КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1377
УДК 004.056.5:004.7

Довженко Надія Михайлівна
кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID:0000-0003-4164-0066
n.dovzhenko@kubg.edu.ua

Іваніченко Євген Вікторович
кандидат технічних наук, доцент, заступник декана з науково-методичної та навчальної роботи,
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID:0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Мамченко Сергій Миколайович
д.п.н.,професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, м. Київ, Україна
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID:0009-0006-8743-5606
s.mamchenko@nubip.edu.ua

Хвостіченко Валерій Миколайович
старший науковий співробітник Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України (ЦНДІ ОВТ ЗС України), м. Київ, Україна
ORCID:0000-0003-3518-2273
vnxvostichenko@gmail.com

Гречко Денис Миколайович
аспірант Інституту проблем математичних машин і систем НАН України, м. Київ, Україна
ORCID:0009-0001-4438-6780
anzh29@gmail.com

РОЗШИРЕНА МОДЕЛЬ ОЦІНЮВАННЯ БЕЗПЕКИ КООПЕРАТИВНОГО ВСТАНОВЛЕННЯ ЗАХИЩЕНИХ КАНАЛІВ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Анотація. Розвиток безпроводових сенсорних мереж та їх інтеграція в інфраструктуру Internet of Things зумовлюють необхідність удосконалення механізмів встановлення захищених каналів між складовими компонентами з обмеженими ресурсами. Одним із підходів до вирішення такого завдання є кооперативне встановлення ключів, за якого формування захищеного каналу між двома сенсорними вузлами здійснюється із залученням множини проміжних кооперуючих сенсорів. Класичний протокол ECCE забезпечує збільшення імовірності існування каналу та його стійкості до компрометації вузлів, однак базова аналітична модель переважно орієнтована на параметри випадкового попереднього розподілу ключів і кількість кооперуючих пристроїв. У роботі запропоновано розширену ймовірнісну модель оцінювання захищеності кооперативного каналу, у якій поряд із параметрами глобального пулу ключів, розміру зв'язків ключів і кількості кооперуючих сенсорів враховано кількість скомпрометованих вузлів та імовірність доступності безпроводової лінії зв'язку. Сформовано показник ефективного захищеного зв'язку, що одночасно характеризує наявність спільного ключового матеріалу, відсутність його компрометації та фізичну доступність лінії зв'язку. На його основі одержано аналітичну оцінку імовірності існування захищеного каналу для прямого та двострибкового кооперативного сценаріїв. Отримані результати підтверджують можливість використання запропонованого підходу для аналізу компромісу між розміром зв'язки ключів, кількістю кооперуючих вузлів, стійкістю до компрометації та якістю безпроводового середовища.

Ключові слова: безпроводова сенсорна мережа, БСМ, IoT, ECCE, кооперативне встановлення ключів, управління ключами, компрометація вузлів, захищений канал, імовірнісна модель, безпека, найдійність.

ВСТУП

Безпроводові сенсорні мережі є одним із базових компонентів сучасних систем моніторингу, автоматизованого керування та технології Internet of Things. Їх застосування передбачає функціонування значної кількості розподілених сенсорних вузлів, які характеризуються обмеженим обсягом пам'яті, обчислювальних ресурсів та енергетичного запасу. Водночас безпроводова природа взаємодії, можливість фізичного доступу до сенсорних пристроїв та децентралізована топологія створюють додаткові ризики для конфіденційності, цілісності та автентичності інформаційного обміну [1].

Одним із фундаментальних завдань забезпечення безпеки таких мереж є встановлення секретного ключа між парою сенсорних вузлів. Класичний підхід випадкового попереднього розподілу ключів передбачає формування глобального пулу криптографічних ключів і завантаження випадкової підмножини цього пулу до пам'яті кожного сенсорного пристрою. Два вузли можуть безпосередньо встановити захищений канал, якщо їх зв'язки ключів мають непорожній перетин [2].

Такий підхід був формалізований у моделі Ешенауера-Глігора, а подальші роботи запропонували механізми $q-$ композитного попереднього розподілу ключів та багатошляхового посилення ключів. Кооперативний протокол ECCE розвинув цей напрям, дозволивши встановлювати захищений канал навіть між вузлами, які не мають безпосередньо спільного попередньо розподіленого ключа, шляхом залучення множини кооперуючих сенсорів. Оригінальна ECCE-модель також передбачає імовірнісну автентифікацію та підвищення стійкості каналу зі збільшенням кількості кооператорів [7].

Водночас сучасні безпроводові сенсорні мережі та IoT-системи оцінюються не лише за криптографічною зв'язністю. Для практичного застосування істотними є якість безпроводової лінії, імовірність доставки пакетів, енергоспоживання, затримка, стійкість до компрометації пристроїв та накладні витрати процедури управління ключами. Сучасні дослідження безпеки безпроводових сенсорних мереж та IoT продовжують розглядати спільну оптимізацію показників безпеки, енергетичної ефективності, затримки та надійності, що підтверджує доцільність такого розширення класичної моделі.

Метою роботи є розроблення розширеної математичної моделі оцінювання захищеності кооперативного встановлення каналу в безпроводовій сенсорній мережі з урахуванням випадкового попереднього розподілу ключів, компрометації вузлів та доступності безпроводових ліній зв'язку[4].

БАЗОВА МОДЕЛЬ СЕНСОРНОЇ МЕРЕЖІ

Нехай безпроводова сенсорна мережа складається з N вузлів:

$$V = \{v_1, v_2, \dots, v_N\}.$$

Мережа представляється неорінтованим графом:

$$G = (V, E), \tag{1}$$

де V – множина сенсорних вузлів, а E – множина логічних захищених зв'язків, що виникають унаслідок наявності спільних ключів (граф ключової зв’язності).

Перед розгортанням мережі формується глобальний пул ключів:

$$\mathcal{P} = \{k_1, k_2, \dots, k_{\mathcal{P}}\}.$$

де $P = |\mathcal{P}|$— загальна кількість криптографічних ключів, тобто загальна потужність пулу.

Кожному сенсорному вузлу v_i випадково без повторень призначається зв'язка ключів (key-ring):

$$KR_i \subset \mathcal{P}, \qquad |KR_i| = K.$$

За такого підходу розподіл ключів описується класичною моделлю Ешенауера-Глігора, у якій кожна зв’язка ключів є рівномірно випадковою $K-$ елементною підмножиною загального пулу [3]. Зазначена модель розроблена спеціально для захисту пристроїв з обмеженими обчислювальними ресурсами та обсягом пам'яті, що є характерним для вузлів безпроводових сенсорних мереж.

Позначимо через наступне (2) біноміальний коефіцієнт:

$$\binom{n}{r} = C(n,r) = \frac{n!}{r!\,(n-r)!}. \quad (2)$$

Два сенсорні вузли v_i та v_j мають прямий захищений зв'язок (Direct-link), якщо:

$$KR_i \cap KR_j \neq \emptyset \quad (3)$$

Розглянемо два основні вузли $a, b \in V$ між якими необхідно встановити захищений канал.

Для цього додатково вводиться множина кооперуючих сенсорів $C = \{c_1, c_2, \ldots, c_{n_c}\}$, де $n_c = |C|$. Множина C може бути сформована як підмножина сусідів a та b у межах їхнього фізичного радіуса зв'язку або як випадкова вибірка з множини $V \backslash \{a, b\}$.

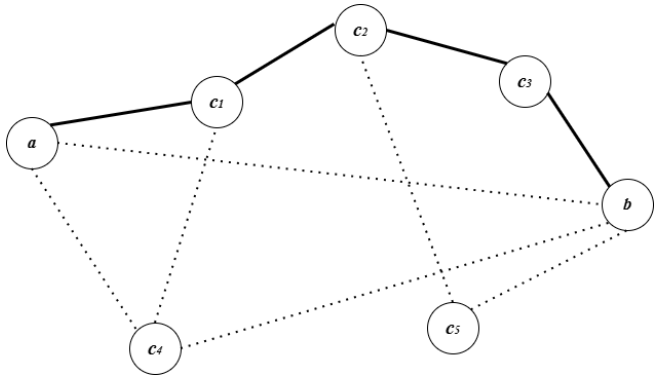

Рис. 1. Структура кооперативного ECCE-каналу між вузлами a і b

На рис.1 представлено приклад типового встановлення захищеного каналу за протоколом ECCE. Вузли a та b – основні суб'єкти взаємодії, вузли $c_1, \ldots, c_5$ – множина кооперуючих сенсорів C. Пунктирні лінії позначають скомпрометовані або фізично відсутні зв'язки. А маршрут $a \to c_1 \to c_2 \to c_3 \to b$ – є прикладом нескомпрометованого з'єднання (безпечний маршрут). Саме наявність такого маршруту гарантує конфіденційність ключа ECCE, так як навіть за відсутності прямого нескомпрометованого зв'язку між a та b канал може бути встановлений через послідовність кооперативних ланок, жодна з яких не відома супротивнику[3, 7].

ІМОВІРНІСТЬ ІСНУВАННЯ ПРЯМОГО МАРШРУТУ

У класичній моделі випадкового попереднього розподілу ключів (модель Ешенауера-Глігора) два вузли можуть встановити прямий захищений зв'язок (Direct-link) тоді і тільки тоді, коли їхні зв'язки ключів мають непорожній перетин [3]. Ймовірність протилежної події (відсутність спільних ключів) визначається точно через відношення біноміальних коефіцієнтів:

$$p_0(P,K) = \frac{\binom{P-K}{K}}{\binom{P}{K}}. \quad (4)$$

Ця величина є ймовірністю того, що $K-$ елементна підмножина, обрана для другого вузла, повністю міститься в доповненні до зв'язки першого вузла (яка також має розмір K). Відповідно, імовірність існування прямого захищеного зв'язку дорівнює:

$$p_{link}(P,K) = 1 - \frac{\binom{P-K}{K}}{\binom{P}{K}}. \quad (5)$$

Формула (5) є одним із базових компонентів класичної моделі випадкового попереднього розподілу ключів і одночасно задає ймовірність появи ребра у випадковому графі зв'язності G.

Для великих значень P і за умови $K \ll P$ справедлива добре відома апроксимація:

$$p_{link}(P,K) \approx 1 - \exp\left(-\frac{K^2}{P}\right). \quad (6)$$

Вона випливає з граничного переходу біноміальних коефіцієнтів і наочно демонструє квадратичну залежність криптографічної зв'язності від розміру key-ring. Збільшення K суттєво підвищує p_{link} проте одночасно зростає обсяг секретного матеріалу, що зберігається на одному пристрої [4]. Унаслідок цього виникає фундаментальний компроміс між зв'язністю мережі та стійкістю до атаки захоплення вузлів (node capture).

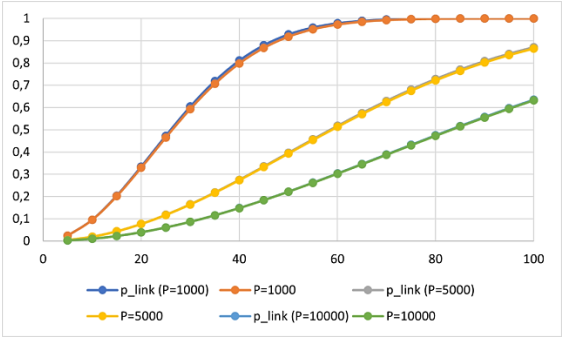

Рис. 2. Порівняння точної формули (5) та апроксимації (6) для ймовірності прямого захищеного зв'язку при різних розмірах пулу P

Аналізуючи рис. 2. можна підкреслити, що криві зростають швидше, чим менший розмір пулу P, що підтверджу квадратичний характер залежності p_{link} від K.

Узагальненням умови (3) є вимога, щоб вузли мали принаймні q спільних ключів ($q \geq 1$). У цьому випадку ймовірність прямого захищеного зв'язку набуває вигляду:

$$p^{(q)}{}_{link}(P,K) = 1 - \sum_{i=0}^{q-1} \frac{\binom{K}{i}\binom{P-K}{K-i}}{\binom{P}{K}}.$$

а для великих P справедлива апроксимація

$$p^{(q)}{}_{link}(P,K) \approx 1 - \sum_{i=0}^{q-1} \frac{1}{i!}\left(\frac{K^2}{P}\right)^i \exp\left(-\frac{K^2}{P}\right).$$

При $q = 1$ формули зводяться до (5)-(6). Збільшення q підвищує стійкість окремого зв'язку, але зменшує ймовірність його існування, що додатково загострює зазначений компроміс [5].

Модель компрометації ключів. Нехай атакувальник фізично скомпрометував W сенсорних вузлів і отримав усі ключі, що зберігалися в їхніх пам'яті. Оскільки зв'язки ключів формуються незалежно та рівноймовірно, імовірність того, що довільний фіксований ключ глобального пулу міститься у зв'язці одного випадкового вузла, дорівнює K/P. Імовірність того, що цей ключ не буде отриманий після компрометації W незалежних вузлів, становить $(1-\frac{K}{P})^W$. Отже, імовірність компрометації окремого ключа може бути розрахована наступним чином:

$$q_k(W) = 1 - (1-\tfrac{K}{P})^W. \quad (7)$$

Формула (7) відповідає стандартній моделі, використаній у базовому аналізі протоколу ECCE, і є точним виразом за припущення незалежності вибору key-ring. Для типових параметрів безпроводових сенсорних мереж ($K \ll P,\ W \ll N$) різниця між (7) і точним гіпергеометричним виразом є незначною [6].

Отримана ймовірність $q_k(W)$ дозволяє безпосередньо оцінити стійкість будь-якого прямого захищеного зв'язку: зв'язок, який захищений m −спільними ключами, залишається нескомпрометованим з імовірністю $(1-q_k(W))^m$.

ІМОВІРНІСТЬ КОМПРОМЕТАЦІЇ ПРЯМОГО ЗАХИЩЕНОГО ЗВ'ЯЗКУ

Нехай випадкова величина I визначає кількість спільних ключів двох довільних сенсорних вузлів. Оскільки зв'язки ключів формуються як рівноймовірні K − елементні підмножини глобального пулу, розподіл I є класичним гіпергеометричним:

$$P_r(I = i) = \frac{\binom{K}{i}\binom{P-K}{K-i}}{\binom{P}{K}}, i = 0,1 \dots K. \quad (8)$$

Прямий захищений зв'язок існує лише за умови $I \geq 1$. Тому для подальшого аналізу стійкості необхідно перейти до умовного розподілу:

$$P_r(I = i \mid I \geq 1) = \frac{P_r(I = i)}{p_{link}(P,K)} = \frac{\binom{K}{i}\binom{P-K}{K-i}}{\binom{P}{K} p_{link}(P,K)}, i = 1 \dots K. \quad (9)$$

У протоколі ECCE (та в механізмі ESP) Direct-key формується з усього набору спільних секретів. Отже, для компрометації вже існуючого прямого захищеного зв'язку атакувальник повинен володіти усіма i ключами, що увійшли до перетину [3, 5]. Для фіксованого i ця ймовірність дорівнює:

$$P_r(\text{зв}'\text{язок скомпрометований} \mid I = i) = [q_k(W)]^i. \quad (10)$$

Варто зауважити, що використання альтернативного виразу $1 - [1 - q_k(W)]^i$ було б коректним лише в моделі, де компрометації хоча б одного ключа достатньо для руйнування зв'язку. Така модель не відповідає логіці ECCE/ESP [7].

Усереднюючи (10) за умовним розподілом (9), отримано ймовірність компрометації існуючого зв'язку:

$$q_L(W) = \sum_{i=1}^{K} [q_k(W)]^i * P_r(I = i \mid I \geq 1) \quad (11)$$

У розгорнутому вигляді:

$$q_L(W) = \frac{1}{\binom{P}{K} p_{link}(P,K)} \sum_{i=1}^{K} [q_k(W)]^i \binom{K}{i}\binom{P-K}{K-i}. \quad (12)$$

Формула (12) є принципово важливою: вона точно враховує необхідність компрометації всього набору спільних ключів і тому дає нижчу оцінку ймовірності компрометації зв'язку порівняно з моделями «компрометації хоча б одного ключа» [8].

Ефективний захищений зв'язок. Класична криптографічна модель вважає, що за наявності спільного ключа відповідна логічна лінія може бути використана для захищеного обміну. У реальному безпроводовому середовищі ця умова часто не виконується через затухання, інтерференцію, втрати пакетів, тимчасову недоступність вузла чи інші фактори каналу [9].

Доцільно ввести параметр $q \in [0,1]$, що визначає ймовірність фізичної доступності безпроводової лінії протягом усієї процедури встановлення каналу (імовірність успішної доставки всіх необхідних повідомлень протоколу).

Тоді для того, щоб зв'язок міг бути реально використаний як захищений, одночасно повинні виконуватися три незалежні події:

- Direct-link криптографічно існує (ймовірність p_{link});
- Direct-link не скомпрометований (ймовірність $1 - q_L(W)$);
- фізична безпроводова лінія доступна (ймовірність q).

Ймовірність ефективного захищеного зв'язку визначатиметься наступною формулою:

$$s = p_{link} * (1 - q_L(W)) * q. \quad (13)$$

Параметр s є центральним показником запропонованої розширеної моделі. На відміну від класичного p_{link}, який характеризує лише криптографічну зв'язність, величина s відображає реальну можливість використання маршруту як захищеного каналу з урахуванням як криптографічної стійкості, так і фізичних обмежень безпроводового середовища.

Далі параметр s замінюватиме класичну ймовірність прямого захищеного зв'язку при обчисленні ймовірності існування кооперативного маршруту та відповідних ресурсних характеристик [5].

КООПЕРАТИВНЕ ВСТАНОВЛЕННЯ КАНАЛУ

У повній моделі протоколу ECCE захищений канал між вузлами a і b може бути побудований як прямим маршрутом, так і довільними шляхами через множину кооперуючих сенсорів C. Для отримання аналітично прозорої та обчислювально зручної оцінки розглядається наближення обмеженого шляху (restricted-path approximation), яке враховує лише прямий маршрут $a \to b$ та двострибкові маршрути $a \to c_i \to b$, де $c_i \in C$.

Такий підхід не замінює повну ECCE-топологію, але дозволяє отримати явну нижню оцінку ймовірності успішного встановлення каналу і слугує зручною базою для подальшого узагальнення [7].

Імовірність того, що прямий захищений канал відсутній, дорівнює $1 - s$.

Для фіксованого кооператора c_i обидва маршрути $a \to c_i$ та $c_i \to b$ повинні бути ефективними та захищеними. За припущення статистичної незалежності цих подій

$$P_r(a \to c_i \to b) = s^2. \tag{14}$$

Відповідно, ймовірність того, що конкретний двострибковий маршрут не існує становить: $1 - s^2$. Якщо всі n_c кооператорів розглядаються як незалежні, то ймовірність того, що жоден із двострибкових маршрутів не існує, дорівнює:

$$(1 - s^2)^{n_c}. \tag{15}$$

Отже, імовірність одночасної відсутності як прямого, так і будь-якого двострибкового кооперативного маршруту розраховується:

$$P_{fail} = (1 - s) * (1 - s^2)^{n_c}. \tag{16}$$

Розширена ймовірність успішного встановлення захищеного каналу набуває вигляду

$$P_{sec} = 1 - (1 - s) * (1 - s^2)^{n_c}. \tag{17}$$

Підставляючи визначення ефективного захищеного зв'язку (13), буде отримано:

$$P_{sec} = 1 - [1 - P_{link}(1 - q_L)q] * \{1 - [P_{link}(1 - q_L)q]^2\}^{n_c}. \tag{18}$$

Таким чином,

$$P_{sec} = \mathrm{f}(\mathrm{P}, \mathrm{K}, \mathrm{W}, \mathrm{q}, n_c). \tag{19}$$

Формула (18) є основною аналітичною формулою запропонованої моделі з обмеженими маршрутами. Необхідно підкреслити, що припущення незалежності маршрутів є апроксимацією. Реальні події спільного володіння ключами, інцидентні одному й тому ж сенсорному вузлу, статистично залежні через його фіксовану key-ring [5, 10].

Розширення для багатострибкових ECCE-маршрутів. Повний протокол ECCE дозволяє використання маршрутів з кількома кооперуючими сенсорами, наприклад: $a \to c_1 \to c_2 \to b$ або $a \to c_1 \to c_2 \to c_3 \to b$. Для одного заданого маршруту, що складається з h-зв'язків за умови незалежності:

$$P_{path}(h) = s^h. \tag{20}$$

Для множини M_{h} незалежних кандидатних маршрутів однакової довжини h:

$$P_h = 1 - (1 - s^h)^{M_{\mathrm{h}}}. \tag{21}$$

На практиці такі ECCE-маршрути мають спільні вузли та зв'язки, тому події їх існування є залежними. З цієї причини (21) може використовуватися лише як верхня оцінка (або як апроксимація при малій щільності спільних елементів) [5, 7].

Модель енергетичних витрат. Кооперативний механізм має істотну ресурсну ціну. Збільшення кількості кооператорів n_c породжує додаткові передавання, приймання та криптографічні операції. Загальні енергетичні витрати процедури встановлення каналу доцільно подавати у вигляді комбінації:

$$E_{total} = N_{tx}E_{tx} + N_{rx}E_{rx} + N_{enc}E_{enc} + N_{hash}E_{hash} + N_{xor}E_{xor} + E_{ctrl} \tag{22}$$

де N_{tx}, N_{rx} – кількість операцій передавання та приймання; $N_{enc}, N_{hash}, N_{xor}$ – кількість операцій симетричного шифрування, хешування та XOR відповідно; $E_{tx}, E_{rx}, E_{enc}, E_{hash}, E_{xor}$ – енергетична вартість однієї відповідної операції; E_{ctrl} — інші контрольні та службові витрати [6, 9].

Для порівняльного аналізу різних конфігурацій зручно використовувати відносну метрику:

$$E_{norm} = \frac{E_{total}}{E_{direct}}, \tag{23}$$

де E_{direct} – енергетична вартість прямого встановлення каналу без залучення кооператорів. Величина E_{norm} безпосередньо відображає ціну підвищення ймовірності P_{sec} за рахунок зростання n_c.

Модель затримки. Загальна затримка процедури встановлення захищеного каналу може бути представлена адитивною декомпозицію:

$$T_{total} = T_d + T_{exch} + T_{cr} + T_q + T_{route}, \tag{24}$$

де T_d – час виявлення ключових сусідів та кооператорів (фаза ESP); T_{exch} – час службового обміну повідомленнями протоколу; T_{cr} – час виконання криптографічних операцій; T_q – затримки, зумовлені чергами та механізмом множинного доступу (MAC); T_{route} – затримка передавання повідомлень між проміжними вузлами маршруту.

Для маршруту з h послідовними зв'язками:

$$T_{route} = \sum_{r=1}^{h} T_r, \tag{25}$$

де T_r –випадкова затримка r –зв'язку (включає час поширення, повторні передачі та обробку на вузлі).

Таким чином, збільшення кількості кооператорів n_c (або довжини маршрутів) може підвищувати ймовірність P_{sec} проте одночасно збільшує як енергетичні витрати E_{total}, так і сумарну затримку T_{total}.Цей ресурсний компроміс є принциповим для практичного застосування протоколу в енергообмежених безпроводових сенсорних мережах [6, 9].

Інтегральний показник. Якщо необхідно виконувати багатокритеріальний вибір параметрів протоколу, зручно перейти до нормованих показників $E^* = \frac{E_{total}}{E_{max}}$, $T^* = \frac{T_{total}}{T_{max}}$, де E_{max} і T_{max} –максимально допустимі (або характерні) значення енергії та затримки для конкретизованого сценарію.

Інтегральний показник якості визначається як зважена сума

$$J = w_s * P_{sec} + w_e * (1 - E^*) + w_t * (1 - T^*), \tag{26}$$

де вагові коефіцієнти задовольняють умови

$$w_s + w_e + w_t = 1, \quad w_s, w_e, w_t \geq 0.$$

Коефіцієнт w_s відображає пріоритет захищеності, w_e – енергоефективності, w_t – оперативності. Задача вибору оптимальних параметрів набуває вигляду:

$$(K^*, n_c^*) = \underset{K, n_c}{arg\max} J(K, n_c), \tag{27}$$

за обмежень:

$$P_{sec} \geq P_{min}, \tag{28}$$

$$E_{total} \leq E_{max}, \tag{29}$$

$$T_{total} \leq T_{max}. \tag{30}$$

Важливо підкреслити, що функція (26) має сенс лише тоді, коли вагові коефіцієнти мають фізично або експертно обґрунтовані значення, узгоджені з вимогами конкретного застосування (наприклад, критичність безпеки у порівняння з жорсткими енергетичними обмеженнями) [11].

За формулою (5) були розраховані значення ймовірності існування прямого зв'язку $p_{\text{link}}(P, K)$ для трьох характерних розмірів глобального пулу ключів. Результати представлено на рис. 3.

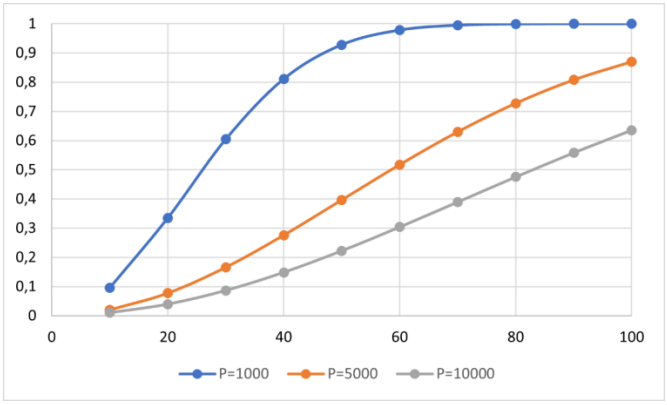

Рис.3. Залежність ймовірності p_{link} від розміру K при різних значеннях потужності пулу P

Отримана залежність має виражено нелінійний характер, що повністю узгоджується з апроксимацією (6). Для відносно малого пулу $P = 1000$ збільшення розміру key-ring від $K = 10$ до $K = 30$ підвищує p_{link} приблизно від 0,096 до 0,604 (зростання більш ніж у шість разів). При значно більшому пулі $P = 10000$ той самий діапазон K забезпечує лише зростання від 0,01 до 0,086.

Представлений результат кількісно підтверджує фундаментальний компроміс моделі випадкового попереднього розподілу ключів: для забезпечення прийнятної криптографічної зв'язності при великих P необхідно суттєво збільшувати K, що, у свою чергу, погіршує стійкість до атаки захоплення вузлів (формули (7) і (12)). Отже, параметри P і K мають обиратися узгоджено з урахуванням як вимог до зв'язності, так і очікуваного рівня компрометації мережі [7, 12].

Наступні розрахунки виконано для фіксованих параметрів $P = 10000$ та $K = 100$. За формулами (7) і (12) розраховано ймовірність компрометації окремого ключа $q_k(W)$ та умовну ймовірність компрометації вже існуючої Direct-link $q_{\text{L}}(W)$ при збільшенні кількості захоплених вузлів W. Результати представлено на рис. 4.

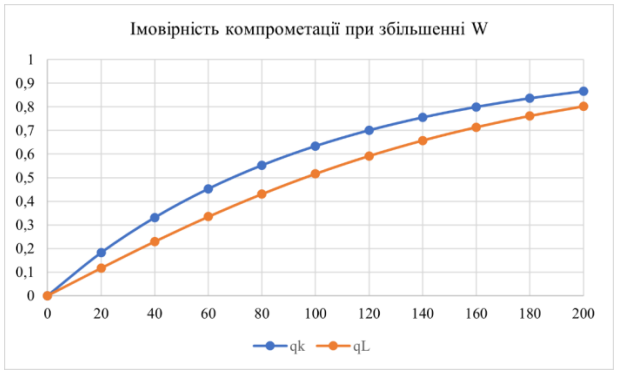

Рис. 4. Залежність імовірностей компрометації q_k (окремого ключа) та q_L (існуючого прямого з'єднання) від кількості захоплених вузлів W

Важливою особливістю отриманих кривих є виконання нерівності $q_L(W) < q_k(W)$ на всьому діапазоні $W > 0$. Пояснюється це тим, що за наявності кількох спільних ключів $(I \geq 2)$ для компрометації атакувальнику необхідно отримати весь відповідний секретний матеріал. Унаслідок цього ймовірність компрометації маршруту зростає повільніше, ніж імовірність компрометації окремого ключа. Різниця $q_k - q_L$ є кількісним підтвердженням переваги використання всього набору спільних ключів (підхід ECCE/ESP) порівняно з моделями, у яких компрометації хоча б одного ключа достатньо для руйнування всього зв'язку [3, 7].

Для кількісного дослідження впливу кооперації на ймовірність успішного встановлення захищеного каналу використано такі базові параметри як: $P = 1000, K = 30, W = 20, q = 0{,}95$. За цих значень безпосередньо з формул (5), (7), (12) і (13) отримано: $p_{\text{link}} = 0{,}604461$, $q_k = 0{,}456206$, $q_L \approx 0{,}3517, s \approx 0{,}372274$.

Підставляючи отримане значення ефективного захищеного зв'язку s у формулу (17), розраховано залежність P_{sec} від кількості кооператорів n_c. Результати представлено на рис. 5.

Отримана залежність демонструє класичний ефект насичення. Найбільший відносний приріст P_{sec} спостерігається при переході від малої кількості кооператорів ($n_c = 0..6$) до середньої.

Подальше збільшення n_c продовжує підвищувати ймовірність, проте кожен наступний кооператор забезпечує все менший граничний приріст. Зазначена властивість є принципово важливою для енергоефективної конфігурації протоколу ECCE: залучення надмірної кількості кооперуючих пристроїв дає лише незначне підвищення захищеності, але суттєво збільшує енергетичні витрати та затримку ((22) і (24)). Отже, існує практично оптимальний діапазон n_c, у якому досягається прийнятний компроміс між P_{sec} та ресурсними витратами [5, 7].

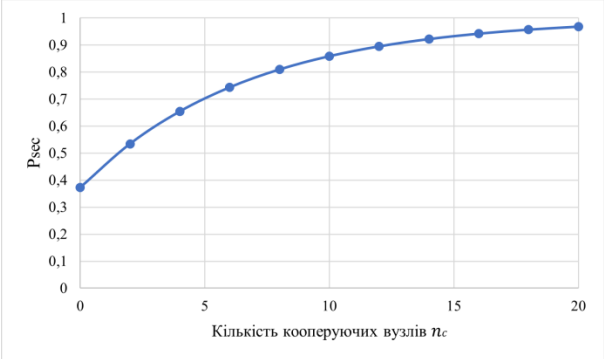

Рис.5. Залежність імовірності успішного встановлення захищеного каналу P_{sec} від кількості кооперуючих вузлів n_c

ВПЛИВ ЯКОСТІ БЕЗПРОВОДОВОГО СЕРЕДОВИЩА

Зберігаючи базові криптографічні параметри $P = 1000, K = 30, W = 20$, було досліджено вплив імовірності фізичної доступності бездротової лінії q на ймовірність успішного встановлення захищеного каналу. Розглянуто чотири характерні значення: $q \in \{0{,}8;\ 0{,}9;\ 0{,}95;\ 1\}$.

Для кожного q за формулою (17) розраховано залежність P_{sec} від кількості кооператорів n_c. Результати представлено на рис. 6.

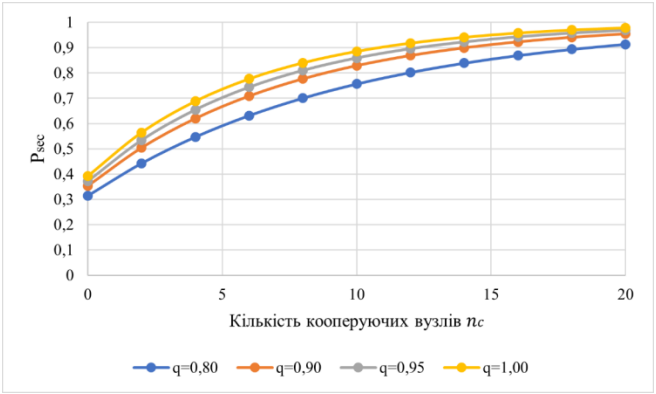

Рис. 6. Залежність P_{sec}від кількості кооперуючих вузлів n_c при різних значеннях якості безпроводового середовища q

Отримані криві демонструють важливий практичний ефект: збільшення кількості кооператорів частково компенсує погіршення якості безпроводового середовища. Наприклад, при $q = 0{,}8$ і відсутності кооперації ($n_c = 0$) маємо $P_{sec} \approx 0{,}313$. При залученні $n_c = 20$ кооператорів ця величина зростає до $\approx 0{,}913$. Аналогічна тенденція спостерігається і для інших значень q.

Таким чином, кооперативна схема ECCE підвищує не лише криптографічну зв'язність, але й структурну відмовостійкість каналу відносно фізичних порушень безпроводового середовища (затухання, інтерференція, тимчасова недоступність ліній). Зазначена властивість робить протокол особливо цінним для реальних сценаріїв безпроводових сенсорних мереж та IoT, де якість радіоканалу є суттєво нестабільною [10, 11].

Компроміс між розміром key-ring та кількістю кооператорів. Для кількісного аналізу можливості обміну ресурсів пам'яті на кооперацію зафіксовано параметри Для $P = 1000, W = 20, q = 0{,}9$. і розраховано P_{sec} для різних комбінацій розміру key-ring K та кількості кооператорів n_c. Результати представлено на рис.7.

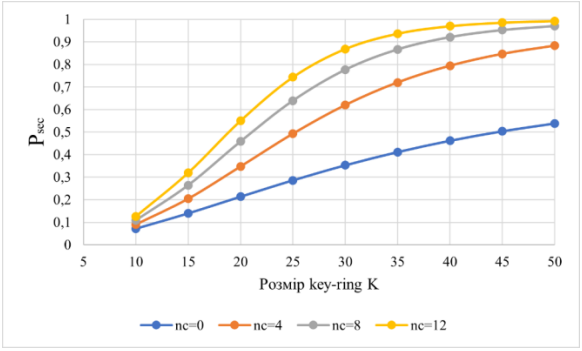

Рис.7. Компроміс між розміром key-ring K та кількістю кооперуючих вузлів n_c

Отримані криві підтверджують можливість обміну ресурсів пам'яті на кооперацію. Зокрема:

- при $K = 40$ і $n_c = 0$ маємо $P_{sec} \approx 0{,}462$;
- при суттєво меншому key-ring $K = 25$ і лише $n_c = 4$ кооператорах отримуємо вже $P_{sec} \approx 0{,}492$

Аналогічні співвідношення спостерігаються і для інших точок. Таким чином, певне скорочення обсягу секретного матеріалу, що зберігається на кожному вузлі, може бути компенсоване помірним залученням кооперуючих сенсорів без втрати (а часто навіть із підвищенням) ймовірності успішного встановлення захищеного каналу.

Приведена властивість є практично важливою для ресурсно-обмежених безпроводових сенсорних мереж: зменшення K звільняє пам'ять для зберігання додаткових ключів ECCE або прикладних даних, а необхідний рівень захищеності забезпечується за рахунок кооперації [7, 8].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі запропоновано розширену математичну модель оцінювання безпеки кооперативного встановлення захищених каналів у безпроводових сенсорних мережах на основі протоколу ECCE. На відміну від класичного підходу, модель одночасно враховує наявність спільного ключового матеріалу, його стійкість до компрометації та фізичну доступність безпроводового зв'язку. Введений показник ефективного захищеного зв'язку дозволив поєднати зазначені характеристики в єдиній імовірнісній моделі та отримати оцінку успішності встановлення прямого і двострибкового кооперативного каналу в межах наближення обмежених зв'язків.

Проведений чисельний аналіз підтвердив нелінійний вплив параметрів моделі на рівень захищеності мережі. Збільшення кількості кооперуючих вузлів підвищує ймовірність успішного встановлення захищеного каналу, однак супроводжується ефектом насичення, за якого граничний приріст від залучення додаткових кооператорів поступово зменшується. Це обґрунтовує необхідність узгодженого вибору кількості кооператорів з урахуванням енергетичних витрат і затримки, моделі яких також сформовано в роботі.

Встановлено, що кооперативне встановлення каналів може частково компенсувати погіршення якості безпроводового середовища завдяки використанню альтернативних маршрутів, підвищуючи тим самим не лише криптографічну захищеність, а й структурну відмовостійкість мережі. Показано також можливість часткової компенсації зменшення розміру key-ring залученням додаткових кооперуючих вузлів. Такий взаємозв'язок створює основу для раціонального використання обмеженої пам'яті сенсорних пристроїв та багатокритеріального вибору параметрів мережі з урахуванням безпеки, енергоефективності й затримки.

Область застосування отриманих результатів визначається прийнятими припущеннями. Запропонована аналітична модель розглядає прямі та двострибкові маршрути, використовує припущення про статистичну незалежність окремих криптографічних і фізичних подій, агреговано описує якість безпроводового середовища та передбачає випадковий характер компрометації вузлів. Енергетична й часова складові мають параметричний характер і для отримання абсолютних кількісних оцінок потребують калібрування на конкретних сенсорних платформах або у валідованому середовищі імітаційного моделювання.

Перспективи подальших досліджень пов’язані з розширенням моделі на багатострибкові ECCE-маршрути з урахуванням статистичної залежності ланок, використанням просторово-залежних моделей безпроводового середовища на основі RSSI та SINR, а також дослідженням сценаріїв із адаптивним супротивником. Доцільним є експериментальне калібрування ресурсних моделей та розроблення механізму динамічного вибору кількості кооперуючих вузлів відповідно до поточного рівня загроз, стану каналів і залишкового енергетичного ресурсу. Подальша інтеграція запропонованої моделі в задачі спільної оптимізації безпеки, енергоефективності та затримки (security–energy–latency) може забезпечити адаптивне керування параметрами захищених БСМ/IoT-систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dovzhenko, N., Ivanichenko, Y., Ausheva, N., Shevchuk, Y., & Lukovskyi, T. (2025). Research on data center architecture with the integration of IoT components to ensure energy efficiency and cyber resilience. *Cybersecurity: Education, Science, Technique, 4*(28), 547–564. https://doi.org/10.28925/2663-4023.2025.28.835
2. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance of sensor networks based on energy consumption and traffic analysis. *Cybersecurity: Education, Science, Technique, 1*(25), 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
3. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (pp. 41–47). https://doi.org/10.1145/586110.586117
4. Dovzhenko, N., Barabash, O., Musienko, A., Ivanichenko, Y., & Krasheninnik, I. (2024). Enhancing sensor network efficiency through optimized flooding mechanism. *CEUR Workshop Proceedings, 3654*, 465–470. https://ceur-ws.org/Vol-3654/short15.pdf
5. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 197–213). https://doi.org/10.1109/SECPRI.2003.1199337
6. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). Methodology for detecting and localizing cyber threats in cloud environments with integrated IoT components based on graph models. *Cybersecurity: Education, Science, Technique, 1*(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938
7. Conti, M., Di Pietro, R., & Mancini, L. V. (2007). ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks. *Ad Hoc Networks, 5*(1), 49–62. https://doi.org/10.1016/j.adhoc.2006.05.013
8. Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in Internet of Things: Challenges, countermeasures, and future directions. *Ad Hoc Networks, 146*, Article 103159. https://doi.org/10.1016/j.adhoc.2023.103159
9. Openko, P., Dovzhenko, N., Orikhovskyi, P., & Ikaiev, D. (2024). Ensuring reliability and security in modern wireless sensor networks based on the implementation of the RSSI metric. *Air Power of Ukraine, 1*(6), 131–136. https://doi.org/10.33099/2786-7714-2024-1-6-131-136
10. Hussain, M., Hussain, M., Aamer, N., et al. (2025). Optimized rank-based key management for energy-efficient routing in wireless sensor networks for IoT applications. *Discover Internet of Things, 5*, Article 127. https://doi.org/10.1007/s43926-025-00224-3
11. Alotaibi, J. (2026). Energy-efficient trust management for secure IoT devices in information-centric wireless sensor networks. *Peer-to-Peer Networking and Applications, 19*, Article 43.
12. Yousefpoor, M. S., & Barati, H. (2019). Dynamic key management algorithms in wireless sensor networks: A survey. *Computer Communications, 134*, 52–69. https://doi.org/10.1016/j.comcom.2018.11.005

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Nadiia Dovzhenko
PhD, Associate Professor, Associate Professor of the Department of Information and Cybernetic Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan university, Kyiv, Ukraine
ORCID:0000-0003-4164-0066
n.dovzhenko@kubg.edu.ua

Yevhen Ivanichenko
PhD, Associate Professor, Deputy Dean for Scientific-Methodological and Educational Work
Borys Grinchenko Kyiv Metropolitan university, Kyiv, Ukraine
ORCID:0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Serhij Mamchenko
Doctor of Technical Sciences, Professor, Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
Borys Grinchenko Kyiv Metropolitan university, Kyiv, Ukraine
ORCID:0009-0006-8743-5606
s.mamchenko@nubip.edu.ua

Valery Khvostichenko
Senior Researcher, Central Scientific Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, Kyiv, Ukraine
ORCID:0000-0003-3518-2273
vnxvostichenko@gmail.com

Denys Hrechko
Postgraduate student of the Institute of Mathematical Machines and System Problems of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID:0009-0001-4438-6780
anzh29@gmail.com

EXTENDED SECURITY ASSESSMENT MODEL FOR COOPERATIVE ESTABLISHMENT OF SECURE CHANNELS IN WIRELESS SENSOR NETWORKS

Abstract. The development of wireless sensor networks and their integration into the Internet of Things (IoT) infrastructure necessitate the improvement of mechanisms for establishing secure channels between resource-constrained components. One approach to addressing this problem is cooperative key establishment, in which a secure channel between two sensor nodes is established with the involvement of a set of intermediate cooperating sensors. The classical ECCE protocol increases the probability of secure channel establishment and improves resilience against node compromise; however, its basic analytical model is primarily focused on the parameters of random key predistribution and the number of cooperating devices. This paper proposes an extended probabilistic model for assessing the security of a cooperative channel. In addition to the parameters of the global key pool, key-ring size, and number of cooperating sensors, the model takes into account the number of compromised nodes and the probability of wireless link availability. An effective secure connectivity metric is introduced, simultaneously characterizing the availability of shared keying material, the absence of its compromise, and the physical availability of the wireless communication link. Based on this metric, an analytical estimate of the probability of secure channel establishment is derived for both direct and two-hop cooperative scenarios. The obtained results demonstrate the applicability of the proposed approach to analyzing the trade-off among key-ring size, the number of cooperating nodes, resilience to node compromise, and wireless channel quality.

Keywords: wireless sensor network, WSN, IoT, ECCE, cooperative key establishment, key management, node compromise, secure channel, probabilistic model, security, reliability.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Dovzhenko, N., Ivanichenko, Y., Ausheva, N., Shevchuk, Y., & Lukovskyi, T. (2025). Research on data center architecture with the integration of IoT components to ensure energy efficiency and cyber resilience. *Cybersecurity: Education, Science, Technique, 4*(28), 547–564. https://doi.org/10.28925/2663-4023.2025.28.835
2. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance of sensor networks based on energy consumption and traffic analysis. *Cybersecurity: Education, Science, Technique, 1*(25), 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400
3. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (pp. 41–47). https://doi.org/10.1145/586110.586117
4. Dovzhenko, N., Barabash, O., Musienko, A., Ivanichenko, Y., & Krasheninnik, I. (2024). Enhancing sensor network efficiency through optimized flooding mechanism. *CEUR Workshop Proceedings, 3654*, 465–470. https://ceur-ws.org/Vol-3654/short15.pdf
5. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 197–213). https://doi.org/10.1109/SECPRI.2003.1199337
6. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). Methodology for detecting and localizing cyber threats in cloud environments with integrated IoT components based on graph models. *Cybersecurity: Education, Science, Technique, 1*(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938
7. Conti, M., Di Pietro, R., & Mancini, L. V. (2007). ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks. *Ad Hoc Networks, 5*(1), 49–62. https://doi.org/10.1016/j.adhoc.2006.05.013
8. Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in Internet of Things: Challenges, countermeasures, and future directions. *Ad Hoc Networks, 146*, Article 103159. https://doi.org/10.1016/j.adhoc.2023.103159
9. Openko, P., Dovzhenko, N., Orikhovskyi, P., & Ikaiev, D. (2024). Ensuring reliability and security in modern wireless sensor networks based on the implementation of the RSSI metric. *Air Power of Ukraine, 1*(6), 131–136. https://doi.org/10.33099/2786-7714-2024-1-6-131-136
10. Hussain, M., Hussain, M., Aamer, N., et al. (2025). Optimized rank-based key management for energy-efficient routing in wireless sensor networks for IoT applications. *Discover Internet of Things, 5*, Article 127. https://doi.org/10.1007/s43926-025-00224-3
11. Alotaibi, J. (2026). Energy-efficient trust management for secure IoT devices in information-centric wireless sensor networks. *Peer-to-Peer Networking and Applications, 19*, Article 43.
12. Yousefpoor, M. S., & Barati, H. (2019). Dynamic key management algorithms in wireless sensor networks: A survey. *Computer Communications, 134*, 52–69. https://doi.org/10.1016/j.comcom.2018.11.005

Отримано редакцією журналу / Received: 22.02.26
Прорецензовано / Revised: 03.03.26
Схвалено до друку / Accepted: 24.09.26