АНАЛІЗ ОСОБЛИВОСТЕЙ ОРГАНІЗАЦІЇ СИСТЕМИ SMART VEHICLE

Колісник М.О., Муравльов В.О.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Розвиток технології Internet of things (IoT) у всьому світі призвело до появи нових систем, зокрема, розумний транспорт (Smart Vehicle - SV). При підключенні до IoT Smart Vehicle має переваги, пов'язаних з усуненням пробок і управлінням не тільки всередині транспортного засобу (ТЗ), але і дистанційно (в напівавтоматичному режимі управління), або в автоматичному режимі. При цьому може встановлюватися спеціальна мережа двох або більше ТЗ або придорожніх станцій «Автомобіль-до-Автомобілю» (Vehicle-to-Vehicle - V2V), яка дозволяє децентралізовано повідомляти ТЗ один одному про перешкоди на своєму шляху, про зміну швидкості для запобігання зіткнень і аварій, використовує дані про місцезнаходження, напрямку руху, а також забезпечення оптимального використання доріг. Кожне ТЗ також є маршрутизатором і дозволяє відправляти повідомлення на більш віддалені ТЗ і придорожні станції. Технологія управління забезпечується на локальні і більш високих рівнях архітектури з урахуванням невизначеностей, затримок, часткових вимірювань, при цьому система повинна бути здатна приймати автоматичні або напівавтоматичні рішення, надаючи попередження/інформацію о потенційно можливих перешкодах.

Технологія «Управління Транспортною Інфраструктурою» (Vehicle-to-Infrastructure Control - V2I) дозволяє ТС взаємодіяти з мережевою інфраструктурою за допомогою пересеченного управління. Інфраструктура збирає глобальну або локальну інформацію про трафік і дорожніх умовах, а потім координує поведінку групи ТЗ.

Технологія «Транспортний Засіб до Всього» (Vehicle-to-Everything - V2X) використовує частотний спектр 5,9 ГГц - Dedicated Short Range Communication, похідну від стандарту IEEE 802.11, спеціально визначеній для швидко рухомих об'єктів, а також технології Bluetooth, IEEE 802.15. 4, Z-wave і LTE-Advanced. Технологія V2X дозволяє попереджати водіїв про потенційні небезпеки на своєму шляху, таких як ризик зіткнення, небезпечний обгін, гальмування автомобіля, виявлення зони сліпої плями або дорожньої небезпеки.

При створенні системи SV безпека даних має важливе значення, так як ТЗ звертається до бази даних, в якій зберігається історія моделей подорожей, індивідуальні деталі поїздки, які вважаються особистою інформацією і, отже, аналіз даних і додатки повинні бути захищені спеціальними методами захисту від різного роду кібер-атак. Тому подальші дослідження доцільно присвятити оцінці гарантоздатності SV з урахуванням методів і засобів захисту інформації від різного роду кібер-атак, а також методів забезпечення надійної роботи компонентів системи Smart Vehicle.