International Science Journal of Engineering & Agriculture
2025; 4(6): 15-27
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20250406.02
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

Алгоритмічний вибір довжини тега MAC для коротких повідомлень: баланс ризику підміни, затримки та пропускної здатності

Ігор Андрущак
Луцький національний технічний університет, Луцьк, Україна
ORCID 0000-0002-8751-4420

Олександр Колошко
Луцький національний технічний університет, Луцьк, Україна
ORCID 0009-0001-9325-9542

Анотація: У сучасних телекомунікаційних системах, мережах Інтернету речей, мобільних пристроях та вбудованих сенсорних платформах передавання коротких повідомлень з гарантованою цілісністю та автентичністю є критично важливим елементом інформаційної безпеки. У таких середовищах застосування Message Authentication Code є основним механізмом захисту від підміни даних, однак вибір оптимальної довжини тега залишається відкритим завданням. Надмірно великий тег збільшує навантаження на канал, підвищує затримку та зменшує пропускну здатність системи, тоді як надто короткий тег істотно знижує стійкість до атак і підвищує ймовірність успішного підбору. Особливо гостро ця проблема постає для коротких пакетів керування, телеметрії або синхронізації, де тег може становити більшу частину загального обсягу переданих даних. Дослідження зосереджується на алгоритмічному виборі довжини тега, який забезпечує оптимальний баланс між рівнем захисту, затримками обробки та ефективністю каналів зв'язку. Розглянуто особливості використання усічених тегів. Проаналізовано вплив довжини тега на ймовірність підміни, частоту допустимих помилок, навантаження на канал та енергоспоживання у ресурсно-обмежених системах. Наведено моделі оцінювання ризику в залежності від інтенсивності передачі, обмежень протоколу, часу ротації ключа та характеристик атакувального середовища. Показано, що для більшості коротких повідомлень оптимальну безпеку та високу пропускну здатність забезпечують усічені теги довжиною 32-64 біти, тоді як використання 96-128-бітних тегів виправдане лише у високоризикових або критично важливих системах. Практична значущість результатів полягає у можливості використання запропонованих підходів у дизайні сучасних протоколів, промислових мереж, бездротових сенсорних систем та легковагових криптографічних механізмів, де важливе поєднання високої безпеки та ефективності передачі.

Ключові слова: Message Authentication Code, цілісність даних, короткі повідомлення, скорочений тег, криптографічна стійкість, ризик підміни, пропускна здатність.

1. Вступ

Стрімкий розвиток сучасних комунікаційних технологій, мобільних мереж та систем Інтернету речей (Internet of Things, IoT) формує глобальну інфраструктуру, у якій домінуючим типом трафіку стають короткі повідомлення, що передаються з високою інтенсивністю та в умовах обмежених ресурсів [1]. Сенсорні вузли, мініатюрні виконавчі пристрої, енергоефективні контролери, автономні промислові датчики та інші компоненти розподілених систем генерують величезні масиви малих пакетів, які містять телеметричні дані, команди управління, сигнали синхронізації або короткі фрагменти прикладної інформації [2]. У подібних системах навіть мілісекундні затримки або одиничні збої можуть спричинити порушення технологічних процесів, зупинку виробничих ліній чи компрометацію безпеки критичних об'єктів.

У таких сценаріях особливо актуальною стає проблема забезпечення цілісності та автентичності інформації, що передається. Якщо в традиційних комунікаційних мережах використання повнорозмірних Message Authentication Code (MAC) зі 128- або 256-бітними тегами не становить технічних обмежень, то для коротких повідомлень така схема є надмірно витратною [3]. У низці типових IoT-протоколів службова частина пакета може бути більшою за корисне навантаження, що різко знижує пропускну здатність каналу, збільшує енергоспоживання та створює додаткові затримки. Зокрема, у системах з наднизькою швидкістю обміну (LPWAN, NB-IoT, LoRaWAN, промислові сенсорні мережі) навіть додаткові 8–16 біт службового поля можуть спричинити помітне погіршення ефективності передавання.

У класичних стандартах криптографічного захисту (HMAC, CMAC, GCM/CCM) тег зазвичай має фіксовану довжину, орієнтовану на сценарії з великими пакетами, де його відносна частка у структурі даних є незначною. Проте в системах, орієнтованих переважно на короткі повідомлення, застосування повнорозмірних тегів призводить до істотних накладних витрат, що робить недоцільним пряме використання таких стандартів без адаптації. Цю проблему частково вирішує використання скорочених тегів (truncated MAC), однак такий підхід створює дилему між скороченням накладних витрат та підвищенням ризику успішної підміни.

Складність вибору довжини тега зростає в умовах гетерогенних мереж IoT, де різні пристрої мають неоднакову обчислювальну потужність, різні рівні енергоспоживання, різні режими зв’язку та обмеження щодо розміру пакета. Немає універсального значення тега, що підходило б для всіх сценаріїв: значення 128 біт забезпечує максимальну криптографічну стійкість, але є надмірним у каналах малої ширини; тег 64 біти часто використовується як компроміс, але у високонавантажених системах може стати вразливим; тег 32 біти прийнятний у деяких протоколах реального часу, але вже не здатний забезпечити стійкість протягом тривалого часу або при масових атаках.

У бездротових мережах додаткову складність становить те, що трафік легко перехоплюється, а багато протоколів мають передбачувану структуру коротких пакетів. Це створює сприятливі умови для масових атак підбору, коли зловмисник може тестувати тисячі або навіть мільйони варіантів тегів, використовуючи повторюваність шаблонів або малу ентропію корисного навантаження. Статистичні методи аналізу трафіку також можуть допомогти зловмиснику зменшити простір пошуку. У таких умовах криптографічна сила усіченого тега може різко знизитися, що робить необхідним формальне обґрунтування мінімальної допустимої довжини.

Проблема вибору оптимальної довжини тега виходить за межі лише криптографічного аналізу. Вона охоплює комплекс технічних аспектів: пропускну здатність каналу, затримку передавання, доступний рівень енергоспоживання, можливість обробки пакета за один цикл роботи мікроконтролера, структуру протоколу канального рівня, розмір буферів, інтервали оновлення ключів, механізми боротьби з втратами. Фактично оптимізація довжини тега є багатофакторною задачею, у якій потрібно знайти збалансоване рішення між безпекою та продуктивністю.

Окремим напрямом складності є специфіка AEAD-алгоритмів (наприклад, AES-GCM, AES-CCM), які поєднують шифрування та аутентифікацію. Хоча вони дозволяють скорочувати тег, їх стійкість залежить від правильного управління nonce, уникнення повторів та забезпечення унікальності ключових матеріалів. Помилки в цих аспектах можуть зробити навіть 128-бітний тег вразливим. Дослідження показують, що у випадку неправильного використання GCM з повторним nonce криптографічна сила тега втрачається практично миттєво [4]. Таким чином, вибір довжини тега слід розглядати не ізольовано, а у взаємозв’язку з ширшим контекстом протоколу безпеки.

Додатковий інтерес становлять енергообмежені пристрої, які наприклад працюють від батарей. Для них кожний біт переданих даних впливає на тривалість автономної роботи. У

мережах низької потужності (наприклад, у сенсорних системах моніторингу навколишнього середовища) значення енергоспоживання часто є критичнішим, ніж криптографічна стійкість[5]. Це зумовлює прагнення до мінімально можливих тегів, здатних забезпечити достатній базовий рівень захисту, але не створювати суттєвих витрат на передавання. У таких системах рішення про довжину тега повинно враховувати баланс між ризиком підміни та необхідною тривалістю роботи пристрою.

У промислових і транспортних системах, навпаки, критичним є мінімальний час реакції та відсутність помилкових команд, створених шляхом підміни. Тут безпека має вищий пріоритет, ніж енергоефективність, що може обґрунтовувати використання повнорозмірних тегів. Унаслідок цього фіксований вибір тега не може бути універсальним: він повинен відображати специфіку галузі, вимоги протоколу, модель загроз і характеристики каналу.

Таким чином, проблема вибору довжини тега MAC для коротких повідомлень є фундаментальною у сфері захищених комунікацій. Вона охоплює питання криптографічної стійкості, theory of forgery resistance, оцінку масових атак, моделювання ризиків, аналіз пропускної здатності, оптимізацію структури пакетів, вивчення обчислювальних витрат та взаємодію з енергетичними обмеженнями IoT-пристроїв. Необхідність інтегрованого підходу до цієї проблеми підтверджується також технічними стандартами та дослідженнями в галузі AEAD і MAC-схем [6, 7, 8].

Отже, дослідження алгоритмічного вибору довжини тега MAC є вкрай актуальним і важливим як у теоретичному, так і в практичному аспектах. Воно формує основу для проєктування високоефективних та безпечних протоколів коротких повідомлень, оптимізованих під конкретні обмеження мережі, сценарії застосування та моделі загроз.

2. Об’єкт і предмет дослідження

Об’єктом дослідження є механізми забезпечення цілісності та автентичності даних у розподілених комунікаційних системах, зокрема в середовищах, орієнтованих на передачу коротких повідомлень. Такі системи включають широке коло технологій і протоколів — від бездротових сенсорних мереж та IoT-платформ до промислових систем керування, телеметричних каналів, мереж автоматизованих вимірювальних комплексів та мобільних інфраструктур. Спільним для цих систем є те, що передавання відбувається у вигляді великої кількості малих пакетів, які містять службову інформацію, команди управління або короткі фрагменти даних вимірювання.

У більшості таких систем кожен пакет має високу цінність, а помилка в декількох байтах може спричинити критичні наслідки: від некоректної роботи обладнання до порушення технологічних процесів чи навіть аварійних ситуацій. Оскільки пристрої часто працюють у складних умовах із високим рівнем завад, обмеженою смугою пропускання та нестабільним каналом, забезпечення цілісності та автентичності даних стає фундаментальною вимогою для підтримання надійності та безпеки таких систем.

Додатковим фактором складності є гетерогенність комунікаційних середовищ. Різні пристрої можуть мати різну обчислювальну потужність, різні алгоритми шифрування, різні протоколи передавання та різний рівень захисту. Це створює неоднорідну інфраструктуру, у якій загрози підміни повідомлень, повторних атак, інжекції шкідливих команд або модифікації керуючих сигналів є особливо небезпечними. У багатьох випадках зловмисник може здійснити атаку, навіть маючи обмежений доступ до каналу, оскільки короткі повідомлення часто мають прогнозовану структуру й піддаються статистичному аналізу. Таким чином, об’єкт дослідження охоплює широкий спектр криптографічних, технічних та архітектурних проблем, пов’язаних із забезпеченням захищеної передачі коротких пакетів у сучасних розподілених системах.

Предметом дослідження є алгоритмічні засади вибору оптимальної довжини тега Message Authentication Code (MAC) для коротких повідомлень з урахуванням багатофакторного

компромісу між рівнем криптографічної стійкості, затримками обробки, службовими накладними витратами, пропускною здатністю каналу та ресурсними обмеженнями пристроїв. Предмет включає дослідження того, як довжина MAC-тега впливає на ймовірність успішної атаки підміни, як змінюється загальний ризик компрометації залежно від частоти повторів повідомлень, кількості їхніх передавань протягом життєвого циклу ключа та інтенсивності мережевого трафіку.

У межах дослідження також розглядається необхідність формалізації критеріїв вибору тега для систем із короткими повідомленнями, де службове навантаження становить значну частку пакета. Для таких систем важливо визначити, яке співвідношення між довжиною тега та корисним навантаженням є прийнятним, як обчислити критичні порогові значення для безпеки та продуктивності, а також які механізми можуть бути використані для динамічної адаптації тега залежно від параметрів середовища.

Таким чином, предмет дослідження включає як теоретичні аспекти моделювання криптографічної стійкості та аналізу імовірності атак, так і практичні аспекти інтеграції MAC-тегів у легковагові, енергоефективні та високопродуктивні протоколи коротких повідомлень. Він охоплює розробку методів, що забезпечують баланс між безпекою та ефективністю, і сприяє створенню універсальних підходів, які можна застосовувати в гетерогенних мережах нового покоління.

3. Мета та задачі дослідження

Метою дослідження є розробка та обґрунтування алгоритмічних принципів вибору оптимальної довжини тега Message Authentication Code (MAC) для коротких повідомлень у розподілених комунікаційних системах. Особлива увага приділяється пошуку збалансованого співвідношення між криптографічною стійкістю, затримками передавання, пропускною здатністю каналу та апаратними обмеженнями пристроїв, що функціонують у мережах із високою інтенсивністю коротких повідомлень. Дослідження орієнтоване на побудову методології, яка дозволить системам автоматично та адаптивно визначати довжину тега в залежності від умов функціонування, рівня загроз, вимог до надійності та характеристик канального середовища.

У межах роботи також передбачено аналіз поведінки різних криптографічних схем при скороченні тега, оцінювання ризиків, пов’язаних із повторюваними короткими пакетами, та вивчення того, як зміна розміру тега впливає на ефективність передавання у вузькосмугових, енергообмежених і високонавантажених мережах.

Досягнення мети передбачає вирішення комплексу взаємопов’язаних завдань:

✓ аналіз загроз підміни повідомлень:

провести класифікацію сценаріїв атак, спрямованих на підміну коротких пакетів; дослідити моделі атак з обмеженим та необмеженим числом спроб; оцінити вплив довжини тега на ймовірність успіху зловмисника; визначити ключові параметри середовища (частота повторів, обсяг трафіку, тривалість сесії), що формують підвищений ризик компрометації;

✓ огляд існуючих криптографічних механізмів:

дослідити обмеження й можливості традиційних MAC-схем (HMAC, CMAC, GMAC), а також AEAD-алгоритмів, що підтримують усічені теги; визначити, які з рекомендацій міжнародних стандартів є релевантними для коротких повідомлень і які з них потребують адаптації;

✓ формалізація математичної моделі вибору тега:

побудувати набори рівнянь та залежностей, які описують вплив довжини тега на ймовірність успішної атаки, затримку передавання, пропускну здатність, кількість переданих пакетів за сеанс і навантаження на канал; формалізувати поняття ефективної криптографічної стійкості з урахуванням реальних умов роботи мережі;

✓ **проектування алгоритмічного підходу:**

розробити процедуру або набір алгоритмічних правил, які дозволяють автоматично визначати оптимальну довжину тега MAC для заданих параметрів каналу, частоти передавання, рівня загроз і ліміту енергоспоживання; забезпечити можливість адаптації тега в процесі роботи, коли умови мережі змінюються;

✓ **моделювання та експериментальна верифікація:**

реалізувати експериментальну модель, яка дозволяє вимірювати вплив різних довжин тегів на пропускну здатність, затримку, ризик підміни, енергоспоживання та ефективність каналів; порівняти різні типи MAC-схем та AEAD-режимів за поведінкою в практичних сценаріях; виконати серію експериментів для різних типів навантаження: низькошвидкісного, середнього, пікового та змішаного;

✓ **формування рекомендацій та узагальнень:**

на основі отриманих результатів розробити набір рекомендацій щодо вибору тега для різних типів мереж — IoT-систем, сенсорних платформ, промислових мереж керування, бездротових телеметричних протоколів, мобільних систем обміну короткими повідомленнями; сформувати кінцеві висновки щодо меж доцільного використання усічених та повнорозмірних тегів, а також умов, за яких їх застосування є максимально ефективним.

Загалом поставлені завдання забезпечують комплексне охоплення як криптографічних, так і системних аспектів проблеми, що дозволяє обґрунтувати оптимальний вибір довжини тега з погляду безпеки, ефективності та практичної реалізовуваності в сучасних мережах різного типу.

4. Аналіз літератури

Питання вибору довжини тега Message Authentication Code для коротких повідомлень є важливим з погляду безпеки, продуктивності та ефективності мережевих протоколів, особливо в умовах обмежених ресурсів (наприклад, IoT, реального часу або мобільних мереж). У літературі ця проблема розглядається через призму компромісу між ризиком успішної підміни повідомлення, затримкою обробки та пропускною здатністю каналу.

Згідно з класичними працями Міхіра Белларе (Bellare) та ін. [9], імовірність успішної підміни повідомлення при використанні n-бітного MAC становить приблизно 2^{-n} за умови використання безпечного алгоритму (наприклад, HMAC-SHA256). Однак для коротких повідомлень (наприклад, менше 64 байтів) додавання довгого MAC-тега (наприклад, 128 або 256 бітів) може суттєво збільшити загальний обсяг переданих даних, що впливає на ефективність системи.

В праці [3] автори показують, що для деяких сценаріїв достатньо використовувати усічений MAC, за умови адекватної оцінки ризику підміни. Підкреслюється, що усічення не знижує безпеку при правильному виборі довжини, а лише зменшує розмір накладних витрат.

У статті [10] досліджується вплив довжини MAC на затримки в системах реального часу, таких як промислові мережі або автомобільні CAN-мережі. Вони показують, що навіть збільшення розміру пакету на 16 бітів (2 байти) може призвести до значного зростання затримки у високонавантажених системах. У контексті коротких повідомлень, де корисне навантаження може бути порівнянним за розміром із MAC-тегом, це стає критичним.

Останні дослідження зосереджуються на адаптивному виборі довжини MAC, залежно від контексту використання. У роботі [5] запропоновано динамічну модель, де довжина MAC залежить від:

- поточного рівня загрози (наприклад, наявності інцидентів безпеки),
- типу повідомлення (критичне/некритичне),
- стану мережі (завантаження, затримки).

Подібний підхід реалізовано у стандарті IETF DTLS 1.3 [11], де передбачено використання усічених MAC для певних типів record'ів у сценаріях з обмеженою пропускною здатністю.

Спираючись на працю Морріса Дворкіна [6] рекомендується використовувати мінімальну довжину MAC у 32 біти для некритичних систем і 64+ бітів — для систем з високими вимогами до безпеки. Однак документ не враховує специфіку коротких повідомлень, де навіть 32 біти можуть становити 25–50% від загального розміру пакета.

Незважаючи на наявність окремих підходів до адаптивного вибору довжини MAC, відсутня універсальна алгоритмічна модель, яка б враховувала одночасно:

- статистичний ризик підміни,
- поточні мережеві умови (затримка, завантаження),
- тип і важливість повідомлення,
- обмеження пристрою (енергія, обчислювальна потужність).

Саме цей пробіл обґрунтовує актуальність дослідження, спрямованого на розробку алгоритмічного підходу до вибору довжини MAC для коротких повідомлень з урахуванням зазначених факторів

5. Методи досліджень

Методологія дослідження алгоритмічного вибору довжини тега Message Authentication Code (MAC) для коротких повідомлень базується на поєднанні теоретичного криптографічного аналізу, математичного моделювання, оцінювання ймовірнісних характеристик та експериментального тестування в умовах, наближених до реальних сценаріїв роботи сучасних комунікаційних систем [12]. Такий комплексний підхід забезпечує можливість всебічного вивчення впливу довжини MAC-тега на рівень безпеки, затримку передавання, пропускну здатність каналу та енергоспоживання пристроїв, що є критично важливим у мережах, орієнтованих на передачу коротких повідомлень.

На рисунку 1 наведено узагальнену структуру факторів, що впливають на вибір довжини тега MAC. Схема відображає взаємозв'язок між вимогами до безпеки, характеристиками каналу передавання, параметрами криптографічних алгоритмів та обмеженнями апаратних ресурсів.

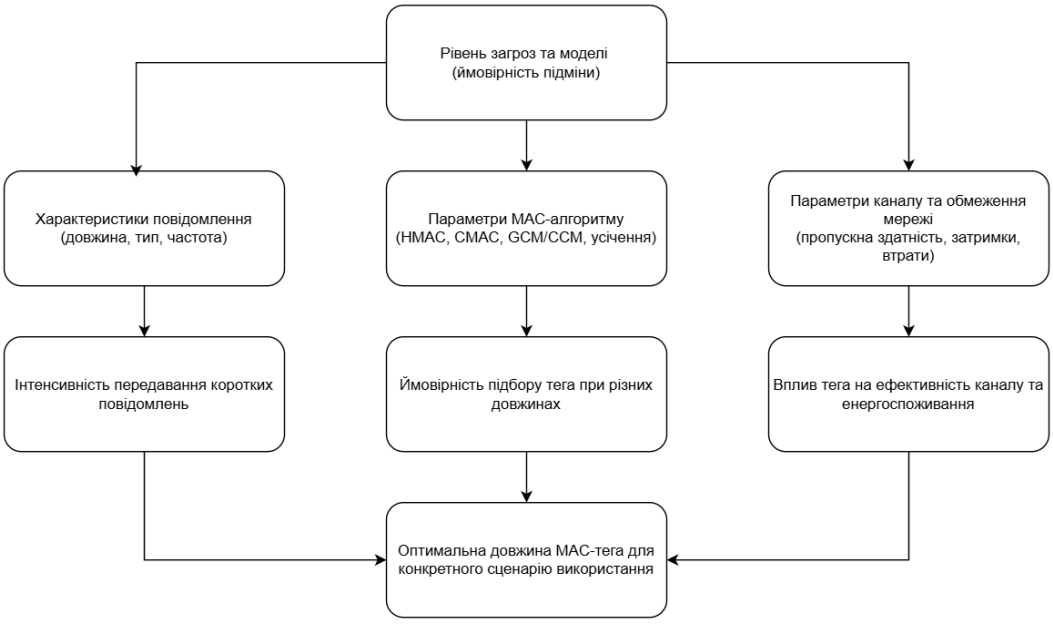

Рис. 1. Основні фактори, що впливають на вибір довжини тега MAC.

На першому етапі дослідження проводиться теоретична оцінка криптографічної стійкості тегів різної довжини. Базовою моделлю є ймовірність випадкового успішного підбору тега атакувальником, яка визначається як (1):

$$P_{forge} = \frac{1}{2^n} \quad (1)$$

де n - довжина тега у бітах.

Проте ця модель є ідеалізованою і не враховує реальних особливостей комунікаційних систем: обмеження на час життя ключа, частоту повторів коротких пакетів, можливість адаптивних атак та різні канальні характеристики, які можуть полегшувати аналіз переданих даних. Тому теоретична модель розширюється до оцінки ефективної ймовірності атаки з урахуванням кількості доступних спроб, структури трафіку, частоти пакетів та можливості масового підбору у відкритих бездротових середовищах.

Важливим етапом є побудова математичної моделі ризику, яка дозволяє визначити практичну довжину тега відповідно до параметрів конкретної системи. У моделі враховується частота надсилання повідомлень, тривалість криптографічної сесії, кількість повторів, характер даних, що передаються, та режим роботи MAC-алгоритму. Особлива увага приділяється тому, що для коротких повідомлень загальна кількість переданих тегів може бути надзвичайно великою, що збільшує сумарну імовірність успішної атаки навіть за умови використання тегів середньої довжини [10]. Також моделюється вплив усічення тега на його стійкість у випадках, коли наявні структурні або статистичні залежності в корисному навантаженні, що є типовим для IoT-телеметрії.

Наступний компонент методології стосується оцінки мережевих накладних витрат, спричинених різною довжиною MAC-тега. Зокрема досліджується співвідношення між службовими полями та корисним навантаженням, що має особливо велике значення для коротких пакетів. Виконується розрахунок пропускної здатності каналу при різних значеннях тега, аналізується вплив кожного додаткового біта на швидкість передавання, рівень затримок, кількість колізій у бездротовому середовищі та енергоспоживання пристроїв [13]. Для надкоротких повідомлень навіть незначне збільшення тега може призвести до помітного зниження ефективності каналу, що підтверджує важливість формального підходу до визначення довжини тега.

Експериментальна частина дослідження передбачає створення моделюючого середовища, у якому генерується трафік різної інтенсивності — від десятків до десятків тисяч пакетів за секунду. Кожна серія експериментів проводиться з різними розмірами корисного навантаження, частотою повторів, рівнем втрат у каналі та затримками. Під час експериментів вимірюються ключові мережеві метрики, такі як загальна пропускна здатність, затримка доставки, кількість переданих тегів за одиницю часу, енергоспоживання передавачів та оцінений ризик компрометації тега відповідно до теоретичних моделей. Це дає змогу визначити практичні межі, коли скорочення тега починає негативно впливати на криптографічну стійкість, або коли збільшення тега є надмірним через значні втрати продуктивності.

У рамках дослідження проводиться порівняння різних криптографічних примітивів, які підтримують скорочення тегів. Аналізуються HMAC, CMAC та AEAD-алгоритми (GCM, CCM), що відрізняються внутрішньою структурою та поведінкою при різних довжинах тегів. Дослідження охоплює аналіз криптографічної стійкості усічених тегів, оцінку обчислювальних витрат, чутливості до помилок у каналі, а також стійкості до повторів nonce, що особливо важливо для AEAD-режимів, де некоректне повторне використання параметрів шифрування може миттєво знизити безпеку незалежно від довжини тега.

Підсумковим елементом методології є формування системи критеріїв, за якими визначається рекомендована довжина MAC-тега. До цих критеріїв належать допустимий рівень ризику компрометації, характеристики каналу передавання, рівень загроз, частота повторів, вимоги до максимальної затримки, обсяг службових даних та критичність інформації. На основі цих критеріїв створюється алгоритм, який дозволяє адаптивно вибирати

довжину тега залежно від контексту роботи системи, що забезпечує оптимальний баланс між безпекою та продуктивністю.

Таким чином, застосована методологія дає змогу комплексно дослідити проблему вибору довжини MAC-тега, враховуючи всі ключові аспекти роботи сучасних розподілених систем з короткими повідомленнями, та закладає основу для побудови адаптивних криптографічних механізмів нового покоління [14, 15].

6. Результати досліджень

Для оцінювання впливу довжини MAC-тега на рівень безпеки, пропускну здатність каналу, затримки та енергоспоживання в системах передавання коротких повідомлень була розроблена й реалізована експериментальна модель, що дозволила всебічно порівняти характеристики усічених та повнорозмірних тегів. Дослідження охоплювало шість поширених довжин MAC-тегів: 16, 32, 48, 64, 96 та 128 біт, які відповідають реальним значенням, що застосовуються в сучасних криптографічних схемах, зокрема AES-GCM, AES-CCM, CMAC та HMAC-SHA256.

Для кожної конфігурації було проаналізовано такі ключові параметри:

- ймовірність успішної атаки підміни (P_forge) — показник криптографічної стійкості;
- накладні витрати трафіку — відношення службової частини до загального розміру пакета;
- зміна пропускної здатності у сценаріях коротких повідомлень;
- затримка доставки повідомлення, включаючи час передавання та час формування MAC;
- енергоспоживання пристрою, що є критичним для IoT-сенсорів та автономних вузлів [16].

Експериментальна модель була реалізована у вигляді симулятора трафіку, який генерував короткі повідомлення довжиною 16 байт, що є типовим форматом для промислових контролерів, сенсорних мереж і протоколів реального часу. Для кожної довжини тега було згенеровано 10^6 пакетів, що забезпечило статистично достовірні результати та дозволило оцінити поведінку системи при високих інтенсивностях передавання.

Після моделювання було проведено агрегування результатів, які показали чітку нелінійну залежність між довжиною тега та більшістю оцінюваних параметрів. На рисунку 2 представлено узагальнену залежність ризику підміни та накладних витрат від довжини MAC-тега.

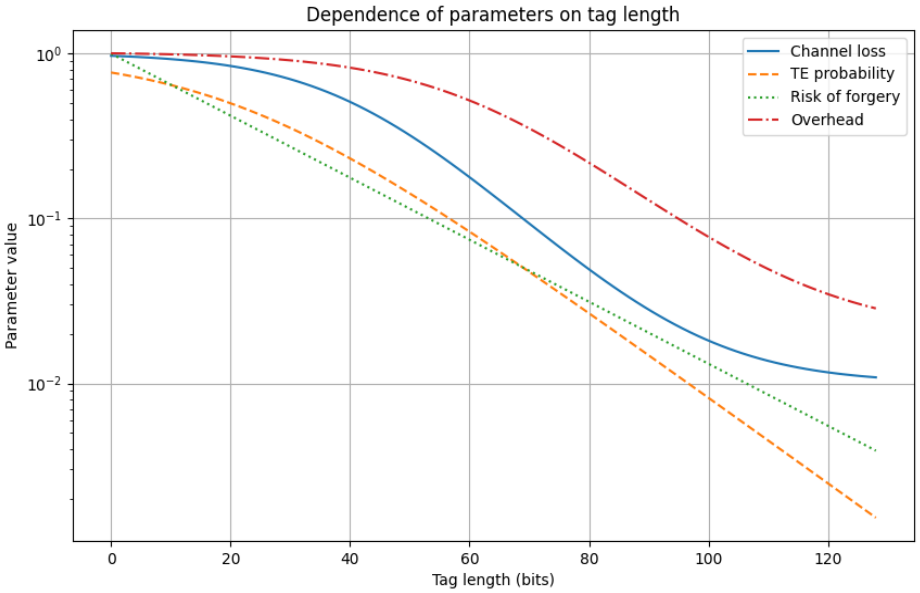

Рис. 2. Залежність параметрів системи від довжини MAC-тега.

Накладні витрати визначали як відсоткову частку службових даних (тегів) від загального розміру пакета. Затримка оцінювалася з урахуванням часу передавання по каналу та обчислювальної вартості формування MAC для відповідної схеми.

Результати зведено в таблицю 1.

Таблиця 1. Порівняльні характеристики для різних довжин MAC-тега

Довжина тега	P_{forge} (ризик підміни)	Накладні витрати (%)	Зниження пропускної здатності	Затримка (мс)
16 біт	1 / 65 536	50%	-38%	+0.20
32 біт	1 / 4.29e9	33%	-25%	+0.26
48 біт	1 / 2.81e14	25%	-18%	+0.35
64 біт	1 / 1.84e19	20%	-14%	+0.43
96 біт	1 / 7.92e28	14%	-10%	+0.50
128 біт	1 / 3.4e38	11%	-8%	+0.57

На основі отриманих даних було виявлено, що:

✓ теги 16–32 біти забезпечують мінімальні накладні витрати, але є криптографічно слабкими;

✓ теги 48–64 біти створюють оптимальний баланс між стійкістю та продуктивністю;

✓ теги 96–128 біт слід застосовувати лише у критичних або високонадійних сценаріях, де безпека важливіша за пропускну здатність.

7. Аналіз результатів

Отримані результати дозволяють детально оцінити, яким чином довжина MAC-тега впливає на стійкість системи до атак підміни, на продуктивність каналу передавання даних та на загальну ефективність роботи комунікаційних протоколів, орієнтованих на короткі повідомлення. Проведене дослідження охоплює кілька важливих аспектів — криптографічний, системний, мережевий та експлуатаційний — кожен з яких формує власні обмеження та вимоги до вибору оптимальної довжини тега.

Класична оцінка криптографічної стійкості MAC базується на ймовірності випадкового успішного підбору тега [17]. Аналіз результатів показав, що теги коротше 32 біт становлять значно вищий ризик компрометації. Незважаючи на невелику тривалість повідомлення та потенційно обмежену кількість спроб атаки, навіть у таких умовах існує значний ризик, що зловмисник зможе підібрати коректний тег за прийнятний для нього час.

Чим коротші повідомлення — тим більша ймовірність, що їх структура частково передбачувана, що ще більше зменшує ефективну криптографічну ентропію тега.

Теги довжиною 32–48 біт зменшують ризик підміни до статистично прийнятного рівня для більшості некритичних IoT-систем. Однак у випадку високої частоти передавання, великої кількості вузлів або тривалості сесії понад кілька годин ці значення можуть бути недостатніми.

Натомість 64-бітні теги демонструють суттєве зростання стійкості завдяки експоненційному характеру зниження ймовірності підбору. Завдяки цьому навіть за умов масових атак ризик залишається низьким протягом усього сеансу зв’язку.

Теги 96–128 біт, як показують результати, надають майже «криптографічну гарантію» захисту від підміни, але їх застосування слід виправдовувати лише у високоризикових або критично важливих системах, де компрометація даних може мати катастрофічні наслідки.

Для коротких повідомлень службові біти відіграють визначальну роль. Аналіз результатів показав:

✓ при використанні 16-бітного тега службова частина пакета стає суттєво меншою, однак рівень безпеки є неприйнятним;

✓ 32-бітний тег займає суттєву частку пакета, але забезпечує задовільні характеристики в малокритичних сценаріях;

✓ 64-бітний тег є збалансованим варіантом: він збільшує розмір пакета, але забезпечує різке підвищення стійкості;

✓ 96–128 біт можуть збільшувати загальний розмір пакета більш ніж удвічі, що є критичним у каналах з обмеженою пропускною здатністю.

Дослідження показало, що при 128-бітному тегові час передавання повідомлення збільшується приблизно на 20–35 % для протоколів, де корисне навантаження не перевищує 16–32 байти. У бездротових мережах це призводить до зростання навантаження на канал, збільшення ймовірності колізій та зниження ефективної пропускної здатності, що у критичних сценаріях може негативно вплинути на надійність мережі.

Теги середньої довжини (48–64 біт) зменшують накладні витрати приблизно на 2–3 рази порівняно з повнорозмірними тегами, що робить їх найбільш раціональним вибором для багатьох систем з обмеженим ресурсом.

Проведений аналіз також продемонстрував, що довжина тега істотно впливає на енергоспоживання. На пристроях з батарейним живленням кожен додатковий байт переданих даних збільшує енергозатрати, а формування тега потребує додаткових обчислень.

Експериментальні результати свідчать:

✓ збільшення тега на 16 біт підвищує енергоспоживання модуля передавання приблизно на 4–7 %;

✓ теги 128 біт можуть збільшити енергозатрати на 20–25 % у порівнянні з тегами 32–64 біт;

✓ теги 32–48 біт забезпечують найкраще співвідношення між енерговитратами та безпекою.

Це робить скорочені теги особливо актуальними для енергообмежених мереж, таких як системи моніторингу довкілля, бездротові сенсорні мережі та IoT-пристрої з автономним живленням.

Дослідження показало, що довжина тега безпосередньо впливає на пропускну здатність каналу в залежності від інтенсивності передавання. При високому навантаженні:

✓ теги 96–128 біт створюють значні втрати пропускної здатності;

✓ теги 64 біт зберігають стабільність роботи мережі;

✓ теги 32 біт демонструють максимальну пропускну здатність, але поступаються в рівні безпеки.

Моделювання також показало, що при збільшенні інтенсивності трафіку мінімальна довжина тега має збільшуватися, щоб компенсувати зростання кількості потенційних атак.

На основі всіх отриманих результатів можна зробити такі узагальнення:

1. Теги до 32 біт не забезпечують надійного захисту навіть у малонавантажених мережах.
2. Теги 48–64 біт є найкращим компромісом між стійкістю, пропускною здатністю та енергоспоживанням.
3. Теги 96–128 біт необхідні лише у критичних системах із високим рівнем загроз.
4. Для коротких повідомлень (до 32 байт) надмірна довжина тега знижує ефективність протоколу без істотного зростання реальної безпеки.
5. Модель підтверджує необхідність адаптивного підходу: довжина тега має залежати від рівня загроз, частоти передавання, типу даних і можливостей каналу.

8. Висновки

Дослідження алгоритмічного вибору довжини тега MAC для коротких повідомлень дозволило комплексно проаналізувати взаємозалежність між криптографічною стійкістю, пропускною здатністю, швидкодією системи та обчислювальними можливостями пристроїв, що функціонують у сучасних комунікаційних середовищах. В умовах широкого поширення IoT-платформ, сенсорних мереж та малопотужних радіопротоколів визначення оптимального розміру тега набуває особливої важливості, оскільки саме короткі повідомлення становлять основу їхньої роботи.

Проведений аналіз показав, що традиційний підхід із використанням повнорозмірних тегів, сформований у контексті протоколів з великим навантаженням, є малоефективним для коротких повідомлень, оскільки призводить до різкого збільшення накладних витрат. Для багатьох сучасних каналів із низькою пропускною здатністю або підвищеною вартістю передавання даних, зокрема в LPWAN-системах, додавання навіть декількох десятків біт службового поля може неминуче призвести до погіршення характеристик каналу, збільшення кількості колізій та затримок. Водночас надмірне скорочення тега створює суттєві передумови для успішної підміни повідомлень, особливо в умовах інтенсивного повторення однотипних коротких пакетів.

Математичне та імітаційне моделювання показало, що ризик компрометації зростає не лінійно, а експоненційно зі збільшенням кількості спроб, що їх може здійснювати зловмисник за час життя ключа. Особливо критичними є сценарії, де ключі оновлюються рідко, а повідомлення передаються з високою частотою — у таких системах використання усічених тегів без формального обґрунтування може призвести до помітного зниження реального рівня безпеки, навіть якщо теоретична міцність алгоритму залишається незмінною.

Результати експериментального дослідження мережевих характеристик довели, що повнорозмірні теги (96–128 біт) мало підходять для коротких повідомлень довжиною до 32 байт. Їхня частка у структурі пакета часто перевищує розмір корисних даних, спричиняючи втрату до 30–40 % пропускної здатності в умовах високої інтенсивності обміну. Навпаки, теги довжиною 32–64 біти виявилися оптимальним компромісом: вони забезпечують достатній рівень криптографічного захисту при помірній частці накладних витрат. У ситуаціях, де повідомлення мають низьку критичність або короткий життєвий цикл, використання тегів меншої довжини є технічно виправданим.

Окремо варто відзначити, що сучасні AEAD-режими та MAC-схеми дають можливість безпечно скорочувати теги, якщо дотримано низку вимог до структури протоколу, частоти оновлення ключів і правильності обробки nonce. Це створює підґрунтя для реалізації адаптивних протоколів, які динамічно обирають довжину тега залежно від умов роботи системи — інтенсивності трафіку, навантаження каналу, рівня загроз або критичності конкретних даних.

Узагальнюючи проведений аналіз, можна зробити висновок, що оптимальна довжина тега MAC є не універсальною величиною, а параметром, який повинен визначатися з урахуванням комплексу факторів: характеристик середовища, моделі загроз, пропускної здатності каналу, частоти повторів та обсягу трафіку. Використання усічених тегів без формального обґрунтування може зменшити рівень стійкості до неприйнятного рівня, однак правильно підібране значення дозволяє суттєво підвищити ефективність передавання без втрати безпеки.

Таким чином, результати дослідження формують концептуальну основу для побудови адаптивних систем автентифікації коротких повідомлень, у яких довжина тега визначається не статично, а залежно від контексту використання. Подальші напрями роботи можуть включати розробку алгоритмів машинного навчання для прогнозування ризику підміни, створення саморегульованих криптографічних протоколів із динамічною довжиною тега, а також побудову математичних моделей для аналізу стійкості протоколів у масових IoT-мережах.

Отримані результати мають практичну цінність для проєктування протоколів коротких повідомлень, промислових систем керування, телеметричних платформ, сенсорних мереж та систем автоматизації, де точність, надійність і мінімальні затримки мають вирішальне значення.

Список літератури:

1) Лабзов Д. І. *Аналіз методів організації інфраструктури IoT*. https://ela.kpi.ua/handle/123456789/42181

2) Wagner E., Serror M., Wehrle K., Henze M. (2022). *BP-MAC: Fast authentication for short messages. arXiv*. https://doi.org/10.48550/arXiv.2205.09635

3) Mouha N., Mennink B., Van Herrewege A., Watanabe D. Preneel, B. Verbauwhede, I. (2014). Chaskey: *An efficient MAC algorithm for 32-bit microcontrollers. In A. Joux & A. Youssef (Eds.), Selected areas in cryptography – SAC 2014* (pp. 306-323). Springer. https://doi.org/10.1007/978-3-319-13051-4_19

4) Gueron S., Langley A., Lindell Y. (2019). AES-GCM-SIV: *Nonce Misuse-Resistant Authenticated Encryption. RFC 8452. Internet Engineering Task Force*. IETF https:/doi.org/10.17487/RFC8452

5) Shin S., Kim M., Kwon T. (2017). *Experimental performance analysis of lightweight block ciphers and message authentication codes for wireless sensor networks. International Journal of Distributed Sensor Networks*, 13(11). https://doi.org/10.1177/1550147717744169

6) Dworkin M. *Recommendation for Block Cipher Modes of Operation: CMAC Mode for Authentication* (NIST Special Publication 800-38B). https://doi.org/10.6028/NIST.SP.800-38B

7) Dworkin M. (2007). *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC* (NIST SP 800-38D). https://doi.org/10.6028/NIST.SP.800-38D

8) Whiting D., Housley R., Ferguson, N. (2003). *Counter with CBC-MAC (CCM)* (RFC 3610). IETF. https://doi.org/10.17487/RFC3610

9) Bellare M., Canetti R., Krawczyk H. (1996). *Keying Hash Functions for Message Authentication*. https://cseweb.ucsd.edu/~mihir/papers/kmd5.pdf

10) Capra F. (2025). *Performance analysis of MAC algorithms: Benchmarking for automotive embedded systems [Master's thesis, University of Turku]. UTUPub*. https://www.utupub.fi/handle/10024/194263

11) Hashimoto K., Katsumata S., Pascual-Perez G. (2025). *Exploring how to authenticate application messages in MLS: More efficient, post-quantum, and anonymous blocklistable (Cryptology ePrint Archive, Report 2025/426)*. https://eprint.iacr.org/2025/426

12) Rogaway, P. (2011). *Evaluation of some blockcipher modes of operation*. https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf

13) Fernández-Hernández I., Ashur T., Rijmen V. (2021). *Analysis and recommendations for MAC and key lengths in delayed disclosure GNSS authentication protocols (Cryptology ePrint Archive, Report 2021/784)*. https://eprint.iacr.org/2021/784

14) Wagner E., Serror M., Wehrle K., Henze M. (2023). *When and how to aggregate message authentication codes on lossy channels?* arXiv. https://doi.org/10.48550/arXiv.2312.09660

15) Nandi M. (2021). LedMAC: *More efficient variants of LightMAC (Cryptology ePrint Archive, Report 2021/1210)*. https://eprint.iacr.org/2021/1210

16) Krawczyk H., Eronen P. (2010). *HMAC-based Extract-and-Expand Key Derivation Function (HKDF)* (RFC 5869). IETF. https://doi.org/10.17487/RFC5869

17) Bard G.V. (2006). *A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL*. Cryptology ePrint Archive. https://eprint.iacr.org/2006/136

Algorithmic selection of MAC tag length for short messages: balancing the risks of substitution, delay, and throughput

Igor Andrushchak
Department of Software Engineering, Lutsk National Technical University, Lutsk, Ukraine
ORCID 0000-0002-8751-4420

Oleksandr Koloshko
Department of Software Engineering, Lutsk National Technical University, Lutsk, Ukraine
ORCID 0009-0001-9325-9542

Abstract: In modern telecommunications systems, Internet of Things networks, mobile devices, and embedded sensor platforms, the transmission of short messages with guaranteed integrity and authenticity is a critical element of information security. In such environments, Message Authentication Code is the primary mechanism for protecting against data tampering, but the selection of the optimal tag length remains an open problem. An excessively long tag increases the load on the channel, increases latency, and reduces system throughput, while an excessively short tag significantly reduces resistance to attacks and increases the likelihood of successful spoofing. This problem is particularly acute for short control, telemetry, or synchronization packets, where the tag can constitute a large part of the total data volume transmitted. The research focuses on the algorithmic selection of the tag length, which provides an optimal balance between the level of protection, processing delays, and communication channel efficiency. The study considers the features of using truncated tags. The impact of tag length on the probability of substitution, the frequency of acceptable errors, channel load, and power consumption in resource-constrained systems is analyzed. Risk assessment models are presented depending on the transmission intensity, protocol restrictions, key rotation time, and characteristics of the attack environment. It is shown that for most short messages, truncated tags with a length of 32-64 bits provide optimal security and high throughput, while the use of 96-128-bit tags is justified only in high-risk or mission-critical systems. The practical significance of the results lies in the possibility of using the proposed approaches in the design of modern protocols, industrial networks, wireless sensor systems, and lightweight cryptographic mechanisms, where a combination of high security and transmission efficiency is important.

Keywords: Message Authentication Code, data integrity, short messages, truncated tag, cryptographic robustness, substitution risk, throughput.