УДК 004.72.056.52:004.738.5
DOI DOI DOI DOI DOI https://doi.org/10.32782/2663-5941/2026.2.1/43

Янко А.С.
https://orcid.org/0000-0003-2876-9316
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Гончаренко С.О.
https://orcid.org/0009-0009-3417-6198
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУРНИХ ТА КРИПТОГРАФІЧНИХ ІННОВАЦІЙ У СПЕЦИФІКАЦІЯХ LORAWAN 1.0.4 ТА 1.1

У статті проведено порівняльний аналіз еволюції протоколу LoRaWAN, зосереджений на переході від специфікації версії 1.0.4 до архітектури версії 1.1. Актуальність дослідження зумовлена масштабуванням систем Інтернету речей (IoT) та посиленням вимог до кібербезпеки критичних інфраструктур, де рішення класу LPWAN стали галузевим стандартом. Розглянуто архітектурні особливості LoRaWAN 1.0.4 як завершального етапу гілки 1.0.x, що забезпечує базову функціональність, проте має обмеження у гнучкому управлінні ключами та підтримці глобального роумінгу. Висвітлено вразливості механізмів активації «по повітрю» (OTAA), притаманні раннім версіям, та обґрунтовано необхідність нових підходів до автентифікації.

Основну увагу приділено концептуальним трансформаціям у LoRaWAN 1.1. Досліджено роль виділеного Join Server (JS), який відокремлює процес автентифікації від функцій мережевого сервера. Таке розділення повноважень визначено як критичний елемент для побудови мультиоператорських середовищ, де довіра між власником пристрою та постачальником послуг має бути чітко розмежована. Проаналізовано модель розподілу серверних ролей на обслуговуючий (sNS) та домашній (hNS) сервери, що створює підґрунтя для безшовного роумінгу та підвищення живучості мереж.

Окремий розділ присвячено аналізу криптографічних інновацій. Висвітлено перехід від єдиного мережевого ключа сесії (NwkSKey) до розширеної ієрархії, що включає спеціалізовані ключі: FNwkSIntKey та SNwkSIntKey для перевірки цілісності висхідного й низхідного каналів, а також NwkSEncKey для шифрування MAC-команд. Доведено, що такий підхід підвищує стійкість протоколу до MITM-атак та захищає від компрометації сегментів мережі. Розібрано вдосконалені механізми управління лічильниками кадрів та введення нових нонсів (Nonces), що нівелює ризики replay-атак.

Результати підтверджують, що LoRaWAN 1.1 є стратегічним кроком до створення захищених промислових IoT-систем. Попри складність реалізації, переваги у безпеці та масштабованості роблять версію 1.1 оптимальною для сфер «розумного міста», моніторингу та енергетики. Практична цінність роботи полягає у формулюванні критеріїв доцільності модернізації мереж на базі LoRaWAN 1.0.4 та наданні рекомендацій щодо впровадження нових безпекових стандартів.

Ключові слова: *LoRaWAN, Інтернет речей, кібербезпека, криптографічний захист, масштабованість мереж, механізмам автентифікації, розподілена серверна архітектура, сесійні ключі.*

Постановка проблеми. Стрімкий розвиток концепції Інтернету речей (IoT) зумовив потребу у масштабованих, енергоефективних та довготривалих мережевих рішеннях для передавання невеликих обсягів даних на великі відстані. Однією з ключових технологій класу LPWAN (Low Power Wide Area Network), що відповідає цим вимогам, є LoRaWAN – відкритий протокол мережевого рівня, розроблений для організації енергоощадних бездротових мереж зіркоподібної топології. Завдяки підтримці великої кількості кінцевих пристроїв, низькому енергоспоживанню та широкому покриттю LoRaWAN активно застосовується у сферах розумного міста, промислового моніто-

рингу, сільського господарства та екологічного контролю [1, с. 1].

Версія LoRaWAN 1.0.4 стала завершальним етапом розвитку гілки 1.0.x, у якій було вдосконалено механізми сумісності, управління пристроями та окремі аспекти MAC-рівня [2, с. 13]. Водночас зростання вимог до безпеки, масштабованості та підтримки роумінгу між мережами зумовило появу специфікації LoRaWAN 1.1, що передбачає суттєві архітектурні та криптографічні зміни [3, с. 41].

На відміну від попередньої версії, LoRaWAN 1.1 запроваджує розширену модель розподілу ключів безпеки, оновлену процедуру активації пристроїв (Join-процес), а також чіткіше розмежування функцій між мережевим, прикладним та join-серверами. Такі зміни безпосередньо впливають на рівень захищеності мережі, керованість пристроями та можливість масштабування інфраструктури.

Отже, аналіз відмінностей між LoRaWAN 1.0.4 та LoRaWAN 1.1 є актуальним з точки зору оцінки еволюції протоколу, визначення переваг нової специфікації та розуміння її впливу на функціонування сучасних LoRaWAN-мереж [4, с. 8]. Подальший розвиток Інтернету речей супроводжується не лише збільшенням кількості підключених пристроїв, але й ускладненням вимог до інфраструктури зв'язку. Для ринку IoT сьогодні характерні три ключові тенденції: масштабування мереж до десятків і сотень тисяч вузлів, прагнення мінімізувати капітальні та операційні витрати, а також суттєве посилення вимог до кібербезпеки. У таких умовах технології класу LPWAN, зокрема LoRaWAN, залишаються одним із найбільш економічно доцільних рішень для побудови розподілених сенсорних мереж.

Разом із тим, широке впровадження LoRaWAN у критично важливих сферах – енергетиці, інфраструктурному моніторингу, промисловості та розумних містах – підвищує ризики, пов'язані з несанкціонованим доступом, компрометацією ключів шифрування та масштабними мережевими атаками. З огляду на тривалий життєвий цикл IoT-пристроїв і обмежені можливості їх оновлення, питання стійкої криптографічної архітектури та гнучкого управління ключами набувають стратегічного значення.

У цьому контексті поява специфікації LoRaWAN 1.1 є відповіддю на сучасні виклики ринку. Нова версія протоколу пропонує вдосконалену модель безпеки, розмежування ролей мережевих компонентів, підтримку роумінгу та підвищену керованість пристроями. Водночас значна частина існуючих розгортань продовжує працювати на базі LoRaWAN 1.0.4, що зумовлює необхідність системного порівняння обох версій [5, с. 1].

Отже, актуальність дослідження полягає у потребі комплексної оцінки архітектурних і протокольних змін у LoRaWAN 1.1 з позиції їх практичного впливу на безпеку, масштабованість і економічну ефективність мереж. Такий аналіз дозволяє визначити доцільність переходу на нову специфікацію та її відповідність сучасним вимогам розвитку IoT-інфраструктур.

Аналіз останніх досліджень і публікацій. Питання еволюції протоколу LoRaWAN та порівняння його версій перебувають у центрі уваги багатьох дослідників. Зокрема, у дослідженнях [6, с. 12] та [7, с. 36] детально розглянуто обмеження перших версій LoRaWAN (1.0.x) щодо масштабованості та ємності мережі в умовах щільного розгортання пристроїв. Автори зазначають, що хоча топологія «зірка зірок» є ефективною для енергоощадності, вона створює певні виклики для безпеки під час передачі ключів через мережеві сервери.

Криптографічні аспекти специфікації 1.1 стали об'єктом системного аналізу у статті [8, с. 348], які проаналізували вразливості механізму активації пристроїв «по повітрю» (з анг. Over-the-Air Activation – OTAA) у версії 1.0.4, зокрема ризики атак повторного відтворення (replay attacks). Дослідники підкреслюють, що впровадження окремого Join Server у версії 1.1 є критичним кроком для забезпечення довіри у мульти-операторських мережах [3, с. 45].

У науковому дослідженні [9, с. 8332] увага приділяється практичному впровадженню роумінгу та архітектурним змінам, що стали можливими завдяки чіткому розділенню функцій між серверами домашньої (hNS) та обслуговуючої (sNS) мереж. Проте, попри очевидні переваги версії 1.1, у публікації [10, с. 5] відзначається, що складність реалізації оновленого стека протоколів та підвищені вимоги до обчислювальних ресурсів кінцевих вузлів сповільнюють масовий перехід від стабільної специфікації 1.0.4 до 1.1.

Незважаючи на значну кількість публікацій, порівняльний аналіз архітектурних інновацій саме в контексті інтеграції безпеки та операційної ефективності між версіями 1.0.4 та 1.1 потребує більш глибокого систематизованого підходу, що і зумовило вибір теми даної статті.

Постановка завдання. Сучасний стан розвитку технологій LPWAN потребує переходу від базової функціональності до побудови архі-

тектурно стійких та криптографічно захищених систем. Незважаючи на стабільність специфікації LoRaWAN 1.0.4, виникає об'єктивна потреба у дослідженні переваг версії 1.1 як стратегічного інструменту для масштабування IoT-інфраструктур.

Метою статті є проведення системного порівняльного аналізу архітектурних рішень та криптографічних інновацій у специфікаціях LoRaWAN версій 1.0.4 та 1.1 для визначення їхнього впливу на рівень захищеності, масштабованість та операційну ефективність сучасних мереж Інтернету речей.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати архітектурні особливості специфікації LoRaWAN 1.0.4, виявивши ключові обмеження щодо розмежування довіри та управління сесійними ключами.

2. Дослідити еволюцію компонентів мережі у версії 1.1, зокрема роль окремого Join Server у забезпеченні безпечного роумінгу та активації пристроїв.

3. Здійснити порівняльну оцінку криптографічних моделей, фокусуючись на переході від єдиного мережевого ключа до розширеного набору (FNwkSIntKey, SNwkSIntKey, NwkSEncKey) для посилення цілісності та конфіденційності даних.

4. Вивчити механізми захисту від атак повторного відтворення (replay-attacks) та принципи управління лічильниками кадрів у новій специфікації.

5. Оцінити вплив впроваджених змін на економічну ефективність та можливості інтеграції пристроїв у мультиоператорські середовища.

6. Сформулювати рекомендації щодо доцільності модернізації існуючих розгортань та переходу на стек протоколів LoRaWAN 1.1 у нових проєктах.

Виклад основного матеріалу. *Архітектурні особливості LoRaWAN 1.0.4.* LoRaWAN 1.0.4 є завершальною версією гілки 1.0.x та зберігає класичну зіркоподібну топологію (star-of-stars), у якій кінцеві пристрої (End Devices) взаємодіють із мережею через шлюзи (Gateways), що передають трафік до мережевого сервера (Network Server, NS). Специфікація 1.0.4 уточнює поведінку MAC-рівня, механізми ADR (Adaptive Data Rate), процедури підтверджених/непідтверджених повідомлень та обробку лічильників кадрів (Frame Counters).

Модель безпеки в LoRaWAN 1.0.4. У версії 1.0.x використовується дворівнева схема ключів:

– NwkSKey – для забезпечення цілісності повідомлень MAC-рівня;

– AppSKey – для шифрування корисного навантаження (FRMPayload).

При активації пристрою через OTAA (Over-The-Air Activation) формується сесійний набір ключів на основі AppKey та параметрів процедури Join. Однак у 1.0.x мережевий сервер фактично має доступ до AppSKey (залежно від реалізації), що обмежує розділення довіри між мережевим та прикладним рівнями. Також у версії 1.0.x відсутнє повноцінне розмежування функцій Join Server, а процедура приєднання має спрощену криптографічну модель, що ускладнює реалізацію масштабного та безпечного роумінгу між мережами різних операторів [11, с. 1].

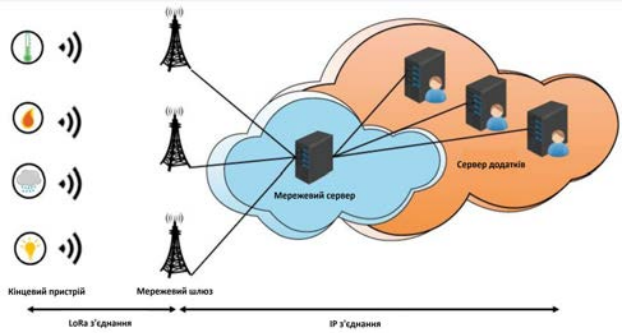

Рис. 1. Архітектура мережі LoRaWAN 1.0.4

Архітектурна еволюція у LoRaWAN 1.1. LoRaWAN 1.1 запроваджує суттєві зміни у структурі мережі та криптографічній архітектурі, що безпосередньо впливають на масштабованість і безпеку.

Розмежування мережевих ролей. У версії 1.1 чітко визначено логічне розділення між Network Server (NS), Application Server (AS) та Join Server (JS).

Join Server стає окремою довіреною сутністю, відповідальною за управління кореневими ключами та генерацію сесійних ключів. Це дозволяє:

– мінімізувати довіру до мережевого оператора;

– реалізувати міжмережевий роумінг;

– централізовано керувати криптографічною інфраструктурою [12, с. 1].

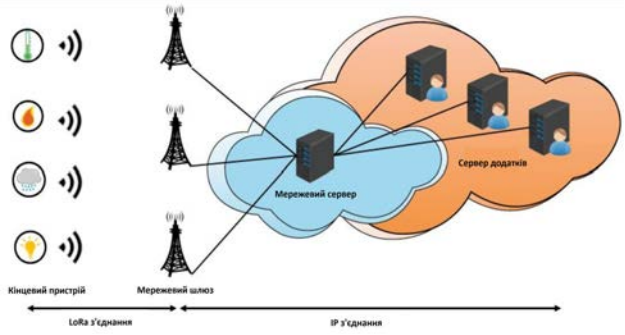

Рис. 2. Архітектура мережі LoRaWAN 1.1

Розширена криптографічна модель LoRaWAN 1.1. Однією з ключових відмінностей є введення нової ієрархії ключів. Кореневі ключі. Замість одного AppKey, у 1.1 використовується:

– NwkKey – для мережевої аутентифікації;

– AppKey – для прикладного рівня.

це забезпечує криптографічне розділення відповідальності між мережею та застосунком.

Сесійні ключі. Суттєвою архітектурною інновацією специфікації LoRaWAN 1.1 є декомпозиція єдиного мережевого ключа сесії (NwkSKey), характерного для версії 1.0.4, на три спеціалізовані вектори безпеки. Такий підхід базується на принципі мінімізації привілеїв та функціонального розділення криптографічних задач:

– FNwkSIntKey – використовується для обчислення та перевірки коду цілісності повідомлення (з анг. Message Integrity Code – MIC) у висхідних лініях зв'язку (uplink), це забезпечує автентифікацію кінцевого пристрою мережевим сервером;

– SNwkSIntKey – призначений для верифікації цілісності даних у низхідних лініях зв'язку (downlink), що гарантує кінцевому пристрою отримання команд саме від легітимного сервера обслуговування;

– NwkSEncKey – застосовується виключно для шифрування та дешифрування корисного навантаження MAC-команд на мережевому рівні.

Завдяки такій диференціації досягається вищий рівень ізоляції функцій безпеки. Зокрема, це унеможливлює компрометацію всієї сесії при витоку одного з ключів та значно підвищує стійкість системи до атак повторного відтворення (replay attacks) за рахунок незалежної індексації лічильників повідомлень [13, с. 2]. Окрім того, розділення ключів на «висхідні» та «низхідні» є необхідною умовою для реалізації безпечного роумінгу, оскільки дозволяє мережі обслуговування (Serving Network) виконувати базові операції з трафіком без надання їй повного доступу до конфіденційних даних домашньої мережі (Home Network).

Процедура Join та механізми автентифікації. У LoRaWAN 1.1 процедура OTAA суттєво вдосконалена:

– введено новий тип ідентифікатора JoinEUI (замість AppEUI);

– додано RJcount для захисту від повторного використання join-запитів;

– розширено перевірку MIC із використанням окремих ключів.

Ці зміни підвищують захист від replay-атак та атак повторного приєднання, що є критично важливим у масштабних IoT-мережах з тривалим життєвим циклом пристроїв [14, с. 1].

Підтримка роумінгу. Одним із стратегічних нововведень 1.1 є нативна підтримка роумінгу між мережами операторів. Роумінг реалізується через:

– розмежування Serving Network Server (SNS) та Home Network Server (HNS);

– збереження контролю над ключами на стороні домашньої мережі;

– централізований Join Server.

Все це відкриває можливість побудови глобальних LoRaWAN-інфраструктур із збереженням безпеки та контролю над пристроями [15, с. 6].

Управління лічильниками кадрів та захист від replay-атак. У LoRaWAN 1.0.x використовуються 16-бітні або 32-бітні лічильники кадрів, однак їх обробка була менш формалізованою. Удосконалення механізмів контролю послідовності пакетів у LoRaWAN 1.1 базується на таких ключових інноваціях:

– формалізація обробки невідповідних значень (Strict Replay Protection);

– посилена верифікація цілісності (MIC) з урахуванням вектора напрямку;

– захист від скидання лічильників при пере підключенні;

– посилено контроль повторних пакетів.

Дані нововведення є критично важливими для масштабованих мереж з високою щільністю вузлів. Саме така архітектура лічильників забезпечує довготривалу стабільність мережі, запобігаючи деградації каналів зв'язку через масовані replay-атаки, які в іншому випадку могли б паралізувати роботу шлюзів та серверів обробки.

MAC-рівень та керування мережею. LoRaWAN 1.1 зберігає механізм класів пристроїв (Class A, B, C), проте уточнює поведінку MAC-команд і їх шифрування через NwkSEncKey. Важливими аспектами є:

– вдосконалений ADR;

– точніше управління параметрами каналу;

– краща сумісність із регіональними специфікаціями.

MAC-команди тепер мають чітке криптографічне розмежування, що унеможливлює їх перехоплення або модифікацію без відповідного ключа. У таблиці 1 наведено список нових MAC-команд у LoRaWAN 1.1 [16, 1. с]:

Вплив змін на масштабованість та економічну ефективність. З технічної точки зору, розділення серверних ролей і ключів:

– зменшує ризик компрометації всієї мережі;

– дозволяє операторам гнучко масштабувати інфраструктуру;

Таблиця 1

Перелік та функціональне призначення MAC-команд у специфікації LoRaWAN 1.1

CID	Назва MAC-команди	Напрям передачі	Функціональне призначення
0x01	ResetInd	End-device → Network	Для ABP пристрою: індикація reset (повернення MAC/радіо параметрів до стандартних) та узгодження minor-версії протоколу; має повторюватися в uplink, доки не буде отримано ResetConf.
0x01	ResetConf	Network → End-device	Підтвердження ResetInd.
0x0B	RekeyInd	End-device → Network	Для OTAA: сигналізація оновлення security context (rekeying) після Join-accept; ED додає RekeyInd у наступні uplink, доки не прийде RekeyConf.
0x0B	RekeyConf	Network → End-device	Підтвердження RekeyInd.
0x0C	ADRParamSetupReq	Network → End-device	Налаштування параметрів ADR_ACK_LIMIT та ADR_ACK_DELAY на боці ED (точніше керування ADR-реакцією пристрою).
0x0C	ADRParamSetupAns	End-device → Network	Підтвердження ADRParamSetupReq.
0x0E	ForceRejoinReq	Network → End-device	Команда мережі “Rejoin негайно” з параметрами періодичності/DR/типу Rejoin та лімітом повторів (для RekeyInd або роумінгу).
0x0F	RejoinParamSetupReq	Network → End-device	Встановлення параметрів періодичного надсилання RejoinReq Type 0 (за часом або за лічильником uplink).
0x0F	RejoinParamSetupAns	End-device → Network	Підтвердження RejoinParamSetupReq.
0x20	DeviceModeInd	End-device → Network	Class C доповнення в 1.1: ED інформує мережу про поточний режим роботи (Class A або Class C) і має повторювати в uplink, доки не отримає DeviceModeConf.
0x20	DeviceModeConf	Network → End-device	Підтвердження DeviceModeInd.

– спрощує інтеграцію з хмарними сервісами.

З економічної точки зору:

– централізований Join Server зменшує витрати на адміністрування ключів;

– підтримка роумінгу дозволяє будувати мультиоператорські мережі;

– покращена безпека знижує потенційні втрати від атак.

Таким чином, LoRaWAN 1.1 є не просто інкрементальним оновленням, а структурною еволюцією протоколу, спрямованою на відповідність сучасним вимогам безпеки [17, с. 329], масштабованості та ринкової інтеграції IoT-рішень [18, с. 2118].

Висновки. У межах проведеного аналізу було розглянуто еволюцію протоколу LoRaWAN від версії 1.0.4 до 1.1 з позиції архітектурних, криптографічних та функціональних змін. Встановлено, що LoRaWAN 1.0.4 є логічним завершенням гілки 1.0.x та забезпечує стабільну роботу мережі, сумісність пристроїв і базовий рівень безпеки, достатній для більшості класичних IoT-застосувань. Водночас ця версія має обмеження щодо розмежування довіри між компонентами мережі, управління ключами та реалізації масштабного роумінгу.

На відміну від попередньої специфікації, LoRaWAN 1.1 пропонує концептуально нову модель безпеки із розподілом кореневих та сесійних ключів, чітким розмежуванням функцій між Network Server, Application Server та Join Server, а також удосконаленими механізмами автентифікації та захисту від replay-атак. Запровадження окремих мережевих ключів (FNwkSIntKey, SNwkSIntKey, NwkSEncKey) та розширеної процедури Join суттєво підвищує криптографічну стійкість системи та зменшує ризики компрометації мережевої інфраструктури.

Крім підвищення рівня безпеки, специфікація 1.1 створює передумови для масштабування та інтеграції LoRaWAN-мереж у мультиоператорські середовища завдяки підтримці роумінгу та розподіленої серверної архітектури. Це відповідає сучасним тенденціям розвитку IoT, які характеризуються зростанням кількості пристроїв, підвищенням вимог до кіберзахисту та необхідністю оптимізації операційних витрат.

Таким чином, LoRaWAN 1.1 слід розглядати не як інкрементальне оновлення, а як стратегічний етап розвитку протоколу, спрямований на забезпечення довгострокової стійкості, безпеки та масштабованості мереж LPWAN. Отримані результати можуть бути використані для обґрунтування доцільності переходу з LoRaWAN 1.0.4 на 1.1 у нових і модернізованих IoT-розгортаннях, з урахуванням вимог конкретного сценарію застосування.

Список літератури:

1. What Is LoRaWAN® Specification / LoRa Alliance. 2023. URL: https://lora-alliance.org/about-lorawan/ (дата звернення: 19.03.2026).
2. LoRaWAN 1.0.4 Specification / LoRa Alliance. 2020. 102 p. URL: https://resource.lora-alliance.org/technical-specifications/lorawan-1-0-4-specification (дата звернення: 19.03.2026).
3. LoRaWAN 1.1 Specification / LoRa Alliance. 2017. 98 p. URL: https://resource.lora-alliance.org/technical-specifications/lorawan-1-1-specification (дата звернення: 19.03.2026).
4. Analysis of LoRaWAN 1.0 and 1.1 Protocols Security Mechanisms / S. Loukil, L. C. Fourati, A. Nayyar, K.-W.-A. Chee. *Sensors*. 2022. Vol. 22, No. 10. Art. 3717. DOI: https://doi.org/10.3390/s22103717.
5. End-to-End IoT Solutions / TEKTELIC. 2026. URL: https://tektelic.com/products/solutions/ (дата звернення: 01.03.2026).
6. Farrell S. LPWAN Overview. RFC 8376. 2018. 32 p. DOI: https://doi.org/10.17487/RFC8376.
7. Understanding the Limits of LoRaWAN / F. Adelantado et al. *IEEE Communications Magazine*. 2017. Vol. 55, No. 9. P. 34–40. DOI: https://doi.org/10.1109/MCOM.2017.1600613.
8. Butun I., Pereira N., Gidlund M. Security Analysis of LoRaWAN v1.1. *2019 IEEE 44th Conference on Local Computer Networks (LCN)*. Osnabrueck, Germany, 2019. P. 348–351. DOI: https://doi.org/10.1109/LCN44234.2019.8990744.
9. Han J., Wang J. The Architecture and Security Analysis of LoRaWAN v1.1. *IEEE Access*. 2018. Vol. 6. P. 8330–8341. DOI: https://doi.org/10.1109/ACCESS.2018.2796191.
10. Lavric A., Popa V. LoRaWAN Gateway: A Comparative Analysis of v1.0.4 and v1.1 Implementations. *Sensors*. 2021. Vol. 21, No. 14. Art. 4872. DOI: https://doi.org/10.3390/s21144872.
11. Ivezic M. LoRaWAN Security 101 (Non-5G IoT Connectivity Options). *PostQuantum*. 2019. URL: https://postquantum.com/5g-security/iot-lorawan-security/ (дата звернення: 07.08.2019).
12. Introducing LoRaWAN 1.1 Support / Mbed. 2026. URL: https://os.mbed.com/blog/entry/Introducing-LoRaWAN-11-support/ (дата звернення: 01.03.2026).
13. Chen X., Lech M., Wang L. A Complete Key Management Scheme for LoRaWAN v1.1. *Sensors*. 2021. Vol. 21, No. 9. Art. 2962. DOI: https://doi.org/10.3390/s21092962.
14. LoRaWAN / Smart Parks Wiki. 2026. URL: https://wiki.smartparks.com/en/concepts/lorawan (дата звернення: 01.03.2026).
15. Янко А. С., Горчаренко С. О. Практичні рекомендації з налаштування LORAWAN-мережі для стабільної роботи та захищеності даних. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління* : тези доповідей п'ятнадцятої міжнар. наук.-техн. конф., 24–25 квітня 2025 р. Баку–Харків–Жиліна, 2025. Т. 3. С. 6–7. DOI: https://doi.org/10.32620/ICT.25.t3.
16. LoRaWAN® Specification v1.1 / LoRa Alliance. 2023. URL: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1 (дата звернення: 15.09.2023).
17. Formal security analysis of LoRaWAN / M. Eldefrawy, I. Butun, N. Pereira, M. Gidlund. *Computer Networks*. 2019. Vol. 148. P. 328–339. DOI: https://doi.org/10.1016/j.comnet.2018.11.017.
18. Naoui S., Elhdhili M. E., Saidane L. A. Novel Enhanced LoRaWAN Framework for Smart Home Remote Control Security. *Wireless Personal Communications*. 2020. Vol. 110. P. 2109–2130. DOI: https://doi.org/10.1007/s11277-019-06832-x.

Yanko A.S., Goncharenko S.O. COMPARATIVE ANALYSIS OF ARCHITECTURAL AND CRYPTOGRAPHIC INNOVATIONS IN LORAWAN 1.0.4 AND 1.1 SPECIFICATIONS

This paper provides a comparative analysis of the LoRaWAN protocol evolution, focusing on the transition from the version 1.0.4 specification to the version 1.1 architecture. The relevance of the study is driven by the scaling of Internet of Things (IoT) systems and the escalating cybersecurity requirements for critical infrastructures, where LPWAN solutions have become an industry standard. The architectural features of LoRaWAN 1.0.4 are examined as the final stage of the 1.0.x branch, which provides basic functionality but possesses limitations in flexible key management and global roaming support. The study highlights vulnerabilities in Over-the-Air Activation (OTAA) mechanisms inherent in earlier versions and justifies the necessity for new approaches to authentication.

The primary focus is placed on the conceptual transformations in LoRaWAN 1.1. The role of the dedicated Join Server (JS) is investigated, which decouples the authentication process from network server functions. This separation of concerns is identified as a critical element for building multi-operator environments, where trust between the device owner and the connectivity provider must be clearly demarcated. The paper analyzes the model of server role distribution into Serving (sNS) and Home (hNS) servers, which establishes the framework for seamless roaming and enhancing network survivability.

A dedicated section is devoted to the analysis of cryptographic innovations. It elucidates the transition from a single network session key (NwkSKey) to an extended hierarchy, including specialized keys: FNwkSIntKey and SNwkSIntKey for uplink and downlink integrity verification, and NwkSEncKey for MAC command encryption. It is demonstrated that this approach enhances the protocol's resilience against MITM attacks and protects against the compromise of network segments. The study details improved frame counter management and the introduction of new Nonces, which eliminate the risks of replay attacks.

The results confirm that LoRaWAN 1.1 is a strategic step toward creating secure industrial IoT systems. Despite implementation complexity, the security and scalability benefits make version 1.1 optimal for smart cities, monitoring, and energy sectors. The practical value of the work lies in formulating criteria for assessing the feasibility of modernizing LoRaWAN 1.0.4-based networks and providing recommendations for implementing new security standards.

Keywords: *LoRaWAN, Internet of Things (IoT), cybersecurity, cryptographic, network scalability, authentication mechanisms, distributed server architecture, session keys.*

Дата першого надходження статті до видання: 14.02.2026
Дата прийняття статті до друку після рецензування: 10.03.2026
Дата публікації (оприлюднення) статті 11.05.2026