

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ У СИСТЕМАХ ЗАРЯДКИ ЕЛЕКТРОМОБІЛІВ

Олег Марків¹, Юрій Ришковець²

^{1,2} Національний університет “Львівська політехніка”,
кафедра інформаційних систем і мереж, Львів, Україна

¹ E-mail: oleh.i.markiv@lpnu.ua, ORCID: 0009-0009-4109-174X

² E-mail: yuriy.v.ryshkovets@lpnu.ua, ORCID: 0000-0001-5831-4000

© Марків О.І., Ришковець Ю.В., 2025

Стаття представляє комплексний аналіз інноваційних інформаційних технологій, критично важливих для розбудови сучасної інфраструктури зарядних станцій електромобілів. Досліджено вплив цифрових рішень на надійність, безпеку, масштабованість та ефективність зарядних мереж, а також проаналізовано виклики, пов'язані з їх імплементацією. Розглянуто актуальні проблеми галузі, серед яких експоненційне зростання кількості електромобілів, необхідність швидкої та безпечної аутентифікації користувачів, забезпечення безперервного моніторингу стану зарядних станцій в режимі реального часу, інтелектуальна оптимізація процесів зарядки. Особливу увагу приділено питанням забезпечення стабільного зв'язку в умовах нестабільного покриття, сумісності обладнання різних виробників та економічної ефективності впроваджуваних технологій. Спираючись на аналіз передових наукових досліджень, стаття розкриває різні архітектурні підходи до побудови інформаційних систем для зарядних станцій, оцінює їхні переваги та недоліки, а також детально описує механізми взаємодії між електромобілями, зарядними станціями та централізованими системами управління. Представлено огляд сучасних методів кібербезпеки та протоколів автентифікації, адаптованих до специфіки зарядної інфраструктури. У висновках узагальнено результати дослідження та надано обґрунтовані рекомендації щодо вибору та впровадження інформаційних технологій для створення надійної, безпечної, масштабованої та економічно ефективної інфраструктури зарядних станцій. Стаття буде корисною для інженерів-дослідників, розробників програмного забезпечення, операторів зарядних мереж, а також представників енергетичних компаній та державних регуляторів.

Ключові слова – електромобілі, станція для зарядки електромобілів, оператор зарядних станцій.

Постановка проблеми

Стрімке зростання електромобільної індустрії кардинально трансформує транспортну екосистему, створюючи нові можливості для сталого розвитку та водночас висуваючи серйозні вимоги до інфраструктури зарядних станцій. Зарядні станції для електромобілів стають критично важливими елементами цієї екосистеми, забезпечуючи безперебійну енергетичну підтримку в дорозі. Водночас, ефективне функціонування таких систем неможливе без інтеграції сучасних інформаційних технологій, що дозволяють здійснювати обмін даними, моніторинг стану обладнання та інтелектуальну взаємодію з енергомережами.

Одним із ключових аспектів розвитку зарядної інфраструктури є забезпечення надійного та безпечного обміну інформацією між усіма компонентами системи - від зарядних станцій і транспортних засобів до операторських платформ і мережевих сервісів. Використання передових

технологічних підходів у сфері збору, опрацювання та аналізу даних дозволяє оптимізувати процеси моніторингу, управління та прогнозування, що, у свою чергу, сприяє підвищенню ефективності, надійності та зручності зарядних рішень для кінцевих користувачів.

Подальше стрімке зростання ринку електромобілів напряму залежить від створення надійної, зручної та безпечної інфраструктури зарядних станцій. Згідно з Національною транспортною стратегією до 2030 року (Resolution of the Cabinet of Ministers of Ukraine dated May 30, 2018), планується значне збільшення частки електротранспорту в країні. Зокрема, розроблений план передбачає, що до 2030 року кількість електромобілів та гібридних авто в Україні може зрости, досягнувши 700 тисяч одиниць, що становить 7 % від загального парку автомобілів. Це створює значне навантаження на існуючу інфраструктуру зарядних станцій та інфраструктуру, що розширюється.

Ефективна робота мережі зарядних станцій безпосередньо залежить від надійних і безпечних інформаційних технологій, які мають забезпечувати швидку та зручну авторизацію користувачів шляхом спрощення та пришвидшення процесу ідентифікації, оплати та доступу до зарядки, що мінімізує час очікування та покращує загальний користувацький досвід; постійний моніторинг стану зарядних станцій через віддалений контроль, комплексну діагностику та оперативне усунення несправностей, що дозволяє зменшити час простою обладнання та гарантує надійність роботи мережі; інтелектуальну оптимізацію процесів зарядки шляхом гнучкого планування сесій з урахуванням динамічного попиту, доступності електроенергії, тарифних планів та індивідуальних потреб користувачів для максимізації ефективності використання енергоресурсів; ефективну інтеграцію з суміжними системами, такими як системи керування енергоспоживанням, інтелектуальні енергетичні мережі, платіжні та навігаційні сервіси, з метою створення комплексної та зручної екосистеми.

Основна проблема, яку необхідно вирішити, полягає в розробці та впровадженні ефективних інформаційних технологій та протоколів передачі даних, які забезпечать надійну та безпечну роботу мережі зарядних станцій, а також оптимізацію процесів зарядки електромобілів. Нездатність ефективно вирішити цю проблему стримуватиме розвиток інфраструктури, знизить зручність використання електромобілів для користувачів та уповільнить перехід до екологічно сталого транспорту, що є критично важливим в умовах глобальних кліматичних змін.

Розглянемо конкретні приклади проблем, які потребують вирішення:

- *Проблема нестабільного інтернет-зв'язку* у віддалених регіонах або зонах з поганим мережевим покриттям, нестабільне інтернет-з'єднання може унеможливити або ускладнити віддалене управління, моніторинг та оновлення програмного забезпечення зарядних станцій, що може спричинити збої в роботі, збільшує час простою та витрати на обслуговування.
- *Ризики для безпеки даних та кібербезпеки* на зарядних станціях, які є елементами критичної інфраструктури і потенційними цілями для кібератак, виникають через недостатній рівень захисту даних, що може призвести до витоку конфіденційної інформації користувачів, порушення функціонування платіжних систем, несанкціонованого доступу до управління станціями та навіть блокування роботи цілих мереж зарядних станцій.
- *Проблема сумісності* виникає через використання обладнання різних виробників зарядних станцій, різних протоколів передачі даних та стандартів, що ускладнює інтеграцію обладнання в єдину мережу, створює обмеження для масштабування та підвищує залежність від конкретних виробників.
- *Економічні виклики впровадження та підтримки* виникають через впровадження сучасних інформаційних технологій, особливо систем кібербезпеки та масштабованих хмарних платформ, що може вимагати значних капітальних інвестицій та експлуатаційних витрат. Пошук економічно ефективних рішень є особливо важливим для малого та середнього бізнесу, що бере участь у розбудові мережі зарядних станцій.
- *Забезпечення безперебійної та надійної роботи в умовах пікового навантаження* мережі зарядних станцій, особливо в години пікового попиту, вимагає резервування каналів зв'язку, дублювання критично важливих компонентів системи та застосування інтелектуальних механізмів управління потоками зарядки.

Таким чином, розробка та впровадження ефективних інформаційних технологій для керування зарядною інфраструктурою є надзвичайно актуальним завданням у контексті стрімкого зростання електромобільного транспорту. Від ефективності обміну даними, стабільності роботи систем, безпеки та масштабованості обраних рішень залежить надійність функціонування зарядної мережі, її інтеграція з іншими цифровими сервісами та здатність задовольняти зростаючий попит. Тому дослідження сучасних підходів до архітектури, протоколів зв'язку та технологій опрацювання інформації має важливе практичне значення та є ключовим етапом на шляху до побудови стійкої та ефективної інфраструктури зарядних станцій.

Аналіз останніх досліджень та публікацій

Сучасна динаміка розвитку інфраструктури зарядки електромобілів визначається інтенсивними дослідженнями у сфері інформаційних технологій та протоколів передачі даних. Ключовим вектором цих досліджень є розроблення та стандартизація протоколів, що гарантують інтероперабельність, тобто можливість створення інформаційних систем з довільних неоднорідних, розподілених компонентів на базі уніфікованих інтерфейсів або протоколів, та продуктивну взаємодію різних елементів екосистеми зарядки. Вибір архітектурної моделі має прямий вплив на ефективність та масштабованість систем зарядки електромобілів. Аналіз архітектурних підходів (Naga, V., 2021) показує, що хмарні рішення, такі як AWS IoT Core або Microsoft Azure IoT Hub, забезпечують значну гнучкість та можливості для централізованого управління великими мережами зарядних станцій. Це особливо актуально в контексті інтеграції з енергосистемами та платформами розумного міста. Проте централізовані підходи, що базуються на локальних серверах, можуть забезпечити кращу контрольованість та швидкість реакції, що є важливим для локальних або приватних зарядних інфраструктур, наприклад, для зарядних станцій на паркінгах бізнес-центрів. В публікації (Ahmed, M. A., Guerrero, L., & Franco, P., 2024) досліджуються гібридні архітектури, які комбінують переваги обох підходів. У статті (Li, J., Gu, C., Xiang, Y., & Li, F., 2022) також аналізується роль периферійних обчислень для оптимізації опрацювання даних безпосередньо на зарядних станціях та зменшення затримки в системах.

У контексті забезпечення сумісності обладнання від різних виробників вирішальну роль відіграють стандартизовані протоколи, безперечним лідером серед яких є Open Charge Point Protocol (OCPP). Дослідження (Alcaraz, C., Cumplido, J., & Trivino, A., 2023) та (Hsaini, S., Ghogho, M., & Charaf, M. E. H., 2022) чітко демонструють важливість OCPP для створення відкритої екосистеми зарядних станцій. Цей протокол усуває залежність від конкретних виробників та спрощує керування мережами зарядних пристроїв. Крім OCPP, в системах зарядки електромобілів активно використовуються протоколи Modbus та MQTT. У статті (Sultana, Z., Basha, C. H., & Irfan, M. M., 2024) розглянуто застосування різних протоколів для розумних зарядних станцій. У публікації (Lund, V. V., 2024) детально аналізуються переваги та недоліки протоколів OCPP, Modbus та MQTT. В даній статті розглядають такі аспекти, як пропускна здатність, затримка, безпека та складність інтеграції, що є критично важливими для застосування в інфраструктурах зарядки.

Безпека є критичним фактором розвитку інфраструктури зарядки електромобілів, оскільки ці системи підключені до інтернету та опрацьовують чутливі дані користувачів, включаючи платіжну інформацію та персональні дані. Аналіз загроз безпеці зарядних станцій та потенційних кібератак, поданий в статті (Pourmirza, Z., & Walker, S., 2021), засвідчує необхідність розроблення комплексних рішень для захисту даних від несанкціонованого доступу та забезпечення цілісності системи. Автори дослідження (Gadacz, H., 2021) фокусуються на методах аутентифікації та авторизації користувачів, наприклад, з використанням OAuth 2.0 або OpenID Connect, шифруванні даних за допомогою TLS 1.3 та AES-256, а також на стандартизації протоколів безпеки для інфраструктури зарядки електромобілів, наприклад, ISO/IEC 15118.

Систематизуючи оглянуті дослідження, можна виділити наступні невіднесені задачі. По-перше, відсутність уніфікованого підходу до вибору оптимальної архітектури системи зарядки, що враховував би специфічні умови експлуатації та вимоги до масштабованості й безпеки. По-друге,

необхідність глибшого порівняльного аналізу протоколів передачі даних за комплексними критеріями для різних сценаріїв застосування. По-третє, потреба у розробленні та обґрунтуванні комплексних механізмів безпеки, що інтегрують як технічні, так і організаційні аспекти. Таким чином, ключовою не вирішеною проблемою, що випливає з аналізу літератури, є недостатнє наукове обґрунтування вибору інтегрованих архітектурно-протокольних та безпекових рішень для інформаційних систем зарядки електромобілів, які б гарантували одночасно високу ефективність, надійність, безпеку та масштабованість в умовах стрімкого розвитку ринку.

Формулювання цілі статті

Виходячи з виявленої проблеми недостатнього наукового обґрунтування вибору інтегрованих рішень, мета дослідження полягає в тому, щоб запропонувати методи вибору оптимальних архітектурних та протокольних рішень у поєднанні з механізмами безпеки для інформаційних систем зарядки електромобілів, що забезпечують високий рівень відмовостійкості та масштабованості, шляхом комплексного порівняльного аналізу сучасних інформаційних технологій та ключових протоколів передачі даних.

Завдання дослідження:

1. Порівняти моделі архітектури систем зарядки (централізована, децентралізована, гібридна) за критеріями ефективності, гнучкості, вартості впровадження та експлуатаційних витрат.
2. Здійснити аналіз існуючих протоколів передачі даних за чітко визначеними критеріями функціональності, безпеки, масштабованості та сумісності, з визначенням областей їх найбільш ефективного застосування.
3. Дослідити та порівняти механізми безпеки та автентифікації систем зарядки електромобілів.

Очікувані результати:

- Систематизований огляд існуючих рішень у галузі інформаційних технологій для зарядної інфраструктури електромобілів, представлений у вигляді аналітичного звіту з порівняльними таблицями.
- Формування рекомендацій щодо вибору оптимального протоколу передачі даних для різних типів зарядних станцій з урахуванням функціональності, безпеки, масштабованості та сумісності.
- Оцінка ефективності механізмів безпеки та автентифікації у системах зарядки електромобілів із визначенням найкращих практик їх впровадження.

Виклад основного матеріалу

4. Інформаційні технології в архітектурах систем зарядних станцій для електромобілів.

Розвиток інфраструктури зарядних станцій для електромобілів є складним завданням, що вимагає інтеграції різноманітних інформаційних технологій та архітектур для забезпечення ефективної, безпечної та зручної зарядки. Технологічна архітектура системи зарядки електромобілів охоплює кілька ключових компонентів і технологій, включаючи зарядний пристрій, систему керування зарядкою, зарядний інтерфейс, зарядну мережу, інтелектуальні системи та оператора зарядних станцій (Charge Point Operator, CPO), відповідального за управління, моніторинг і технічне обслуговування зарядної інфраструктури. Крім того, важливими є засоби захисту зарядного обладнання (Arrow Electronics., 2024). Ці компоненти спільно забезпечують ефективну, дієву та безпечну зарядку електромобілів.

Централізовані архітектури систем зарядки електромобілів зазвичай передбачають наявність центрального сервера або системи керування, яка контролює та здійснює моніторинг багатьох зарядних станцій. У таких системах зарядні точки або станції для зарядки підпорядковуються центральній системі керування, яка відповідає за широкий спектр функцій. До ключових компонентів

систем зарядки електромобілів з централізованими архітектурами належать зарядні точки, центральна система управління, комунікаційні мережі, а також потенційні підключення до енергетичної мережі та інших інтелектуальних систем.

Принцип роботи систем зарядки електромобілів з централізованими архітектурами полягає в тому, що вона вирішує такі завдання, як аутентифікація користувачів, керування сеансами зарядки, виставлення рахунків, балансування навантаження та віддалена діагностика. Хмарні системи керування, що пропонуються такими платформами, як AWS, демонструють централізований підхід, де різні сервіси AWS використовуються для керування різними аспектами інфраструктури зарядки (Building a Charging Station Management System with AWS | Amazon Web Services., 2024).

Хоча системи зарядки електромобілів з централізованими архітектурами забезпечують легкість керування, агрегацію даних та можливість реалізації складних стратегій управління, таких як інтелектуальна зарядка у великій мережі, залежність від центрального сервера робить їх потенційно вразливими до єдиної точки відмови та може призвести до затримок залежно від стану мережевої інфраструктури.

Децентралізовані архітектури систем зарядки електромобілів розподіляють контроль та прийняття рішень між багатьма суб'єктами або на рівні окремих зарядних станцій чи локальних агрегаторів. Такі системи можуть включати інтелектуальні зарядні станції з локальними можливостями опрацювання даних, зв'язок між сусідніми станціями або регіональними агрегаторами, що координують зарядку в межах обмеженої географічної зони.

У системах зарядки електромобілів з децентралізованими архітектурами рішення щодо зарядки можуть прийматися на основі локальних умов, переваг користувачів або розподілених алгоритмів, що потенційно зменшує залежність від центрального органу. Метод регулювання частоти, описаний у статті (Striani, S., Pedersen, K. L., Engelhardt, J., & Marinelli, M., 2024), де динамічно коригується внесок залежно від терміновості зарядки, визначеної користувачами, і наведено приклад розподіленої архітектури управління ресурсами. Концепція багатьох агрегаторів, що керують зарядкою в різних регіонах (Al-Alwash, H. M., Eugen Borcoci, Marius-Constantin Vochin, Indika A.M. Balapuwaduge, & Li, F. Y., 2024), також ілюструє децентралізацію. Децентралізовані системи можуть забезпечити більшу стійкість до відмов та потенційно нижчу затримку для локального керування. Однак координація зарядки у великій, повністю децентралізованій мережі може бути складною. Безпека та узгодженість даних також можуть становити проблеми.

Гібридні архітектури систем зарядки електромобілів поєднують аспекти як централізованих, так і децентралізованих систем, прагнучи використати переваги кожної з них (Ampcontrol., 2025). Такі системи можуть включати центральну систему управління для координації дій, тоді як локальні блоки управління або інтелектуальні зарядні станції опрацьовують дані для коригування зарядки в реальному часі та взаємодіють з транспортними засобами. Шлюзи виступають посередниками між різними комунікаційними протоколами.

У системах зарядки електромобілів з гібридними архітектурами може бути реалізована ієрархічна структура управління, де локальні блоки приймають автономні рішення в межах параметрів, встановлених центральною системою. Локальні системи керування навантаженням (EV charging - electrical architectures, 2023), що працюють під наглядом центрального оператора мережі, також можна вважати гібридними. Гібридні архітектури можуть забезпечити баланс між централізованим контролем та локальною автономією, що потенційно призводить до більшої ефективності та стійкості систем. Однак складність керування такими системами зростає.

Різні архітектури систем зарядки електромобілів відрізняються за такими факторами, як масштабованість, надійність, безпека, вартість (як початкових інвестицій, так і експлуатаційних витрат), затримка, складність управління та придатність для різних сценаріїв використання (наприклад, домашня зарядка, громадська зарядка, зарядка автопарку). Централізовані системи можуть бути більш масштабованими для великих громадських мереж, але можуть бути менш надійними через єдину точку відмови. Децентралізовані системи можуть бути більш придатними для локального керування енергією та стійкості, але можуть зустрітися з проблемами глобальної координації. Гібридні системи прагнуть оптимізувати ці компроміси. У таблиці 1 наведено порівняння основних характеристик різних архітектур.

Таблиця 1

Порівняння архітектур зарядних станцій для електромобілів

Характеристика	Централізована	Децентралізована	Гібридна
Масштабованість	Висока для великих мереж	Обмежена для великих мереж	Залежить від реалізації
Надійність	Залежить від центрального сервера	Вища стійкість до локальних відмов	Компроміс між централізацією та децентралізацією
Безпека	Централізований контроль, потенційні єдині точки атаки	Розподілена, складніше керувати глобальною безпекою	Поєднує підходи, залежить від реалізації
Вартість (початкова)	Вища для центрального обладнання	Нижча початкова вартість для окремих станцій	Залежить від комбінації компонентів
Вартість (експлуатаційна)	Може бути нижчою завдяки централізованому управлінню	Може бути вищою через розподілене управління	Залежить від балансу централізації та децентралізації
Затримка	Може бути вищою залежно від мережі	Нижча для локальних операцій	Залежить від розподілу функцій
Складність управління	Висока складність центрального управління	Складність координації великої кількості незалежних станцій	Висока складність інтеграції та управління
Найкраще використання	Великі громадські мережі, керування автопарками	Локальні енергетичні системи, приватні зарядні станції	Гнучкі рішення, що потребують як центрального контролю, так і локальної автономії

Аналіз архітектур показує, що їх вибір залежить від конкретних вимог проєкту, таких як масштаб мережі, бюджет, вимоги до безпеки та гнучкості. Централізовані системи є економічно вигідними для малих мереж, тоді як хмарні та комбіновані архітектури демонструють високу ефективність і гнучкість у масштабних інфраструктурах. Децентралізовані рішення доцільні в умовах, де критичною є автономність і надійність. Комбіновані моделі є перспективним напрямком, що інтегрує найкращі характеристики кожної архітектури для створення збалансованих рішень.

5. Протоколи передачі даних для інфраструктури зарядки електромобілів.

Інфраструктура зарядки електромобілів використовує різноманітні протоколи передачі даних для забезпечення зв'язку між різними компонентами системи, включаючи зарядні станції, електромобілі та центральні системи керування. Стандартизовані протоколи сприяють сумісності, ефективності та безпеці операцій зарядки. У цій статті ми запропонували класифікацію протоколів, що дозволяє систематизувати існуючі рішення та виявити області їх найбільш ефективного застосування. Вона ділить протоколи на три основні категорії: протоколи, що забезпечують комунікацію між електромобілем та зарядною станцією, протоколи, що відповідають за зв'язок між зарядною станцією та оператором зарядних станцій, та протоколи інтерфейсу користувача.

Таблиця 2

**Класифікація протоколів передачі даних
у системах зарядних станцій для електромобілів**

Категорія протоколів	Протоколи
Протоколи взаємодії електромобіля та зарядної станції	ISO 15118, IEC 61851, CAN
Протоколи взаємодії зарядної станції та оператора зарядних станцій	OCPP, OCPI, IEC 63110, Modbus, MQTT
Протоколи інтерфейсу користувача	HTTP/HTTPS, REST (через HTTP/HTTPS), MQTT (для оновлень у реальному часі), власні протоколи (за наявності)

Протоколи взаємодії електромобіля та зарядної станції (EV-to-EVSE Communication). Перша категорія протоколів охоплює комунікацію, що відбувається безпосередньо між електромобілем та зарядною станцією під час процесу зарядки. Основною метою цих протоколів є забезпечення безпечного, ефективного та сумісного обміну енергією, а також реалізація додаткових функцій, таких як автоматична аутентифікація та оптимізація процесу зарядки. До цієї категорії належать стандарти, що визначають фізичний та інформаційний обмін даними між автомобілем та станцією. Ці протоколи визначають "мову", якою "спілкуються" пристрої для управління процесом зарядки, незалежно від фізичного типу конектора. Серед найпоширеніших можна виділити:

- ISO 15118 - це міжнародний стандарт, що визначає протокол зв'язку між зарядною станцією та електромобілем. ISO 15118 забезпечує функціональність "Plug & Charge" для автоматичної ідентифікації та авторизації (Sule, U., & Kristianto, K., 2024). Зокрема він підтримує двостороннє заряджання, дозволяє передавати дані про енергію між електромобілем та зарядною станцією для розумного заряджання. Підвищення безпеки досягається завдяки TLS-з'єднанню та V2G-PKI (інфраструктура відкритих ключів). Він використовується як для дротового (AC та DC), так і для бездротового заряджання. ISO 15118 підтримує регулювання заряджання на основі умов енергосистеми, переваг користувача та тарифів на енергію (Agnihotri, N., 2024), забезпечує автоматичну аутентифікацію та оплату за допомогою цифрових сертифікатів та використовується для заряджання важких транспортних засобів.
- IEC 61851 - це міжнародний стандарт для дротових систем заряджання електричних транспортних засобів. Він охоплює характеристики та умови експлуатації обладнання для заряджання електромобілів. Стандарт визначає з'єднання між зарядною станцією та електромобілем (Charging Standards. Vector Informatik GmbH, 2025). Частина IEC 61851-24 регламентує цифровий зв'язок між зарядними станціями постійного струму та електромобілями для керування процесом заряджання. Стандарт використовує широтно-імпульсну модуляцію для низькорівневого зв'язку між електромобілем і зарядною станцією, зокрема визначає значення коефіцієнта заповнення сигналу широтно-імпульсної модуляції для індикації доступного струму заряджання, а також підтримує високошвидкісний зв'язок з використанням IP-протоколів через технологію зв'язку по лініях електроживлення у комбінованій системі заряджання.
- Controller Area Network (CAN) - це надійний та широко використовуваний протокол зв'язку в автомобільній промисловості. Він забезпечує ефективний та надійний зв'язок між різними електронними блоками керування в автомобілі (Revolutionizing Electric Vehicle Charging with CAN Bus Technology. TC CHARGER., 2023). CAN використовується для зв'язку між

системою керування батареєю електромобіля та зарядним пристроєм, сприяє алгоритмам розумного заряджання на основі стану батареї, температури та напруги, забезпечує сумісність за принципом "підключи і працюй" шляхом обміну важливими параметрами заряджання. Крім того, він надає зворотний зв'язок у реальному часі про процес заряджання водієві. Протокол підтримує діагностику, звітування про несправності та використовується для керування навантаженням, інтеграції з енергосистемою, зв'язуючись з системами керування енергосистемою. CAN використовується іншими протоколами, такими як IEC 61851, для керування подачею живлення під час заряджання. Також він застосовується для високошвидкісного зв'язку в стандартах заряджання DC GB/T та DC CHAdeMO.

Отже, CAN, як головна внутрішньо-автомобільна мережа, поширює свій вплив на інтерфейс заряджання, що підкреслює тісну інтеграцію між внутрішніми системами автомобіля та зовнішньою зарядною інфраструктурою. ISO 15118 є значним кроком до більш орієнтованого на користувача та інтегрованого з енергосистемою досвіду заряджання EV, забезпечуючи таку функцію, як Plug & Charge. При цьому здатність електромобілів автоматично автентифікуватися та авторизувати заряджання без втручання користувача спрощує процес заряджання. IEC 61851 забезпечує базову основу для безпечного та стандартизованого провідного заряджання електромобілів, причому різні режими відповідають різним сценаріям заряджання та вимогам до потужності. Спостерігається чітка еволюція складності зв'язку, що вказує на тенденцію до більш інтелектуальних та інформаційно насичених взаємодій між електромобілями та зарядними пристроями.

Протоколи взаємодії зарядної станції та оператора зарядних станцій (EVSE-to-CPO Communication). Друга категорія протоколів фокусується на комунікації між зарядною станцією та центральним сервером управління. Ці протоколи забезпечують основу для управління мережею зарядних станцій, моніторингу їхнього стану, авторизації користувачів, опрацювання платежів та інтеграції з різними сервісами. Основними є:

- Open Charge Point Protocol (OCPP) є де-факто стандартом для зв'язку між зарядними станціями та серверами управління. Відкрита архітектура та широкий функціонал роблять його універсальним рішенням для операторів зарядних мереж. OCPP забезпечує широкий спектр функцій, включаючи моніторинг стану станцій, дистанційне керування, авторизацію користувачів, керування сесіями зарядки, опрацювання платежів та збір статистичних даних. Безпека в OCPP реалізується за допомогою TLS шифрування та аутентифікації на основі сертифікатів, а OCPP 2.0 та новіші версії пропонують покращені механізми безпеки. Протокол розроблений для високої масштабованості, дозволяючи керувати великими мережами станцій. Сумісність OCPP є однією з його ключових переваг, завдяки широкій підтримці виробників обладнання та програмного забезпечення. OCPP є незамінним для операторів зарядних мереж та бекенд-систем управління, забезпечуючи ефективне керування та моніторинг інфраструктури зарядних станцій.
- Open Charge Point Interface (OCPI) відіграє важливу роль у забезпеченні роумінгу та інтероперабельності між різними зарядними мережами. Він дозволяє операторам обмінюватися необхідною інформацією для забезпечення зручного доступу до зарядних послуг для користувачів різних мереж, включаючи дані про доступність станцій, ціни та деталі сесій. Безпека OCPI забезпечується за допомогою API ключів та TLS для захисту міжмережевої комунікації. Протокол розроблений для підтримки обміну інформацією між великою кількістю операторів, сприяючи масштабованості ринку зарядних послуг. Сумісність OCPI підтримується багатьма операторами зарядних мереж та платформами електронної мобільності (eMSP), забезпечуючи інтероперабельність та роумінг. OCPI ефективно застосовується для забезпечення роумінгу, створення платформ eMSP та інтеграції різних зарядних інфраструктур в єдиний відкритий ринок.
- IEC 63110 - це міжнародний стандарт, що розробляється для керування інфраструктурами заряджання та розряджання електромобілів (Lesjak, Ž., 2024). Він має на меті стандартизувати протоколи для електромобілів, EVSE, систем керування зарядними

станціями. IEC 63110 охоплює керування передачею енергії, керування активами EVSE та аутентифікацію/ авторизацію/оплату. Очікується, що цей стандарт принесе значні покращення в галузь заряджання електромобілів. Деякі експерти вважають, що він стане оновленням OCPP з ширшим міжнародним визнанням.

- Modbus - це протокол зв'язку, спочатку розроблений для програмованих логічних контролерів і широко використовуваний у промислових електронних пристроях (Modbus and OCPP: Caburn Telecom, 2024). Він використовується для моніторингу та керування процесом заряджання в межах зарядної станції. Modbus забезпечує зв'язок між різними компонентами зарядної станції, такими як лічильники електроенергії та RFID-зчитувачі. Він підтримує динамічне керування навантаженням та інтеграцію відновлюваної енергії на рівні зарядного пристрою.
- Message Queuing Telemetry Transport (MQTT) - це легкий протокол обміну повідомленнями за моделлю "видавець-підписник", оптимізований для застосувань IoT. Він розроблений для стійкого та надійного зв'язку навіть у ненадійних мережах, що полегшує масштабування мереж заряджання. Протокол забезпечує зв'язок у реальному часі, сприяючи миттєвій передачі та отриманню даних (Hübschmann, I., 2021). MQTT знаходить широке застосування в заряджанні електромобілів. Він використовується для зв'язку між контролерами зарядних пристроїв EV та центральними системами керування. Протокол забезпечує керування енергією в мережах заряджання, включаючи оптимізацію розподілу енергії в реальному часі. MQTT використовується для діагностики в реальному часі та звітування про стан зарядного пристрою. Він також забезпечує локальний зв'язок без підключення до Інтернету для роботи пристроїв на місці.

Отже, OCPP є домінуючим протоколом для віддаленого керування зарядними станціями EV, що свідчить про сильний консенсус у галузі щодо цього стандарту для основних функцій керування. Широке впровадження OCPP різними виробниками та операторами мереж свідчить про його ефективність у забезпеченні стандартизованого способу моніторингу, керування та адміністрування зарядної інфраструктури. Ця сумісність має вирішальне значення для зростання та масштабованості мереж заряджання EV. Наявність протоколу роумінгу OCPP підкреслює потребу в безперебійному заряджанні в різних мережах, але також свідчить про певну фрагментацію підходу до досягнення цієї сумісності. Оскільки впровадження електромобілів зростає, водії очікують можливості заряджати свої транспортні засоби незалежно від оператора мережі. Розробка IEC 63110 свідчить про постійні зусилля зі створення більш комплексного міжнародного стандарту для керування інфраструктурою заряджання EV, потенційно на основі існуючих протоколів, таких як OCPP. Потреба в загально визнаному стандарті, який охоплює всі аспекти керування інфраструктурою заряджання EV, від електромобіля до енергосистеми, стає дедалі важливішою. IEC 63110 має на меті задовольнити цю потребу, що потенційно призведе до більшої сумісності та стандартизації в глобальному масштабі. Постійна актуальність Modbus у межах зарядних станцій EV для зв'язку внутрішніх компонентів та інтеграції з системами керування будівлею демонструє важливість усталених промислових протоколів у цій галузі, що розвивається. Хоча для зовнішнього зв'язку та розширених функцій з'являються новіші протоколи. Протоколи, які добре себе зарекомендували, такі як Modbus, продовжують відігравати вирішальну роль у внутрішній роботі зарядних станцій та їхній інтеграції з існуючою інфраструктурою будівлі. MQTT явно згадується як цінний протокол на цьому рівні зв'язку завдяки своїй ефективності, масштабованості та можливостям роботи в реальному часі. Фрагменти дослідження неодноразово підкреслюють переваги MQTT для підключення розподілених пристроїв та опрацювання даних у реальному масштабі часу, що робить його природним вибором для зв'язку між численними зарядними станціями та центральним сервером керування. Його інтеграція з OCPP ще більше зміцнює його роль у підвищенні продуктивності та швидкості реагування мереж заряджання.

На рис.1 зображено схематичне представлення протоколів передачі даних, які використовуються в процесі заряджання електромобіля.

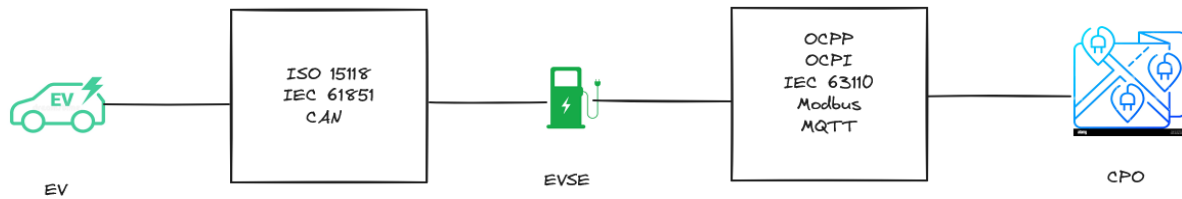


Рис. 1. Протоколи передачі даних у процесі заряджання електромобіля

Протоколи інтерфейсу користувача. Протоколи цієї категорії відіграють ключову роль у забезпеченні зручної та інтуїтивно зрозумілої взаємодії користувача із зарядною інфраструктурою. Вони охоплюють різні аспекти взаємодії, від відображення інформації на дисплеї станції до функціональності мобільних додатків та веб-порталів, а також безконтактної аутентифікації.

Розглянемо детальніше основні протоколи та технології, що використовуються для реалізації інтерфейсу користувача:

- HTTP/HTTPS - це основа веб-комунікації. Використовується для інтерфейсів користувача, доступних через веб-браузери, для керування сесіями заряджання, перегляду стану або доступу до інформації облікового запису. HTTPS забезпечує безпечний зв'язок через Інтернет.
- Інтерфейси прикладного програмування (API) використовуються мобільними додатками для зв'язку з бекенд-серверами та отримання або надсилання даних, пов'язаних із зарядними станціями та обліковими записами користувачів. Ці API часто використовують такі протоколи, як REST (Representational State Transfer), який зазвичай використовує HTTP/HTTPS для передачі даних та JSON для формату даних.
- MQTT використовується для передачі оновлень у реальному масштабі часу (наприклад, статус заряджання, доступність) до інтерфейсів користувача за допомогою механізму "видавець-підписник". Він дозволяє користувачам отримувати миттєвий зворотний зв'язок про процес заряджання або стан зарядних станцій без необхідності постійно оновлювати інтерфейс.
- Власні протоколи використовуються деякими виробниками та постачальниками послуг для зв'язку зі своїми конкретними інтерфейсами користувача.

Стандартні веб-протоколи (HTTP/HTTPS) та RESTful API, є основними засобами взаємодії користувачів із системами заряджання EV завдяки їхньому широкому впровадженню та сумісності з веб та мобільними платформами. Користувачі зазвичай взаємодіють із послугами заряджання через веб-портали або мобільні застосунки. Ці платформи використовують стандартні інтернет-протоколи для зв'язку з бекенд-інфраструктурою. Механізм MQTT "видавець-підписник" робить його придатним для надання оновлень у реальному масштабі часу інтерфейсам користувача, покращуючи таким чином досвід користувача, пропонуючи негайний зворотний зв'язок про статус заряджання та доступність станцій. Замість того, щоб покладатися на періодичне опитування або ручне оновлення, MQTT може передавати оновлення до інтерфейсу користувача одразу після їх появи, забезпечуючи більш безперебійний та інформативний досвід. Наприклад, користувач може бачити прогрес заряджання свого автомобіля в реальному часі або отримувати миттєве сповіщення, коли зарядна станція стає доступною.

6. Механізми безпеки та автентифікації в зарядці електромобілів.

Безпека є критично важливим аспектом систем зарядки електромобілів, що вимагає надійних механізмів шифрування, аутентифікації та авторизації для захисту конфіденційних даних та запобігання несанкціонованому використанню.

Шифрування відіграє першочергову роль у захисті конфіденційних даних (платіжна інформація, облікові дані користувачів, дані транспортного засобу), що передаються під час зарядки електромобілів. Такі стандарти, як ISO 15118, вимагають використання надійних методів шифрування для забезпечення конфіденційності та цілісності даних. Серед них можна виділити:

- Transport Layer Security (TLS) використовується для захисту зв'язку між електромобілями та зарядними станціями та між зарядними станціями та центральними системами керування. TLS забезпечує шифрування, цілісність даних та автентифікацію (Should TLS be Omitted to Have a Faster Charging Session Start? Hnject.com, 2024). Новіші версії TLS (наприклад, 1.3) є кращими для підвищення безпеки.
- Шифрування на основі сертифікатів значною мірою покладається на цифрові сертифікати та інфраструктуру відкритих ключів (PKI) для автентифікації та безпечного зв'язку. ISO 15118 та OCPP 2.0 використовують керування сертифікатами.
- Симетричне та асиметричне шифрування характерне для ISO 15118, який використовує гібридний підхід, застосовуючи асиметричне шифрування для автентифікації та обміну ключами, та симетричне шифрування (наприклад, AES-128) для шифрування основної частини даних під час сеансу зарядки.

Для керування доступом до інфраструктури зарядки електромобілів та забезпечення безпеки транзакцій використовується широкий спектр *методів автентифікації та авторизації*:

- RFID (радіочастотна ідентифікація) як поширений метод ідентифікації та автентифікації користувачів на зарядних станціях. Користувачі пред'являють RFID-картку або брелок для початку зарядки.
- Мобільні додатки використовують багато зарядних мереж для автентифікації користувачів, керування сеансами та оплати.
- Платіжні системи в інтеграції з терміналами для кредитних/дебетових карток або іншими платіжними шлюзами дозволяють здійснювати пряму оплату на зарядній станції.
- Plug & Charge (ISO 15118) забезпечує автоматичну автентифікацію та авторизацію, як тільки електромобіль підключається до сумісної зарядної станції, використовуючи цифрові сертифікати (Mültin, M., 2020).
- Віддалена авторизація при сеансі зарядки забезпечує авторизацію віддалено через центральну систему керування (бекенд OCPP).
- MAC-адреса (AutoCharge) використовується деякими системами для авторизації, але цей метод має обмеження щодо безпеки.
- Біометрична автентифікація включає використання даних інерційних давачів з ручок зарядних кабелів або смарт-годинників для неявної автентифікації (Sturgess, J., Köhler, S., Birnbach, S., & Martinovic, I., 2023).
- Єдиний вхід (SSO) дозволяє користувачам отримувати доступ до послуг зарядки електромобілів з тими самими обліковими даними, що використовуються для інших програм, підвищуючи зручність та безпеку (SSO for EV charging: Unify authentication and fortify security., 2023).
- Ідентифікація транспортного засобу на основі штучного інтелекту з використанням камер та штучного інтелекту забезпечує автоматичну ідентифікацію електромобілів для авторизації.

Безпека зарядки електромобілів залежить від надійних методів шифрування, таких як TLS та системи на основі сертифікатів, особливо в рамках ISO 15118. Автентифікація та авторизація опрацьовуються різними методами, з акцентом на більш безперебійні та безпечні варіанти, такі як Plug & Charge та SSO. Сумісність та зручність для користувачів є ключовими факторами в еволюції цих механізмів.

У таблиці 3 наведено порівняння методів аутентифікації та авторизації.

Таблиця 3

**Порівняння методів аутентифікації та авторизації
в зарядних станціях для електромобілів**

Метод	Рівень безпеки	Зручність для користувача	Складність впровадження	Сумісність
RFID	Середній	Висока	Низька	Широка
Мобільний застосунок	Середній	Висока	Середня	Залежить від мережі
Платіжна система	Високий (залежить від системи)	Середня	Середня	Широка
Plug & Charge (ISO 15118)	Високий	Дуже висока	Висока	Обмежена (потрібна підтримка стандарту)
Віддалена авторизація	Середній	Висока	Середня	Залежить від мережі
MAC-адреса (AutoCharge)	Низький	Висока	Низька	Обмежена, проблеми з безпекою
Біометрична аутентифікація	Високий	Середня	Висока	Обмежена
Єдиний вхід (SSO)	Високий	Дуже висока	Середня	Залежить від провайдера SSO
Ідентифікація на основі ІП	Високий	Висока	Висока	Обмежена

Наукова новизна отриманих результатів полягає у проведенні комплексного порівняльного аналізу моделей архітектури (централізованої, децентралізованої, гібридної), ключових протоколів передачі даних (з їх класифікацією за рівнями взаємодії EV-EVSE, EVSE-CPO, UI) та механізмів безпеки для інформаційних систем зарядки електромобілів за критеріями - масштабованість, надійність, безпека, вартість, сумісність. На відміну від існуючих досліджень, що часто розглядають ці аспекти окремо, запропонований підхід дозволяє оцінити їх у взаємозв'язку. Це забезпечує науково обґрунтовану базу для вибору інтегрованих рішень, що сприяє підвищенню ефективності проектування та експлуатації безпечних і масштабованих мереж зарядних станцій. Практична значимість дослідження полягає у можливості використання отриманих результатів для створення більш ефективних, надійних і безпечних систем зарядки, а також для розробки галузевих стандартів та рекомендацій щодо інформаційного забезпечення інфраструктури електротранспорту.

Висновки

У статті розглянуто інформаційні технології, архітектури та протоколи передачі даних, що є критично важливими для сучасних систем зарядних станцій електромобілів. На основі проведеного дослідження зроблено наступні висновки:

Аналіз моделей архітектури систем показав, що вибір між централізованою, децентралізованою та гібридною архітектурою залежить від специфіки проекту. Централізовані системи підходять для управління великими мережами, децентралізовані – для локальних систем з вимогою високої автономності, а гібридні пропонують збалансований підхід, поєднуючи переваги обох, хоча й зі збільшеною складністю управління.

Порівняльний аналіз протоколів передачі даних підтвердив домінуючу роль OCPP для зв'язку станції з оператором, важливість ISO 15118 для розширеної взаємодії між електромобілем та станцією (включаючи Plug & Charge), та визначив ніші для Modbus (внутрішньостанційна комунікація) і MQTT (ефективна передача даних у реальному часі, особливо в IoT-контексті). Запропонована класифікація протоколів за рівнями взаємодії систематизує їх застосування.

Дослідження механізмів безпеки та автентифікації виявило критичну важливість шифрування (TLS) та інфраструктури відкритих ключів (PKI), особливо в рамках ISO 15118. Встановлено, що поряд з традиційними методами (RFID, мобільні застосунки), зростає значення автоматизованих та більш безпечних підходів, таких як Plug & Charge та єдиний вхід (SSO), хоча їх впровадження потребує відповідної інфраструктурної підтримки.

Висновки, зроблені на основі аналізу архітектур систем, протоколів та механізмів безпеки, мають прямі практичні наслідки для всіх учасників ринку зарядної інфраструктури. Розуміння виявлених переваг, недоліків та ключових вимог дозволяє сформулювати наступні цільові рекомендації, спрямовані на оптимізацію їхньої діяльності та сприяння гармонійному розвитку галузі.

Для операторів мереж заряджання рекомендується розглянути можливість використання MQTT у поєднанні з OCPP для покращення зв'язку в реальному часі, масштабованості та інтеграції з екосистемою IoT. Впровадження надійних протоколів роумінгу, таких як OCPP, забезпечить безперебійний досвід заряджання для водіїв електромобілів у різних мережах. Також важливо відстежувати розвиток та потенційне впровадження нових стандартів.

Виробникам електромобілів слід забезпечити відповідність та підтримку ключових протоколів зв'язку, включаючи CAN, ISO 15118 та IEC 61851, для гарантування безперебійної взаємодії з зарядною інфраструктурою. Варто також розглянути переваги впровадження MQTT для розширених функцій інтерфейсу користувача.

Операторам енергосистем та постачальникам енергії необхідно сприяти впровадженню протоколів, таких як OCPP та IEEE 2030.5, для полегшення розумного заряджання та інтеграції електромобілів в енергосистему. Співпраця з операторами зарядних мереж є ключовою для забезпечення сумісності та ефективного управління навантаженням.

Розробникам технологій слід продовжувати інновації та розробляти рішення, що підвищують продуктивність, безпеку та сумісність протоколів зв'язку для зарядки електромобілів. Основний акцент потрібно зробити на створенні надійних та масштабованих платформ, що підтримують кілька протоколів, включаючи MQTT, OCPP та протоколи роумінгу.

Майбутній розвиток протоколів передачі даних у сфері заряджання електромобілів буде спрямований на задоволення зростаючих потреб у розумному заряджанні та автономному заряджанні. Стандартизація та сумісність відіграватимуть вирішальну роль у сприянні широкого впровадження електромобілів, наголошуючи на необхідності багатопроTOCOLьного підходу для задоволення різноманітних вимог комунікації в екосистемі заряджання електромобілів.

СПИСОК ЛІТЕРАТУРИ

1. Agnihotri, N. (2024, February 19). *What are the communication protocols in EVs?* EV Engineering & Infrastructure. <https://www.evengineeringonline.com/what-are-the-communication-protocols-in-evs/>
2. Ahmed, M. A., Guerrero, L., & Franco, P. (2024). Network Modeling and Analysis of Internet of Electric Vehicles Architecture for Monitoring Charging Station Networks—A Case Study in Chile. *Sustainability*, 16(14), 5915–5915. <https://doi.org/10.3390/su16145915>
3. Al-Alwash, H. M., Eugen Borcoci, Marius-Constantin Vochin, Indika A. M. Balapuwaduge, & Li, F. Y. (2024). Optimization Schedule Schemes for Charging Electric Vehicles: Overview, Challenges, and Solutions. *IEEE Access*, 1–1. <https://doi.org/10.1109/access.2024.3371890>
4. Alcaraz, C., Cumplido, J., & Triviño-Cabrera, A. (2023). OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0. *International Journal of Information Security*, 22(5), 1395–1421. <https://doi.org/10.1007/s10207-023-00698-8>

5. Ampcontrol. (2025, January 13). *The Role of Modbus in EV Charger Infrastructure*. Ampcontrol.io; Ampcontrol. <https://www.ampcontrol.io/post/the-role-of-modbus-in-ev-charger-infrastructure>
6. Arrow Electronics. (2024, June 12). *Analysis of electric vehicle charging architecture and safety protection solutions*. Arrow.com. <https://www.arrow.com/en/research-and-events/articles/analysis-of-electric-vehicle-charging-architecture-and-safety-protection-solutions>
7. *Building a Charging Station Management System with AWS | Amazon Web Services*. (2024, September 12). Amazon Web Services. <https://aws.amazon.com/blogs/industries/building-a-charging-station-management-system-with-aws/>
8. *Charging Standards*. (2025). Vector Informatik GmbH. <https://www.vector.com/se/en/know-how/smart-charging/charging-standards/>
9. *EV charging - electrical architectures - Electrical Installation Guide*. (2023). Electrical-Installation.org. https://www.electrical-installation.org/enwiki/EV_charging_-_electrical_architectures
10. Gadacz, H. (2021). *Evaluation of electric mobility authentication approaches*. 1–10. <https://doi.org/10.1145/3488904.3493384>
11. Hsaini, S., Ghogho, M., & Charaf, M. E. H. (2022). An OCPP-Based Approach for Electric Vehicle Charging Management. *Energies*, 15(18), 6735. <https://doi.org/10.3390/en15186735>
12. Hübschmann, I. (2021, January 4). *The Pros and Cons of Using MQTT Protocol in IoT*. Nabto. <https://www.nabto.com/mqtt-protocol-iot/>
13. Lesjak, Ž. (2024, Decemeber 17). *EV Charging Protocols And Standards: A Comprehensive Guide*. Tridens. <https://tridenstechnology.com/ev-charging-protocols-standards/>
14. Li, J., Gu, C., Xiang, Y., & Li, F. (2022). Edge-cloud Computing Systems for Smart Grid: State-of-the-art, Architecture, and Applications. *Journal of Modern Power Systems and Clean Energy*, 10(4), 805–817. <https://doi.org/10.35833/mpce.2021.000161>
15. Lund, V. V. (2024). *Reimagining Data Exchange: OPC UA to MQTT and OCPP Conversion for Mobile Charging Stations* (Master's thesis, University of Agder).
16. *Modbus and OCPP: Caburn Telecom (By CSL Group)*. Caburn Telecom. (2024). <https://caburntelecom.com/the-role-of-modbus-ocpp-protocols-in-ev-charge-points/>
17. Mültin, M. (2020, November 15). *The basics of Plug & Charge*. Switch. <https://www.switch-ev.com/blog/basics-of-plug-and-charge>
18. Naga, V. (2021). An Optimal Cloud Based Electric Vehicle Charging System. *Asia Pacific Journal of Energy and Environment*, 8(2), 39–48. <https://doi.org/10.18034/apjee.v8i2.604>
19. On approval of the National Transport Strategy of Ukraine for the period until 2030. Resolution of the Cabinet of Ministers of Ukraine dated May 30, 2018. URL: <https://zakon.rada.gov.ua/laws/file/text/123/f541675n27.pdf>
20. Pourmirza, Z., & Walker, S. (2021). Electric Vehicle Charging Station: Cyber Security Challenges and Perspective. *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*. <https://doi.org/10.1109/sege52446.2021.9535052>
21. *Revolutionizing Electric Vehicle Charging with CAN Bus Technology*. (2023). TC CHARGER. <https://onboard-charger.com/blogs/on-board-charger/revolutionizing-electric-vehicle-charging-with-can-bus-technology>
22. *Should TLS be Omitted to Have a Faster Charging Session Start?* (2024). Hsubject.com. <https://www.hsubject.com/blog-posts/should-tls-be-omitted-to-have-a-faster-charging-session-start>
23. *SSO for EV charging: Unify authentication and fortify security*. (2023, May 2). AMPECO. <https://www.ampeco.com/blog/sso-for-ev-charging-unify-authentication-and-fortify-security/>
24. Striani, S., Pedersen, K. L., Engelhardt, J., & Marinelli, M. (2024). Experimental Investigation of a Distributed Architecture for EV Chargers Performing Frequency Control. *World Electric Vehicle Journal*, 15(8), 361. <https://doi.org/10.3390/wevj15080361>
25. Sturgess, J., Köhler, S., Birnbach, S., & Martinovic, I. (2023). CableAuth: a biometric second factor authentication scheme for electric vehicle charging.
26. Sule, U., & Kristianto, K. (2024, July 9). *Testing the EV ecosystem (part one)*. Thoughtworks. <https://www.thoughtworks.com/en-us/insights/blog/compliance/testing-the-EV-ecosystem-part-one>
27. Sultana, Z., Basha, C. H., & Irfan, M. M. (2024). Communication Protocols for Electric Vehicles: A Comprehensive Analysis. 127–133. <https://doi.org/10.1109/icses63445.2024.10763347>

**INFORMATION TECHNOLOGIES AND DATA TRANSMISSION PROTOCOLS
IN ELECTRIC CAR CHARGING SYSTEMS****Oleh Markiv¹, Yuriy Ryshkovets²,**^{1,2} Lviv Polytechnic National University,
Information Systems and Networks Department, Lviv, Ukraine¹ E-mail: oleh.i.markiv@lpnu.ua, ORCID: 0009-0009-4109-174X² E-mail: yuriy.v.ryshkovets@lpnu.ua, ORCID: 0000-0001-5831-4000

© Markiv O.I., Ryshkovets Yu.V., 2025

The article presents a comprehensive analysis of innovative information technologies that are critical for the development of modern electric vehicle charging station infrastructure. The impact of digital solutions on the reliability, security, scalability, and efficiency of charging networks is investigated, and the challenges associated with their implementation are analyzed. Current industry problems are considered: the exponential growth in the number of electric vehicles, the need for fast and secure user authentication, ensuring continuous real-time monitoring of the condition of charging stations, and intelligent optimization of charging processes. Particular attention is paid to issues of ensuring stable communication in conditions of unstable coverage, compatibility of equipment from different manufacturers, and the economic efficiency of implemented technologies. Based on an analysis of cutting-edge scientific research, the article reveals various architectural approaches to building information systems for charging stations, evaluates their advantages and disadvantages, and describes in detail the mechanisms of interaction between electric vehicles, charging stations, and centralized management systems. An overview of modern cybersecurity methods and authentication protocols adapted to the specifics of charging infrastructure is presented. The conclusions summarize the research results and provide substantiated recommendations for the selection and implementation of information technologies to create a reliable, secure, scalable, and cost-effective charging station infrastructure. The article will be useful for research engineers, software developers, charging network operators, as well as representatives of energy companies and government regulators.

Keywords - electric vehicles, electric vehicle supply equipment, charge point operator.