

УДК 04.738:656.11

DOI: 10.31673/2412-9070.2025.061209

В. О. ПЕТРЕНКО, інженер відділу комп'ютерних систем та інформаційної безпеки
ДП "ДержавтотрансНДІпроект";
ORCID: 0009-0006-6792-2984

О. Г. ГРИГОРЕНКО, канд. техн. наук, доцент,
ORCID: 0000-0001-5019-9060

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

ТЕХНОЛОГІЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ МЕРЕЖ IoT В ІНТЕЛЕКТУАЛЬНІ ТРАНСПОРТНІ СИСТЕМИ

У статті розглядаються технологічні аспекти впровадження мереж Інтернету речей (IoT) в інтелектуальні транспортні системи (ІТС) міської інфраструктури. Представлено концептуальну модель IoT-архітектури, визначено ключові компоненти, підходи до кіберзахисту та напрямки практичного застосування. Метою дослідження є розробка концептуальної моделі IoT-мережі для ІТС з урахуванням можливостей збирання, передавання та обробки даних у режимі реального часу, а також впровадження засобів кіберзахисту з використанням сучасних методів шифрування, автентифікації та моніторингу подій. Об'єктом дослідження є автоматизація процесів у транспортній інфраструктурі за допомогою IoT-технологій. Інтенсивний розвиток міських агломерацій і збільшення кількості транспортних засобів спричиняє зростаючі навантаження на транспортну систему, що вимагає впровадження новітніх рішень для підвищення ефективності управління дорожнім рухом, покращення безпеки та екологічної ситуації. Інтелектуальні транспортні системи, засновані на IoT, забезпечують взаємодію між транспортними засобами, інфраструктурою та користувачами завдяки використанню сенсорів, камер відеоспостереження, шлюзів передавання даних та хмарних сервісів. У роботі розглянуто приклад моделювання IoT-архітектури для реального перехрестя вулиць міста Києва із використанням LoRaWAN-технології, MQTT-протоколу, серверної обробки та хмарної платформи AWS. Наведено етапи розробки моделі, особливості розміщення пристроїв та архітектуру обробки даних. Результати імітаційного моделювання у Cisco Packet Tracer продемонстрували ефективність побудованої мережі, її готовність до масштабування та інтеграції з міськими системами.

Ключові слова: інтелектуальні транспортні системи; міська інфраструктура; Інтернет речей; V2X-комунікації; LoRaWAN; хмарні обчислення; сенсорні пристрої; мережеві шлюзи; кібербезпека; протокол MQTT; моделювання; управління дорожнім рухом.

Вступ

Інтернет речей (IoT) – це мережа фізичних об'єктів, що містять вбудовану технологію для спілкування та взаємодії із зовнішнім середовищем. Тобто, це екосистема пристроїв, підключених через Інтернет, які постійно збирають, обробляють і передають дані. У транспортній сфері IoT дозволяє реалізувати моніторинг дорожнього трафіку у реальному часі, інтелектуальне управління світлофорами, виявлення надзвичайних ситуацій (ДТП, заторів), системи розумного паркування, а також комунікацію між транспортними засобами та інфраструктурою (V2X-vehicle-to-everything). Крім того, за допомогою IoT можна здійснювати збір аналітичної інформації для планування міського руху. Компоненти IoT-систем в ІТС включають різноманітні датчики для реєстрації швидкості, присутності транспорту та рівня забруднення, камери відеоспостереження з функціями розпізнавання номерів, IoT-шлюзи для передавання даних до серверів, хмарні платформи для зберігання, обробки й аналізу інформації, та використовую-

© Петренко В. О., Григоренко О. Г., 2025

ють програмне забезпечення для візуалізації, аналітики та управління системою, а також засоби кіберзахисту, включаючи шифрування, автентифікацію та захист від атак. Переваги впровадження IoT у транспортну сферу полягають у підвищенні безпеки дорожнього руху, зниженні заторів і часу перебування у дорозі, зменшенні витрат на обслуговування інфраструктури, а також у покращенні екологічної ситуації завдяки зменшенню рівня викидів.

Аналіз останніх досліджень і публікацій

У сучасних наукових публікаціях простежується стійкий інтерес до впровадження IoT у сферу інтелектуальних транспортних систем (ІТС), що обумовлено стрімким розвитком цифрових технологій та зростанням навантаження на міську інфраструктуру.

У статті [1] запропоновано безпечну архітектуру IoT-орієнтованої інтелектуальної транспортної системи (IoT-ITS), яка зосереджується на реальному моніторингу трафіку та ефективному управлінні ресурсами транспорту. Стаття аналізує загрози безпеці, зокрема підкреслює ризики втручання у комунікаційні канали між транспортними засобами та інфраструктурою. Запропонована модель інтегрує алгоритми шифрування даних, автентифікацію пристроїв та моніторинг аномальної активності для захисту системи.

Стаття [2] присвячена аналізу архітектури Інтернету транспортних засобів (IoV) на основі 5G-технологій. Автори досліджують ключові елементи інфраструктури, а також ефективність маршрутизації даних у реальному часі між транспортними засобами та інфраструктурою за допомогою мереж 5G та протоколів V2X. Стаття висвітлює критичну роль протоколів безпеки і надійної комунікації при реалізації IoV, зазначаючи потребу в низьких затримках і високій стабільності з'єднання. Це дослідження має безпосереднє відношення до теми IoT в інтелектуальному транспорті, оскільки пропонує глибокий огляд технічних аспектів побудови комунікаційних систем майбутнього.

У роботі [3] розглядаються переваги та виклики впровадження IoT в інтелектуальні транспортні системи (ІТС). Автори детально описують, як IoT може сприяти зниженню заторів, підвищенню безпеки дорожнього руху, оптимізації витрат на обслуговування інфраструктури, а також мінімізації негативного екологічного впливу. Особливу увагу приділено технологічним викликам: проблемам масштабованості мереж, забезпеченню енергозбереження сенсорних пристроїв, управлінню великими обсягами даних і необхідності інтеграції різних типів пристроїв у єдину платформу. Окремо виділено питання кібербезпеки та приватності даних, які є критичними для довіри користувачів до ІТС.

Таким чином, результати аналізу сучасних досліджень підтверджують актуальність і важливість тематики даної статті. Отримані висновки із проаналізованих джерел щодо побудови IoT-архітектур для ІТС, зокрема принципів забезпечення кібербезпеки, вибору ефективних протоколів комунікації (V2X, MQTT, LoRaWAN), використання хмарних обчислювальних платформ, стали основою для розробки власної концептуальної моделі IoT-мережі, врахування вимог до безпеки даних, масштабованості, енергоефективності та оптимізації інформаційних потоків в умовах міської транспортної інфраструктури.

Мета дослідження полягає у розробці концептуальної моделі IoT-мережі для міської транспортної інфраструктури, яка забезпечить ефективне передавання даних, оперативне управління рухом та високий рівень кіберзахисту.

Аналіз дорожньої інфраструктури міста

Для побудови концептуальної IoT-моделі в рамках інтелектуальної транспортної системи (ІТС) було обрано перехрестя вулиць Борщагівська – Олексі Тихого – Ковальський провулок (район будинку №128 по вул. Борщагівська, зупинка трамваю «Польова»). Ця ділянка є вузловим транспортним перехрестям поблизу корпусів КПП, зокрема інституту ІЕЕ, має інтенсивний автомобільний та пішохідний трафік. Інфраструктура потребує модернізації в частині систем моніторингу, керування світлофорами, підвищення безпеки пішоходів, а також оперативного реагування на надзвичайні ситуації. Наявність зупинок громадського транспорту та навчальних закладів (КПП) вимагає особливої уваги до організації руху та інформування учасників дорожнього руху.

Визначення точок встановлення IoT-пристроїв

Для забезпечення ефективного збору даних на критичному перехресті вулиць Борщагівська – Академіка Янгеля – Олекси Тихого було визначено оптимальні точки встановлення IoT-пристроїв (рис. 1). Обране місце має підвищену аварійність, зокрема на трамвайній зупинці та у напрямку виїзду на вул. Польову.

Було розміщено:

- 6 датчиків руху – для реєстрації напрямку, швидкості та наявності транспорту, особливо на підходах до перехрестя з усіх сторін;
- 2 HD-камери – орієнтовані на трамвайну зупинку та тротуар біля будинку №128, для відеофіксації небезпечних ситуацій;
- 1 шлюз LoRaWAN – для збору й передавання даних від усіх сенсорів у мережу.

На рис. 1 представлено карту з позначенням усіх пристроїв та їх типів, що дозволяє легко оцінити покриття зони контролю.



Рис. 1. Схема розміщення IoT-пристроїв на перехресті

Проектування структури мережі передавання даних

Для обраної ділянки міської транспортної інфраструктури спроектовано структуру бездротової мережі на базі технології LoRaWAN, що забезпечує ефективне передавання даних із сенсорів руху та відеокамер до серверної частини. Система включає приватну мережу LoRaWAN з відповідними шлюзами, сервером мережі та MQTT-брокером, який передає дані до обчислювальної інфраструктури. На серверному рівні розміщено приймач, сервер застосунків, сервер сповіщень та API-сервер, які разом забезпечують обробку, аналіз, реагування та інтеграцію інформації. Усі дані зберігаються в базі часових рядів і документній базі даних, що дозволяє вести історію подій, формувати аналітику та забезпечити доступ до актуальної інформації у реальному часі. Така архітектура дозволяє створити надійну та масштабовану систему моніторингу і управління дорожнім рухом в умовах щільної міської забудови.

Структурна схема на рис. 2 демонструє повний шлях даних у системі: від збору інформації з транспортного рівня до її обробки, збереження та подальшої доставки користувачам. Сенсори та камери передають дані через LoRaWAN-мережу до серверної інфраструктури. MQTT-брокер забезпечує ефективне передавання потоків даних до відповідних серверів. Обробка інформації відбувається на рівні сервера застосунків, результати зберігаються у базах даних, а сервер сповіщень та API інтерфейс забезпечують зворотний зв'язок з учасниками дорож-

нього руху або іншими системами. Така побудова IoT-інфраструктури є основою для надійної, гнучкої та масштабованої транспортної системи майбутнього.

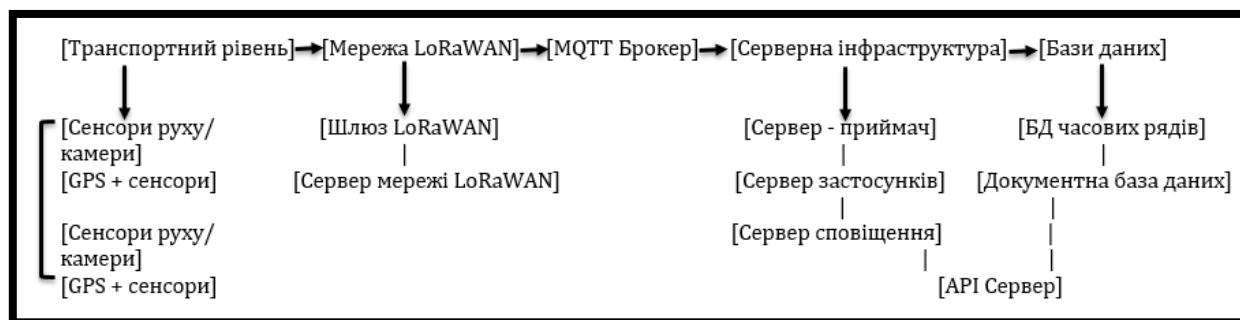


Рис. 2. Концептуальна схема IoT-архітектури

Вибір хмарної платформи та засобів кіберзахисту

Для реалізації обробки, зберігання та управління даними з IoT-пристроїв, встановлених на перехресті вулиць Борщагівська – Академіка Янгеля – Олекси Тихого, обрано хмарну платформу Amazon Web Services (AWS), зокрема її сервіс AWS IoT Core. Ця платформа забезпечує надійний прийом телеметричних даних із сенсорів руху та відеокамер через протокол MQTT, їх обробку, зберігання та подальше реагування. Архітектура побудована таким чином, що дані з пристроїв, підключених через LoRaWAN, передаються на MQTT-брокер, звідки потрапляють до AWS IoT Core, де відбувається маршрутизація до інших сервісів (таблиця 1).

Компоненти AWS у проєкті [4]

Компонент AWS	Призначення
AWS IoT Core	Приймає та обробляє MQTT-повідомлення від сенсорів
AWS Lambda	Автоматично запускає обробку даних: аналізує трафік, виявляє небезпеки
Amazon DynamoDB	Зберігає дані з сенсорів у структурованій формі (стан перехрестя, аварії)
Amazon S3	Архівує відеопотоки з камер
Amazon SNS	Надсилає push-повідомлення водіям про аварії або перевантаження дороги
Amazon CloudWatch	Моніторинг стану пристроїв, збоїв або перевантажень у мережі

Для забезпечення кіберзахисту (таблиця 2) всі комунікації шифруються за допомогою протоколу TLS 1.2, а кожен пристрій має унікальний сертифікат X.509 для аутентифікації. Доступ до ресурсів обмежується системою ролей та прав AWS IAM (Identity and Access Management), що виключає можливість несанкціонованого доступу. Крім того, на рівні API використовується файрвол AWS WAF (Web Application Firewall) для фільтрації вхідного трафіку. Усі події записуються у log-файли за допомогою AWS CloudTrail, що дозволяє відслідковувати будь-які зміни або спроби втручання. Дані регулярно резервуються через механізми Snapshot у DynamoDB та S3.

Засоби кіберзахисту в системі [5]

Засіб захисту	Застосування у схемі	Опис
TLS 1.2 (шифрування трафіку)	Передавання від шлюзів до MQTT	Захищає MQTT-повідомлення від перехоплення
Аутентифікація пристроїв (X.509 сертифікати)	Шлюзи LoRaWAN, камери	Забезпечує ідентифікацію кожного пристрою
IAM (керування доступом)	Серверна частина, API, бази даних	Обмежує доступ користувачів і сервісів до ресурсів

AWS WAF (веб-брандмауер)	На рівні API-сервера	Захищає від DDoS-атак та фільтрує вхідний HTTP-трафік
CloudTrail (реєстрація у журналах)	Вся система	Реєструє усі дії користувачів, виклики API, зміни у налаштуваннях
Snapshot (резервне копіювання)	DynamoDB, S3	Автоматично зберігає резервні копії даних для відновлення після збоїв

Така інтеграція хмарної платформи AWS з багаторівневою системою кіберзахисту забезпечує безперебійну, захищену та масштабовану роботу IoT-мережі в умовах реального міського середовища.

Моделювання у спеціальному ПЗ

Для перевірки працездатності спроектованої IoT-системи, її логіки передавання даних та реакцій на події було проведено імітаційне моделювання у середовищі Cisco Packet Tracer, яке підтримує компоненти IoT-мереж, включаючи сенсори, шлюзи, хмару, сервери та механізми взаємодії між ними.

У середовищі Cisco Packet Tracer 8.2.2 було створено віртуальну IoT-мережу, що моделює перехрестя вулиць Борщагівська – Академіка Янгеля – Олексії Тихого з метою тестування ключових процесів взаємодії між сенсорними пристроями, шлюзом LoRaWAN, серверною інфраструктурою, а також перевірка логіки передавання та обробки даних за допомогою протоколу MQTT.

Крок 1. Додавання пристроїв до схеми (рис. 3):

- 6 датчиків руху (Motion) – розташовані з обох боків дороги для виявлення наближення автомобіля;
- 2 вебкамери (Webcam) – розташовані на трамвайній зупинці для відеофіксації порушень;
- 2 транспортних засоби (Old Car) – умовно позначають автомобілі, які перетинають зону контролю;
- Шлюз LoRaWAN (DLC100 Home Gateway) – центральний вузол збору даних від сенсорів і камер;
- 3 сервери (Server-PT): приймач (192.168.0.2), сервер застосунків (192.168.0.3) та база даних (192.168.0.4).

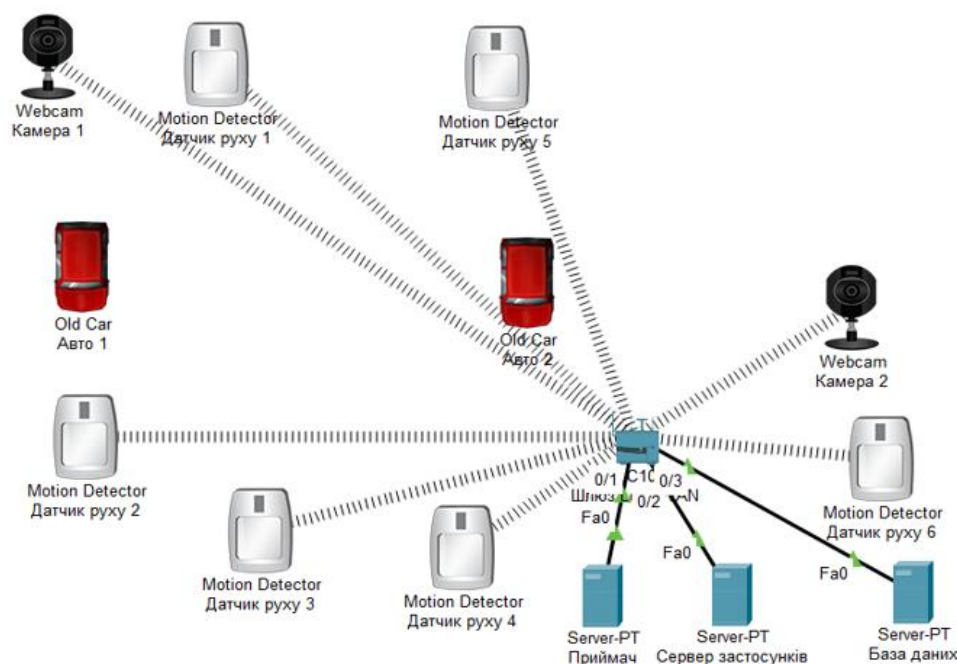


Рис. 3. Концептуальна модель підключених IoT датчиків до шлюзу

Крок 2. Налаштування IP-адрес зазначено у таблиці 3.

IP-адреси для шлюзу і серверів були встановлені вручну.

Налаштовані IP-адреси для шлюзу і серверів

Пристрій	IP-адреса	Призначення
Шлюз LoRaWAN	192.168.0.1	Центр збору даних
Приймач	192.168.0.2	Обробка повідомлень
Сервер застосунків	192.168.0.3	Виконання бізнес-логіки
База даних	192.168.0.4	Збереження часових рядів

Крок 3. Програмування датчиків руху

Для кожного датчика було створено скрипт на JavaScript у вкладці Programming, що реалізує наступну логіку: при виявленні руху (motion === true) – надсилається команда sendCommand(...) на відповідну вебкамеру, щоб вона увімкнулася.

Приклад коду для датчика 1:

```
function main() {
  var motion = getInput(«motion1»);
  if (motion === true) {
    sendCommand(«webcam1», «state», true); // Ввімкнути камеру 1
  } else {
    sendCommand(«webcam1», «state», false); // Вимкнути камеру 1
  }
  delay(1000);
}
```

Крок 4. Програмування камер

Камери були налаштовані як пристрої з цифровим слотом, що реагують на вхідні команди state = true/false. Камери змінюють стан (візуально світиться червоним) відповідно до сигналу з прив'язаного датчика руху.

Крок 5. Підключення серверної інфраструктури

Сервери були під'єднані до шлюзу через Ethernet з використанням дротових підключень. Усі пристрої мають єдину підмережу (маска - 24 біти).

Крок 6. Перевірка мережевої активності

Було перевірено зв'язність між усіма пристроями за допомогою утиліти ping. Також використовувалась симуляція пакетів у режимі Simulation, де спостерігалось проходження повідомлень (рис. 4):

- Від сенсорів → до шлюзу;
- Від шлюзу → до кожного сервера;
- Відсутність руху – вимкнення камери.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Датчи...	Датчик ру...	ICMP		10.001	N	0	(edit)	
	Successful	Каме...	Камера 2	ICMP		10.009	N	1	(edit)	

Рис. 4. Результати з'єднання

Результати дослідження

У процесі моделювання були проведені перевірки логіки спрацювання IoT-системи при виникненні подій, зокрема – виявленні руху транспортних засобів на перехресті. Було змодельовано ситуацію, коли автомобіль наближається до датчика руху, який запрограмований так, щоб при фіксації руху надсилати команду на увімкнення до відповідної вебкамери. Камери у свою чергу змінюють свій стан на активний, а дані передаються через шлюз LoRaWAN до серверної інфраструктури, що складається з трьох серверів: приймача, застосунків і бази даних.

Таким чином, логіка взаємодії сенсорів і виконавчих пристроїв працює, але для повної функціональності передавання даних на сервери необхідна додаткова конфігурація або вико-

ристання більш потужного середовища для IoT-моделювання, наприклад, Cooja, GNS3 або IoT Simulators з підтримкою MQTT та реального сценарію обробки пакетів.

У результаті моделювання у середовищі Cisco Packet Tracer було досягнуто:

- стабільного з'єднання між сенсорами, шлюзом і сервером;
- відображення реакцій системи у вигляді сповіщень у віртуальному додатку;
- взаємодії у режимі реального часу.

Висновки і перспективи подальших досліджень

У результаті проведеного дослідження було розроблено концептуальну модель IoT-мережі для міської інфраструктури, що дозволяє забезпечити ефективне управління трафіком, підвищити безпеку, знизити витрати. Представлена модель охоплює ключові апаратні та програмні компоненти, включаючи сенсори, шлюзи, серверну інфраструктуру та захист даних. Ураховано економічну ефективність впровадження. Робота підтверджує доцільність впровадження IoT в ІТС як необхідного кроку до побудови сучасного «розумного» міста.

Список літератури

1. Alotaibi, E., Hassan, M. M., & Alsamhi, S. H. (2023). A Secured IoT-Based Intelligent Transport System (IoT-ITS) Framework. *Sensors*, 23(5), 2401. <https://doi.org/10.3390/s23052401>
2. Wu, G., Taleb, T., & Letaief, K. B. (2020). Architecture and Key Terminal Technologies of 5G-Based Internet of Vehicles. *Science China Information Sciences*, 63(8), 1–18. <https://doi.org/10.1007/s11432-019-2897-3>
3. Yaqoob, I., Ahmed, E., Hashem, I. A. T., & Gani, A. (2019). Internet of Things (IoT) in Intelligent Transportation Systems: Benefits and Challenges of Implementation. *International Journal of Communication Systems*, 32(17), e3983. <https://doi.org/10.1002/dac.3983>
4. Amazon Web Services. (n.d.). What is AWS IoT Core?. Електронний ресурс: <https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html>
5. Amazon Web Services. (n.d.). Security best practices for AWS IoT. Електронний ресурс: <https://docs.aws.amazon.com/iot/latest/developerguide/security-best-practices.html>

V. Petrenko, O. Hryhorenko

TECHNOLOGICAL ASPECTS OF IMPLEMENTING IOT NETWORKS IN INTELLIGENT TRANSPORT SYSTEMS

This paper explores the technological aspects of implementing Internet of Things (IoT) networks in intelligent transport systems (ITS) within urban infrastructure. A conceptual model of IoT architecture is presented, highlighting key components, cybersecurity solutions and directions for practical application. The main objective of the study is to design a conceptual IoT network model for ITS that takes into account real-time data collection, transmission, and processing capabilities, along with the integration of cybersecurity mechanisms such as encryption methods, device authentication, and event monitoring. The object of the study is the automation of processes within urban transport infrastructure using IoT technologies. Rapid urbanization and the growing number of vehicles increase pressure on transport systems, demanding advanced solutions to enhance traffic efficiency, safety, and environmental sustainability. IoT-based intelligent transport systems enable automated interaction between vehicles, infrastructure, and users by employing sensors, video surveillance cameras, data transmission gateways, and cloud platforms. The paper presents a case study of modeling IoT architecture for a real intersection in Kyiv using LoRaWAN technology, the MQTT protocol, server-side processing, and the AWS cloud platform. The stages of model development, optimal placement of IoT devices, and data processing architecture are described in detail. Simulation results using Cisco Packet Tracer demonstrated the effectiveness of the proposed architecture and its readiness for real-world integration and scaling within urban environments.

Keywords: intelligent transport systems; urban infrastructure; Internet of Things; V2X communication; LoRaWAN; cloud computing; sensor devices; network gateways; cybersecurity; MQTT protocol; simulation; traffic management.