КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.760
УДК 342.9:5.08

Клімушин Петро Сергійович
кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID ID: 0000-0002-1020-9399,
klimushyn@ukr.net

Світличний Віталій Анатолійович
кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID ID: 0000-0003-3381-3350
vit.svet@ukr.net

Гнусов Юрій Валерійович
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та DATA-технологій
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID ID: 0000-0002-9017-9635
duke6969@i.ua

Онищенко Юрій Миколайович
кандидат наук з державного управління, доцент, заступник директора інституту
з освітньої та науково-дослідної діяльності навчально-наукового інституту № 4
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID ID: 0000-0002-7755-3071
onischenko1980@gmail.com

АВТОМОБІЛЬНА ЕЛЕКТРОНІКА ТА КІБЕРБЕЗПЕКА: СИСТЕМНИЙ ОГЛЯД АТАК НА БЕЗПЕКУ ТА ЗАХОДІВ ПРОТИДІЇ

Анотація. Сучасна автомобільна електроніка — це складна система датчиків, електронних блоків керування (ECU) і виконавчих механізмів, з'єднаних через різні типи автомобільних мереж для контролю та моніторингу стану автомобіля. Крім того, сучасні транспортні засоби все більше підключаються до зовнішнього світу за допомогою технологій автомобілі для всього (V2X). Вони створюють нові поверхні для атак, які збільшують ризик кібербезпеки для сучасних транспортних засобів. З появою інтелектуальних транспортних структур фокус перемістився до структури узгоджених міжтранспортних систем, символом яких є інтеграція інфраструктури, людей, транспортних засобів, міських територій та навколишнього середовища. Це поєднання комп'ютерних технологій та автомобільних інновацій підняло безліч питань щодо кібератак на автомобілі, які відіграють важливу роль у розробці та використанні автомобільних технологій. Удосконалена бездротова технологія дозволяє транспортним засобам обмінюватися та передавати інформацію один одному та навколо себе в режимі реального часу, що допоможе зменшити кількість аварій, заторів та підвищити ефективність мобільних засобів. Багато передових технологій, як-от хмарні обчислення, штучний інтелект, технологія V2X і вдосконалені системи допомоги водієві, все ширше використовуються в автомобілях, що робить транспортні засоби більш інтелектуальними для надання комфортних послуг людям і забезпечення безпеки водіїв і пасажирів. Однак у міру того, як автомобілі стають більш підключеними до Інтернету, бездротових мереж, один з одним та з іншою інфраструктурою транспортних мереж ризик кібератак викликає все більше проблем. У цієї оглядової статті спочатку аналізуються вразливості мереж автомобіля та визначаються основні атаки кібербезпеки на транспортні засоби. Проаналізовано технології підвищення кібербезпеки мереж транспортних засобів за технологічними напрямами: шифрування даних, автентифікації повідомлень, виявлення вторгнень в мережу, побудови довіреної платформи та реалізацією концепції Crypto-Engine.

Ключові слова: автомобільна електроніка; автомобільна кібербезпека; мережі автомобіля; шифрування даних; автентифікація повідомлень; технологія виявлення вторгнень; модуль довіреної платформи; концепція Crypto-Engine.

ВСТУП

Постановка проблеми. Історично автомобільна промисловість була зосереджена на питаннях фізичної безпеки, таких як захист від зіткнень і безпека пасажирів. Однак із зростаючою інтеграцією складної електроніки та каналів зв'язку фокус тепер розширився, включивши кібербезпеку як критичну проблему безпеки транспортних засобів. Виробники комплектного обладнання (OEM) повинні мати можливість забезпечити конфіденційність, цілісність, і доступність систем автомобіля [37].

Для виконання функціональних процесів сучасних автомобілів використовується від 70 до 100 мікропроцесорних електронних блоків керування, які об'єднані в мережу по всьому транспортному засобу. Вбудований зв'язок із зовнішнім світом робить сучасні автомобілі частиною Інтернету речей (IoT). На додаток до великої кількості ECU, сучасні транспортні системи оснащені кількома датчиками, приводами, камерами, радарами та пристроями зв'язку. Ці системи призначені для підвищення продуктивності, ефективності, інтелектуальних послуг і безпеки для користувачів автомобілів шляхом збору та інтерпретації різних даних.

Сьогодні транспортні засоби дедалі більше підключаються через різноманітні канали зв'язку, що вимагає безпечного доступу для авторизованих користувачів, захисту даних допомоги водієві та автономного водіння, а також забезпечення цілісності даних для захисту від неправильного використання чи маніпулювання. Незважаючи на переваги цих нових технологій, за останні роки було зареєстровано численні випадки вторгнення, що підкреслює вразливі місця в поточних системах. Зменшення ризиків кібербезпеки є проблемним завданням, яке потребує практичних рішень.

Транспортний засіб, який відчуває навколишнє середовище та безпечно пересувається практично без втручання людини, називається самокерованим автомобілем або підключеним транспортним засобом (ICV). Ці досягнення в першу чергу стали можливими завдяки складній електричній/електронній (E/E) архітектурі, яка полегшує ефективний зв'язок між різними компонентами автомобіля. Оскільки транспортні засоби стають більш взаємопов'язаними та залежними від мікропроцесорних систем, вони стають чутливими до потенційних ризиків кібербезпеки та зовнішнього втручання.

Підключені автомобілі піддаються загрозам безпеці мережі, таким як комп'ютерні віруси, порушення конфіденційності, цілісності та доступності, несанкціонований доступ, крадіжки даних, шкідливі програми, злом і витік даних. Порівняно зі зломом апаратного забезпечення, віддалені безконтактні атаки є більш загрозливими для підключених автомобілів, які в основному проявляються в чотирьох проблемних аспектах: 1) ризик викрадення та контролю інформації про транспортний засіб; 2) ризик злому та крадіжки передачі інформації між людьми, транспортними засобами, дорогами та хмарними обчисленнями транспортних засобів; 3) ризики безпеки в системі керування шиною та передачі інформації підключеного автомобіля; 4) ризики безпеки в хмарі, тобто надсилання шкідливих файлів через хмару.

Для вирішення цих проблем в статті проведено аналіз характеристик та вразливостей автомобільних мереж, розглянуто еволюція архітектури E/E і на базі цього запропонована ієрархічна архітектура безпеки. Надано характеристики мережевих атак на фізичному, канальному та прикладному рівнях. Визначено основні проблеми з

захисту підключеного автомобіля. Проведено порівняльний аналіз технологій підвищення мережевої безпеки автомобіля. Проаналізовано технології підвищення кібербезпеки мереж транспортних засобів за технологічними напрямами: шифрування даних, автентифікації повідомлень, виявлення вторгнень в мережу, побудова довіреної платформи та реалізація концепції Crypto-Engine для захисту кластеризованих вузлів мережі всередині транспортного засобу і встановлення захищених сеансів зв'язку.

Аналіз останніх досліджень і публікацій. В роботі [17] автори пропонують концептуальну модель системної динаміки для оцінки кібербезпеки підключених автомобілів. Ця модель об'єднує різні елементи, такі як структура зв'язку, безпечний фізичний доступ, людський фактор, рівні проникнення, регуляторні закони, рамки політики та довіра в галузі і громадськості.

El-Rewini та ін. [11] пропонують трирівневу структуру кібербезпеки зондування, зв'язку та контролю, щоб забезпечити повне розуміння загроз безпеці. Серед них комунікаційний рівень визначено як найбільш вразливий.

У роботі [29] пояснюються різні методи захисту шини CAN від кібератак, такі як обмін ключами, криптографічні паролі та автентифікація шини CAN. Запропоновано використання криптографічного алгоритму AES для захисту від крадіжки даних і кібератак у транспортних засобах.

Aldhyani та Alkahtani [2] розробили високопродуктивну систему, використовуючи підхід машинного навчання для захисту мереж транспортних засобів від кіберзагроз. Запропоноване рішення безпеки було перевірено за допомогою набору даних реальної мережі транспортного засобу. Цю модель можна інтегрувати в деякі ECU як програмні пакети або як спеціальну систему виявлення вторгнень (IDS).

В іншому дослідженні Kukkala та ін. [24] представляють архітектуру, пов'язану з підключеними транспортними засобами, і визначають вразливості в цієї архітектурі, а також пропонують рішення захисту. Методи виявлення зловмисного програмного забезпечення поділяються на підходи на основі сигнатур, поведінки, хмари, евристики та машинного навчання. Автори рекомендують, щоб майбутні дослідження боротьби з атаками зловмисного програмного забезпечення зосередилися на легкій криптографічній автентифікації, системах брандмауерів, глибокому навчанні з використанням механізмів розвантаження обчислень і програмно-визначеній безпеці.

Chandwani та ін. [9] визначають поточні виклики безпеці та рекомендує рішення для пом'якшення кіберзагроз для електромобілів та їх бортових систем зарядки. Як приклад використання представлені топології бортового зарядного пристрою разом із їхніми потенційними векторами загрози та відповідними контрзаходами.

Wang та ін. [38] розробили структуру для аналізу продуктивності підключених автомобілів у різних середовищах водіння. Ця модель допомагає розробляти вимоги до кібербезпеки для нових ECU та створювати сценарії тестування для перевірки системи.

Sabaliauskaite та ін.[33] досліджували взаємозалежності між безпекою та кібербезпекою, досліджуючи, як заходи безпеки впливають на кібербезпеку і навпаки. Вони розробили методологію для управління компромісами між автомобільною безпекою та кібербезпекою.

Застосування штучного інтелекту (ШІ) в безпеці транспортних засобів є перспективним, але все ще обмеженим через велике споживання пам'яті та процесорних ресурсів [31]. З цих причин ШІ планується використовувати здебільшого в хмарних системах і менше в транспортних засобах, де використовуються вбудовані процесори.

IDS на основі машинного навчання були запропоновані для аналітики великих даних у мережах транспортних засобів [7], тоді як методи глибокого навчання можуть

бути використані для розробки IDS. Інтеграція ШІ в автомобільну промисловість призвела до потреби в інноваційних методах перевірки систем самонавчання і може пом'якшити функціональні ризики та ризики інформаційної безпеки.

Інтернет речей все більше інтегрується в автомобільну промисловість, насамперед через інтелектуальні датчики. Архітектуру IoT на основі глибоких нейронних мереж можна адаптувати для використання в системах моніторингу кібератак [32].

В автомобільних мережах тепер можливо безпечне оновлення мікропрограми по без дроту [34]. Щоб задовольнити вимоги автомобільної промисловості щодо електромагнітної сумісності та захищеності, був розроблений новий стандарт Ethernet, який підтримує повнодуплексну роботу по одній витій парі. Автомобільний Ethernet набирає популярності в мережах автомобілів завдяки високій швидкості передачі даних і розширеним функціям кібербезпеки [10]. Ці дослідження також виявили вразливі місця в безпеці зв'язку Ethernet і представили можливі контрзаходи.

Системний підхід до управління конфіденційністю автомобілів був розроблений в режимі реального часу [28]. Цей підхід було підтверджено як технічне рішення для конфіденційності даних за допомогою сценаріїв тестування безшумності за даними GPS про місцезнаходження транспортного засобу.

Kong та ін. [23] вивчають рішення для збереження конфіденційності для моніторингу драйверів за допомогою технології блокчейн і визначають, що найбільш трудомістким етапом є передача даних між транспортним засобом і хмарними центрами, і проводять огляд вимог до кібербезпеки для хмарних додатків підключених транспортних засобів.

У оглядовому дослідженні [14] спочатку аналізуються причини, чому поточна мережа автомобіля є вразливою до мережевих атак, і підсумовуються три методи реалізації загроз мережевій безпеці. Після короткого ознайомлення з безпекою автомобільної мережі цей оглядовий документ визначає основні атаки безпеки на інтелектуальні підключені транспортні засоби. Потім представлено технологія підвищення безпеки мереж транспортних засобів з трьох аспектів, включаючи технологію шифрування даних у мережі автомобіля, технологію автентифікації повідомлень у мережі автомобіля та технологію виявлення аномалій мережі автомобіля. Актуальні подальші дослідження в сфері розгортання безпеки мереж за рахунок впровадження сучасних спеціалізованих компонент криптографічних перетворень та прискорювачів.

Основна мета статті [13] пов'язана з аналізом процесів втручання зовнішніх об'єктів в роботу електроніки транспортного засобу та заходами, які вживаються для її захисту. Підкреслено значний вплив законодавства на автомобільну кібербезпеку. Запроваджено рекомендації та правила для покращення загального стану кібербезпеки в автомобільній промисловості. У цьому документі досліджувано потенційні вразливості, які впливають на загрозу кібербезпеці, і механізми захисту для пом'якшення ризиків. Однак обмеження статті базується на знаннях, наявних на сьогоднішній день, і не розголошуються комерційні таємниці виробників автомобілів чи компаній із кібербезпеки.

Таким чином, останнім часом автомобільний сектор приділяє більшу увагу кібербезпеці, розробляються нові стандарти, норми та рекомендації, щоб встановити єдині вимоги як до кібербезпеки, так і до функціональної безпеки та забезпечити практичні інструменти для їх впровадження.

Мета статті полягає в тому, щоб зосередитися на проблемах кібербезпеки транспортних засобів та способах їх вирішення відповідно. У статті проаналізовано причини вразливості транспортних засобів до мережевих атак. Було проаналізовано

переваги та недоліки запропонованих засобів захисту. Детально порівняно методи виявлення аномальних вторгнень у мережу транспортного засобу та актуальні криптографічні рішення з використанням модулів довіреної платформи, криптографічних співпроцесорів та прискорювачів, крипто-двигунів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Сучасні транспортні засоби оснащені великою кількістю ECU, кожен з яких відповідає за певні функції, наприклад керування двигуном, системи безпеки, інформаційно-розважальні системи та функції допомоги водієві. Транспортний засіб є потужною сенсорною платформою, яка передає близько 2500 сигналів усередину з приблизно 100 ECU, підключеними через мережу всередині автомобіля. Автомобільна мережа полегшує обмін даними між датчиками, ECU та виконавчими механізмами, забезпечуючи роботу автомобіля.

На рис. 1 показано внутрішня структуру автомобільних підмереж. Кожна підмережа базується на різних мережевих технологіях залежно від вимог систем, підключених до цієї конкретної мережі. Сьогодні існує такі найпоширеніші типи автомобільних підмереж:

– *Мережа контролера (CAN)* є найпопулярнішою серед автомобільних шинних систем. Це єдина централізована мережева шина, на яку транслюються всі дані всередині автомобіля. Цей тип мережі використовується в системах керування газорозподілом двигуна, антиблокувальних системах гальм, електронному управлінні дросельною заслінкою тощо.

Рис. 1. Огляд внутрішніх підмереж автомобіля

Повідомлення за протоколом CAN не використовують пряму адресацію одержувачів або ідентифікацію відправників. Тобто, кадри повідомлень не містять адреси відправника чи одержувача. Замість цього приймачі фільтрують трафік на шині для прийнятих ідентифікаторів (ID) повідомлень CAN. Ідентифікатор повідомлення використовується як непряма адреса. CAN використовує арбітражний механізм (логічний 0 на шині називається домінуючим і перекриває логічну 1) для забезпечення доступу до шини. Таким чином, ідентифікатори повідомлень, переданих одночасно, будуть арбітражні автоматично, і пройде найнижчий ідентифікатор повідомлення.

Технологія CAN забезпечує пропускну здатність до 1 Мбіт/с і корисне навантаження до 8 байт, яка наразі перевантажена і не може задовольнити попит на наступне покоління автомобільних електронних систем.

– *Мережа контролера з гнучкою швидкістю передачі даних (CAN FD)* є вдосконаленням традиційної шини CAN і повністю сумісна із CAN. *CAN FD* визначає новий формат кадру, використовуючи два різних тактових сигналу для різних частин кадру. Однак у сегменті даних тактова частота збільшена до 8 разів, що дозволяє передавати до 64 байтів на кадр. Тобто, CAN-FD є вдосконаленою технологією зв'язку, яка забезпечує високу пропускну здатність до 8 Мбіт/с і корисне навантаження до 64 байтів. Дослідження щодо нового протоколу CAN XL з використанням технології автомобільного Ethernet дозволяють досягти пропускну здатність до 20 Мбіт/с з корисним навантаженням 2048 байт.

В роботі [4] запропоновано нова модель безпеки CAN FD на використанні шифрування та автентифікації. Шифрування з симетричним ключем AES-256 застосовується до першого блоку кадру даних, а до другого блоку даних виконується автентифікація за допомогою реалізації хеш-функції HMAC/SFIA-256. Результати показали, що запропонована модель безпеки має вищу ефективність шифрування, ніж існуючі методи.

– *Локальна мережа з'єднання (LIN)* — економічна система зв'язку для простих операцій комутації або для передачі мінімальної діагностичної інформації таких як датчики температури або дощу, невеликих двигунів, ламп, люка або керування опаленням з пропускної здатністю значно нижчою, ніж у CAN. Один кадр повідомлення містить від 2 до 8 байт даних. Доступ до шини контролюється єдиним головним вузлом, який запитує підлеглі вузли на передачу за потреби. Подібно до CAN ідентифікація досягається за допомогою ідентифікаторів повідомлень. LIN часто використовується для підключення одного чи невеликого набору вузлів у підмережі до пристрою CAN.

– *FlexRay* — це змішана система зв'язку, що запускається за часом і за подіями і пропонує значно вищі швидкості передачі, ніж CAN. Його частина, що запускається за часом, статичний сегмент, дозволяє узгоджувати передачі відповідно до загального часу, синхронізованого по всій мережі. Це може значно скоротити час відповіді в найгіршому випадку та має вирішальне значення для систем, яким потрібно швидко реагувати, наприклад гарантувати безпеку транспортних засобів. Динамічний сегмент FlexRay використовує підхід множинного доступу з гнучким розподілом часу, надаючи доступ до шини в часових інтервалах, які ECU можуть розширювати за потреби, реалізуючи таким чином схему пріоритетів.

Через часові інтервали в статичному і динамічному сегменті реалізується неявна схема адресації. Оскільки всі пристрої синхронізовані за часом, передавачі та приймачі можуть надсилати й отримувати в часові інтервали, призначені під час розробки.

Основна мета цього типу мережі полягає в підтримці нових систем бездротового керування, таких як кермування і гальмування, які вимагають управління із високою швидкістю передачі.

– *Медіа-орієнтовані системи транспорту (MOST)* — має найбільшу пропускну здатність серед усіх мереж і в основному використовується для аудіо-, відео-, навігаційних і телекомунікаційних систем.

MOST використовує кільцеву архітектуру та для критично важливих для безпеки середовищ може бути налаштований у подвійну кільцеву структуру для досягнення надмірності. Кожна шина MOST містить майстер синхронізації, що генерує кадри для синхронізації часу для інших вузлів. Доступ до шини також контролюється цим майстром синхронізації, залишаючи простір у кадрах для асинхронних або синхронних даних, які передаються у так званих каналах.

Шина MOST є досить складною системою зв'язку, яка вимагає великих зусиль і витрат на проєктування та впровадження. Останніми роками MOST відчуває все більший тиск з боку дротового автомобільного Ethernet, який пропонує аналогічну пропускну здатність за нижчою ціною.

Низка протоколів була розроблена спеціально для автомобільної сфери, включаючи мережу контролера CAN, FlexRay, локальну мережу з'єднань (LIN) і транспортну систему, орієнтовану на MOST.

Зазвичай використовуються стандартизовані протоколи для мережі CAN контролера (ISO 11898-1:2024), мережі LIN локального з'єднання (ISO 17458-1:2013) і високошвидкісної шини FlexRay (ISO 17987-1:2016) передачі даних, яка застосовується на особливо відповідальних ділянках обміну даними. FlexRay може використовуватися як основна шина в мультидоменній мережній архітектурі, наприклад, гальмо за проводом. CAN широко використовується для зв'язку в автомобілях завдяки своїй надійності та міцності, наприклад в системи виявлення зіткнень. Це дозволяє декільком ECU обмінюватися даними через спільну шину, забезпечуючи передачу даних і контроль у реальному часі. LIN є більш простим і економічно ефективним протоколом, який підходить для менш критичних додатків, таких як керування внутрішнім освітленням або системою багатофункціонального ключа.

Існуючі мережеві протоколи транспортних засобів, такі як CAN і Flex Ray, не мають механізму захисту інформації на початку свого проєктування, що робить мережу автомобіля вразливою до перехоплення, підробки, модифікації та повторного відтворення. Шина CAN є основною точкою проблеми інформаційної безпеки автомобіля, оскільки це єдина централізована мережева шина, на яку транслюються всі дані всередині автомобіля. Повідомлення за протоколом CAN не використовують пряму адресацію одержувачів або ідентифікацію відправників, що є вразливістю в процесах автентифікації повідомлень.

Керування електронним обладнанням автомобіля виконується через систему шин CAN і OBD (бортова діагностика). Шина CAN забезпечує спосіб для різних компонентів автомобіля спілкуватися один з одним і обмінюватися даними. Система OBD, з іншого боку, насамперед спрямована на допомогу механікам і технікам у діагностиці несправностей двигуна та інших компонентів.

Еволюція архітектури транспортного засобу E/E складається з трьох архітектур: розподілена E/E архітектура використовувалася до 2019 року, доменно-централізована архітектура є сьогоднішньою транспортною архітектурою, зональна архітектура показує майбутню архітектуру E/E автомобіля.

Розподілена архітектура E/E складається з центрального шлюзу та з функціональних ECU, які з'єднані через шину мережі контролера CAN. Використання центрального шлюзу забезпечує більш тісну співпрацю між ECU, здатність виконувати більш складні функції.

Доменно-централізована архітектура E/E об'єднує доменно-спеціальні ECU за допомогою шини CAN і з'єднання Ethernet. Крім того, у цьому типі архітектури використовується центральний шлюз ECU. Ця архітектура здатна обробляти більш складні функції і вартість архітектури можна оптимізувати за допомогою консолідації функцій для інтеграції та зв'язку у кожному домені, що призводить до підвищення продуктивності та ефективності.

Зональна архітектура кластеризує ECU на основі конкретних зон автомобіля. Ця архітектура включає: центральний високопродуктивний обчислювальний блок, зональні ECU, підключення шини CAN та автомобільний Ethernet. Даний підхід забезпечує кращу координацію та зв'язок між різними доменами, підвищуючи загальний інтелект автомобіля та швидкість реагування [5].

На рис. 2 наведена удосконалена ієрархічна архітектура безпеки автомобіля, яка включає наступні рівні: комунікаційний, безпеки, мережевий та компонентів [1].

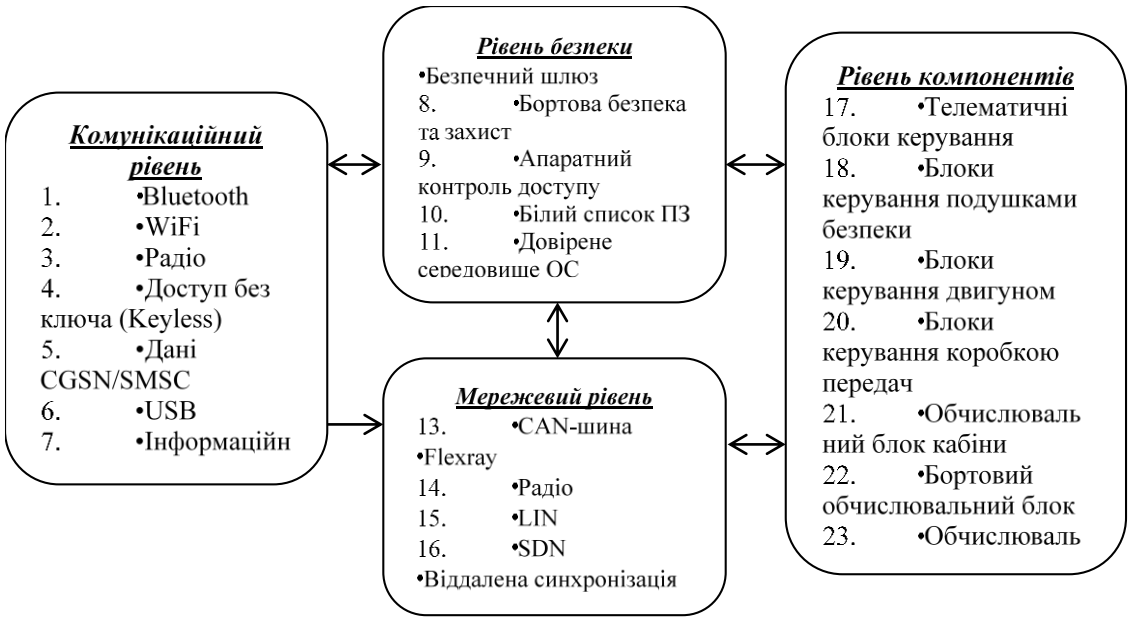

Рис. 2. Найсучасніша архітектура безпеки транспортних засобів

До появи концепції підключеного автомобіля не приділялось особливої уваги кібербезпеці, оскільки зловмисникам для здійснення атаки потрібен був фізичний доступ. Сьогодні маємо автомобілі з кількома точками підключення до зовнішніх мереж, включаючи підключення до Інтернету. Якщо будь-яка функція автомобіля буде скомпрометована, уся внутрішня мережа потенційно опиниться під загрозою, оскільки ці ECU взаємопов'язані, і залежно від досвіду зловмисника можна контролювати деякі критичні системи. Чотири основні проблеми у захисті підключеного автомобіля знаходяться в таких областях:

– бездротові оновлення є складними для автомобільної промисловості, оскільки деякі оновлення можуть бути дуже критичними та потенційно небезпечними для безпеки водія та пасажирів, якщо їх не встановити вчасно.

Нині можливо активне дистанційне оновлення або потрібне відвідування сервісного центру;
- обмеженість обчислювальної потужності - на користь зловмисників;
- складність контролювати стан автомобільної електроніки сертифікованим органом, оскільки автомобіль не завжди підключений до Інтернету;
- складність гетерогенної апаратної архітектури автомобіля, що підвищує вразливість безпеки та ризик атаки на мережі транспортних засобів;
- вартість створення безпечного апаратного та програмного забезпечення автомобіля.

Один заражений автомобіль на дорозі становить потенційну небезпеку для всіх навколишніх транспортних засобів, і кожна нова вразливість системи безпеки відкриває нові проблеми безпеки. Оскільки загрози безпеці змінюються динамічно, набагато складніше розробити механізми безпеки, які забезпечуватимуть цілісність системи протягом усього життєвого циклу.

Потенційні зловмисники часто здійснюють різні рівні мережевих атак на автомобілі через зовнішні інтерфейси. Характеристики цих мережевих атак наступні:

Атаки сенсорного/фізичного рівня реалізуються через серію вдосконалених датчиків, таких як лідар, радар міліметрового діапазону, камера та GPS, які використовуються для збору сприйнятої інформації про зовнішнє середовище та забезпечують здатність сприймати середовище для автоматичного прийняття рішень під час водіння.

Незаконний доступ (канальний рівень) через відсутність шифрування даних і механізму перевірки повідомлень у мережі транспортного засобу, коли зловмисник отримує доступ до мережевого обладнання, він може легко здійснити атаку. Режими атаки канального рівня включають введення кадру, підробку кадру, перехоплення кадру, паузу та DoS-атаку.

Атаки з інтерфейсу (рівень прикладної програми). через системи бездротового зв'язку такі як Bluetooth, Wi-Fi тощо. Для таких атак дослідники в основному зосереджуються на розробці методів виявлення вторгнень на основі машинного навчання [18].

Щоб відповідати вимогам Системи управління кібербезпекою (UN Regulation No 155), виробник комплектного обладнання повинен спочатку виявити й оцінити потенційні загрози, а потім розробити й підтвердити засоби контролю безпеки, які спрямовані на вирішення цих загроз. Виробник комплектного обладнання повинен мати можливість довести, що вимоги системи керування кібербезпекою були належним чином реалізовані [25].

Співтовариство автотранспортних інженерів SAE запропонувала новий стандарт під назвою J1939-91C для мереж CAN-FD, який надає методи для встановлення довіри та захисту взаємних повідомлень за допомогою додаткового шифрування. J1939-91C забезпечує автентичність, цілісність і конфіденційність повідомлень шляхом реалізації складних криптографічних операцій, включаючи хеш-функції та генерацію випадкового ключа. Уповноважені ECU автентифікуються в автомобілі за допомогою цифрових сертифікатів в інфраструктурі відкритих ключів і згодом отримують спільний секрет, який використовується для захисту відповідних повідомлень. [27].

Виробники комплектного обладнання, постачальники, а також наукові кола реагують на виклики безпеці, але потрібно багато зусиль, щоб належним чином захистити транспортні засоби. Це також пов'язано з тим, що життєвий цикл транспортного засобу відносно довгий. Час розробки нового покоління транспортного

засобу зазвичай становить щонайменше 3 роки, тоді як термін служби транспортного засобу на дорозі становить більше 10 років. Розробити заходи безпеки, щоб уникнути атак із можливостями, які матиме майбутній зловмисник протягом такого тривалого періоду часу, важко. В даний час стан впровадження безпеки в автомобільних системах значно обмежений.

Рис. 3 демонструє десять основних внесків у безпеку внутрішньоавтомобільних мереж. Переважання цих внесків також може застосовуватися до міжавтомобільних мереж.

Рис. 3. Перелік стратегій безпеки для автомобільних мереж

Система виявлення вторгнень IDS зосереджена на виявленні шкідливих повідомлень. IDS не порушують існуюче обладнання, інфраструктуру чи комунікації; швидше, вони просто підключаються до мережі та відстежують підозрілий трафік. IDS захищає мережу, відстежуючи трафік і подає тривогу, якщо виявлено підозрілий трафік.

Система запобігання вторгненням (IPS) — це, по суті, система виявлення вторгнень, яка має можливість вживати заходів для захисту мережі. IPS буде контролювати мережу та виявляти вторгнення точно так само, як це робить IDS: коли вторгнення буде виявлено, IPS спробує заблокувати або помістити зловмисника в карантин. Одним з варіантів є те, що IPS просто відкидає підозрілі пакети. Якщо IDS пасивний, то IPS активний — жоден трафік не може досягти місця призначення без проходження через IPS. Однак IPS стає єдиною точкою збою, і якщо вона не закриється, законне використання мережі буде серйозно обмежено, що погіршує продуктивність системи [27].

Криптографія, яка включає автентифікацію та шифрування, використовує математичні принципи для захисту інформації та зв'язку. Автентифікація змушує кожен ECU — підтвердити свою ідентичність. Завдяки автентифікації шкідливий вузол більше не може маскуватися під законний модуль керування передачею. Шифрування забезпечує конфіденційність, і зловмисник не може спостерігати та відтворювати повідомлення у широкомовній шини CAN. Однак традиційна технологія шифрування повідомлень і автентифікації стикається з проблемами неоднорідності архітектури, обмеженості пропускної здатності та обчислювальних ресурсів у мережевому середовищі автомобіля. Тому будь-який контрзахід безпеки повинен враховувати ці проблеми і не перевантажувати шину CAN.

Ряд дослідників адаптували криптографічні процеси для автомобільної сфери використанням спеціалізованої програми інфраструктури відкритих ключів (PKI) для міжавтомобільних мереж. Подібно до звичайної PKI, кожен транспортний засіб, має бути оснащений парою відкритих/приватних ключів. Кожен транспортний засіб використовує свій закритий ключ для підпису вихідних повідомлень, і кожен транспортний засіб перевіряє підписи вхідних повідомлень за допомогою відкритого ключа відправника.

Наприклад, щоб обмежити вартість розповсюдження ключів автори роботи [39] розробили нову структуру безпеки для шини CAN на основі попереднього обчислювання криптографічних функцій, що потребують інтенсивних обчислень.

Динамічний арбітраж — це тактика автомобільної безпеки, специфічна для шини CAN. Багато атак на шину CAN залежать від передбачуваності арбітражних ідентифікаторів. Для підвищення безпеки шини CAN автори [16] запропонували динамічне призначення арбітражних ідентифікаторів. Цей підхід вимагає, щоб усі ECU були модифіковані для підтримки динамічного перепризначення арбітражних ідентифікаторів.

Брандмауери та фільтрація — запозичені з традиційних мереж. Брандмауери повинні регулювати вхідний і вихідний трафік відповідно до заздалегідь визначених правил. Брандмауер є вибірково проникним, згідно з правилами фільтрації, він блокує одні типи трафіку, дозволяючи інші типи трафіку.

Захищене апаратне забезпечення — реалізує принцип інтеграції безпеки в апаратних модулях безпеки (HSM). Апаратне забезпечення стає надійним будівельним блоком для інших заходів безпеки. Будівельні блоки HSM включають механізми симетричної та асиметричної криптографії, механізм криптографії, криптографічну хеш-функцію, генератор випадкових чисел, внутрішній годинник, лічильники монотонності тощо.

Щоб усунути атаки на ECU транспортних засобів та реалізувати взаємну автентифікацію та безпечне шифрування запропоновано фізичні неклоновані функції (PUF) як довірена комунікаційна технологія захисту шини CAN у автомобільній мережі на основі незахищених каналів зв’язку.

Безпечна архітектура — інтегрує безпеку в архітектуру. Захищена архітектура підкреслює безпеку на чотирьох рівнях: інтерфейси, шлюзи, мережі та блоки обробки. Захищені інтерфейси забороняють несанкціонований доступ до мереж автомобіля. Захищені шлюзи полегшують сегментацію мережі — високошвидкісні, критично важливі для безпеки шини ізольовані від низькошвидкісних, комфортних шин. Захищені мережі захищають комунікації між ECU, а захищені блоки обробки реалізовані в ECU для захисту критично важливих для безпеки функцій.

Сегментація мережі — це практика ізоляції різних мереж або різних частин однієї мережі. Якщо мережі належним чином розділені, то компрометація однієї мережі не призведе до компрометації сусідньої мережі.

У деяких комерційно доступних автомобілях сегментація мережі реалізована через шлюз ECU, який керує потоком трафіку між підмережами, які він з’єднує. Однак, якщо шлюз ECU скомпрометовано, то сегментація неефективна. Крім того, виробники автомобілів, як відомо, відмовляються від сегментації мережі на користь скорочення витрат і простоти обслуговування. Також виробники автомобілів часто з’єднують дві окремі мережі, щоб відображати оперативні дані (справність двигуна, поточну швидкість тощо) на екрані інформаційно-розважальної системи. На жаль, інформаційно-розважальна система зазвичай підтверджена найбільшим поверхневим атакам в автомобілі. Точки входу можуть включати Bluetooth, Wi-Fi і стільниковий зв’язок. Ефективна сегментація мережі стане важливим кроком у захисті автомобільних мереж. Автори роботи [15] описали низку заходів безпеки для інтелектуальних транспортних систем (ITC). Вони відзначили, що сегментація мережі зменшить перевантаження, покращить безпеку та обмежить збої. Крім того, вони запропонували ізолювати контролери ITS від корпоративних мереж.

Медові горщики — це системи, які точно імітують реальні системи та призначені для безпечного збору конфліктного трафіку, щоб вчитися на ньому.

Нарешті, традиційні методи безпеки — це найкращі методи безпеки, які походять із традиційних мереж і можуть бути адаптовані до проблеми безпеки автомобільної мережі.

У порівнянні із засобами підвищення інформаційної безпеки, такими як шифрування повідомлень, контроль доступу та автентифікація протоколу, виявлення вторгнень має характеристики невеликої пропускної здатності і легкого розгортання. Ця технологія більше підходить для мереж транспортних засобів з обмеженими ресурсами та вартістю. Технологію поділяють на методи виявлення, засновані на спостереженні за ознаками, теорії інформації та статистичному аналізі і машинному навчанні (рис. 4).

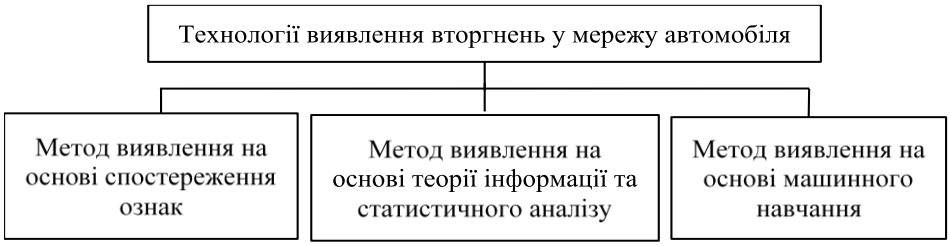

Рис. 4. Класифікація технологій виявлення вторгнень у мережу транспортних засобів

Метод спостереження за ознаками (функціями) є одним із поширених способів виявлення вторгнень, який широко використовується в дослідженнях виявлення вторгнень на основі аномалій у мережу транспортних засобів. До мережевих функцій, які можна використовувати для спостереження за виявленням вторгнень, в основному включають ідентифікацію унікального коду пристрою, зміщення годинника, спостереження за частотою і віддалений кадр тощо. Метод виявлення, заснований на спостереженні аномалії, часто може досягти високої точності виявлення для конкретних моделей атак і має характеристики короткого часу відгуку та низьких накладних витрат на пропускну здатність мережі [41].

Метод виявлення на основі теорії інформації та статистичного аналізу заснований на аналізі інформаційної ентропії за множеною повідомлень CAN. Виявлено, що середня інформаційна ентропія в CAN автомобіля становить 11,436 і у випадку зловмисних атак інформаційна ентропія CAN транспортного засобу буде значно зменшена, що широко використовується в дослідженнях виявлення мережевих вторгнень транспортних засобів з обмеженими ресурсами. Теоретичний аналіз та експериментальні результати показують, що цей метод ефективний і може визначити атаки в режимі реального часу та значно підвищити точність виявлення вторгнень у мережеве середовище автомобіля [36].

Метод виявлення на основі машинного навчання заснований на використанні класу машини опорних векторів з ядром радіальної базисної функції, щоб вивчати нормальну поведінку та класифікувати відхилення як винятки для часових рядів повідомлень електронного блоку керування (ECU). Ця технологія може контролювати комутаційні пакети в мережі автомобіля та забезпечувати високу швидкість виявлення в режимі реального часу. У літературі [8] використовується метод мережі Байєса для швидкої ідентифікації атак зловмисних повідомлень на CAN і для моделювання повідомлень CAN у реальних транспортних засобів. Недоліком є те, що його точність виявлення не може відповідати вимогам функціональних рівнів безпеки.

Сучасні алгоритми машинного навчання зосереджуються на конкурентних загрозах на підключені транспортні засоби та окреслюють рішення для захисту від змагальних атак у різних ситуаціях засновуюсь на неоднорідні характеристики та архітектури автомобільних мереж [30].

За результатами проведених досліджень в табл. 1 надано порівняльний аналіз технологій підвищення безпеки мережі автомобіля за трьома технологіями: шифрування даних, автентифікація повідомлення та виявлення вторгнень [14].

Система виявлення аномальних вторгнень у мережу транспортного засобу має такі характеристики, як сильна масштабованість, низька вартість і низхідна сумісність і її можна застосувати до традиційного мережевого середовища автомобіля з обмеженими ресурсами. Це технологія інформаційної безпеки, яка може ефективно забезпечити автентичність і доступність повідомлень інтелектуальної мережі автомобіля.

Таблиця 1

Порівняльний аналіз технологій підвищення безпеки мережі автомобіля

Технології	Сфера застосування	Інструменти	Гарантія інфор. безпеки	Характеристики та проблеми
Шифрування даних	Канальний рівень	Легкий AES, апаратний модуль прискорення, декомпозиція MAC	Безпека, цілісність і коректність	Підвищення безпеки, цілісності та коректності. Дотримання балансу між безпекою та обчислювальними ресурсами
Автентифікація повідомлення	Фізичний рівень, канальний рівень	Tesla, MAuth-CAN, односторонній хеш-ланцюг	Коректність	Покращений захист правильності передачі мережев. повідомлень. Обмеження в широко-смугових мережах.
Виявлення вторгнень	Фізичний рівень, канальний рівень, прикладний рівень	Клас SVM, глибока нейронна мережа, Байєсова мережа, Рекурентні нейронні мережі (RNN — LSTM)	Доступність і цілісність	Підвищення захисту доступності та цілісності мережі, забезпечення високої точності та надійності виявлення, зниження частоти помилкових тривог і часу реакції виявлення.

У порівнянні з технологією шифрування даних і автентифікації повідомлень, технологія виявлення вторгнень у мережу транспортного засобу більше підходить для мережевого середовища транспортного засобу з інтелектуальними транспортними засобами, підключеними до мережі, з ключовими функціями, обмеженими ресурсами та чутливістю до вартості. Вона може ефективно компенсувати накладні витрати на обчислення та зв’язок, викликані механізмами шифрування та автентифікації, які можна передбачити. Виявлення вторгнень у мережу транспортних засобів залишається важливим напрямком розвитку інтелектуальних мережевих досліджень щодо покращення інформаційної безпеки транспортних засобів на довгий час у майбутньому.

Не всі обчислення ECU виконуються в центральному процесорі. Додаткові блоки обчислень дозволяють ефективно обчислювати певні функції безпеки. Прикладом цього є криптографічні прискорювачі та графічні прискорювачі. У контексті цієї статті особливо важливі криптографічні прискорювачі. Великі та частково середні ECU часто оснащені криптографічними співпроцесорами. У той час як апаратні прискорювачі дозволяють зберігати криптографічні ключі та можуть прискорити деякі функції шифрування, співпроцесори забезпечують повне обчислювальне середовище, дзеркально відображаючи основну систему, включаючи безпечну пам’ять, підключення зовнішніх пристроїв тощо. Оскільки сучасні ядра мікроконтролерів часто інтегрують апаратні прискорювачі та функції співпроцесора, багато процесорів ECU доступні з апаратною підтримкою криптографічного забезпечення за аналогічною ціною [22].

Вбудовані апаратні прискорювачі кібербезпеки в нові автомобільні обчислювальні блоки для підтримки шифрування реалізують методи безпеки в реальному часі, такі як алгоритм AES із симетричним ключем [20]. Також розробляються більш складні алгоритми, такі як алгоритм цифрового підпису еліптичної кривої (ECDSA) для криптографії з відкритим ключем 21. Вбудовані механізми підпису необхідні для автентифікації всіх відправників в процесі спілкування в системі автомобільної шини. Усі неавторизовані повідомлення можуть бути оброблені окремо або негайно відхилені.

Таким чином, кожному контролеру потрібен сертифікат для автентифікації щодо шлюзу як дійсного відправника. Сертифікат може складатися з ідентифікатора контролера, відкритого ключа та повноважень відповідного контролера. Шлюз, у свою чергу, повинен надійно зберігати список відкритих ключів усіх акредитованих OEM-виробників для розглянутого автомобіля. Кожен сертифікат контролера має цифровий підпис OEM відповідним секретним ключем. Шлюз використовує відповідний відкритий ключ OEM для перевірки дійсності сертифіката контролера. Якщо процес автентифікації проходить успішно, відповідний контролер додається до списку дійсних контролерів [6].

Встановлення так званого кореня довіри є критичною проблемою в криптографічних реалізаціях. Загальним рішенням є переміщення кореня довіри в апаратне забезпечення. Добре відомим рішенням у цьому сенсі є модуль довіреної платформи (TPM). TPM дозволяє безпечно генерувати та зберігати секрети (наприклад, криптографічні ключі, сертифікати тощо), щоб вони залишалися конфіденційними і міцно прив’язані до мережі автомобіля.

Значні переваги у захисті внутрішньоавтомобільних мереж може принести концепція крипто-двигунів (Crypto-Engine), еталонний дизайн логічної архітектури якої показаний на рисунку 5 [35].

Crypto-Engine у порівнянні з TPM призначені не тільки для генерації та зберігання ключів, але також діє як активний криптографічний прискорювач і можуть самостійно виконувати операції шифрування та підпису.

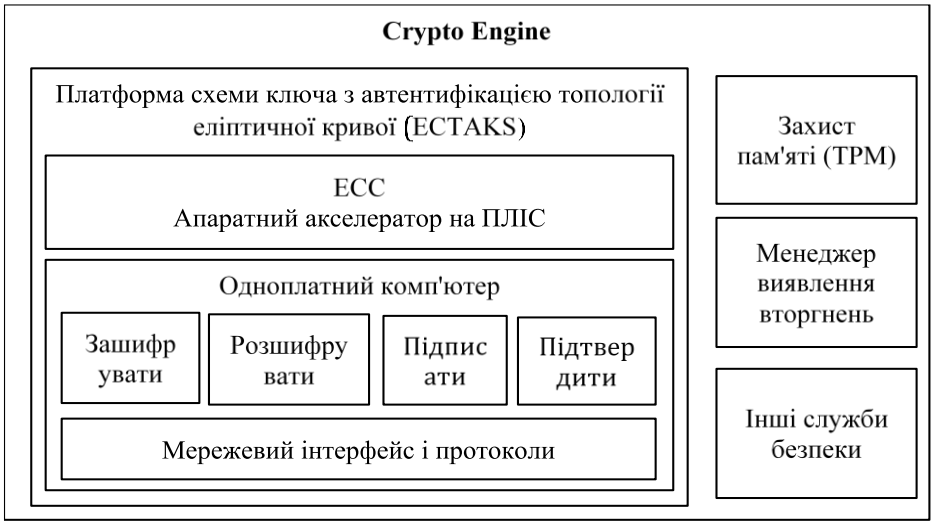

Рис. 5. Блок-схема Crypto-Engine

Основним криптографічним рішенням, прийнятим у Crypto-Engine, є схема ключа з автентифікацією топології еліптичної кривої (ECTAKS), яка використовується для захисту кластеризованих вузлів мережі всередині транспортного засобу і встановлення захищених сеансів зв’язку. Однією з відповідних властивостей схеми ECTAKS є автентифікація між

підключеними сторонами відповідно до довільної топології сеансу. Модуль ECTAKS забезпечує генерацію ключів, розповсюдження, шифрування та керування ключами.

Топологія автентифікованої мережі (ANT) визначає доступні з'єднання. ANT реалізується шляхом генерації та попереднього розподілу ключових компонентів ECTAKS між вузлами і виконується кожного разу, коли встановлюється новий ANT.

Кожного разу, коли вузол (Аліса) в ANT хоче почати зв'язок з іншим вузлом (Бобом) за допомогою ECTAKS, вони повинні погодитися на спільний секрет, тобто ключ автентифікації топології еліптичної кривої (ECTAK), який буде використовуватися як симетричний ключ. ECTAKS робить це можливим завдяки використанню криптографії еліптичної кривої (ECC) у поєднанні з ключовими компонентами двох вузлів. Після реконструкції криптографічного ключа з ключових компонентів симетричні служби шифрування Crypto-Engine використовують алгоритм AES, використовуючи ECTAK як симетричний ключ. Для служб підпису з відкритим ключем Crypto-Engine використовує ключові компоненти ECTAKS у рішенні на основі ECDSA, яке містить код автентифікації повідомлення на основі хешу (HMAC) як функцію автентифікації повідомлення (MAC) і SHA256 для хешування повідомлення, яке потрібно підписати (тобто HMAC-SHA256).

Основні переваги ECTAKS можна підсумувати наступним чином: стійкість проти атак на топологічну цілісність мережі; генерація спільних секретів на сеансах зв'язку з довільною топологією та масштабованість сеансів багатоадресної та конверсійної трансляції.

Crypto-Engine спеціально розроблено для підтримки внутрішнього та зовнішнього апаратного прискорення з точки зору продуктивності для криптографічних обчислень. У випадку ECTAKS Crypto-Engine підтримує апаратне прискорення криптографії еліптичної кривої (ECC) для примітивних операцій над точками еліптичної кривої, наприклад, додавання точок, подвоєння точок і множення точок. Це дозволяє реалізувати змішане апаратно-програмне забезпечення Crypto-Engine, яке можна адаптувати до різних сценаріїв, платформ і вимог.

Таким чином, Crypto-Engine базується на схемі ECTAKS, яка використовує стандартну криптографію еліптичної кривої та механізми розподілу ключів для визначення логічної топології вузлів і допустимих каналів зв'язку.

Удосконалення результатів досліджень [35] демонструють, що прийняття концепції Crypto-Engine разом із ECTAKS може принести значні переваги у захисті внутрішньоавтомобільних мереж завдяки своїй гнучкій архітектурі, визначенню та забезпеченню автентифікованої топології і підтримці найсучаснішої криптографії на основі еліптичної кривої з незначними накладними витратами на затримку в процесах шифрування та автентифікації. Крім того, підтримка апаратних прискорювачів для криптографічних операцій може допомогти ще більше підвищити продуктивність і розширити підтримку впровадження нових рішень кібербезпеки транспортних засобів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У цієї оглядової статті проаналізовано вразливості мереж автомобіля та визначено основні атаки кібербезпеки на транспортні засоби. Надано характеристики мережевих атак на фізичному, канальному та прикладному рівнях. Визначено основні проблеми з захисту безпеки підключеного автомобіля. Порівняно технології підвищення кібербезпеки мереж транспортних засобів за технологічними напрямами: шифрування даних, автентифікації повідомлень, виявлення вторгнень в мережу, побудова довіреної

платформи та реалізація концепції Crypto-Engine для захисту кластеризованих вузлів мережі всередині транспортного засобу і встановлення захищених сеансів зв'язку.

Аналіз характеристик та вразливостей автомобільних мереж показав, що керування електронним обладнанням автомобіля виконується через систему шин заснованих на різних мережевих технологіях за спеціально розробленими протоколами для автомобільної сфери з різною пропускною здатністю та навантаженням. Існуючі мережеві протоколи транспортних засобів, такі як CAN і Flex Ray, не мають механізму захисту інформації на початку свого проєктування, що робить мережу автомобіля вразливою до перехоплення, підробки, модифікації та повторного відтворення. Шина CAN є основною точкою проблеми інформаційної безпеки автомобіля, оскільки це єдина централізована мережева шина, на яку транслюються всі дані всередині автомобіля. Повідомлення за протоколом CAN не використовують пряму адресацію одержувачів або ідентифікацію відправників, що є вразливістю в процесах автентифікації повідомлень. Однією з поширених вразливостей є відсутність належної сегментації та ізоляції між критично важливими для безпеки та некритичними системами всередині автомобіля, а також поза ним.

Мережа контролера з гнучкою швидкістю передачі даних *(CAN FD)* є вдосконаленням традиційної шини CAN і повністю сумісна із CAN. CAN FD визначає новий формат кадру, використовуючи два різних тактових сигналу для різних частин кадру. CAN-FD є вдосконаленою технологією зв'язку, яка забезпечує високу пропускну здатність до 8 Мбіт/с і корисне навантаження до 64 байтів. Дослідження щодо нового протоколу CAN XL з використанням технології автомобільного Ethernet дозволяють досягти пропускну здатність до 20 Мбіт/с з корисним навантаженням 2048 байт. Актуальними завданнями є впровадження моделі безпеки CAN FD з використанням шифрування симетричним ключем AES-256 та автентифікації повідомлень за допомогою реалізації хеш-функції HMAC/SFIA-256. Шифрування застосовується до першого блоку кадру даних, а до другого блоку даних виконується автентифікація Результати показали, що запропонована модель безпеки має вищу ефективність шифрування, ніж існуючі методи.

Еволюція архітектури E/E транспортного засобу складається з трьох типів: розподілена E/E архітектура використовувалася до 2019 року, забезпечується тісна співпраця між ECU з допомогою центрального шлюзу; доменно-централізована архітектура є сьогоднішньою транспортною архітектурою надає можливість оптимізації та консолідації функцій зв'язку у кожному домені; зональна архітектура пропонує майбутню архітектуру E/E автомобіля, кластеризує ECU на основі конкретних зон автомобіля, включає компоненти: високопродуктивний обчислювальний блок, зональні ECU та автомобільний Ethernet, забезпечує кращу координацію та безпечний зв'язок між різними доменами, підвищуючи загальний інтелект автомобіля та швидкість реагування. Тенденцією підвищення кібербезпеки є класифікація та ізоляція мереж, доменів та зон архітектури E/E, створення поглиблених багаторівневих програмно-апаратних засобів захисту безпеки.

Існуючі дослідження технології виявлення вторгнень у мережу транспортних засобів засновані на теорії інформації і поділяють на методи спостереженні за ознаками, статистичному аналізі і машинному навчанні. Ця технологія більше підходить для мереж транспортних засобів з обмеженими ресурсами та вартістю. Модель виявлення має високу точність виявлення в обмежених станах транспортного засобу, але її стійкість не відповідає вимогам безпеки високого рівня в поточному рівні інтеграції автомобільної безпеки. Сучасні алгоритми машинного навчання зосереджуються на конкурентних загрозах на підключені транспортні засоби та окреслюють рішення для захисту від змагальних атак у різних

ситуаціях. Ці алгоритми можуть контролювати комутаційні пакети в мережі автомобіля та забезпечувати високу швидкість виявлення в режимі реального часу.

Обчислювальні блоки автомобіля дозволяють ефективно визначати функції безпеки. Додатковими блоками є криптографічні співпроцесори та прискорювачі. Криптографічні співпроцесори дозволяють генерування сеансових ключів Діффі-Хеллмана (ECDH), шифрування даних за алгоритмом симетричного блочного шифрування AES, та виконувати несиметричного перетворення інформації для алгоритмів цифрового підпису еліптичної кривої (ECDSA), проводити автентифікацію контролерів ECU за їх цифровими сертифікатами. Апаратні прискорювачі дозволяють зберігати криптографічні ключі та можуть прискорити деякі функції шифрування. Додавання механізмів шифрування даних і автентифікації повідомлень до мережі автомобіля може ефективно уникнути кібератак на мережу автомобіля.

Встановлення так званого кореня довіри є критичною проблемою в криптографічних реалізаціях. Загальним рішенням є переміщення кореня довіри в апаратне забезпечення. Добре відомим рішенням у цьому сенсі є модуль довіреної платформи (TPM). TPM дозволяє безпечно генерувати та зберігати секрети, наприклад, криптографічні ключі, сертифікати тощо, щоб вони залишалися конфіденційними і міцно прив’язані до мережі автомобіля.

Значні переваги у захисті внутрішньоавтомобільних мереж може принести концепція крипто-двигунів (Crypto-Engine). Ця концепція інтегрує технології довіреної платформи TPM захищеного зберігання з технологією апаратної реалізації криптографічних перетворень з використанням спеціалізованих співпроцесорів, технологією виявлення вторгнень та служб безпеки для ефективного виконання операції шифрування, підпису та сертифікації зв’язку електронних пристроїв автомобіля. Основні переваги концепції: стійкість проти атак на топологічну цілісність мережі; генерація спільних секретів на сеансах зв’язку з довільною топологією та масштабованість сеансів багатоадресної та конверсійної трансляції.

Нинішній стан автомобільної інфраструктури безпеки підлягає подальшим дослідженням у кількох галузях зі збільшенням попиту на автомобільні послуги [26], розгортання автомобільної мережі та електричну інфраструктуру автомобіля [40]. Ці дослідницькі аспекти генерують всеосяжне уявлення про повсюдність зв’язаних, розумних і автономних екосистем, що швидко наближається.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Adu-Kyere, A., Nigussie, E., & Isoaho, J. (2023). Self-Aware CybersecurityArchitecture for AutonomousVehicles: Security throughSystem-Level Accountability. *Sensors, 23, 8817*. https://doi.org/10.3390/s23218817
2. Aldhyani, T.H.H., & Alkahtani, H. (2022). Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors, 22, 360*.
3. Al-Jarrah, O.Y., El Haloui, K., Dianati, M., & Maple, C. (2023). A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks. *IEEE Open J. Veh. Technol., 4,* 271–280.
4. Andrade, R, Dias Santos, M. M., Justo J. F., Yoshioka, L. R., Hof, H.-J., & Kleinschmidt J. H. (2023). Security architecture for automotive communication networks with CAN FD. *Computers & Security, 129,* 103203
5. Askaripoor, H., Hashemi Farzaneh, M., & Knoll, A. (2022). E/E Architecture Synthesis: Challenges and Technologies. *Electronics, 11, 518*. https://doi.org/10.3390/electronics11040518
6. Baldanzi, L., Crocetti, L., Bertolucci, M., Fanucci, L., & Saponara, S. (2019). Analysis of Cybersecurity Weakness in Automotive In-Vehicle Networking and Hardware Accelerators for Real-time Cryptography.

In book: Applications in Electronics Pervading Industry, Environment and Society, 11–18. https://doi.org/10.1007/978-3-030-11973-7_2

7. Bari, B. S., Yelamarthi, K., & Ghafoor, S. (2023). Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study. *Sensors, 23, 3610*.
8. Casillo, M., Coppola, S., Santo, M.D., Pascale, F., & Santonicola, E. (2019). Embedded intrusion detection system for detecting attacks over CAN-BUS. *In Proceedings of the 4th International Conference on System Reliability and Safety*.
9. Chandwani, A., Dey, S., & Mallik, A. (2020). Cybersecurity of Onboard Charging Systems for Electric Vehicles-Review, Challenges and Countermeasures. *IEEE Access, 8,* 226982–226998.
10. De Vincenzi, M., Costantino, G., Matteucci, I., Fenzl, F., Plappert, C., Rieke, R., & Zelle, D. (2024). A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet. *ACM Comput. Surv., 56, 135.*
11. El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity Challenges in Vehicular Communications. *Vehicular Communications, 23, 100214*.
12. El-Rewini, Z., Sadatsharan, K., Sugunaraj, N., Selvaraj, D.F., Plathottam, S.J., & Ranganathan, P. (2020). Cybersecurity Attacks in Vehicular Sensors. *IEEE Sens. J., 20,* 13752–13767.
13. Fernandes, R. S. (2023) *Vehicle Electronics and Cybersecurity: Current Interactions, Vulnerabilities, and Recommendations.* European mobility group. Report from UTAC. https://www.mobilitygroup.eu/emg-members-other-news/vehicle-electronics-and-cybersecurity
14. Guan, T., Han, Y., Kang, N., Tang, N., Chen, X., & Wang, S. (2022). An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles. *Sustainability, 14, 5211*. https://doi.org/10.3390/su14095211
15. Harvey, J., & Kumar, S. (2020). A survey of intelligent transportation systems security: Challenges and solutions. *Proc. IEEE 6th Int. Conf. Big Data Security Cloud (BigDataSecurity) IEEE Int. Conf. High Perform. Smart Comput. (HPSC) IEEE Int. Conf. Intell. Data Security (IDS),* 263-268. https://ieeexplore.ieee.org/document/9123012
16. Islam, R., & Refat, R. U. D. (2020). Improving CAN bus security by assigning dynamic arbitration Ids. *Journal of Transportation Security, 13,* 19-31. https://link.springer.com/article/10.1007/s12198-020-00208-0
17. Khalid Khan, S., Shiwakoti, N., & Stasinopoulos, P. (2022). A Conceptual System Dynamics Model for Cybersecurity Assessment of Connected and Autonomous Vehicles. *Accident Analysis & Prevention, 165, 106515.*
18. Khan, Z., Chowdhury, M., Islam, M., Huang, C.Y., & Rahman, M. (2019). *In-vehicle false information attack detection and mitigation framework using machine learning and software defined networking*. arXiv:1906.10203.
19. Kifor, C. V., & Popescu A. (2024). Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies. *Sensors, 24, 6139*. https://doi.org/10.3390/s24186139
20. Klimushin, P., Solianyk, T., Kolisnyk, T., & Mozhaev, O. (2021). Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things. *Advanced Information Systems, 5,* 103-111. https://doi.org/10.20998/2522-9052.2021.3.14
21. Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., & Yanov, V. (2021), Hardware support procedures for asymmetric authentication of the internet of things. *Innovative Technologies and Scientific Solutions for Industries, 4 (18),* 31–39. https://doi.org/10.30837/ITSSI.2021.18.031
22. Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., & Svitlychny, V. (2022). Crypto-resistantmethods and random number generatorsin internet of things (IOT) devices. *Innovative Technologies and Scientific Solutions for Industries, 2(20),* 22–34. https://doi.org/10.30837/ITSSI.2022.20.022
23. Kong, Q.L., Lu, R.X., Yin, F., & Cui, S.G. (2021). Blockchain-Based Privacy-Preserving Driver Monitoring for MaaS in the Vehicular IoT. *IEEE Trans. Veh. Technol., 70,* 3788–3799.
24. Kukkala, V. K., Thiruloga, S. V., & Pasricha, S. (2022). Roadmap for Cybersecurity in Autonomous Vehicles. *IEEE Consumer Electronics Magazine, 11,* 13–23. https://doi.org/10.48550/arXiv.2201.10349
25. Lampe, B., & Meng, W. (2023). Intrusion Detection in the Automotive Domain: A Comprehensive Review. *IEEE Communications Surveys & Tutorials, 25(4).* https://doi.org/10.1109/COMST.2023.3309864
26. Ma, R., Cao, J., Feng, D., Li, H., Li, X., & Xu, Y. (2022). A robust authentication scheme for remote diagnosis and maintenance in 5G V2N. *J. Netw. Comput. Appl, 198, 103281.*
27. Mokhadder, M., Zachos, M., & Potter, J. (2023). Evaluation of vehicle system performance of an SAE J1939-91C network security implementation, *Proc. WCX SAE World Congr. Exp., 6.* https://saemobilus.sae.org/content/2023-01-0041

28. Pape, S., Syed-Winkler, S., Garcia, A.M., Chah, B., Bkakria, A., Hiller, M., Walcher, T., Lombard, A., Abbas-Turki, A., & Yaich, R. (2023). A Systematic Approach for Automotive Privacy Management. *In Proceedings of the 7th ACM Computer Science in Cars Symposium CSCS*.
29. Pervez, L., Khan, A., & Ain, N. (2020). Cyber Security Challenge in an Automobile. *International Journal of Scientific and Research Publications*, *10(12),* 162–166. https://doi.org/10.29322/IJSRP.10.12.2020.p10815
30. Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. *IEEE Commun. Surv. Tutor.*, *22*, 998–1026.
31. Rajapaksha, S., Kalutarage, H., Al-Kadri, M.O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey. *ACM Comput. Surv*., *55, 237.*
32. Rodriguez, E., Otero, B., & Canal, R. (2023). A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things. *Sensors, 23,* 1252.
33. Sabaliauskaite, G., Bryans, J., Jadidbonab, H., Ahmad, F., Shaikh, S., & Wooderson, P. (2024). TOMSAC-Methodology for Trade-off Management between Automotive Safety and Cyber Security. *Comput. Secur.*, *140, 103798.*
34. Shin, Y., & Jeon, S. (2024). MQTree: Secure OTA Protocol Using MQTT and MerkleTree. *Sensors*, *24, 1447.*
35. Tiberti, W., Civino, R., Gavioli, N., Pugliese, M., & Santucci, F. (2023). A Hybrid-Cryptography Engine for Securing Intra-Vehicle Communications. *Appl. Sci. 13, 13024*. https://doi.org/10.3390/app132413024
36. VanWyk, F., Wang, Y., Khojandi, A., & Masoud, N. (2020). Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Trans. Intell. Transp. Syst*., *21,* 1264–1276.
37. *Vehicle Electronics and Cybersecurity: Current Interactions, Vulnerabilities, and Recommendations. European mobility group. Report from UTAC.* (2023). https://www.mobilitygroup.eu/emg-members-other-news/vehicle-electronics-and-cybersecurity
38. Wang, P., Wu, X., & He, X. (2020). Modeling and Analyzing Cyberattack Effects on Connected Automated Vehicular Platoons. *Transportation Research Part C: Emerging Technologies, 115, 102625.*
39. Wang, Z., & Li, X. (2021). Intrusion prevention system design. Proc. Int. Conf. *Inf. Eng. Appl. (IEA), 218*, 375-382, URL: https://link.springer.com/chapter/10.1007/978-1-4471-4847-0_47
40. Wu, Z., Tian, E., & Chen, H. (2023). Covert Attack Detection for LFC Systems of Electric Vehicles: A Dual Time-Varying Coding Method. *IEEE/ASME Trans. Mechatron*, 3(28), 681–691.
41. Wu,W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2020). A survey of intrusion detection for in-vehicle networks. *IEEE Trans. Intell. Transp. Syst.*, *21*, 919–933.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Petro Klimushyn
PhD, Associate Professor of the Department of Counteracting Cybercrime
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID ID: 0000-0002-1020-9399,
klimushyn@ukr.net

Vitaliy Svitlychny
PhD, Associate Professor of the Department of Counteracting Cybercrime
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID ID: 0000-0003-3381-3350
vit.svet@ukr.net

Yuriy Gnusov
PhD, Associate Professor, Head of the Department of Cybersecurity and DATA-Technologies
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID ID: 0000-0002-9017-9635
duke6969@i.ua

Yuriy Onyshchenko
PhD, Associate Professor, Deputy Director of the Institute for
Educational and Research Activities of Educational and Scientific Institute No. 4
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID ID: 0000-0002-7755-3071
onischenko1980@gmail.com

AUTOMOTIVE ELECTRONICS AND CYBERSECURITY: A SYSTEMATIC REVIEW OF SECURITY ATTACKS AND COUNTERMEASURES

Abstract. Modern automotive electronics are a complex system of sensors, electronic control units (ECUs) and actuators connected through various types of automotive networks to control and monitor the condition of the vehicle. In addition, modern vehicles are increasingly connected to the outside world through vehicle-to-everything (V2X) technologies. These create new attack surfaces that increase the cybersecurity risk for modern vehicles. With the advent of intelligent transportation structures, the focus has shifted to the structure of coordinated inter-vehicle systems, symbolized by the integration of infrastructure, people, vehicles, urban areas and the environment. This combination of computer technology and automotive innovation has raised numerous questions about cyberattacks on cars, which play a significant role in the development and use of automotive technology. Advanced wireless technology allows vehicles to exchange and transmit information with each other and around them in real time, which will help reduce accidents, congestion and improve the efficiency of mobile vehicles. Many advanced technologies, such as cloud computing, artificial intelligence, V2X technology, and advanced driver assistance systems, are increasingly being used in cars, making vehicles more intelligent to provide convenient services to people and ensure the safety of drivers and passengers. However, as cars become more connected to the Internet, wireless networks, each other, and other transportation network infrastructure, the risk of cyberattacks is becoming more and more problematic. This review article first analyzes the vulnerabilities of vehicle networks and identifies the main cybersecurity attacks on vehicles. Technologies for improving the cybersecurity of vehicle networks are analyzed in the following technological areas: data encryption, message authentication, network intrusion detection, building a trusted platform, and implementing the Crypto-Engine concept.

Keywords: automotive electronics, automotive cybersecurity, vehicle networks, data encryption, message authentication, intrusion detection technology, trusted platform module, Crypto-Engine concept.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Adu-Kyere, A., Nigussie, E., & Isoaho, J. (2023). Self-Aware CybersecurityArchitecture for AutonomousVehicles: Security throughSystem-Level Accountability. *Sensors, 23, 8817*. https://doi.org/10.3390/s23218817
2. Aldhyani, T.H.H., & Alkahtani, H. (2022). Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors, 22, 360.*
3. Al-Jarrah, O.Y., El Haloui, K., Dianati, M., & Maple, C. (2023). A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks. *IEEE Open J. Veh. Technol., 4,* 271–280.
4. Andrade, R, Dias Santos, M. M., Justo J. F., Yoshioka, L. R., Hof, H.-J., & Kleinschmidt J. H. (2023). Security architecture for automotive communication networks with CAN FD. *Computers & Security, 129,* 103203
5. Askaripoor, H., Hashemi Farzaneh, M., & Knoll, A. (2022). E/E Architecture Synthesis: Challenges and Technologies. *Electronics, 11, 518.* https://doi.org/10.3390/electronics11040518
6. Baldanzi, L., Crocetti, L., Bertolucci, M., Fanucci, L., & Saponara, S. (2019). Analysis of Cybersecurity Weakness in Automotive In-Vehicle Networking and Hardware Accelerators for Real-time Cryptography. *In book: Applications in Electronics Pervading Industry, Environment and Society*, 11–18. https://doi.org/10.1007/978-3-030-11973-7_2
7. Bari, B. S., Yelamarthi, K., & Ghafoor, S. (2023). Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study. *Sensors, 23, 3610*.
8. Casillo, M., Coppola, S., Santo, M.D., Pascale, F., & Santonicola, E. (2019). Embedded intrusion detection system for detecting attacks over CAN-BUS. *In Proceedings of the 4th International Conference on System Reliability and Safety*.
9. Chandwani, A., Dey, S., & Mallik, A. (2020). Cybersecurity of Onboard Charging Systems for Electric Vehicles-Review, Challenges and Countermeasures. *IEEE Access, 8,* 226982–226998.
10. De Vincenzi, M., Costantino, G., Matteucci, I., Fenzl, F., Plappert, C., Rieke, R., & Zelle, D. (2024). A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet. *ACM Comput. Surv., 56, 135.*
11. El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity Challenges in Vehicular Communications. *Vehicular Communications, 23, 100214.*
12. El-Rewini, Z., Sadatsharan, K., Sugunaraj, N., Selvaraj, D.F., Plathottam, S.J., & Ranganathan, P. (2020). Cybersecurity Attacks in Vehicular Sensors. *IEEE Sens. J., 20,* 13752–13767.
13. Fernandes, R. S. (2023) *Vehicle Electronics and Cybersecurity: Current Interactions, Vulnerabilities, and Recommendations.* European mobility group. Report from UTAC. https://www.mobilitygroup.eu/emg-members-other-news/vehicle-electronics-and-cybersecurity
14. Guan, T., Han, Y., Kang, N., Tang, N., Chen, X., & Wang, S. (2022). An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles. *Sustainability, 14, 5211.* https://doi.org/10.3390/su14095211
15. Harvey, J., & Kumar, S. (2020). A survey of intelligent transportation systems security: Challenges and solutions. *Proc. IEEE 6th Int. Conf. Big Data Security Cloud (BigDataSecurity) IEEE Int. Conf. High Perform. Smart Comput. (HPSC) IEEE Int. Conf. Intell. Data Security (IDS),* 263-268. https://ieeexplore.ieee.org/document/9123012
16. Islam, R., & Refat, R. U. D. (2020). Improving CAN bus security by assigning dynamic arbitration Ids. *Journal of Transportation Security, 13,* 19-31. https://link.springer.com/article/10.1007/s12198-020-00208-0
17. Khalid Khan, S., Shiwakoti, N., & Stasinopoulos, P. (2022). A Conceptual System Dynamics Model for Cybersecurity Assessment of Connected and Autonomous Vehicles. *Accident Analysis & Prevention, 165, 106515.*
18. Khan, Z., Chowdhury, M., Islam, M., Huang, C.Y., & Rahman, M. (2019). *In-vehicle false information attack detection and mitigation framework using machine learning and software defined networking*. arXiv:1906.10203.
19. Kifor, C. V., & Popescu A. (2024). Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies. *Sensors, 24, 6139.* https://doi.org/10.3390/s24186139
20. Klimushin, P., Solianyk, T., Kolisnyk, T., & Mozhaev, O. (2021). Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things. *Advanced Information Systems, 5,* 103-111. https://doi.org/10.20998/2522-9052.2021.3.14

21. Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., & Yanov, V. (2021), Hardware support procedures for asymmetric authentication of the internet of things. *Innovative Technologies and Scientific Solutions for Industries, 4 (18),* 31–39. https://doi.org/10.30837/ITSSI.2021.18.031
22. Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., & Svitlychny, V. (2022). Crypto-resistantmethods and random number generatorsin internet of things (IOT) devices. *Innovative Technologies and Scientific Solutions for Industries, 2(20),* 22–34. https://doi.org/10.30837/ITSSI.2022.20.022
23. Kong, Q.L., Lu, R.X., Yin, F., & Cui, S.G. (2021). Blockchain-Based Privacy-Preserving Driver Monitoring for MaaS in the Vehicular IoT. *IEEE Trans. Veh. Technol., 70,* 3788–3799.
24. Kukkala, V. K., Thiruloga, S. V., & Pasricha, S. (2022). Roadmap for Cybersecurity in Autonomous Vehicles. *IEEE Consumer Electronics Magazine*, *11,* 13–23. https://doi.org/10.48550/arXiv.2201.10349
25. Lampe, B., & Meng, W. (2023). Intrusion Detection in the Automotive Domain: A Comprehensive Review. *IEEE Communications Surveys & Tutorials, 25(4).* https://doi.org/10.1109/COMST.2023.3309864
26. Ma, R., Cao, J., Feng, D., Li, H., Li, X., & Xu, Y. (2022). A robust authentication scheme for remote diagnosis and maintenance in 5G V2N. *J. Netw. Comput. Appl*, *198, 103281.*
27. Mokhadder, M., Zachos, M., & Potter, J. (2023). Evaluation of vehicle system performance of an SAE J1939-91C network security implementation, *Proc. WCX SAE World Congr. Exp., 6.* https://saemobilus.sae.org/content/2023-01-0041
28. Pape, S., Syed-Winkler, S., Garcia, A.M., Chah, B., Bkakria, A., Hiller, M., Walcher, T., Lombard, A., Abbas-Turki, A., & Yaich, R. (2023). A Systematic Approach for Automotive Privacy Management. *In Proceedings of the 7th ACM Computer Science in Cars Symposium CSCS.*
29. Pervez, L., Khan, A., & Ain, N. (2020). Cyber Security Challenge in an Automobile. *International Journal of Scientific and Research Publications, 10(12),* 162–166. https://doi.org/10.29322/IJSRP.10.12.2020.p10815
30. Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. *IEEE Commun. Surv. Tutor., 22,* 998–1026.
31. Rajapaksha, S., Kalutarage, H., Al-Kadri, M.O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey. *ACM Comput. Surv., 55, 237.*
32. Rodriguez, E., Otero, B., & Canal, R. (2023). A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things. *Sensors, 23,* 1252.
33. Sabaliauskaite, G., Bryans, J., Jadidbonab, H., Ahmad, F., Shaikh, S., & Wooderson, P. (2024). TOMSAC-Methodology for Trade-off Management between Automotive Safety and Cyber Security. *Comput. Secur., 140, 103798.*
34. Shin, Y., & Jeon, S. (2024). MQTree: Secure OTA Protocol Using MQTT and MerkleTree. *Sensors, 24, 1447.*
35. Tiberti, W., Civino, R., Gavioli, N., Pugliese, M., & Santucci, F. (2023). A Hybrid-Cryptography Engine for Securing Intra-Vehicle Communications. *Appl. Sci. 13, 13024*. https://doi.org/10.3390/app132413024
36. VanWyk, F., Wang, Y., Khojandi, A., & Masoud, N. (2020). Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Trans. Intell. Transp. Syst., 21,* 1264–1276.
37. *Vehicle Electronics and Cybersecurity: Current Interactions, Vulnerabilities, and Recommendations. European mobility group. Report from UTAC.* (2023). https://www.mobilitygroup.eu/emg-members-other-news/vehicle-electronics-and-cybersecurity
38. Wang, P., Wu, X., & He, X. (2020). Modeling and Analyzing Cyberattack Effects on Connected Automated Vehicular Platoons. *Transportation Research Part C: Emerging Technologies, 115, 102625.*
39. Wang, Z., & Li, X. (2021). Intrusion prevention system design. Proc. Int. Conf. *Inf. Eng. Appl. (IEA), 218,* 375-382, URL: https://link.springer.com/chapter/10.1007/978-1-4471-4847-0_47
40. Wu, Z., Tian, E., & Chen, H. (2023). Covert Attack Detection for LFC Systems of Electric Vehicles: A Dual Time-Varying Coding Method. *IEEE/ASME Trans. Mechatron*, 3(28), 681–691.
41. Wu,W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2020). A survey of intrusion detection for in-vehicle networks. *IEEE Trans. Intell. Transp. Syst., 21,* 919–933.