УДК 004.75+519.7+629.05+62-6

Кривошапов Сергій Іванович

Студент Харківського національного автомобільно-дорожнього університету

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ МОНІТОРИНГУ ВИТРАТ ПАЛИВА ТРАНСПОРТНИХ ЗАСОБІВ АВТОМОБІЛЬНОГО ТРАНСПОРТУ

Анотація. Розглянута система дистанційного моніторингу споживання палива на транспортному засобі автомобільного транспорту з позиції кіберзахисту даних. Ключовим моментом є забезпечення безпеки підключення та взаємодії сторонніх пристроїв, які підключаються CAN-шина автомобіля. На другому етапі досліджено передачу даних від вбудованих в автомобіль діагностичних систем до центру зберігання та обробки даних. Розглянуто вимоги до ідентифікації транспортного засобу та безпеки каналу зв'язку через GPRS-модем та віддалений сервер. На третьому етапі розглянуто питання безпеки даних на сервері та їх передачу операторам технічної та транспортної служб на підприємстві автомобільного транспорту.

Ключові слова: дорожньо-транспортній засіб, витрата палива, моніторинг, CAN-шина, GPS-тракер, розподільча програмне забезпечення, GPRS-модем.

Коли автомобіль рухається по дорозі він споживає паливо (бензин, дизель, газ). Кількість витрати палива необхідно контролювати з багатьох причин. Це матеріальний ресурс, вартість якого враховуються в собівартості транспортної операції окремою позицією. Використання палива в натуральному та вартісному вигляді враховується у бухгалтерських проводках. Постійний контроль палива на автомобілів у процесі його руху та зупинки знижує ймовірність його розкрадання. Витрата палива постає як діагностичний параметр технічного стану транспортного засобу. За величиною витрати палива можна судити про складність умов експлуатації автомобіля, проводити оцінку ресурсу та коригувати періодичність проходження технічного обслуговування для транспортного засобу [1].

Система моніторингу транспортного засобу дозволяє відстежувати місцезнаходження, швидкість, витрату палива та стан автомобілів у

реальному часі. Система моніторингу - це розподілена інформаційна система, що включає елементи, що встановлюються на рушійному автомобілі, комп'ютери та сервери, що розташовуються безпосередньо на підприємстві або у хмарних сховищах [2].

Звичайно така система складається з наступних складових [3], які додатково встановлюється на автомобілі:

1) GPS-тракер, якій встановлюється на автомобіль, дає інформація про розташування та швидкість руху транспортного засобу.

2) Адаптер OBD-II, якій підключається до діагностичного роз'єму, де передається данні про витрати палива, швидкість руху, показників робочих процесів двигуна та трансмісії тощо.

3) Додаткові датчики та системні інтерфейси для отримання додаткової інформації про стан транспортного засобу.

4) Електронний блок збирання та передачі даних по мережі бездротового зв'язку.

При підключенні до CAN-шини (Controller Area Network) виникають серйозні ризики кібербезпеки, оскільки класичний протокол CAN розроблявся без вбудованих функцій безпеки. У ньому відсутні шифрування, автентифікація пристроїв та перевірка цілісності даних. Будь-який пристрій, підключений до шини, може прочитати всі пакети або надіслати підроблену команду (наприклад, для вимкнення сигналізації чи блокування двигуна).

Підключення пристрою до CAN-шини вимагає дотримання фізичних та логічних параметрів мережі. Необхідно враховувати рівень напруги на дротах шині (в стані спокою на CAN-H близько 2.5-2.6 В, на CAN-L близько 2.4-2.5 В, в активному режимі напруги розходяться), швидкість передачі даних (різні сегменти автомобіля можуть працювати на різних швидкостях - 125 кбіт/с, 250 кбіт/с або 500 кбіт/с), підтримувати різни протоколи (стандартний CAN 2.0A/2.0B або J1939).

Підключення мікроконтролерів зовнішнього пристрою до CAN-шини буде залежить від типу контролера. Мікроконтролери Atmel з архітектурою AVR (приклад, ATmega328P) не можуть безпосередньо працювати з фізичними рівнями напруг автомобільної мережі. Тому, для підключення потрібні контролер CAN (відповідає за логіку протоколу) та трансівер CAN (відповідає за фізичні рівні CAN-H та CAN-L). Можна використовувати модуль MCP2515, який поєднує в собі і контролер MCP2515 і трансівер TJA1050). Зв'язок модуля із мікроконтролером здійснюється по шині SPI. Модуль MCP2515 потребує 5 В живлення.

Микроконтролери сімейства ESP32 вже вбудований апаратний CAN-контролер (TWAI). Для зв'язку потрібен лише зовнішній трансівер - наприклад, модуль SN65HVD230 (він працює від 3.3 В). Підключається до будь-яких двох цифрових пін (TX/RX).

Микроконтролери сімейства STM32 також мають вбудований апаратний CAN-периферіал (bxCAN або FDCAN у новіших лінійках, таких як G4, H7, G0). Підходять трансівери SN65HVD230 або VP230. У STM32 апаратний фільтр вимкнено за замовчуванням (всі повідомлення блокуються). Щоб побачити хоч один пакет мережі, ініціалізація структури CAN_FilterTypeDef обов'язкова.

Важливо пам'ятати про узгоджувальний резистор. На кінцях CAN-шини мають стояти резистори 120 Ом. У модулях (MCP2515 та SN65HVD230) цей резистор зазвичай вже розпаяний. При підключенні до шини автомобіля цей резистор на модулі потрібно випаяти, щоб не просаджувати сигнал в мережі. Земля (GND) мікроконтролера має бути надійно з'єднана з масою автомобіля.

Трансівери забезпечують передання даних у дві сторони: від CAN-шини до мікроконтролера і від мікроконтролера до CAN-шини. Якщо інформація з CAN-шини тільки зчитуватиметься, то це не вплине на логіку роботи шини та безпеку даних, які по ній передаються. У цьому випадку

вбудоване програмне забезпечення в мікроконтролер зовнішнього пристрою не повинно містити команди передачі даних на CAN-шину.

Коли на CAN-шину зовнішній пристрій передаватиме дані, то це може порушити нормальну роботу шини, якщо не буде дотримано відповідність протоколу взаємодії. Недотримання протоколу може призвести до затирання даних, що передаються по шині іншими блоками керування автомобіля. Зовнішній пристрій може припинити роботу шину на тривалий час, протягом якого неможливо буде обмінюватися даними. Неправильна система команд і адресація можуть помилково зчитуватися іншими пристроями автомобіля, які підключені до шини, що порушує їхню роботу.

В системі моніторингу дані з автомобіля, якій рухається по дорозі, передається до стаціонарних комп’ютерів-серверів, де ці дані будуть зберігатися та оброблятися. Для передачі даних використовуються технології, що працюють через інтернет чи радіоканали великої дальності. Найбільш поширений бездротовий канал передачі даних є стільниковий зв'язок (GSM/4G/LTE), якій працює скрізь, де є мобільний зв'язок. З одного боку, на автомобілі використовується зв'язування «Мікроконтролер + 4G-модем». З іншого боку, дані поступають на телематичний сервер або власний виділений сервер (VPS).

Для передачі даних з автомобіля к мікроконтролеру додається SIM-модуль (SIM7600 або аналогічний). Модуль SIM7600 від компанії SIMCom Wireless Solutions призначен для роботи в мережах 4G LTE, 3G (UMTS/HSPA+) та 2G (GSM/GPRS/EDGE). Працює на живлені 3,3 В. З мікроконтролерами може зв’язуватися по UART, I2C та SPI. Управляється AT-командами. Модуль може працювати в текстовому режимі (Text Mode) для відправки або прийому SMS-повідомлень, використовувати вбудований TCP/IP-стек модуля (HTTP, MQTT, TCP/UDP) або режим модему (NDIS / PPP / ECM) через USB.

Дані упаковуються в легковаговий протокол MQTT або надсилаються через HTTP POST-запити на власний виділений сервер (VPS), де їх приймає скрипт на Python/Node.js та записує до бази даних (InfluxDB, PostgreSQL).

Можна використовувати безкоштовні/платні платформи (Wialon, GPS-Trace, Traccargos) або підняти свій безкоштовний сервер з відкритим кодом (Traccar). На ПК дані відкриваються у браузері або через програму-клієнт.

При передачі даних від автомобіля до сервера реалізується спеціальний протокол, який повинен містити шифр системи, ідентифікацію конкретного транспортного засобу, послідовність даних про час, витрату палива, швидкість автомобіля та іншу необхідну інформацію, контрольну суму пакета. Для підвищення кібербезпеки всі або частина даних у пакеті шифрують.

Зв'язок між GPRS-модем та сервером може бути в одному або в двох напрямках. Канал повинен бути захищений від DoS-атак та DDoS-атак. У програмному забезпеченні мікроконтролера, якій встановлюється на автомобілі, повинно бути прописані адреса серверу з якім він працює, відхиляти недійсні команді та мати здатність працювати та передавати дані без команд із серверу. На сервері повинно встановлюватися додаткове забезпечення, яке аналізує вхідний трафік та зупиняє атаки, виконувати фільтрацію за джерелом підключення, виконувати налаштування мережного обладнання та міжмережевих екранів (WAF) для відсікання аномальних запитів. Можливо використовувати хмарні сервери для первинного зберігання даних, де трафік та безпека контролюється системою хмарного сховища.

Обробка даних на сервері може виконуватися кількома рівнями: один модуль (ПЗ) приймає дані з мережі та контролює їх цілісність, другий модуль (ПЗ) здійснює ідентифікацію та передачу даних у систему зберігання даних (базу даних), у системі управління базою даних

контролюється унікальність даних, ще модуль (ПЗ) передає дані з бази для кінцевого споживача.

У системі моніторингу реалізується ще один канал передачі: від сервера до клієнтського комп'ютера, де інформацію дивитиметься диспетчер технічної чи транспортної служб підприємства. Передача даних від сервера до клієнтської програми можна організувати за принципом "тонкого клієнта", забезпечуючи додатковий рівень безпеки.

Побудова та впровадження системи моніторингу витрати палива транспортного засобу потребує всебічного аналізу можливих відмов та помилок, негативного впливу та кіберзахищеності системи.

Список використаних джерел

1. Sergey Krivoshapov, Igor Marmut, Ivan Nahliuk, Alexandr Nazarov, Yriy Gorbik, Mikhail Nahliuk, Yriy Zybtsev, Volodymyr Bezridnyi, Mykola Mysiura. Change in engine life and maintenance intervals depending on the fuel consumption of the vehicle during operation. *AIP Conf. Proc*. 10 August 2023; 2868 (1): 020002. https://doi.org/10.1063/5.0165624.
2. Волков В.П., Грицук І.В., Грицук Ю.В., Волкова Т.В., Кашканов В.А., Волков Ю.В. Особливості побудови інформаційної системи оцінювання параметрів технічного стану автомобілів в умовах експлуатації», *ВМТ*, 2019, Вип. 10, Вип. 2, С. 10–15.
3. Волков В.П., Грицук І.В., Комов А.П., Волков Ю.В. Особливості моніторингу і визначення статусу несправностей транспортного засобу у складі бортового інформаційно-діагностичного комплексу. *Вісник Національного транспортного університету*, 2014, Вип. 30, С. 51–62.