DOI: https://doi.org/10.36910/6775-2524-0560-2024-57-06
УКД 004.62
**Іванчук Олексій Вікторович**, аспірант
https://orcid.org/0000-0002-2058-4707
**Козел Віктор Миколайович**, к.т.н., доцент
https://orcid.org/0000-0002-2627-2499
Херсонський національний технічний університет, м. Хмельницький, Україна

# ДОСЛІДЖЕННЯ ВПЛИВУ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБСЯГИ ПАКЕТІВ ДАНИХ ПРОТОКОЛІВ ІНТЕРНЕТУ РЕЧЕЙ

**Іванчук О.В., Козел В.М. Дослідження впливу захисту інформації на обсяги пакетів даних протоколів інтернету речей.** У статті розглянуто проблему збільшення обсягів трафіку внаслідок використання шифрування. Для аналізу було обрано пакети даних стандартів Wi-Fi, Bluetooth, 6LoWPAN, а також протоколи ZigBee, WirelessHART і NB-IoT. Було визначено, які частини пакету шифруються і які алгоритми використовуються для цього. Wi-Fi, Bluetooth, ZigBee, 6LoWPAN і WirelessHART застосовують алгоритм AES із 128-бітним ключем, тоді як NB-IoT використовує 128-EEA2 із таким же розміром ключа. Обидва алгоритми (AES та 128-EEA2) вимагають, щоб обсяг даних був кратним розміру ключа, тому до корисних даних додається бітова послідовність для досягнення потрібного розміру. Це збільшує загальний обсяг пакету, що передається. Було проведено дослідження цього впливу, та побудовано графіки, що показують залежність обсягу доповнення від кількості корисних даних. Графіки мають пилкоподібну форму через те, що за певних обсягів корисних даних доповнення досягає максимального значення. Також були обчислені середні обсяги доповнень для кожного стандарту: Wi-Fi - 2.13%, Bluetooth - 10.64%, ZigBee - 24.81%, 6LoWPAN - 23.22%, WirelessHART - 23.08%, NB-IoT - 25.96%. Окремо досліджували середні значення доповнень для пакетів до 64 байт: Wi-Fi - 9.95%, Bluetooth - 16.31%, ZigBee - 8.00%, 6LoWPAN - 11.55%, WirelessHART - 10.12%, NB-IoT - 20.21%. За відсутності обмежень на розмір корисних даних найкращий результат показав стандарт Wi-Fi, а найгірший — NB-IoT. У випадках з обмеженим розміром корисних даних найкращі результати були у ZigBee, а найгірші - у NB-IoT.
**Ключові слова**: інтернет речей, протоколи, шифрування, Wi-Fi, Bluetooth, ZigBee, WirelessHART, 6LoWPAN, NB-IoT, AES.

**Ivanchuk O., Kozel V. Study of the impact of information protection on the volumes of data packets of Internet of Things protocols.** The article discusses the problem of increasing traffic volumes due to the use of encryption. Data packets of Wi-Fi, Bluetooth, 6LoWPAN standards, as well as ZigBee, WirelessHART and NB-IoT protocols were selected for analysis. It was determined which parts of the packet are encrypted and which algorithms are used for this. Wi-Fi, Bluetooth, ZigBee, 6LoWPAN and WirelessHART use the AES algorithm with a 128-bit key, while NB-IoT uses 128-EEA2 with the same key size. Both algorithms (AES and 128-EEA2) require the data to be a multiple of the key size, so a bit sequence is added to the payload to achieve the desired size. This increases the total size of the packet being transmitted. A study of this effect was carried out, and graphs were made showing the dependence of the amount of addition on the amount of useful data. The graphs have a sawtooth shape due to the fact that at certain volumes of useful data, the addition reaches its maximum value. The average volumes of additions for each standard were also calculated: Wi-Fi - 2.13%, Bluetooth - 10.64%, ZigBee - 24.81%, 6LoWPAN - 23.22%, WirelessHART - 23.08%, NB-IoT - 25.96%. The average values of add-ons for packets up to 64 bytes were studied separately: Wi-Fi - 9.95%, Bluetooth - 16.31%, ZigBee - 8.00%, 6LoWPAN - 11.55%, WirelessHART - 10.12%, NB-IoT - 20.21%. In the absence of restrictions on the size of useful data, the best result was shown by the Wi-Fi standard, and the worst by NB-IoT. In cases with limited payload size, ZigBee performed best and NB-IoT performed worst.
**Keywords**: Internet of Things, protocols, encryption, Wi-Fi, Bluetooth, ZigBee, WirelessHART, 6LoWPAN, NB-IoT, AES.

**Постановка проблеми.** Зростання кількості нових пристроїв Інтернету речей призводить до збільшення навантаження на середовище передачі, в якому вони функціонують. При використанні шифрування в протоколах передачі даних може збільшуватися обсяг інформації, що передається в пакеті даних. Тому важливо провести аналіз пакетів даних протоколів і стандартів Інтернету речей, щоб оцінити рівень впливу та вибрати оптимальний протокол або стандарт, де цей вплив є найменшим.

Данна стаття продовжує аналіз протоколів і стандартів Інтернету речей, розпочатий у роботі [1]. У ній було описано автоматизований процес вибору протоколів під час проєктування систем Інтернету речей за допомогою програмного забезпечення, яке на основі параметрів, введених користувачем, обирає оптимальні протоколи для використання в системі. Дослідження впливу шифрування дасть змогу вдосконалити цей процес, додавши додатковий критерій, що може стати вирішальним при виборі протоколів, якщо кілька з них матимуть схожі характеристики та відповідатимуть вимогам.

**Аналіз останніх досліджень і публікацій** У роботі [2] розглядається вплив шифрування на розміри пакетів медіа-даних, але в Інтернеті речей існують різні протоколи та стандарти, тому оцінити вплив шифрування на них, спираючись лише на дані роботи [2], неможливо.

У роботі [3] досліджується шифрування у мікроконтролерах, що використовується при розробці пристроїв Інтернету речей. Отримані результати показують, що шифрування впливає на час обробки даних, але при цьому не враховуються потенційні затримки під час передачі шифрованих даних.

**Формулювання мети дослідження**. Формулювання мети дослідження. Провести аналіз пакетів даних у протоколах та стандартах Інтернету речей для оцінки впливу шифрування на їх розміри. Визначити наявність додаткових даних у пакетах при шифруванні та їх обсяги, якщо такі є. Визначити протоколи та стандарти, у яких шифрування має найменший вплив на розміри пакетів даних.

**Виклад основного матеріалу дослідження**.

Найчастіше для Інтернету речей використовуються такі стандарти та протоколи: Wi-Fi, Bluetooth, ZigBee, WirelessHART, 6LoWPAN та NB-IoT.

Стандарт Wi-Fi використовується для організації бездротової локальної мережі. Для роботи мережі використовуються радіохвилі у частотному діапазоні 900 МГц, 2,4 ГГц або 5 ГГц відповідно до стандарту IEEE 802.11 [4]. У якості топології застосовується зірка, що передбачає наявність центрального координатора мережі (роутера), до якого підключаються всі пристрої. Зазвичай за допомогою Wi-Fi смартфони, планшети, ноутбуки та SMART-телевізори отримують доступ до Інтернету. З поширенням Інтернету речей Wi-Fi також почав використовуватися для підключення нових пристроїв до мережі Інтернет.

Усі пристрої, що підключені до Wi-Fi мережі, використовують єдиний для всіх частотний діапазон, через що часто виникають помилки через одночасну передачу даних декількома пристроями. Ця проблема вирішується за допомогою механізму уникнення колізій під час передачі у мережі – CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) [5]. При додаванні нових пристроїв до мережі збільшується обсяг даних, що передаються у мережі. Аналіз стандарту щодо методів шифрування дозволить визначити, чи має шифрування суттєвий вплив на обсяг трафіку одного пристрою, що може надовго блокувати середовище передачі.

Структура пакету даних стандарту Wi-Fi зображена на рисунку 1 [8].

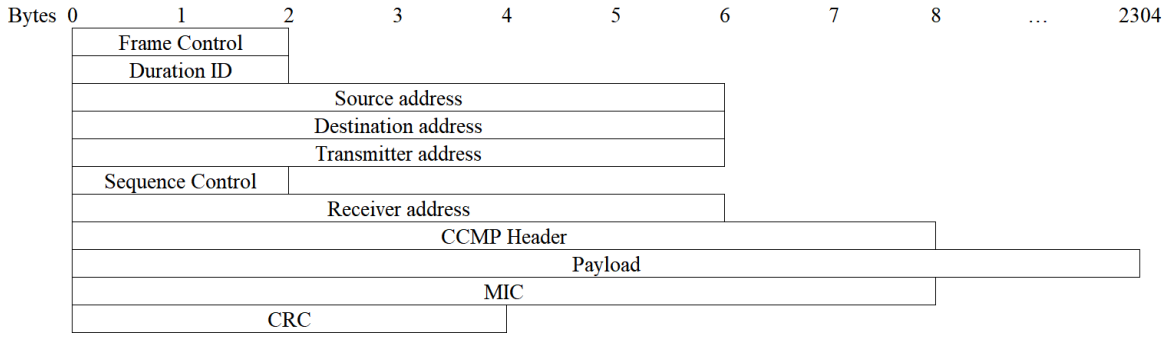


Рис. 1. Структура пакету даних Wi-Fi

Основну увагу потрібно приділити частинам пакету CCMP Header, Payload та MIC, які беруть участь у шифруванні даних. Для шифрування корисних даних використовується алгоритм AES у парі з протоколом CCMP [6, 7, 9]. Частина MIC – це код, який розраховується як контрольна сума корисних даних (Payload) у пакеті та дозволяє перевірити правильність передачі даних. Частини Payload та MIC шифруються як одне ціле. Алгоритм AES має кілька варіантів шифрування. Для шифрування даних у Wi-Fi використовується версія AES-CTR з ключем на 128 біт (16 байт). На вхід алгоритму подається лічильник, який збільшується з моменту старту. Для кожного блоку корисних даних використовуються унікальні значення лічильника, що зменшує ризик розшифровки сторонніми особами. На початку процесу шифрування корисні дані мають бути доповнені до розміру, кратного розміру ключа, що дорівнює 128 бітам. Доповнення початкових даних може сягати до 127 біт, що має додатковий негативний вплив на обсяг даних для передачі. Обсяг даних, отриманий після доповнення, не змінюється під час шифрування.

Другим доповненням до обсягу пакету даних є заголовок CCMP. У ньому зберігається номер пакету даних, порожній байт, зарезервований на майбутнє, та байт параметрів шифрування. У цьому байті 5 біт завжди встановлені у значення 1, що вказує на шифрування за допомогою AES. Біти 6-7 зберігають ідентифікатор ключа, за яким виконувалося шифрування, якщо ключі були заздалегідь

узгоджені. Біти 0-4 є зарезервованими на майбутнє. З цього випливає, що додатково додається один байт для шифрування, і загальний обсяг пакету даних збільшується від 8 до 8+127 = 135 біт, залежно від обсягу доповнення початкових даних. При малих обсягах розмір корисних даних може бути меншим за обсяг додаткової інформації, необхідної для шифрування.

Стандарт Bluetooth використовується для обміну даними на невеликі відстані (до 10 метрів) [10]. Як стандарт Інтернету речей, Bluetooth став використовуватися після появи енергоефективної версії Bluetooth LE [11]. Для обміну даними використовується радіоканал на частоті 2,4 ГГц. Як і Wi-Fi, стандарт використовує топологію "зірка" для своєї роботи. Стандарт має таку ж проблему з колізіями і використовує CSMA/CA для їх уникнення.

Структуру пакету даних стандарту Bluetooth наведено на рисунку 2.

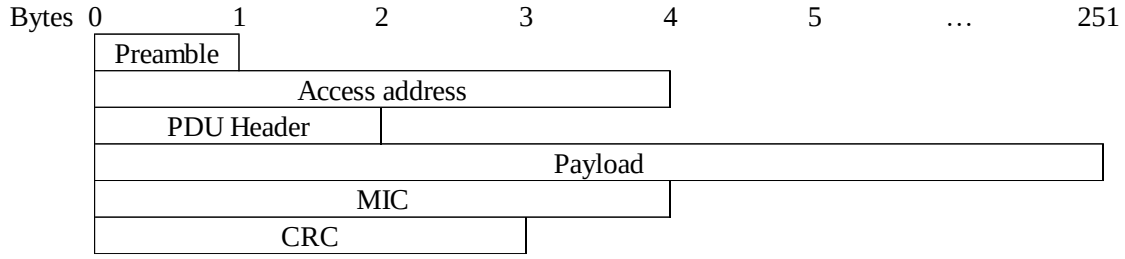


Рис. 2. Структура пакету даних Bluetooth

В стандарті Bluetooth є дві основі частини, що задіяні у шифруванні – Payload та MIC. Bluetooth має схожий з Wi-Fi алгоритм шифрування. Він використовує метод шифрування AES у версії AES-CTR з ключем на 128 біт [12]. Частина Payload відповідає за корисні дані, а MIC - за контрольну суму для перевірки цілісності корисних даних. Під час шифрування Payload та MIC об'єднуються та шифруються як одне ціле. Оскільки алгоритм AES вимагає, щоб довжина даних була кратна ключу шифрування (128 біт), то об'єднані дані доповнюються до кратності. На відміну від Wi-Fi, у стандарті Bluetooth немає додаткового байту з параметрами шифрування, тому максимальне збільшення розмірів пакету може складати до 127 біт.

Протокол ZigBee створювався для реалізації «розумного будинку» на основі стандарту IEEE 802.15.4 [13]. Протокол має 3 частотні радіодіапазони для роботи: 866 МГц у Європі, 915 МГц у США та Австралії та 2.4 ГГц в інших країнах [14]. Мережа ZigBee побудована на комірчастій топології, що дозволяє використовувати пристрої мережі для вільної маршрутизації трафіку, доки він не дійде до координатора мережі.

Структура пакету даних зображена на рисунку 3.

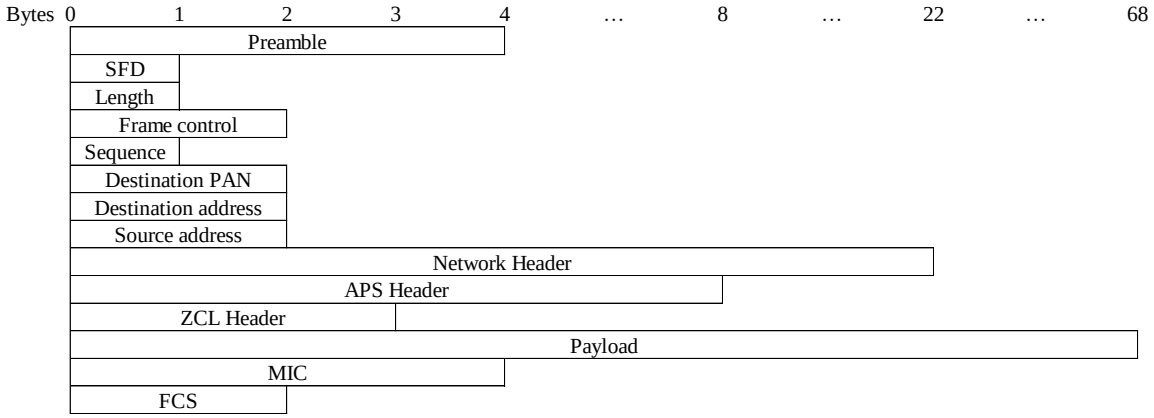


Рис. 3. Структура пакету даних ZigBee

У пакеті шифруються частини APS Header, ZCL Header та Payload. Частина Payload зберігає корисні дані, що передаються у пакеті. APS Header відповідає за контроль зв'язку з кластером, до якого належить пристрій, що передає дані. ZCL Header визначає напрямок передачі пакету між клієнтом та сервером, а також тип команди, що передається.

Для шифрування використовується алгоритм AES у версії AES-CTR з ключем шифрування на 128 біт [15]. Оскільки необхідно забезпечити кратність ключу, виконується доповнення пакету даних до кратності ключу, що може сягати до 127 біт, і це впливає на обсяги трафіку.

Окремо шифрується частина MIC за алгоритмом AES у версії AES-CBC. Після шифрування залишається лише старша частина з 4 байт. Оскільки розмір частини MIC є фіксованим, це не впливає на загальний розмір пакету даних.

Стандарт 6LoWPAN також створювався спеціально для Інтернету речей. У своїй основі він використовує стандарт IEEE 802.15.4 для роботи на нижчих рівнях моделі OSI [16]. Топологія використовує комірчасту мережу з частотою передачі 2,4 ГГц. Головною відмінністю від ZigBee є використання адресації за протоколом IPv6. Структура пакету зображена на рисунку 4 [19].

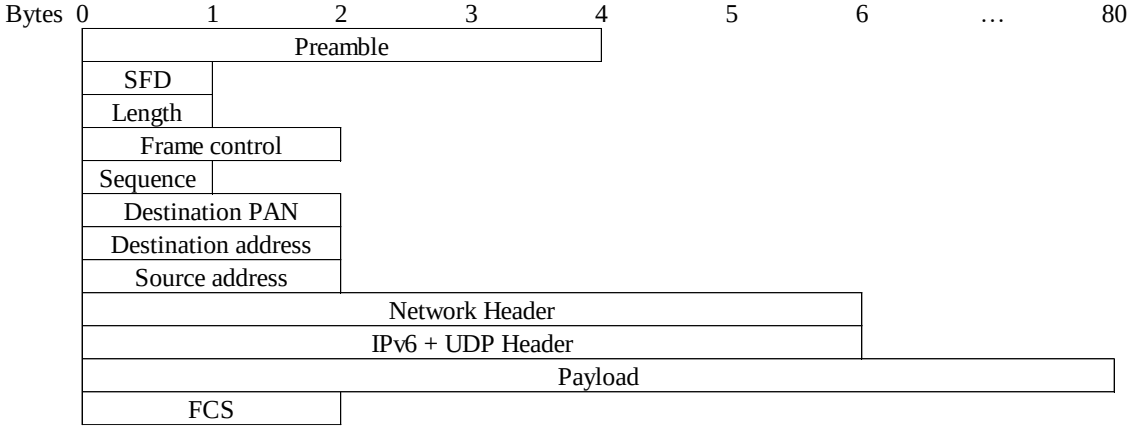


Рис. 4. Структура пакету даних 6LoWPAN

У пакеті даних шифруються частини IPv6+UDP Header та Payload. Частина Payload містить корисні дані. У IPv6+UDP Header зберігаються дані адресації за протоколом IPv6 та заголовки передачі даних за протоколом UDP.

Для шифрування використовується алгоритм AES у версії AES-CTR з ключем розміром 128 біт [17,18]. Під час шифрування ці частини об'єднуються в єдиний текст і шифруються разом. Для шифрування потрібне доповнення від 1 до 127 біт, що впливає на обсяг даних у пакеті.

Протокол WirelessHART більше схожий на ZigBee, ніж на 6LoWPAN. Він також побудований на основі стандарту IEEE 802.15.4 [20, 21]. На рисунку 5 зображено пакет даних цього протоколу.

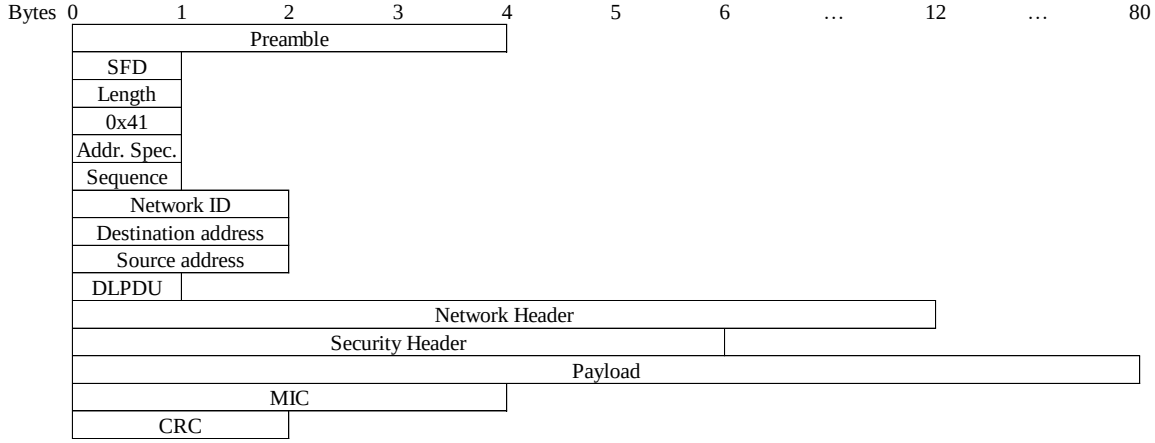


Рис. 5. Структура пакету даних WirelessHART

У пакеті даних шифруються частини Security Header та Payload. Для шифрування використовується алгоритм AES у версії AES-CBC [22]. Алгоритм вимагає доповнення даних до розміру ключа, який складає 128 біт. Через це обсяг доповнення може становити від 1 до 127 бітів, що збільшує розмір пакету.

NB-IoT — це протокол Інтернету речей, який використовує стільникову мережу на частоті радіоканалу 800, 900 або 1800 МГц, що забезпечує з'єднання пристроїв на відстані кількох

кілометрів [23]. Значну частину своєї специфікації протокол успадкував від LTE, що дозволяє розгортати систему на вже існуючому обладнанні стільникових мереж.

На рисунку 6 зображено структуру пакету даних NB-IoT.

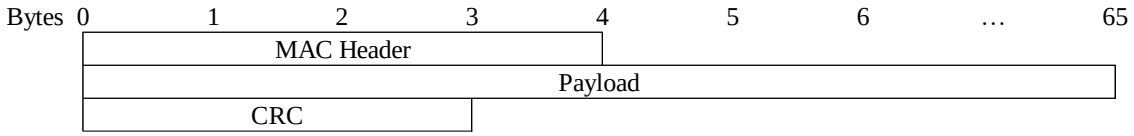


Рис. 6. Структура пакету даних NB-IoT

Під час передачі даних шифрується частина Payload. Для шифрування використовується протокол ESP на основі алгоритму 128-EEA2 [24,25]. Цей алгоритм передбачає доповнення корисних даних до розміру ключа, який складає 128 біт. Через це обсяг зашифрованих даних може збільшитися на 1 до 127 біт.

У кожному з представлених протоколів існує проблема збільшення пакету, що передається, внаслідок шифрування даних. Шифрування вимагає доповнення корисних даних додатковими бітами до розміру ключа. Оскільки це доповнення має очевидний негативний вплив, необхідно проаналізувати співвідношення обсягу доповнення до корисних даних, щоб мати підстави для вибору оптимального протоколу. Для цього були побудовані графіки обсягів доповнень у відсотках відносно обсягу корисних даних для кожного протоколу (рис. 7-12).

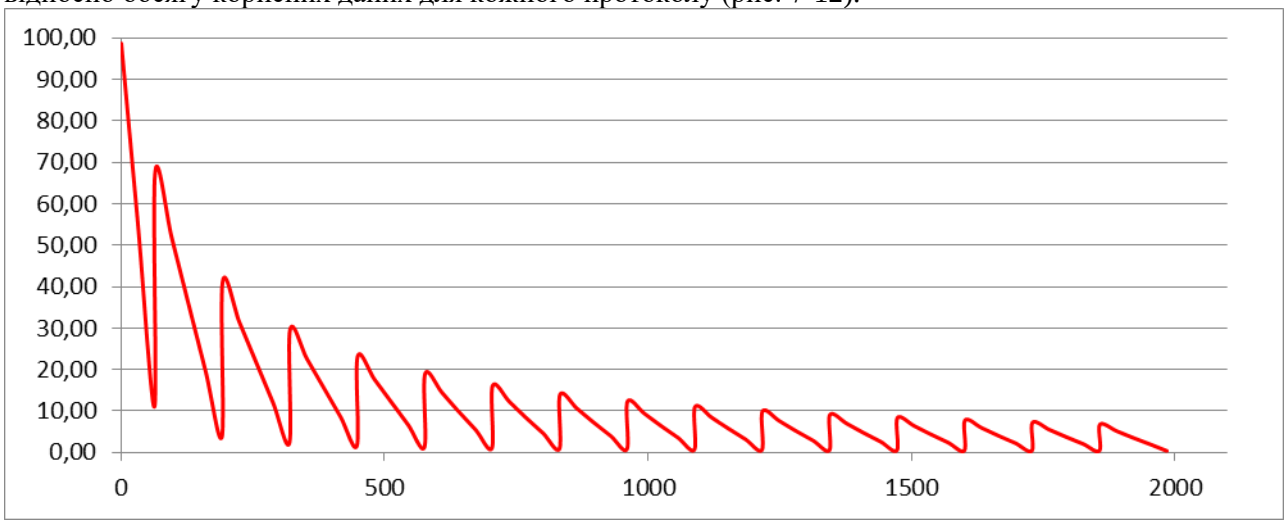


Рис. 7. Обсяги доповнень у стандарті Wi-Fi

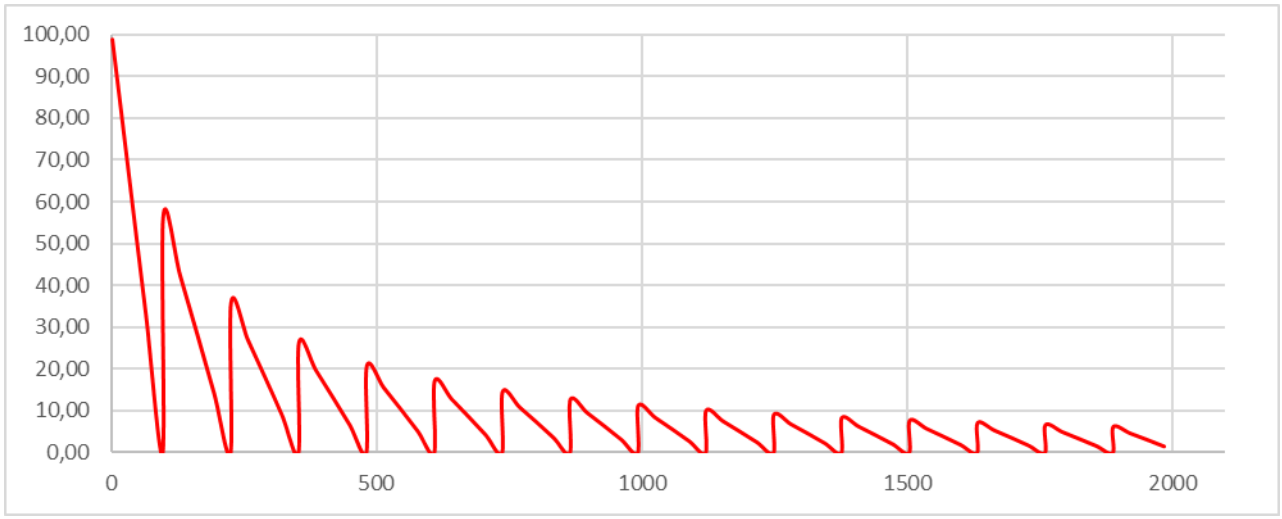


Рис. 8. Обсяги доповнень у стандарті Bluetooth

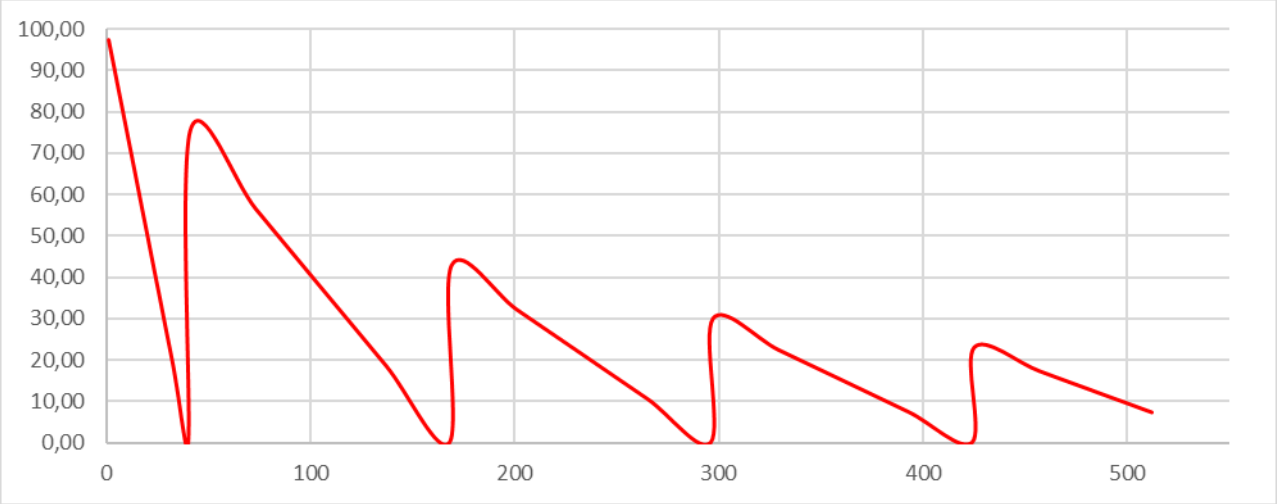


Рис. 9. Обсяги доповнень у протоколі ZigBee

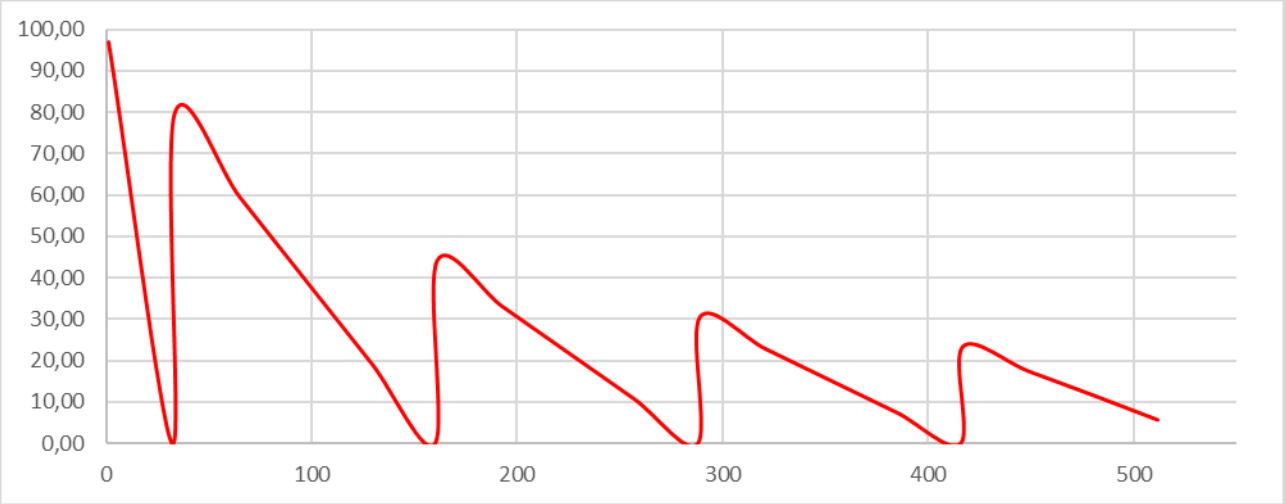


Рис. 10. Обсяги доповнень у стандарті 6LoWPAN

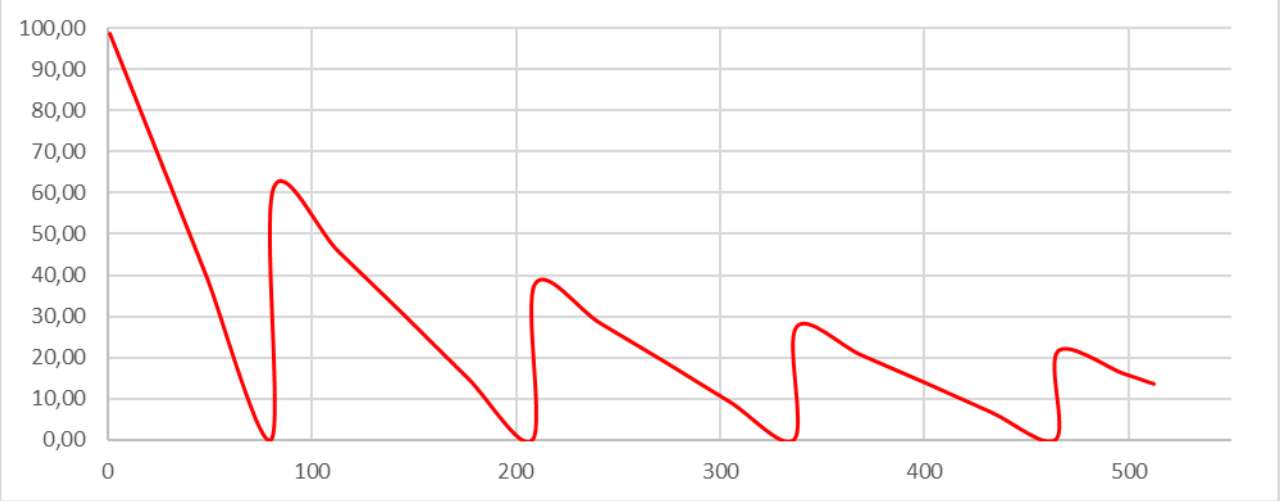


Рис. 11. Обсяги доповнень у протоколі WirelessHART

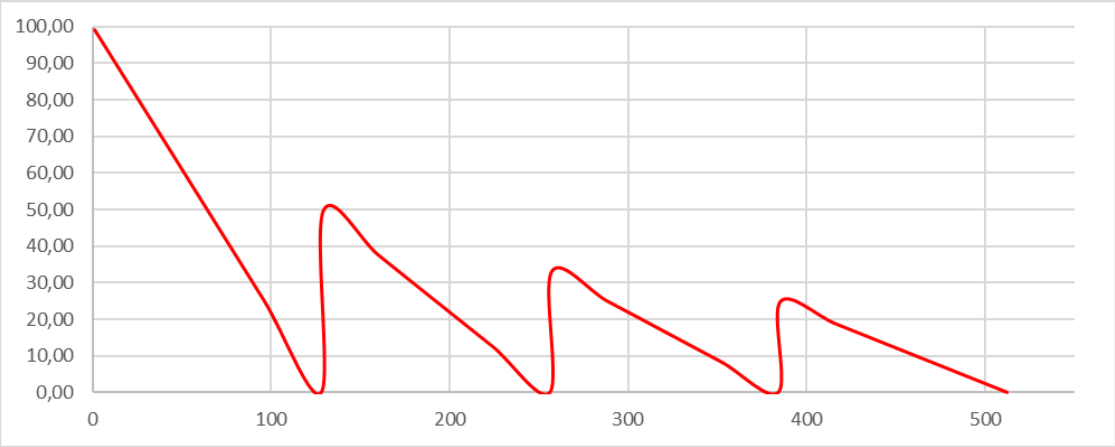


Рис. 12. Обсяги доповнень у протоколі NB-IoT

З графіків видно, що зі збільшенням обсягу корисних даних вплив доповнення на загальний обсяг пакету даних зменшується. Окремо варто відзначити піки на графіку, які виникають, коли необхідно виконати доповнення на велику кількість бітів для досягнення кратності ключа шифрування.

Також було проведено аналіз середнього значення відсотка доповнення відносно корисних даних для кожного протоколу та стандарту. Результати представлені у таблиці 1.

Таблиця 1. Середній відсоток доповнень

| Протокол або стандарт | Середній відсоток доповнень відносно корисних даних | Максимальний обсяг корисних даних |
|---|---|---|
| Wi-Fi | 2.13% | 2304 байт |
| Bluetooth | 10.64% | 251 байт |
| 6LoWPAN | 23.22% | 80 байт |
| WirelessHART | 23.08% | 80 байт |
| ZigBee | 24.81% | 68 байт |
| NB-IoT | 25.96% | 65 байт |

З таблиці 1 видно, що чим більший обсяг даних здатний передавати протокол або стандарт, тим менший середній відсоток доповнень міститиме пакет даних. Проте сучасні пристрої Інтернету речей є енергоефективними та передають невеликі обсяги даних, тому обчислення долі доповнень відносно корисних даних недоцільно проводити на основі їх максимального обсягу.

Якщо обмежити максимальний обсяг корисних даних до 64 байт, можна розрахувати середній відсоток для більшості енергоефективних систем, які мають малі обсяги трафіку (табл. 2).).

Таблиця 2. Середній відсоток доповнень відносно 64 байтів корисних даних

| Протокол або стандарт | Середній відсоток доповнень при обсязі корисних даних до 64 байт |
|---|---|
| Wi-Fi | 9.95% |
| Bluetooth | 16.31% |
| 6LoWPAN | 11.55% |
| WirelessHART | 10.12% |
| ZigBee | 8.00% |
| NB-IoT | 20.21% |

Обсяги доповнення найбільший вплив мають на протокол NB-IoT. Далі за ним йде стандарт Bluetooth. Найкраще себе показує протокол ZigBee, що може свідчити про те, що від добре підходить для систем з обмеженими за обсягом корисними даними.

**Висновки та перспективи подальших досліджень**. Сучасні стандарти та протоколи Інтернету речей включають обов'язкове шифрування даних. Оскільки алгоритми шифрування вимагають доповнення корисних даних до розміру ключа, який зазвичай становить 128 біт, виникає

необхідність передачі «зайвої» інформації, що в середньому складає близько 26% від загального обсягу корисних даних у пакеті. Загальний вплив на обсяги трафіку в більшості протоколів становить приблизно 10%, за винятком Bluetooth (16%) та NB-IoT (20%).

Для оптимізації обсягів трафіку слід враховувати розмір пакета даних, оскільки шифруються не тільки корисні дані, але й інші частини пакету. Аналіз популярних протоколів щодо частки "додаткової" інформації, пов'язаної з шифруванням, показав, що протокол ZigBee є найбільш рекомендованим для використання в системах з обмеженим обсягом корисних даних.

Отримані результати дозволять більш точно обирати протокол або стандарт під час проєктування систем Інтернету речей, оскільки є можливість провести моделювання передачі даних у системі та визначити, чи буде передаватися надлишкова інформація.

**Список бібліографічного опису**

1. Kozel V., Ivanchuk O., Drozdova I., Prykhodko O. Automation of the Protocol Selection Process for IoT Systems. *International Journal of Computing*. 2022. № 21(2). P. 251-257. DOI: 10.47839/ijc.21.2.2594
2. Vasileios A. Memos, Kostas E. Psannis. Encryption algorithm for efficient transmission of HEVC media. *Journal of Real-Time Image Processing*. 2016. № 12. P. 473-482. DOI: 10.1007/s11554-015-0509-3
3. Victor Kathan Sarker, Tuan Nguyen Gia, Hannu Tenhunen, Tomi Westerlund, Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes. *IEEE International Conference on Communications (ICC)*. Dublin, 2020. DOI: 10.1109/ICC40277.2020.9149359
4. E Gregersen. Wi-Fi. *Encyclopaedia Britannica*. 2023. URL: https://www.britannica.com/technology/Wi-Fi (дата звернення 14.10.2024).
5. R Laufer, L Kleinrock. The Capacity of Wireless CSMA/CA Networks. *IEEE/ACM Transactions on Networking*. 2016. № 24. P. 1518-1532. DOI: 10.1109/TNET.2015.2415465
6. Ali M. Alsahlany, Zainalabdin H. Alfatlawy, Alhassan R. Almusawy. Experimental Evaluation of Different Penetration Security Levels in Wireless Local Area Network. *Journal of Communications*. 2018. № 13 (12). P. 723-729. DOI: 10.12720/jcm.13.12.723-729
7. Rasika Nayanajith. CWSP – CCMP Encryption Method. 2014. URL: https://mrncciew.com/2014/08/19/cwsp-ccmp-encryption-method/ (дата звернення 14.10.2024).
8. Firdaus, Eko Nugroho, Alvin Sahroni. ZigBee and wifi network interface on Wireless Sensor Networks. M*akassar International Conference on Electrical Engineering and Informatics (MICEEI)*. 2014. DOI: 10.1109/MICEEI.2014.7067310
9. Iman Saberi, Bahareh Shojaie, Mazleena Salleh, Mahan Niknafskermani. Enhanced AES-CCMP key structure in IEEE 802.11i. *Proceedings of 2011 International Conference on Computer Science and Network Technology*. 2011. DOI: 10.1109/ICCSNT.2011.6182011
10. Kai Ren, Higher Speed How Fast Can It Be? *Bluetooth blog*. 2017. URL: https://www.bluetooth.com/blog/exploring-bluetooth-5-how-fast-can-it-be/ (дата звернення 14.10.2024).
11. Jacopo Tosi, Fabrizio Taffoni, Marco Santacatterina, Roberto Sannino, Domenico Formica, Performance Evaluation of Bluetooth Low Energy: A Systematic Review. *Sensors*. 2017. DOI: 10.3390/s17122898

**References**

1. Kozel V., Ivanchuk O., Drozdova I., Prykhodko O. Automation of the Protocol Selection Process for IoT Systems. International Journal of Computing. 2022. No. 21(2). P. 251-257. DOI: 10.47839/ijc.21.2.2594
2. Vasileios A. Memos, Kostas E. Psannis. Encryption algorithm for efficient transmission of HEVC media. Journal of Real-Time Image Processing. 2016. No. 12. P. 473-482. DOI: 10.1007/s11554-015-0509-3
3. Victor Kathan Sarker, Tuan Nguyen Gia, Hannu Tenhunen, Tomi Westerlund, Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes. IEEE International Conference on Communications (ICC). Dublin, 2020. DOI: 10.1109/ICC40277.2020.9149359
4. E Gregersen. Wi-Fi. Encyclopaedia Britannica. 2023. URL: https://www.britannica.com/technology/Wi-Fi (accessed 10/14/2024).
5. R Laufer, L Kleinrock. The Capacity of Wireless CSMA/CA Networks. IEEE/ACM Transactions on Networking. 2016. No. 24. P. 1518-1532. DOI: 10.1109/TNET.2015.2415465
6. Ali M. Alsahlany, Zainalabdin H. Alfatlawy, Alhassan R. Almusawy. Experimental Evaluation of Different Penetration Security Levels in Wireless Local Area Network. Journal of Communications. 2018. No. 13 (12). P. 723-729. DOI: 10.12720/jcm.13.12.723-729
7. Rasika Nayanajith. CWSP – CCMP Encryption Method. 2014. URL: https://mrncciew.com/2014/08/19/cwsp-ccmp-encryption-method/ (accessed 10/14/2024).
8. Firdaus, Eko Nugroho, Alvin Sahroni. ZigBee and wifi network interface on Wireless Sensor Networks. Makassar International Conference on Electrical Engineering and Informatics (MICEEI). 2014. DOI: 10.1109/MICEEI.2014.7067310
9. Iman Saberi, Bahareh Shojaie, Mazleena Salleh, Mahan Niknafskermani. Enhanced AES-CCMP key structure in IEEE 802.11i. Proceedings of the 2011 International Conference on Computer Science and Network Technology. 2011. DOI: 10.1109/ICCSNT.2011.6182011
10. Kai Ren, Higher Speed How Fast Can It Be? Bluetooth blog. 2017. URL: https://www.bluetooth.com/blog/exploring-bluetooth-5-how-fast-can-it-be/ (accessed 10/14/2024).
11. Jacopo Tosi, Fabrizio Taffoni, Marco Santacatterina, Roberto Sannino, Domenico Formica, Performance Evaluation of Bluetooth Low Energy: A Systematic Review. Sensors. 2017. DOI: 10.3390/s17122898