do usuário pode ser exposta, se a empresa utilizar a chave homomórfica antes da agregação dos dados.

Joshi et al. propõem um esquema de preservação de privacidade com criptografia homomórfica [Joshi et al. 2022]. Os medidores autenticam-se na empresa de energia e recebem as chaves criptográficas homomórficas. As medições são criptografadas com as chaves públicas e enviadas para um servidor computacional, que desconhece as chaves privadas. O servidor realiza a agregação através da propriedade homomórfica e depois envia o resultado da agregação para a empresa de distribuição. O servidor computacional é gerenciado por uma empresa terceira. Por mais que as empresas obedeçam aos protocolos

do sistema, não há garantia de que o servidor não venderá os dados criptografados dos clientes para a empresa de energia.

Finster e Baumgart propuseram o uso de assinaturas às cegas para assinar os pseudônimos dos medidores inteligentes [Finster and Baumgart 2013]. Os pseudônimos dos medidores são assinados às cegas pelo gerenciador de chaves. Os autores utilizam uma rede anonimizada para evitar que a empresa de energia mapeie a identidade do pseudônimo através da interface de rede. Nessa rede, as medições são transmitidas aleatoriamente entre alguns medidores antes de ir para a empresa de distribuição. No final, os autores criam perfis de consumidores vinculados aos pseudônimos. O problema desta solução é que os perfis criados para os consumidores podem ser cruzados com outras fontes de dados, possibilitando o mapeamento entre os pseudônimos e as identidades dos usuários.

Também foram desenvolvidas soluções com *secure multi-party computation* [Tonyali et al. 2018], mas o custo computacional e de comunicação são altos, dificultando a escalabilidade do sistema em medidores inteligentes.

Esse trabalho propõe um mecanismo de preservação de privacidade dos dados de medição. A assinatura às cegas dificulta o mapeamento entre pseudônimos e a identidade real dos medidores. A agregação descentralizada, feita pelos próprios medidores, protege a rede contra agregadores curiosos. A cada rodada, um novo medidor é responsável pela agregação dos dados de uma região. Os medidores validadores e o agregador são escolhidos de forma aleatória através de funções *hash*. As configurações de rede dificultam o mapeamento da identidade dos medidores através da interface de rede. Assim, a proposta protege o usuário contra agentes maliciosos externos ao sistema e também contra empresas curiosas.

3. Mecanismo de Privacidade Proposto

O sistema proposto trabalha com dois tipos de dados de medição: dados de faturamento e dados de operação. O foco do artigo e desta seção é a privacidade dos dados de operação, coletados a cada 15 minutos. A medição dos dados de faturamento é descrita na Subseção 3.6. A medição dos dados de operação, ilustrada na Figura 1, é composta pelos seguintes elementos:

- Medidor inteligente: responsável por coletar as informações de medição do cliente e enviar, a cada 15 minutos, para o agregador.
- Agregador: neste trabalho, o agregador é um medidor inteligente responsável pelo recebimento dos dados de consumo dos outros medidores, agregação e envio do consumo consolidado para o centro de controle. A cada rodada, um novo agregador é escolhido.
- Validadores: medidores com a responsabilidade de validar a agregação. Em caso de falha do agregador, os validadores escolhem um novo agregador. O número de validadores da região (V) corresponde a equação $V = 2F + 1$, onde F é o número de falhas na validação suportadas pelo mecanismo para manter o funcionamento correto.
- *Gateway* local: realiza a interligação entre o centro de controle, o gerenciador de chaves e os medidores.
- Gerenciador de chaves: elemento responsável pela autenticação dos medidores e assinatura às cegas dos pseudônimos.

- Centro de controle: elemento responsável pelo processamento dos dados coletados pelos agregadores, realizando análises e tomadas de decisões.

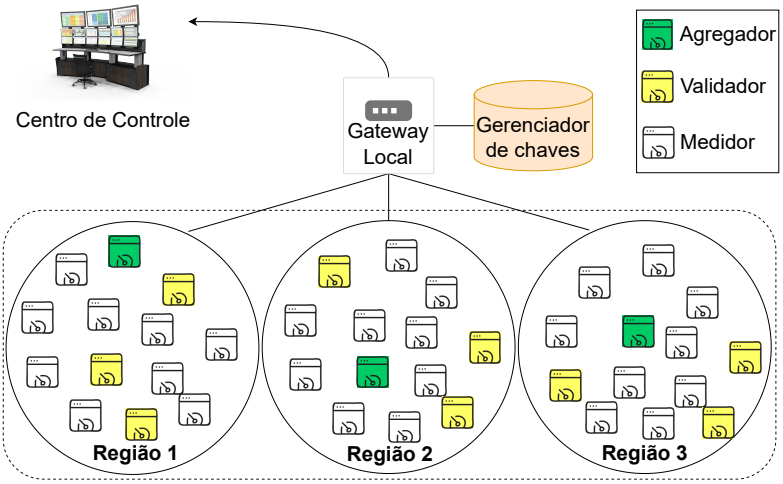

Figura 1. Visão geral do sistema.

Os medidores estão agrupados por região. A cada rodada um agregador e os validadores são escolhidos para região. Os dados são agregados na região e enviados para o centro de controle através do *gateway* local. Durante este trabalho, o agregador e os validadores também são chamados de líderes.

3.1. Pseudônimos Assinados às Cegas

Os pseudônimos são assinados com uma técnica denominada assinatura às cegas para garantir a autenticidade das mensagens e o anonimato dos usuários. Esta técnica permite ao servidor assinar mensagens, pertencentes a usuários autenticados, sem conhecer o real conteúdo da mensagem. No esquema de assinatura com RSA (Rivest-Shamir-Adleman) às cegas, o cliente gera uma mensagem, atribui um fator de cegueira à mensagem e envia para um servidor. O servidor devolve para ao cliente a mensagem assinada. O cliente retira o fator de cegueira obtendo a mensagem original assinada pelo servidor. Partindo do princípio que d é a chave privada RSA, e é a chave pública e m a mensagem original. O cliente introduz na mensagem um fator de cegueira $r^e mod(n)$, conforme a Equação 1. O r é um número tal que $1 < r < n$ e que obedece à Equação 2. O n é o produto dos números primos usados para gerar as chaves RSA. O servidor recebe e assina m' conforme a Equação 3. O cliente recebe s', retira o fator de cegueira e obtém m assinada, conforme a Equação 4.

$$m' = mr^e mod(n) \tag{1}$$

$$mdc(r, n) = 1 \tag{2}$$

$$s' = (m')^d mod(n) \tag{3}$$

$$s = (s')r^{-1} mod(n) = m^d mod(n) \tag{4}$$

No caso dos pseudônimos, o medidor do cliente gera uma chave pública RSA para ser o pseudônimo do medidor. O pseudônimo é assinado às cegas pelo gerenciador de chaves. Assim, o medidor tem um pseudônimo validado pela assinatura do gerenciador de chaves,

mas o gerenciador de chaves desconhece a associação do pseudônimo e seu respectivo medidor.

3.2. Funcionamento do Modelo Proposto

Na inicialização do sistema, os medidores inteligentes autenticam-se no gerenciador de chaves utilizando suas identidades reais. Em seguida, cada medidor gera um par de chaves RSA, onde a chave pública é o seu pseudônimo. Estes pseudônimos são assinados às cegas pelo gerenciador de chaves. Os medidores divulgam seus pseudônimos assinados para a região. Os primeiros validadores e o agregador são selecionados através do critério de proximidade à média dos valores das chaves públicas (após convertê-las em números usando hash SHA-256).

Após a fase de inicialização, começa a etapa de medição. O consumo c é criptografado com as chaves públicas do agregador K_{Pub_AG} ou dos validadores K_{Pub_VL}, e depois é concatenado com o tempo de medição t, conforme a Equação 5. A mensagem final de medição, enviada para os líderes da rede, está representada pela Equação 6. Onde m é o resultado da Equação 5, $Ass(m, K_{Priv\_Pseud})$ é a assinatura de m com a chave privada do medidor, $Pseud$ é o pseudônimo, e $Ass(Pseud, K_{Priv\_Gerenciador})$ é a assinatura do pseudônimo com a chave privada do gerenciador de chaves.

$$m = E(K_{Pub\_AG}, c)||t \quad ou \quad m = (K_{Pub\_VL}, c)||t \tag{5}$$

$$M_{final} = m||Ass(m, K_{Priv\_Pseud})||Pseud||Ass(Pseud, K_{Priv\_Gerenciador}) \tag{6}$$

Essa estrutura de mensagem previne o vazamento de informação caso a mensagem seja interceptada por um terceiro. O consumo foi criptografado com a chave pública do agregador, garantindo que apenas o agregador, ao utilizar sua chave privada, possa decifrar e acessar o valor da medição. A segunda informação, assinatura $Ass(m, K_{Priv\_Pseud})$, impede que um atacante tente se passar pelo medidor. Não basta conhecer um pseudônimo válido, o atacante também precisa da chave privada do medidor. A assinatura do pseudônimo certifica que o pseudônimo pertence a um medidor válido na rede.

As mensagens são enviadas para o medidor agregador e para os validadores. O agregador processa os dados de medição e solicita a validação da agregação, encaminhando os dados para os validadores. O funcionamento do agregador está descrito na Subseção 3.3. Os validadores verificam os dados agregados, comparando com os dados recebidos diretamente dos medidores. Se não houver erros, a agregação é validada e devolvida para o agregador. Se houver erros, os validadores realizam ações de tratamento de erro. O funcionamento dos validadores está descrito na Subseção 3.4. Ao receber a validação, o agregador envia a agregação para o centro de controle. Depois, seleciona os novos líderes, conforme Subseção 3.5, e transmite uma lista com os novos líderes aos medidores da rede. Os medidores verificam a lista com novos líderes e uma nova rodada é iniciada.

3.3. Agregação

As etapas operacionais do medidor agregador seguem o fluxograma da Figura 2. A caixa verde corresponde ao início do fluxo e a caixa vermelha encerra as operações do agregador. Na caixa de erro, V/2 é o número de validadores da região dividido por 2. CC corresponde ao Centro de Controle.

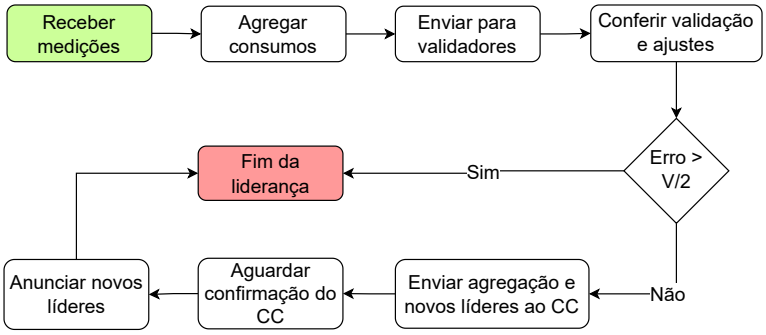

Figura 2. Fluxograma de funcionamento do agregador.

Inicialmente, os medidores enviam os dados de medição para o agregador. Ao receber uma mensagem, o agregador verifica o pseudônimo assinado pelo gerenciador de chaves $Ass(Pseud, K_{Priv\_Gerenciador})$, e o consumo assinado com o pseudônimo $Ass(m, K_{Priv\_Pseud})$. Vale ressaltar que o pseudônimo corresponde à chave pública RSA do medidor. Se houver algum erro, a mensagem é descartada. Na ausência de erro, o agregador descriptografa o dado de consumo e utiliza-o no processo de agregação. Nesse processo, os dados dos medidores são somados e enviados para os validadores. Os validadores recebem a soma dos consumos e uma lista do consumo por IP do medidor. Se a agregação for aprovada pela maioria dos validadores, o agregador envia a soma dos consumos assinada para o centro de controle, atualiza a rede com os novos líderes e executa as funções para encerrar sua rodada como líder. Se houver erro, os validadores trocam mensagens com o agregador, identificando inconsistências e enviando as assinatura das mensagens recebidas. Após a verificação das inconsistências, se a maior parte dos validadores encontrar erro na agregação, o agregador perde a liderança e os validadores selecionam um novo agregador, conforme explicado na Subseção 3.5. O agregador notifica o centro de controle com as inconsistências existentes.

3.4. Validação

As etapas de funcionamento dos validadores estão descritas na Figura 3. A caixa verde corresponde ao início do fluxo e a caixa vermelha encerra as operações do validador. Na caixa de erro, V é o número de validadores da região. Os validadores são responsáveis por verificar e validar os dados processados pelos agregadores. O validador recebe os dados de consumo dos medidores e aguarda a solicitação de validação enviada pelo agregador. Junto com os dados de consumo, o validador envia um *Nonce* para os outros validadores. O *Nonce* é um valor aleatório usado na escolha dos novos líderes. A solicitação do agregador contém a soma dos consumos assinada pelo agregador e uma lista de consumo por IP dos medidores. O validador verifica a assinatura e compara a soma dos consumos enviada pelo agregador com a soma dos dados recebidos diretamente dos medidores. Se as somas forem diferentes, os validadores conferem a lista das medições recebidas pelo agregador com as medições recebidas pelos validadores. Os validadores trocam mensagens com o agregador para mitigar inconsistências. Na persistência do erro, o validador anuncia o erro aos demais validadores e aguarda as respostas. Caso a maioria dos validadores aprove a agregação, o erro é do validador e a mensagem de validação é enviada notificando o erro do validador. Se o erro for detectado pela maioria dos validadores, o erro é do agregador. Os validadores notificam o erro ao centro de controle. Um dos vali-

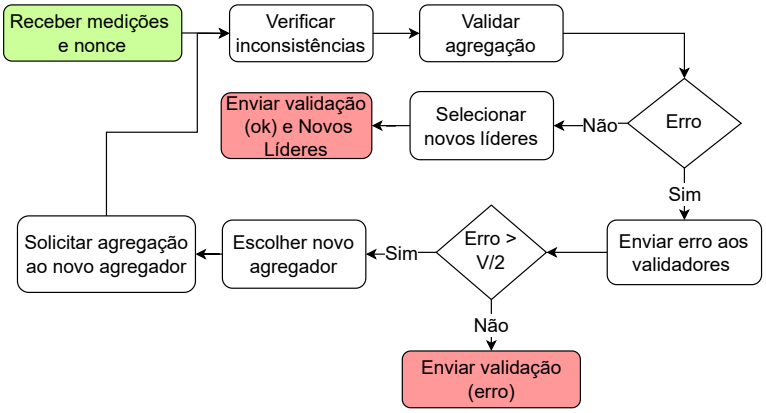

Figura 3. Fluxograma de funcionamento do validador.

dadores se torna o novo agregador, conforme a Subseção 3.5. Em seguida, os validadores solicitam agregação ao novo agregador. Ao aprovar uma agregação, o validador envia a validação e os novos líderes assinados ao agregador.

3.5. Seleção de Novos Líderes

Os medidores armazenam a lista de IP por pseudônimo. Esta lista é utilizada na seleção dos líderes para a próxima rodada. A lista está em ordem de IP, para que todos tenham listas iguais. Para a seleção de novos líderes, os validadores somam os *Nonces* recebidos pelos validadores durante a etapa de envio de medição. A soma dos *Nonces* (incrementada com +1, +2...) alimenta funções hash para calcular índices da lista de medidores. Os medidores correspondentes aos índices selecionados serão os novos líderes, onde o medidor de maior índice será o agregador. Os validadores enviam os novos líderes assinados para o agregador, junto com a validação. O agregador envia a agregação e os novos líderes assinados para o centro de controle. A rodada de medição encerra com o agregador atualizando a rede com os novos líderes assinados pelo centro de controle.

3.6. Dados de Faturamento e Configurações de Rede

Os dados de faturamento precisam conter a identidade real do medidor. O faturamento é realizado a cada 15 ou 30 dias. Neste tipo de medição, o medidor envia o consumo consolidado do período de medição diretamente para a empresa. Estes dados não expõem os hábitos de consumo do usuário. Entretanto, a empresa pode identificar o pseudônimo correspondente ao medidor através da informação de rede. Através da mensagem de faturamento, a empresa pode mapear o endereço de IP, ou MAC, correspondente ao medidor. E com a mensagem de operação a empresa pode mapear o pseudônimo referente ao IP, ou ao MAC. Para evitar essa associação entre medidor e pseudônimo, todos os medidores de uma região utilizam dois endereços de IP e dois MACs. O IP1 e o MAC1 são usa nos dados de faturamento, onde o IP1 é atribuido com DHCPv6 e o MAC1 é o MAC da interface de rede. O IP2 e MAC2 são usados nas medições de operação, onde o IP2 é obtido utilizando SLAAC e o MAC2 é um MAC temporário.

Para lidar com falhas de rede, o mecanismo proposto utiliza *timeout* durante as etapas de medição/agregação, validação e atualização da rede. Se um líder não receber

mensagem de algum medidor, esta medição é complementada na verificação de inconsistências da etapa de validação.

4. Análise e Resultados

As análises estão divididas em duas etapas. A primeira etapa mede o custo computacional e de comunicação dos modelos de medição com diferentes técnicas de privacidade. Estes modelos são emulações implementadas em Python usando as bibliotecas PyCryptodome, python-Paillier e shamirs. A segunda etapa verifica a segurança e a privacidade do modelo proposto, comparando-o a outros modelos. Neste trabalho, a criptografia AES(*Advanced Encryption Standard)* possui chave do tamanho de 128 bits. As criptografias de Paillier e RSA possuem chaves com tamanho de 1024 bits. O Raspberry Pi 3 Model B é usado na emulação, com CPU 1.2GHz x 4, 1GB de RAM.

4.1. Modelo do Atacante

A empresa é considerada honesta mas curiosa [Joshi et al. 2022]. Ou seja, a empresa não tem interesse em adulterar os dados de medição, mas se tiver oportunidade deseja invadir a privacidade dos usuários. Se tiver acesso aos dados de medição, coletados quase em tempo real, a empresa curiosa poderá extrair informações sensíveis sobre a privacidade dos clientes, como os horários em que a casa fica vazia, hábitos de consumo do usuário e até mesmo os dispositivos elétricos presentes em uma casa. A rede está vulnerável a ataques de agentes maliciosos externos, que podem interceptar, replicar mensagens antigas ou injetar dados falsos. Além disso, também está sujeita a ameaças internas, onde agentes maliciosos podem adulterar medidores para manipular a agregação, validação e medições.

4.2. Modelos de Medição para Comparação

A primeira etapa de análise compara o desempenho de quatro modelos de medição: RSA às cegas, Homomórfico, Terceiro confiável e Shamir. O modelo RSA às cegas, usa assinaturas às cegas para assinar os pseudônimos [Finster and Baumgart 2013]. O medidor utiliza a identidade real para autenticar no gerenciador de chaves, em seguida, o gerenciador de chaves assina às cegas o pseudônimo do medidor, que é uma chave pública RSA. As mensagem enviadas ao agregador são criptografadas usando o pseudônimo do agregador. O agregador consolida os dados de medição de uma região e envia o consumo total para o centro de controle.

O modelo Homomórfico utiliza um sistema de criptografia parcialmente homomórfica de Paillier [Tonyali et al. 2015]. Os medidores possuem a chave pública de Paillier e o centro de controle possui a chave privada. Os medidores criptografam os dados e enviam para os agregadores. Os agregadores recebem os dados criptografados e realizam a soma com a propriedade homomórfica aditiva de Paillier. O centro de controle recebe os dados do agregador, descriptografa e identifica o consumo da região.

No modelo Terceiro confiável, o gerenciador de chaves autentica os pseudônimos do cliente [Tonyali et al. 2015]. A troca de chave AES é feita por meio da criptografia RSA. Durante a medição, a chave AES criptografa o consumo. O agregador recebe os dados, descriptografa e realiza a soma dos consumos da região. O agregador envia os dados consolidados para o centro de controle.

O modelo Shamir é baseado em *secure multi-party computation* e utiliza *shamir secret sharing* para realizar a soma dos consumos dos medidores pertencentes a região [Rottondi et al. 2012]. Em cada rodada os medidores dividem o consumo medido em N partes, onde N representa o número de medidores da rede. Em seguida, armazenam uma parte do segredo e enviam as demais partes, assinadas, para os outros medidores. Os medidores somam todas as partes recebidas e enviam ao agregador. O agregador soma todas as somas recebidas e realiza a interpolação para descobrir a agregação dos dados. Depois envia a agregação para o centro de controle.

4.3. Desempenho dos Modelos de Medição

A comparação de desempenho é composta por análises de custo computacional (uso da CPU) e de taxa de transferência da rede (carga de rede). O uso de CPU é medido durante as trocas de mensagens de medição, variando-se o número de nós associados ao agregador. Os testes consistem na execução de 10 rodadas de medição com intervalos de 15 minutos entre cada rodada, conforme a frequência de coleta dos dados de monitoramento. A Figura 4(a) ilustra os resultados desses testes.

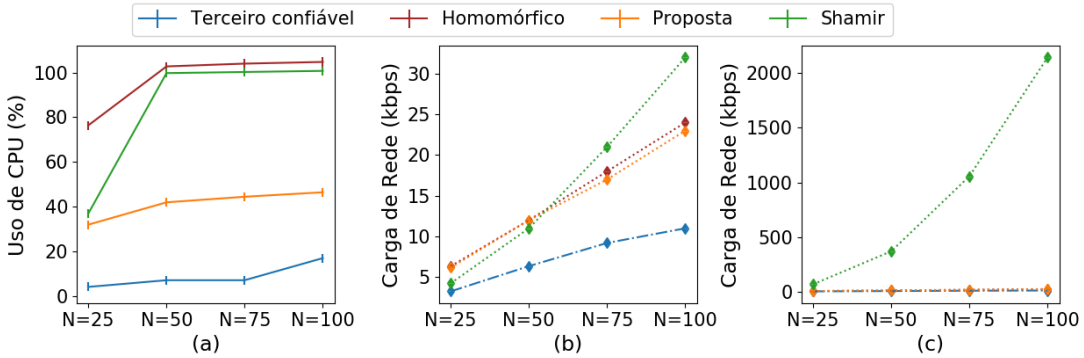

Figura 4. (a) Uso de CPU no agregador. (b) Carga de rede dos agregadores. (c) Carga de rede referente a todos os nós da rede.

Os modelos Homomórfico e Shamir apresentam os maiores custos computacionais, com uso de CPU próximos de 100%. O uso máximo de CPU do modelo Terceiro confiável é de 17%, representando o menor custo computacional. O modelo RSA às cegas obteve um custo computacional intermediário, quando comparado aos demais modelos, chegando a ser 44% menor que o Homomórfico e 46% menor que o Shamir.

A segunda análise avalia a variação da carga de rede (kbps) de acordo com o número de nós associados ao agregador. A Figura 4(b) mostra a carga de rede no agregador, e a Figura 4(c) mostra a carga de rede em todos os nós da região. Os modelos Homomórfico e o RSA às cegas apresentam fluxo de dados no agregador maior que o modelo Terceiro confiável. Isso ocorre porque o texto cifrado AES é muito menor que o texto cifrado de Paillier ou do RSA às cegas. O modelo Shamir tem a carga de rede no agregador um pouco maior que os outros modelos, porém apresenta o maior crescimento da carga total à medida que o número de nós na rede aumenta, conforme ilustrado na Figura 4(c). Esse crescimento ocorre devido à intensa troca de mensagens entre todos os nós durante a etapa de medição. Em uma rede com 100 nós, a carga total de rede no

modelo Shamir é 93 vezes maior que a do modelo proposto. Por esse motivo, o modelo Shamir torna-se inviável para medições inteligentes.

Os modelos Homomórfico e Terceiro confiável utilizam técnicas criptográficas frequentemente aplicadas em soluções de medições inteligentes. Logo, os testes de desempenho mostram a viabilidade do uso de assinatura às cegas, por apresentar custo computacional e de rede intermediários aos modelos Homomórfico e Terceiro confiável. Entretanto, por serem técnicas orientadas à privacidade, a análise de segurança é essencial na escolha da técnica apropriada para um sistema de medição inteligente. A análise quantitativa pode desqualificar um modelo devido à impossibilidade de uso prático em um sistema real. Porém, o modelo deve proteger a privacidade dos usuários contra agentes maliciosos. O modelo Terceiro confiável, por exemplo, tem o melhor desempenho entre os modelos, mas possui falhas graves de segurança apresentadas na Subseção 4.4.1.

4.4. Análise de Segurança e Privacidade

Esta seção apresenta análises qualitativas dos modelos. A primeira análise compara a segurança e a privacidade da proposta em relação aos demais modelos de medição. A segunda análise apresenta o comportamento do modelo proposto diante de ataques de segurança.

4.4.1. Comparação entre os Modelos

O modelo Shamir mostrou-se inviável do ponto de vista de desempenho, por isso não está contemplado nesta análise. Os requisitos mínimos de segurança são baseados no trabalho [Asghar et al. 2017]: confidencialidade, integridade, autenticidade e não repúdio.

No modelo Homomórfico, o medidor assina as mensagens com a chave privada RSA, atendendo assim aos requisitos de autenticidade, não repúdio e integridade. Se a mensagem for adulterada, a verificação da assinatura falhará. A criptografia de dados impede que agentes externos ao sistema tenham acesso aos dados do usuário. A agregação homomórfica dos dados promove privacidade em relação aos agentes internos. Apenas o centro de controle possui a chave privada Paillier. Entretanto, a empresa de energia pode interceptar os dados de medição antes que cheguem ao agregador e utilizar a chave privada de Paillier, pertencente ao centro de controle, para descriptografar as medições, obtendo assim o consumo do pseudônimo em cada rodada.

Apesar do Terceiro confiável ter o melhor desempenho, com a menor carga de rede e uso de CPU abaixo de 20%, a criptografia AES falha ao não garantir o não repúdio ou autenticidade do usuário originário. A chave criptográfica não é conhecida exclusivamente pelo medidor, e o pseudônimo do medidor é conhecido pelos outros participantes da rede. Quanto à confidencialidade, este é um modelo baseado na confiança de terceiros. O gerenciador de chaves conhece a associação entre o pseudônimo e seu medidor. Por se tratarem de dados valiosos, mesmo que o terceiro confiável seja gerenciado por outra empresa, há o risco de vazamento desses dados, comprometendo a privacidade de todo o sistema. Permanece o grande desafio de encontrar um terceiro que seja verdadeiramente confiável.

No modelo RSA às cegas, as mensagens são assinadas com a chave privada RSA do medidor, garantindo a origem da mensagem. Os dados são criptografados com a

chave pública RSA do agregador, garantindo que somente o agregador acesse os dados de medição. Os pseudônimos são assinados às cegas, e mesmo o gerenciador de chaves desconhece a associação entre o pseudônimo e seu respectivo medidor. Entretanto, somente o uso de assinatura às cegas não garante a privacidade dos dados de medição. A associação entre pseudônimo e identidade real pode ser feita através da interface de rede.

Finster e Baumgart utilizam uma rede anonimizada para impedir a associação direta entre o pseudônimo e identidade dos medidores [Finster and Baumgart 2013]. Porém, criaram perfis de consumo dos pseudônimos, possibilitando a associação indireta através do cruzamento de outras bases de informação dos clientes.

Nesta proposta, o uso da agregação distribuída evita a criação de perfis de consumo por parte de um agregador curioso. A configuração de rede com dois IPs e dois MACs dificulta a associação da identidade do medidor através da interface de rede. A Tabela 1 apresenta a comparação de segurança dos modelos de medição, onde a solução proposta se mostrou mais adequada para preservação de privacidade em medições inteligentes.

Tabela 1. Comparação da proposta com os outros modelos.

Características	Terceiro Confiável	Homomórfico	RSA às cegas	Finster e Baumgart	Proposta
Confidencialidade	✓	✓	✓	✓	✓
Autenticidade	✗	✓	✓	✓	✓
Não repúdio	✗	✓	✓	✓	✓
Integridade	✗	✓	✓	✓	✓
Evita o gerenciador de chaves de mapear os pseudônimos	✗	✗	✓	✓	✓
Evita conluio entre empresa de energia e terceiros	✗	✗	✓	✓	✓
Evita o agregador curioso	✗	✗	✗	✓	✓
Evita a criação de perfis de consumo para os pseudônimos	✗	✗	✗	✗	✓

4.4.2. Ataques ao Modelo Proposto

Com base no modelo do atacante, esta subseção analisa o modelo proposto diante de agentes maliciosos.

Em relação aos ataques externos, o uso de pseudônimo protege a identidade do usuário caso uma medição seja interceptada. Somente o agregador possui a chave para descriptografar o consumo, conforme mostrado na Equação 6. Se um atacante obtiver o pseudônimo de um medidor, não conseguirá gerar mensagens falsas, pois a assinatura das mensagens requer a posse da chave privada. Se uma mensagem antiga for replicada, as etiquetas de tempo das medições permitirão que os medidores identifiquem o ataque.

Em relação a ataques internos, foram realizados testes medindo a taxa de sucesso na agregação mediante a ataques de medidores maliciosos. O mecanismo proposto funciona de forma correta se o número de validadores honestos for maior que o número de medidores maliciosos. Ao assumir uma posição de liderança, os medidores maliciosos modificam a agregação dos dados para enganar o centro de controle. A Figura 5 apresenta a taxa de sucesso do mecanismo variando-se o número de medidores maliciosos e o número de validadores. Para os teste foram realizados 100 *rounds* de medição em uma

rede com 100 nós. Os resultados obtidos confirmam as expectativas teóricas: a taxa de

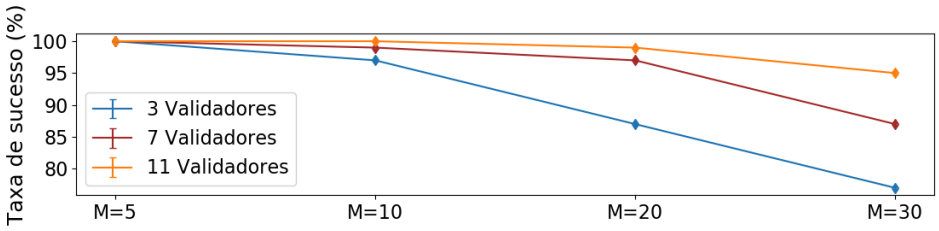

Figura 5. Taxas de sucesso na agregação diante de medidores malicioso(M).

sucesso reduz à medida que o número de medidores maliciosos aumenta e o número de validadores diminui. Os testes também demonstraram a resiliência do sistema. Teoricamente, uma rede com 5 medidores maliciosos precisaria de 11 validadores para evitar falhas. Entretanto, as simulações realizadas com apenas 3 validadores não registraram erros de agregação. Ou seja, o mecanismo de validação apresenta uma robustez maior do que o esperado.

5. Conclusão

Preservar a privacidade dos usuários durante a medição inteligente é uma questão crítica em redes inteligentes. Este artigo apresenta um mecanismo de preservação de privacidade contra empresas curiosas, usando assinatura às cegas e agregação descentralizada. A proposta foi validada através da análise de desempenho e por meio da análise qualitativa dos modelos de medição de preservação de privacidade, comparando-os em termos de desempenho e segurança. Na avaliação de desempenho, a técnica de assinatura às cegas apresentou um uso de CPU 44% menor que o do modelo Homomórfico e 46% menor que o do modelo Shamir. Em comparação com o modelo Terceiro Confiável, a proposta exige mais recursos computacionais e de rede, oferecendo, em contrapartida, maior segurança e privacidade. O mecanismo demonstrou ser eficiente tanto na proteção da privacidade dos dados de medição contra agentes maliciosos externos quanto contra ameaças internas ao sistema. A proposta apresentou melhor equilíbrio entre privacidade, custos computacionais e de comunicação, impedindo a criação de perfis de consumidores que pudessem revelar a identidade dos usuários. Em trabalhos futuros, seria interessante analisar o comportamento dos modelos de medição diante de ataques de medidores maliciosos, realizar análises com número maior de medidores por região. Além disso, seria interessante estender a análise de privacidade aos dados de serviços, contemplando os requisitos dos diferentes serviços que podem ser oferecidos.

Referências

Ahir, R. K. and Chakraborty, B. (2022). A novel cluster-specific analysis framework for demand-side management and net metering using smart meter data. *Sustainable Energy, Grids and Networks*, 31:100771.

Asghar, M. R., Dán, G., Miorandi, D., and Chlamtac, I. (2017). Smart meter data privacy: A survey. *IEEE Communications Surveys & Tutorials*, 19(4):2820–2835.

Devlin, M. A. and Hayes, B. P. (2019). Non-intrusive load monitoring and classification of activities of daily living using residential smart meter data. *IEEE transactions on consumer electronics*, 65(3):339–348.

Eibl, G. and Engel, D. (2014). Influence of data granularity on smart meter privacy. *IEEE Transactions on Smart Grid*, 6(2):930–939.

Finster, S. and Baumgart, I. (2013). Pseudonymous smart metering without a trusted third party. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1723–1728. IEEE.

Finster, S. and Baumgart, I. (2015). Privacy-aware smart metering: A survey. *IEEE communications surveys & tutorials*, 17(2):1088–1101.

Joshi, S., Li, R., Bhattacharjee, S., Das, S. K., and Yamana, H. (2022). Privacy-preserving data falsification detection in smart grids using elliptic curve cryptography and homomorphic encryption. In *2022 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 229–234. IEEE.

Junior, W. L. R., Borges, F. A., Veloso, A. F. d. S., de AL Rabêlo, R., and Rodrigues, J. J. (2019). Low voltage smart meter for monitoring of power quality disturbances applied in smart grid. *Measurement*, 147:106890.

Kua, J., Hossain, M. B., Natgunanathan, I., and Xiang, Y. (2023). Privacy preservation in smart meters: current status, challenges and future directions. *Sensors*, 23(7):3697.

Lazzari, F., Mor, G., Cipriano, J., Gabaldon, E., Grillone, B., Chemisana, D., and Solsona, F. (2022). User behaviour models to forecast electricity consumption of residential customers based on smart metering data. *Energy Reports*, 8:3680–3691.

Li, K., Yang, Y., Wang, S., Shi, R., and Li, J. (2021). A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid. *Computers & Security*, 103:102189.

Rottondi, C., Savi, M., Polenghi, D., Verticale, G., and Krauß, C. (2012). Implementation of a protocol for secure distributed aggregation of smart metering data. In *2012 International Conference on Smart Grid Technology, Economics and Policies (SG-TEP)*, pages 1–4. IEEE.

Singh, P., Masud, M., Hossain, M. S., and Kaur, A. (2021). Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid. *Computers & Electrical Engineering*, 93:107209.

Sultan, S. (2019). Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey. *Computers & Security*, 84:148–165.

Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A. S., and Nojoumian, M. (2018). Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems. *Future Generation Computer Systems*, 78:547–557.

Tonyali, S., Saputro, N., and Akkaya, K. (2015). Assessing the feasibility of fully homomorphic encryption for smart grid ami networks. In *2015 Seventh International Conference on Ubiquitous and Future Networks*, pages 591–596. IEEE.

Van Aubel, P. and Poll, E. (2019). Smart metering in the netherlands: What, how, and why. *International Journal of Electrical Power & Energy Systems*, 109:719–725.

Zhang, S., Zhang, Y., and Wang, B. (2023). Antiquantum privacy protection scheme in advanced metering infrastructure of smart grid based on consortium blockchain and rlwe. *IEEE Systems Journal*.