

Plataforma para Coleta de Dados de Eletropostos para Veículos Elétricos: Prototipação em Bancada de Testes Real

Felipe Araújo¹, Stefany Pinheiro¹, Iago Medeiros¹, Denis Rosário¹,
Eduardo Cerqueira¹, Ubiratan Bezerra¹, Maria Tostes¹, Andréia Antloga²

¹Universidade Federal do Pará (UFPA) – Belém, PA – Brazil

²Norte Energia S.A – Brasília, DF – Brazil

stefpinheiro9@gmail.com, iago.medeiros@itec.ufpa.br

{felipearaujo, denis, cerqueira, bira, tostes}@ufpa.br,

andreianascimento@norteenergiasa.com.br

Abstract. *Electric vehicles are a promising option to contribute to energy diversification and the goal of reducing greenhouse gas emissions. However, as the market grows, the demand for charging stations increases, which requires a new structure to manage them. Internet of Things (IoT) technologies stand out as one of the most prominent strategies, as electric stations become smart, connected, and easily accessible for remote support and maintenance. In this context, this paper proposes a real test bench carried out at the Federal University of Pará, containing a charging station and an electric vehicle, communicating through message exchange with a central system based on the OCPP protocol. The data from these transactions are sent to DOJOT, a middleware IoT that makes it possible to store, process, and integrate the information collected with various sensors.*

Resumo. *Os veículos elétricos são uma opção promissora para contribuir na diversificação energética e nos objetivos de redução das emissões de gases do efeito estufa. Contudo, à medida que o mercado cresce, a demanda por estações de recarga aumenta, o que requer uma nova estrutura para gerenciar essas demandas de carregamento. As tecnologias de Internet das Coisas (IoT) destacam-se como uma das estratégias mais proeminente, uma vez que os eletropostos tornam-se inteligentes, conectados e facilmente acessíveis para suporte e manutenção remotos. Nesse contexto, este artigo propõe uma bancada de testes real realizada na Universidade Federal do Pará, contendo um eletroposto, abastecendo um veículo elétrico, e comunicando por meio de troca de mensagens com um sistema central baseado no protocolo OCPP. Os dados dessas transações são enviados à plataforma DOJOT, um middleware IoT que torna possível armazenar, processar e integrar as informações coletadas de diversos sensores.*

1. Introdução

Os Veículos Elétricos (VEs) fazem parte das tecnologias com potencial de impacto no desempenho dos sistemas de transporte futuro, sendo uma opção promissora para contribuir com a diversificação energética e redução da emissão de gases do efeito estufa

[Lombardi et al. 2018]. Esses são alguns dos motivos por trás do apoio na implantação dessa modalidade de transporte. Um sistema de VE requer estações de recarga dos veículos, também conhecidas como eletropostos, além de um sistema central de gerenciamento. Os dados desse sistema são coletados por meio da adoção de protocolos de comunicação na infraestrutura de carregamento de veículos elétricos, tal como o Open Charge Point Protocol¹ (OCPP). Contudo, à medida que o mercado cresce, a demanda por estações de recarga aumenta, o que requer uma nova estrutura para gerenciar essas demandas de carregamento [Eisenbarth et al. 2021]. Por exemplo, a maioria dos postos de abastecimento de veículos elétricos são descentralizados e têm uma estrutura muito complexa, o que dificulta o gerenciamento e manutenção dos sistemas.

As estações de carregamento de veículos elétricos precisam estar *online* o tempo todo, pois os usuários carregam seus carros com um aplicativo. Contudo, caso uma estação fique *offline*, isso deve ser informado o mais rápido possível, pois a compreensão do *status* em tempo real dos eletropostos pode fornecer informações valiosas aos usuários e ao operador do sistema, como disponibilidade e reservas. Nesse sentido, as tecnologias de computação ubíqua e pervasiva podem ser aplicadas ao propor plataformas que facilitem o gerenciamento das informações de sistemas de abastecimento inteligente. Por exemplo, as tecnologias de Internet das Coisas, do inglês *Internet of Things* (IoT), destacam-se como uma das estratégias mais proeminentes, capaz de controlar objetos em tempo real e prover informações inteligentes aos usuários [Mota et al. 2019].

Com a tecnologia IoT, as estações de carregamento de VE tornam-se inteligentes, conectadas e, portanto, facilmente acessíveis para suporte e manutenção remotos. Entretanto, para a análise eficaz dos dados do sistema, é importante considerar um *middleware* IoT, tal como a DOJOT², que centralize a coleta e disponibilização das informações provenientes dos diferentes sensores [Saleem et al. 2019]. Um *middleware* de IoT pode ser definido como um *software* (plataforma) que atua entre os componentes do ecossistema de IoT, viabilizando a comunicação entre esses elementos, com o objetivo de integrar sistemas heterogêneos.

Dessa forma, as informações poderiam ser facilmente gerenciadas e disponibilizadas por meio de diversas possibilidades de conectividade e processamento que podem ser aplicados na coleta de dados, bem como para previsões de situações do cotidiano [Modesto et al. 2021]. Por exemplo, através do protocolo OCPP é possível coletar informações de carregamentos, autenticar e autorizar os usuários, assim como validar o carregamento dos VEs [Răboacă et al. 2021]. Sendo assim, o OCPP provê meios para coletar informações para gerenciamento dos eletropostos, tais como *status* (online/offline) e variáveis de carregamento (corrente, tensão, consumo etc.). Essas informações poderiam ser enviadas e armazenadas em um *middleware* IoT e requisitadas por um software de gerenciamento de abastecimento dos VEs.

Para atender a tais questões, o objetivo desse trabalho é apresentar um estudo de caso da integração entre o OCPP e a DOJOT (*middleware* IoT), a fim de disponibilizar os dados coletados das estações de recarga em uma nuvem e permitir a conferência e análise de consumo no cenário de VEs. Para isso, um sistema central de gerenciamento será desenvolvido com base na padronização do protocolo OCPP, para lidar com autenticação

¹<https://www.openchargealliance.org/>

²<https://dojot.com.br/>

e transações de recargas. Vale a pena enfatizar que uma contribuição importante deste artigo se dá pela apresentação de uma bancada de testes real que compreende uma infraestrutura de VE, eletroposto e *middleware* IoT implantados na Universidade Federal do Pará (UFPA). Essa bancada de testes tem como objetivo oferecer a perspectiva de experimentações em sistemas de recarga de VEs e *middleware* IoT com alto nível de acurácia, e ser expansível para suportar novas tecnologias de ponta sem sofrer com obstáculos de incompatibilidade comuns em sistemas fechados.

Este trabalho será apresentado da seguinte forma. Seção 2 apresenta os principais trabalhos relacionados a este trabalho, onde é ressaltado a importância do uso de eletropostos e sistemas de gerenciamento para carregamento. Seção 3 apresenta a arquitetura do sistema proposto, o protocolo de comunicação OCPP, o *middleware* IoT, além de detalhar o nosso protótipo de bancada de teste. Seção 4 conclui este artigo.

2. Trabalhos Relacionados

[Venkata Pruthvi, Thota et al. 2019] revisaram as funcionalidades que o OCPP oferece e como pode ser utilizado na infraestrutura de carregamento de VEs. Nesse contexto, os autores demonstraram a implementação de um sistema baseado em OCPP, listando as principais funcionalidades e mensagens associadas que são tipicamente implementadas para fornecer funcionalidades básicas a um eletroposto.

[Alcaraz et al. 2017] estudaram as principais propriedades de segurança do OCPP, p.e., comunicação entre os eletropostos e o sistema de gerenciamento de energia. De acordo com os autores, o uso de subversões do protocolo assim como a comunicação com entidades maliciosas pode acarretar a desestabilização das redes de energia.

[Antoun et al. 2020] realizaram uma avaliação detalhada da segurança do ecossistema de carregamento de VEs. De acordo com os autores, diferentes entidades estão envolvidas no processo de carregamento dependendo do local (público ou privado), o que pode comprometer a segurança do sistema. Nesse contexto, eles destacaram e categorizam as possíveis ameaças de acordo com as vulnerabilidades de cada cenário.

[Devendra et al. 2021] projetaram e fabricaram estações de recarga, baseadas no protocolo OCPP, para equipamentos de duas rodas (escooter). Os autores discutem o design do produto com base na fabricação, acessibilidade e capacidade de fabricação em massa. A construção desses eletropostos considerou os pré-requisitos de segurança dos administradores do sistema, instaladores, consumidores, órgãos governamentais e outros.

[Răboacă et al. 2021] analisaram as especificações do OCPP com ênfase no projeto do aplicativo baseado no estado da arte atual. Sendo assim, os autores forneceram uma visão geral de veículos híbridos e elétricos, uma classificação de topologias de estações de carregamento, assim como uma classificação dos protocolos OCPP, considerando as direções de pesquisas futuras.

Com base na análise dos trabalhos relacionados, foi possível concluir que o gerenciamento de eletropostos é essencial para tornar o carregamento de VEs cada vez mais estável, sem possíveis problemas para o usuário final. Assim, plataformas *middleware* podem melhorar questões relacionadas à segurança, armazenamento, processamento e integração das informações de diferentes sensores.

3. Sistema para Coleta e Análise de Dados de Eletropostos

Esta seção apresenta a arquitetura do sistema proposto para gerenciamento de estações de carregamento de veículos elétricos. O trabalho tem duas etapas principais: (1) comunicação entre o eletroposto e o sistema central através do protocolo OCPP; e (2) envio das informações de carregamento dos VEs do sistema central para o *middleware* IoT (DOJOT) através do protocolo *Message Queue Telemetry Transport* (MQTT³). Os detalhes da arquitetura, protocolo OCPP, plataforma DOJOT e a prototipação em bancada de testes real serão descritos a seguir.

3.1. Arquitetura

A Figura 1 apresenta a arquitetura do sistema para permitir a coleta e análise de dados de eletropostos. O sistema de gerenciamento de recarga de veículos elétricos é composto por eletropostos, sistema central, plataforma IoT (*middleware* IoT) e front-end (aplicação). Os eletropostos, também conhecidos como estações de recarga, são os sistemas físicos com um ou mais conectores, no qual múltiplos VEs podem ser carregados. O sistema central, também conhecido como OCPP back-end, administra essas estações e obtém as informações para autorização do usuário. Além disso, ele acompanha as mudanças de estado dos sistemas, que podem indicar fases do carregamento ou falhas.



Figura 1. Arquitetura do sistema

Durante a fase de carregamento, o OCPP back-end coleta informações como corrente, tensão e energia (consumo) e as envia para a plataforma IoT. Neste artigo, considerou-se a plataforma DOJOT como *middleware* IoT. Essa plataforma é responsável por armazenar os dados recebidos em banco de dados e fornecê-los a aplicações externas de forma fácil. Por exemplo, os dados podem ser requisitados através de rotas de uma interface de programação de aplicação (API, do inglês Application Programming Interface) ou através do protocolo *Message Queue Telemetry Transport* (MQTT). Sendo assim, através do *middleware* IoT é possível gerenciar dados de diversos eletropostos e sensores heterogêneos.

3.2. Open Charge Point Protocol

O OCPP é um protocolo aberto padronizado pela Open Charge Alliance (OCA) para comunicação entre eletroposto e um sistema central, também conhecido como OCPP back-end. O OCPP conta com diferentes versões implementadas que passaram por atualizações e acréscimo de funcionalidades. Neste trabalho, optou-se por estudar e implementar a versão 1.6 para a transmissão das mensagens, uma vez que é a versão mais recente suportada pelo fabricante do eletroposto. O OCPP 1.6 possui novos recursos, como: mensagens em JSON (*JavaScript object Notation*) e tecnologia *Websockets*, melhores possibilidades de diagnósticos, mais status de carregamento e mensagem de gatilho. O formato JSON é utilizado para troca de dados entre o sistema central e o eletropostos, devido a um menor

³<https://mqtt.org/mqtt-specification/>

tamanho da mensagem. Além disso, o protocolo possui suporte a carregamento inteligente para balanceamento de cargas e uso de perfis de carregamento.

Existem diferentes perfis de implementação do sistema OCPP, a saber: **Core**, principal perfil e responsável pela funcionalidade básica de um eletroposto; **Firmware Management**, responsável pelo gerenciamento de atualização do *firmware* e o *download* do arquivo de diagnóstico; **Local Auth List**, responsável pelo gerenciamento da lista local de autorizações no eletroposto e **Smart Charging**, responsável pelo carregamento inteligente básico. Esses perfis podem ser usados por um cliente para determinar se um produto OCPP 1.6 possui a funcionalidade necessária para seu caso de negócios.

Toda implementação do protocolo OCPP deve conter, pelo menos, o perfil Core, pois este é o perfil que possui os principais requisitos/operações para o correto funcionamento dos eletropostos. As ações pertencentes ao perfil CORE são: i) *Authorize*: autorização/autenticação do usuário; ii) *BootNotification*: notificação sobre a configuração do eletroposto cada vez que ele inicia ou reinicia; iii) *ChangeAvailability*: mudança de *status* de disponibilidade do eletroposto; iv) *ChangeConfiguration*: mudança de parâmetros de configuração do eletroposto; v) *ClearCache*: executa a limpeza do *cache* de autorização vi) *DataTransfer*: envio de mensagens não suportadas pelo protocolo OCPP; vii) *GetConfiguration*: coleta de informações sobre uma determinada configuração do eletroposto viii) *Heartbeat*: notificação enviada ao sistema central para informar que a conexão ainda está ativa ix) *MeterValues* envio de informações sobre o *hardware* de sensoriamento elétrico do eletroposto; x) *RemoteStartTransaction*: requisição do início da transação de forma remota xi) *RemoteStopTransaction*: requisição do término da transação de forma remota xii) *Reset*: reinício do eletroposto xiii) *Start transaction*: requisição do início de um carregamento; xiv) *Status notification*: mensagem enviada pelo eletroposto ao sistema central para informá-lo de possíveis erros e mudanças de *status*; xv) *Stop transaction*: requisição do término de um carregamento; xvi) *UnlockConnector*: solicitação de desbloqueio do conector.

A OCPP define três tipos de mensagens para a execução das operações acima listadas: CALL, CALLRESULT e CALLERROR. O primeiro refere-se a uma mensagem de requisição para executar uma operação específica ou informar sobre algum atributo (por exemplo, *status* do eletroposto). Se a chamada de requisição for enviada e puder ser tratada corretamente, a resposta será uma mensagem do tipo CALLRESULT. Caso contrário, a resposta será uma mensagem do tipo CALLERROR, informando algum tipo de erro ocorreu. Embora a maioria das mensagens de requisição sejam enviadas do eletroposto para o sistema central, alguns procedimentos são iniciados pelo sistema central.

A mensagem do tipo CALL é composta por quatro campos: i) *MessageTypeId*, referente ao identificador do tipo de mensagem (neste caso, 2); ii) *MessageId*, identificador único da mensagem; iii) *Action*, ação a ser executada; iv) *Payload*, contém os argumentos relevantes para a operação determinada. A mensagem de resposta do tipo CALLRESULT é composta por três campos: i) *MessageTypeId*, identificador do tipo de mensagem (neste caso, 3); ii) *MessageId*, identificador único da mensagem; iii) *Payload*, contém os argumentos relevantes para a operação determinada. O identificador da mensagem de resposta deve ser o mesmo da mensagem de requisição para identificar a qual requisição a resposta pertence. Além disso, o *Payload* possui o conteúdo de resposta. Caso ocorra um erro após ou durante o envio da requisição, o sistema

central retorna a mensagem de erro `CALLERROR`. Esse tipo de mensagem contém cinco campos: i) `MessageTypeId`, referente ao identificador do tipo de mensagem (neste caso, 4); ii) `MessageId`, identificador único da mensagem; iii) `ErrorCode`, código do erro; iv) `ErroDescription`, descrição do erro; v) `ErrorDetails`, detalhes do erro.

Por exemplo, quando um eletroposto é ligado ou reiniciado, ele deve enviar uma requisição (mensagem do tipo `CALL`) ao sistema central para informá-lo sobre a sua configuração (versão, modelo, fornecedor, etc.). Essa ação é conhecida como *BootNotification*. Caso não ocorra um erro após o envio da mensagem de requisição, o sistema central envia para o eletroposto uma mensagem do tipo `CALLRESULT` contendo os seguintes campos: i) `currentTime`, informa o dia e o horário atual; ii) `interval`, define a cada quanto tempo o eletroposto deve notificar o *back-end* que a conexão ainda está ativa (ação denominada *Heartbeat*); iii) `status`, indica o *status* do registro do eletroposto no sistema central (`ACCEPTED`, `REJECTED` ou `PENDING`). Caso ocorra um erro após ou durante o envio da requisição, o sistema central retorna a mensagem de erro `CALLERROR`.

3.3. DOJOT

A DOJOT é uma plataforma brasileira de *software* de código aberto, que surgiu com o objetivo de desenvolver e demonstrar tecnologias para facilitar o desenvolvimento de soluções de IoT [CPqD 2020]. Neste trabalho, utilizou-se a versão 0.7 da DOJOT. Essa plataforma é projetada para coletar e armazenar grandes volumes de dados dos dispositivos. O usuário pode configurar um dispositivo IoT na plataforma através de uma interface gráfica ou através requisições HTTP (API). Os dispositivos IoT são representações virtuais de dispositivos ou entidades reais como, por exemplo, os eletropostos. Dessa forma, para cada eletroposto conectado ao sistema central, é criado também, na DOJOT, um dispositivo virtual para armazenar os dados.

As informações de todos os eletropostos são capturadas pelo sistema central por meio do protocolo OCPP e são enviadas à plataforma DOJOT através do protocolo MQTT. O MQTT tornou-se um padrão para comunicações IoT devido a sua flexibilidade de oferecer suporte a diversos cenários de aplicativos e dispositivos e serviços IoT. Foi projetado como um transporte de mensagens extremamente leve, ideal para conectar diversos dispositivos remotos com uma largura de banda de rede mínima. O protocolo permite o envio de mensagens entre dispositivo para nuvem e da nuvem para dispositivo, facilitando assim a transmissão de mensagens para um grupo de aplicações. Sendo assim, os dados recebidos podem ser visualizados em tempo real na interface web da DOJOT, armazenado em banco de dados, como também podem ser consumidos por outras aplicações externas. A plataforma DOJOT poderá, então, fornecer as informações armazenadas para um *front-end* (página web), com o objetivo de fornecer informações sobre os eletropostos e recargas realizadas.

3.4. Protótipo

Foi definido um estudo de caso no âmbito do projeto de P&D ANEEL intitulado de “Sistema Inteligente de Gestão Eficiente de Mobilidade Elétrica Multimodal”, também chamado de projeto SIMA. Figura 2 ilustra a bancada de testes real que compreende uma infraestrutura de VE e eletroposto implantados no Campus Guamá da UFPA. Especificamente, existe 1 eletroposto da ABB no modelo Terra 54 (T54) com capacidade de recarga de 50 kW e 1 Ônibus elétrico para o transporte dos usuários do Campus Guamá da UFPA.

Para a coleta das informações, o modelo T54 da ABB permite a comunicação e coleta de informações através do protocolo OCPP. Este sistema está sendo implantado na universidade, sendo interligado à rede de distribuição do Campus Guamá. Para avaliação de bancada de teste, foram hospedados o OCPP *back-end* (sistema central de gerenciamento) e *middleware* IoT (DOJOT) em um servidor Power Edge T440 conectado na rede local, o qual conta com o sistema operacional Linux Ubuntu Server 18.04, 64GB de memória RAM e processador Intel Xeon Silver 4210 (2 unidades).



Figura 2. Bancada de testes real durante o processo de recarga

Ainda de acordo com a documentação, foram coletadas as seguintes informações dos eletropostos: i) `Current.Import`: fluxo de corrente instantâneo para o veículo. ii) `Energy.Active.Import.Register`: valor numérico lido (Wh ou kWh) do medidor elétrico (mais confiável) que mede a energia importada (do fornecimento da rede). iii) `Power.Active.Import`: potência ativa instantânea importada pelo veículo elétrico. iv) `SoC`: estado do carregamento do veículo (em porcentagem). v) `Voltage`: tensão instantânea medida nos medidores DC do conector durante o carregamento. vi) `Current.Offered`: corrente máxima oferecida ao veículo elétrico com base na capacidade máxima do veículo fornecida durante a configuração da sessão de carregamento. vii) `Power.Offered`: potência máxima oferecida ao veículo elétrico com base na capacidade máxima do veículo fornecida durante a configuração da sessão de carregamento. viii) `Temperature`: temperatura.

A Figura 3 exibe um diagrama de sequência das operações e troca de mensagens via OCPP durante uma sessão completa de recarga de um VE, conforme demonstrado na bancada de testes. De acordo com o OCPP, para iniciar e finalizar um carregamento, é necessário, primeiro, verificar a autenticação do usuário. Dessa forma, o eletroposto requisita autorização ao sistema central através da operação *Authorize*, contendo o identificador (`idTag`). Por sua vez, o *back-end* responde informando o *status* da autorização através do campo `idTagInfo`.

Caso o usuário seja autorizado pelo sistema, o eletroposto requisita o início da transação, ou seja, do carregamento do veículo através da operação *StartTransaction* contendo as seguintes informações: `connectorId`, informa qual conector do eletroposto está sendo utilizado; `idTag`, identificador utilizado na autorização; `meterStart`, contém o valor do medidor em Wh para o conector no início da transação e `timestamp`, dia e hora do início da sessão de carregamento. O OCPP *back-end*, então, envia uma mensa-

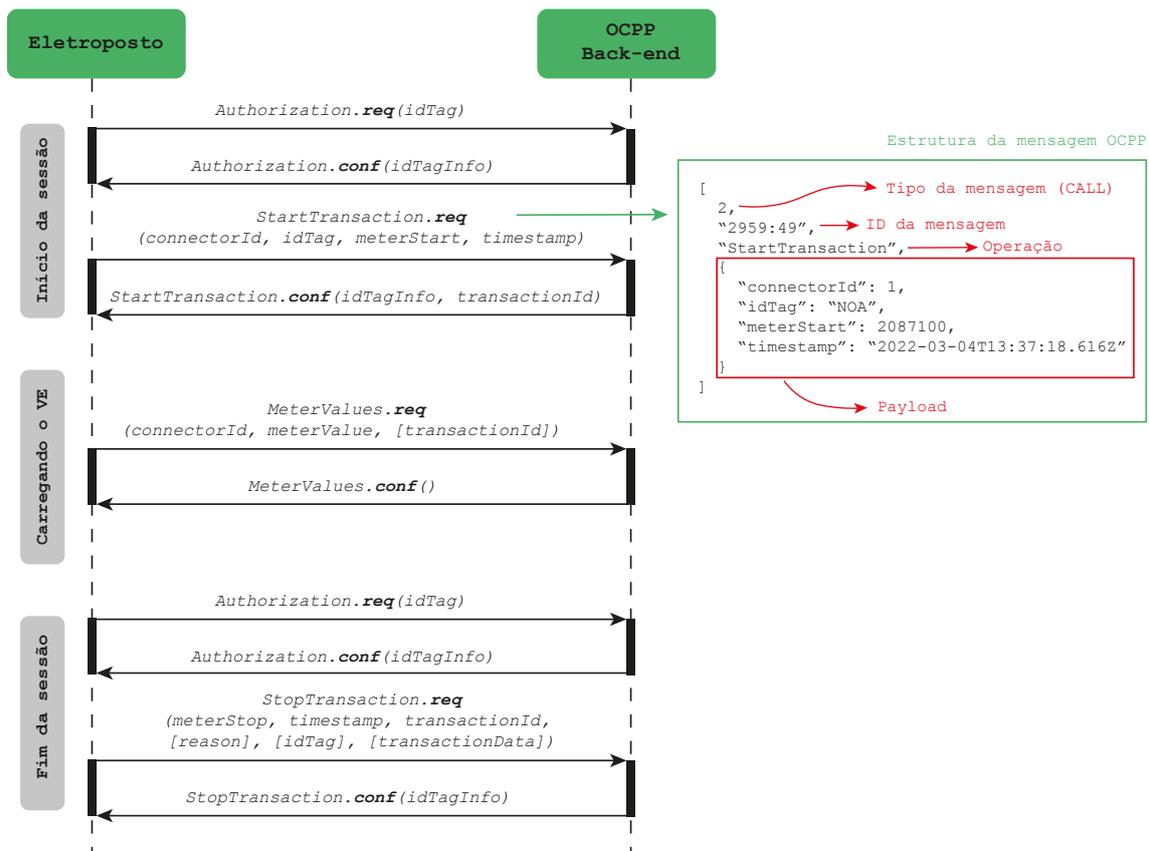


Figura 3. Fluxo de comunicação e estrutura de mensagens OCPP durante a sessão de recarga de um veículo elétrico

gem de resposta contendo o status de autorização (positivo, neste caso) e o identificador da transação (`transactionId`).

Após estas operações, inicia-se, então, o processo de carregamento do VE. Durante esse processo, o eletroposto envia informações (energia, corrente, tensão etc.) ao sistema central através da operação `MeterValues`. As informações e o período de envio são configurados logo que o eletroposto é ligado. Nesse estudo de caso, definiu-se um intervalo de 10 segundos. Para que seja efetuado o término do carregamento, o eletroposto executa novamente uma operação de autorização (`Authorize`) para verificar se o usuário que requisitou é o mesmo que iniciou o processo de carregamento. Após autorizado, o eletroposto envia uma requisição solicitando o fim da transação, através da operação `StopTransaction`. Essa mensagem contém as seguintes informações obrigatórias: `meterStop`, contém o valor do medidor em Wh para o conector no final da transação, `timestamp` dia e hora do término de carregamento, `transactionId`, identificador da transação; além de outras informações opcionais.

A Figura 3 também exhibe a estrutura da mensagem de requisição da operação de início de transação (`StartTransaction`) enviada ao sistema central durante um carregamento, registrada no *log* da aplicação. No final de todo o processo de carregamento, os dados de todo o *log* de transações entre o eletroposto e sistema central (OCPP *back-end*) são salvos e persistidos no banco de dados disponível na DOJOT e podem ser acessados facilmente.

A Figura 4 exibe a quantidade de energia total coletada dos medidores (através do protocolo OCPP) durante algumas sessões de recarga do VE efetuadas no mês de Março na UFPA. A duração de cada uma dessas sessões variou entre 3 e 7 horas e são diretamente proporcionais ao valor total de energia fornecida. Além disso, há várias outras informações extras registradas em nosso log e banco de dados que não foram ilustradas aqui por limite de páginas. Entretanto, vale ressaltar a finalização total da bancada de testes e que ocorreu de forma bem-sucedida.

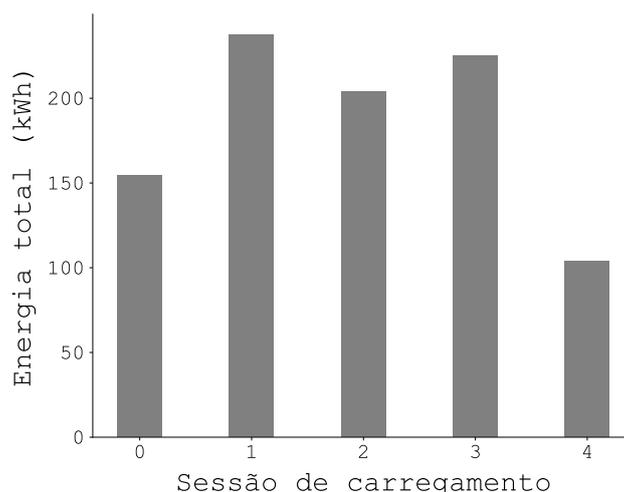


Figura 4. Energia total importada do fornecimento da rede por sessão de carregamento

4. Conclusão

Este artigo apresentou um estudo de caso que considera o protocolo OCPP para gerenciar a comunicação entre sistema central e eletroposto. A plataforma DOJOT foi considerada como uma opção para facilitar o armazenamento e análise de informações sobre eletropostos e recargas realizadas. Tais dados permitem análise de consumo e outras informações úteis para os usuários. O protótipo foi realizado por meio de bancada de testes na UFPA, usando um ônibus elétrico, um sistema de carregamento e um sistema central, onde as informações de carregamento foram registradas através do protocolo OCPP. Com objetivo de melhorar as análises de consumo dos VEs, foi realizada a comunicação entre o sistema central e a DOJOT, e a exibição e análise destas informações na plataforma. A completa prototipação, bancada de testes e visualização das informações de carregamento foram bem sucedidos e satisfatórios, e nos permitem continuar a implementação e análise de outras variáveis no futuro, seja a respeito de precificação ou mais informações sobre o veículo elétrico.

Agradecimento

Este trabalho conta com apoio financeiro da Norte Energia para o projeto o projeto de P&D ANEEL intitulado de “Sistema Inteligente Multimodal na Amazônia (SIMA)”.

Referências

- Alcaraz, C., Lopez, J., and Wolthusen, S. (2017). Ocpp protocol: Security threats and challenges. *IEEE Transactions on Smart Grid*, 8(5):2452–2459.
- Antoun, J., Kabir, M. E., Moussa, B., Atallah, R., and Assi, C. (2020). A detailed security assessment of the ev charging ecosystem. *IEEE Network*, 34(3):200–207.
- CPqD (2020). Dojot soluções para iot - plataforma de desenvolvimento para iot. <http://www.dojot.com.br/>. (Acessado em 03/09/2021).
- Devendra, D., Malkurthi, S., Navnit, A., and Hussain, A. M. (2021). Compact electric vehicle charging station using open charge point protocol (ocpp) for e-scooters. In *2021 International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*, pages 1–5.
- Eisenbarth, M., Wegener, M., Scheer, R., Andert, J., Buse, D. S., Klingler, F., Sommer, C., Dressler, F., Reinold, P., and Gries, R. (2021). Toward smart vehicle-to-everything-connected powertrains: Driving real component test benches in a fully interactive virtual smart city. *IEEE Vehicular Technology Magazine*, 16(1):75–82.
- Lombardi, M., Panerali, K., Rousselet, S., and Scalise, J. (2018). Electric vehicles for smarter cities: the future of energy and mobility. In *World Economic Forum*. http://www3.weforum.org/docs/WEF_2018_%20Electric_For_Smarter_Cities.pdf.
- Modesto, W., Neto, A. V., Rosário, D., and Cerqueira, E. (2021). Sg2iot - uma arquitetura para integracao de dispositivos eletricos inteligentes de abordagem legada em sistemas smart grid baseados na iot. In *Anais do XIII Simposio Brasileiro de Computacao Ubiqua e Pervasiva*, pages 31–40, Porto Alegre, RS, Brasil. SBC.
- Mota, R., Riker, A., and Rosário, D. (2019). Adjusting group communication in dense internet of things networks with heterogeneous energy sources. In *11th Brazilian Symposium on Ubiquitous and Pervasive Computing*, Porto Alegre, RS, Brasil. SBC.
- Răboacă, M. S., Meheden, M., Musat, A., Viziteu, A., Creanga, A., Vlad, V., Filote, C., Rață, M., and Lavric, A. (2021). An overview and performance evaluation of open charge point protocol from an electromobility concept perspective. *International Journal of Energy Research*, 46:523 – 543.
- Saleem, Y., Crespi, N., Rehmani, M. H., and Copeland, R. (2019). Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. *IEEE Access*, 7:62962–63003.
- Venkata Pruthvi, Thota, Dutta, Niladri, Bobba, Phaneendra Babu, and Vasudeva, B Sai (2019). Implementation of ocpp protocol for electric vehicle applications. *E3S Web Conf.*, 87:01008.