Парфьонов Володимир Миколайович, студент гр. АЕ-42-22, Харківський національний автомобільно-дорожній університет

ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНТЕРНЕТУ ТРАНСПОРТНИХ ЗАСОБІВ

У сучасну епоху, завдяки технологічній революції в галузі Інтернету речей IoT (Internet of Things (IoT)) та штучного інтелекту, спостерігається швидке та масове зростання та інтенсивне впровадження нових інформаційних технологій в різних сферах життя. Це сприяло виникненню такої галузі як Інтернет транспортних засобів IoV (Internet of Vehicles (IoV)).

Інтернет транспортних засобів IoV – це нова технологія, метою якої є об'єднання транспортних засобів, інфраструктури та інших пристроїв для забезпечення роботи інтелектуальних транспортних систем ITS (Intelligent Transport Systems (ITS)). Одним з ключових завдань Інтернету транспортних засобів IoV є підвищення енергоефективності транспортних засобів, в тому числі електромобілів, та безпеки дорожнього руху за рахунок впровадження безпечного та ефективного зв'язку між транспортними засобами різних типів, дорожнього середовища та можливостей ефективного керування всіма транспортними процесами.

В Інтернеті транспортних засобів IoV бортові електронні пристрої OBU (on-board units (OBU)), встановлені в транспортних засобах, відіграють вирішальну роль в обміні інформації з придорожніми блоками RSU (roadside units (RSU)), розташованими по обидва боки дороги. Придорожні блоки RSU можуть передавати зібрані повідомлення транспортним засобам, що проїжджають повз, для надання інформації про дорожній рух у режимі реального часу. Цей обмін інформацією дозволяє транспортним засобам оперативно виявляти дорожні ситуації та вживати необхідних заходів.

Інтернет транспортних засобів. складається з трьох взаємозв’язаних рівнів:

- рівень транспортних засобів та інших учасників дорожнього руху, наприклад, пішоходів;
- рівень дорожнього обладнання, що складається з придорожніх блоків RSU, інтелектуальних світлофорів та іншого оснащення;
- рівень хмарного сервера CS (cloud server (CS)), який відповідає наприклад, за автентифікацію транспортних засобів, проводить швидкі розрахунки щодо дорожньої ситуації [1].

Інтернет транспортних засобів IoV стосується моделей, які ініціюють зв'язок між інтелектуальними транспортними засобами та іншими об'єктами, використовуючи наступні зв'язки:

- «транспортний засіб до всього» V2X (Vehicle-to-Everything (V2X)) ;
- «транспортний засіб-транспортний засіб» V2V (Vehicle-to-Vehicle (V2V));
- «транспортний засіб-дорожнє обладнання» V2R (Vehicle-to-Road (V2R));
- «транспортний засіб-інфраструктура» V2I (Vehicle-to-Infrastructure (V2I));
- «транспортний засіб-датчик» V2S (Vehicle-to-Sensor (V2S));
- «транспортний засіб-пішохід» V2R (Vehicle to Pedestrian (V2R)).

Окремо для електромобілів у Інтернеті транспортних засобів IoV існують наступні технології:

- «транспортний засіб-будинок» V2B (Vehicle-to-Building (V2B));
- «транспортний засіб-електрична мережа» V2G (Vehicle-to-Grid (V2G));
- «транспортний засіб-дім» V2H (Vehicle-to-Home (V2H));
- «транспортний засіб -пристрій» V2D (Vehicle-to-Device (V2D)) [1-5].

В теперішній час впровадження Інтернету транспортних засобів IoV стикається з кількома критичними викликами, які необхідно вирішити для забезпечення безпеки дорожнього руху, цілісності даних та надійності цієї технології у майбутньому. Такі проблеми варіюються від технічних до юридичних обмежень.

Основні проблеми при впровадженні Інтернету транспортних засобів IoV стосуються безпеки та конфіденційності:

- безпека є найбільшою перешкодою, оскільки скомпрометовані системи можуть призвести до смертельних аварій;
- злом та віддалене захоплення даних. Неавторизовані користувачі можуть отримати контроль над цифровими системами транспортного засобу, потенційно маніпулюючи системою гальмування, швидкістю двигуна або функціями системи безпеки;
- маніпулювання даними та неправдива інформація. Зловмисники можуть поширювати оманливу інформацію про дорожній рух, таку як фальшиві дорожньо-транспортні пригоди або небезпеки на дорогах, що призводить до заторів або небезпечних маневрів;
- крадіжка особистих даних та конфіденційності. Збір величезних обсягів даних про переміщення транспортного засобу може призвести до відстеження особи та місцезнаходження користувача, що порушує конфіденційність особистого життя;
- кібератаки Sybil та Replay. Кібератаки Sybil зосереджені на маніпуляції з інформаційними даними в мережі шляхом підробки кількох ідентифікаційних даних, тоді як кібератаки Replay (повторного відтворення) передбачають захоплення та повторне надсилання легітимних даних для обману системи. Зловмисні вузли можуть використовувати підроблені ідентифікаційні дані для заповнення мережі повідомленнями або повторно використовувати старі, недійсні дані для обману інших транспортних засобів. Наприклад, у таких середовищах, як автомобільна спеціальна мережа VANET (з англ. Vehicular Ad Hoc Networks (VANET)), один транспортний засіб може транслювати інформацію як десятки автомобілів-«привидів», створюючи затор, та змушуючи інші транспортні засоби, що прямують за ним, повертати зі свого напрямку слідування та об'їжджати неіснуючий затор.

На рисунку 1 продемонстровано подібний сценарій кібератаки Sybil в автомобільної спеціальної мережі VANET у якому автомобілі «бачать» затор на дорозі та звертають наліво для його об’їзду, який розглянутий у дослідженні [4]. Зменшення кіберзагроз у системі зв'язку Інтернету транспортних засобів за допомогою надійної кластеризації та маршрутизації наведено у статті [5].

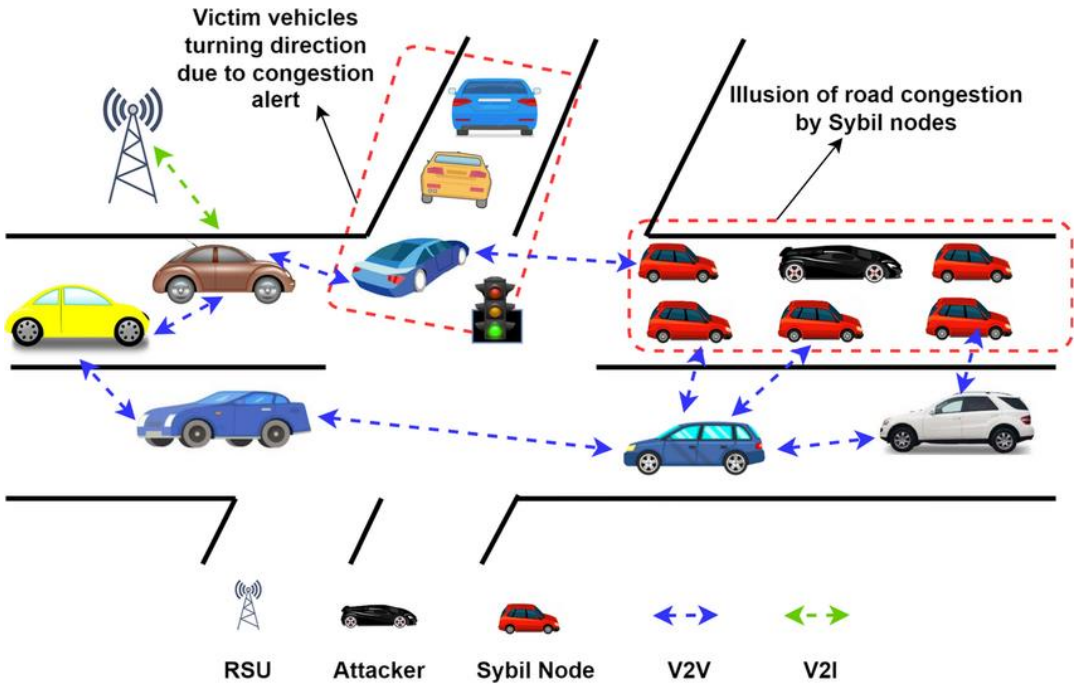

Рисунок 1 – Сценарій кібератаки Sybil у VANET [4]

Проблеми при впровадженні Інтернет транспортних засобів IoV стосуються також зв’язку транспортних засобів з мережею та надійним підключенням до неї. Динамічний характер рухомих транспортних засобів створює унікальні технічні перешкоди для стабільного зв'язку:

- висока мобільність та нестабільне з’єднання. Транспортні засоби, що швидко рухаються, часто в’їжджають та виїжджають із зони дії придорожніх пристроїв, що призводить до періодичних відключень від мережі;

- блокування сигналу. Фізичні перешкоди, такі як висотні будівлі, мости та дерева в міському середовищі, можуть порушувати бездротове з'єднання між транспортними засобами;

- інформаційні витрати. У високощільному трафіку величезний обсяг даних, що передаються, може перевантажити мережу, що призведе до затримок передачі;

- вимоги до затримки. Багато застосувань безпеки вимагають надзвичайно низької затримки (мінімальної затримки) для ефективності. Навіть кілька мс затримки можуть перешкодити своєчасному попередженню про зіткнення.

Широкомасштабному впровадженню Інтернету транспортних засобів IoV ускладнює відсутність єдиної глобальної системи та проблеми, що охоплюють питання технічної реалізації відповідної інфраструктури:

- відсутність взаємодії між різними виробниками, які використовують різні протоколи зв'язку та апаратне забезпечення, що ускладнює безперебійне «спілкування» автомобілів різних марок;

- впровадження IoV вимагає значних інвестицій у розумну придорожню інфраструктуру, таку як придорожні блоки RSU та покриття 5G/6G, встановлення яких є дорогим та трудомістким;

- обробка «великих даних», що генеруються безлічами підключених датчиків, вимагає високоефективної обробки та зберігання, що наразі створює

навантаження на традиційні хмарні архітектури.

Нетехнічні проблеми, які пов’язані з правовими та соціальними засадами також перешкоджають та уповільнюють впровадження технології IoV:

- нормативна та правова складність, наприклад, визначення того, хто несе відповідальність у ДТП за участю підключеного або автономного транспортного засобу — водія, виробника чи розробника програмного забезпечення — залишається серйозною юридичною проблемою;

- етичні дилеми, що пов’язані з розробкою програмного забезпечення для вирішення етичних сценаріїв в аварійних ситуаціях, в яких автоматичної системі курування транспортним засобом доведеться вибирати між двома (або більше) неминучими негативними наслідками аварії;

Таким чином, в сучасних умовах в реальному світі Інтернет транспортних засобів IoV стикається зі значними проблемами, пов'язаними з неоднорідністю транспортних засобів та ризиками зіткнень, які разом впливають на безпеку та ефективність. Ризики зіткнень виникають через непослідовний зв'язок, високу швидкість, змінену поведінку людини, проблеми затримки та проблеми безпеки, що створюють такі загрози, як підвищений ризик аварій та порушення руху транспорту.

Література

5. Wu, T.-Y., Wu, H., Tang, M., Kumari, S., & Chen, C.-M. (2025). CD-AKA-IoV: A Provably Secure Cross-Domain Authentication and Key Agreement Protocol for Internet of Vehicle. Computers, Materials & Continua, 1–10. https://doi.org/10.32604/cmc.2025.065560

6. Adnan, I., Umer, T., Arsalan, A., Al Dabel, M. M., Bashir, A. K., & Ansif, A. (2025). Data driven vehicular heterogeneity based intelligent collision avoidance system for Internet of Vehicles (IoV). Digital Communications and Networks. https://doi.org/10.1016/j.dcan.2025.03.010

7. Mishra, P., & Singh, G. (2025). Internet of Vehicles for Sustainable Smart Cities: Opportunities, Issues, and Challenges. Smart Cities, 8(3), 93. https://doi.org/10.3390/smartcities8030093

8. Sultana, R., Grover, J., Tripathi, M., Sachdev, M. S., & Taneja, S. (2024). Detecting Sybil Attacks in VANET: Exploring Feature Diversity and Deep Learning Algorithms with Insights into Sybil Node Associations. Journal of Network and Systems Management, 32(3). https://doi.org/10.1007/s10922-024-09827-7

9. Kadam, M. V., Mahajan, H. B., Uke, N. J., & Futane, P. R. (2023). Cybersecurity Threats Mitigation in Internet of Vehicles Communication System using Reliable Clustering and Routing. Microprocessors and Microsystems, 104926. https://doi.org/10.1016/j.micpro.2023.104926

Науковий консультант: Смирнов Олег Петрович, д.т.н., професор, Харківський національний автомобільно-дорожній університет, smirnov1oleg@gmail.com