

**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

Киричок Роман Васильович

PhD, доцент,

доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID: 0000-0002-9919-9691

r.kyrychok@kubg.edu.ua

**АНАЛІТИЧНА МОДЕЛЬ ОЦІНЮВАННЯ ОЗНАК КОМПРОМЕТАЦІЇ ВУЗЛІВ
БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖ**

Анотація. Розвиток безпроводових сенсорних мереж та їх застосування в сучасних системах моніторингу призводить до необхідності вдосконалення механізмів виявлення потенційно можливої компрометації вузлів, особливо в умовах обмежених обчислювальних ресурсів, нестійкого зв'язку та ризику фізичного захоплення пристроїв. Традиційні механізми контролю присутності, ґрунтовані на періодичному обміні повідомленнями про працездатність, не дозволяють достовірно відрізнити природну недоступність вузла від порушення його програмно-апаратної цілісності. У роботі запропоновано аналітичну модель оцінювання ознак потенційної компрометації вузлів на основі порогового контролю присутності із залученням m призначених спостерігачів та використанням правила k із m . За припущенням про пуассонівський характер надходження незалежних автентифікованих підтверджень отримано аналітичні вирази для визначення ймовірності відсутності нового підтвердження та виникнення хибної групової тривоги. Отримані вирази враховують інтенсивність контактів, тривалість інтервалу очікування та поріг кооперації. Модель розширено шляхом врахування корельованих порушень зв'язності каналів та доступності спостерігачів. Додатково уточнено процедуру ухвалення рішень із повторною перевіркою підозрілих вузлів та розглянуто підхід до дистанційної атестації для виявлення порушень програмної цілісності. Отримані результати демонструють залежність ризику хибних тривог від параметрів контактної взаємодії, ступеня кооперації та корельованих порушень зв'язності. Показано, що підвищення порогу групового підтвердження зменшує ймовірність хибного спрацьовування, але водночас знижує своєчасність формування тривоги. Одержані залежності створюють основу для обґрунтування вибору параметрів механізмів виявлення потенційно можливої компрометації з урахуванням особливостей функціонування сенсорних мереж.

Ключові слова: безпроводова сенсорна мережа, IoT, БСМ, захист, захоплення вузла, компрометація, мобільність, кооперація, тривога, безпека, надійність, ймовірнісна модель.

ВСТУП

Функціонування безпроводових сенсорних мереж (БСМ) характеризується динамічною зміною топології, включаючи просторове розташування вузлів, їх сусідство та маршрути передачі даних. В таких



умов довіра до окремого пристрою залежить не тільки від результатів криптографічної автентифікації, а й від своєчасного отримання та перевірки інформації про його стан. Важливим завданням є встановлення причин порушення інформаційної взаємодії, оскільки відсутність повідомлень може бути спричинена різними факторами: виходом вузла за межі радіопокриття, тимчасовою втратою зв'язку, апаратною несправністю або навмисним втручанням [11].

Однією із поширених загроз для сенсорних компонентів є фізичне захоплення, за якого зломисник отримує безпосередній доступ до апаратних компонентів і потенційно може змінювати програмну конфігурацію, вилучати криптографічні ключі або модифікувати результати вимірювань [5, 17]. При цьому необхідно чітко розмежовувати фізичне вилучення пристрою та його можливу компрометацію, при якій він продовжує функціонувати з використанням легітимних даних. У другому випадку успішна автентифікація повідомлень не гарантує безпеку програмного середовища чи достовірність отриманих даних. Таким чином, мережева активність сама по собі не може розглядатися як доказ відсутності несанкціонованого впливу.

Складність виявлення потенційної компрометації полягає у необхідності розмежування спостережуваних подій та їхніх причин. Відсутність своєчасного підтвердження присутності свідчить про недоступність вузла для конкретного спостерігача протягом певного визначеного проміжку часу, але не визначає причину цього стану [15]. Помилкова інтерпретація такої події може призвести до необґрунтованого обмеження функцій легітимного компонента мережі, порушення маршрутизації (зв'язності між вузлами) та зниження доступності мережевих сервісів. Водночас недостатньо чутливий механізм моніторингу може затримати реагування на фактичне вилучення вузла або інші події, що потребують додаткової верифікації [16]. Тому при визначенні підстав для формування підозри слід враховувати не лише тривалість відсутності зв'язку, але й достовірність, незалежність і своєчасність отриманих даних.

У децентралізованих системах контролю додаткову невизначеність створює можливість одночасної втрати зв'язку з вузлом декількома спостерігачами через спільні порушення радіосередовища. Таким чином, збіг локальних повідомлень про відсутність контакту не завжди означає наявність незалежних доказів потенційної загрози. Це створює необхідність формального визначення умов формування колективної тривоги, оцінки ймовірності хибних спрацьовувань та розмежування процедур попереднього виявлення аномалій і подальшого підтвердження порушення безпеки.

Метою дослідження є розробка аналітичного підходу до оцінювання ознак потенційної компрометації вузлів БСМ, що базується на достовірних контактних спостереженнях з урахуванням невизначеності безпроводового середовища. Основна увага приділяється формалізації умов виникнення локальних і групових підозр, визначенню меж їх достовірної інтерпретації та обґрунтуванню необхідності додаткової перевірки перед застосуванням обмежувальних заходів щодо пристрою.

АНАЛІЗ ВІДОМИХ ПІДХОДІВ І ПОСТАНОВКА ЗАДАЧІ

У сучасних методах моніторингу стану сенсорних вузлів використовуються різноманітні джерела даних. До них належать періодичні службові повідомлення, результати безпосередньої взаємодії між пристроями, а також криптографічні свідчення про стан програмного середовища. Відмінності між цими механізмами визначають не лише спосіб отримання даних, а й характер висновків, які можуть бути сформовані на їх основі. Тому оцінка доцільності певного методу вимагає аналізу того, які саме властивості вузла він перевіряє, за яких умов отримані свідчення вважаються достовірними та наскільки вони залежать від поточного стану зв'язності мережі.

Адаптивні підходи до виявлення кіберзагроз в IoT розглядаються також на прикладі спеціалізованих інфраструктур, зокрема підсистем дата-центрів [7]. На рівні загальних вимог до IoT-пристроїв рекомендації NIST визначають базові функції кібербезпеки та організаційні заходи їх забезпечення протягом життєвого циклу продукції [10, 12].

Централізований моніторинг за допомогою періодичних повідомлень про працездатність (heartbeat) включає реєстрацію часу останнього звернення вузла та перевірку дотримання встановленого інтервалу між повідомленнями [15]. Перевагами такого механізму є відносна простота реалізації та мінімальний обсяг інформації, необхідної для підтримки контролю. Водночас його ефективність залежить від своєчасної доставки повідомлень до точки моніторингу. У мережах зі змінною топологією збоїв в маршрутизації або збільшення затримок доставки можуть призвести до помилок спрацювань, навіть якщо вузол працює нормально. Застосування довшого інтервалу очікування зменшує чутливість до короточасних порушень зв'язку, проте збільшує час реагування на тривалу недоступність вузла [16]. Крім того, частота службових повідомлень впливає на мережевий трафік та енергоспоживання, що є важливими аспектами, які слід враховувати при забезпеченні безпеки та відмовостійкості сенсорних мереж [13].



Інший підхід базується на використанні локальної взаємодії між вузлами та кооперативному обміні інформацією. Дослідження [2] розглядає застосування мобільності та кооперації для протидії загрозам фізичного захоплення вузлів у мобільних ad hoc мережах. Важливим аспектом розподіленого контролю є можливість формування спостережень різними учасниками без необхідності постійного звернення до центрального координатора. Ключовими елементами організації такої взаємодії є захищене встановлення каналів між сенсорними пристроями [1] та ефективне поширення повідомлень у мережі [3]. Однак навіть за наявності захищеного передавання даних, достовірність висновків, зроблених на їх основі, не гарантується. Наприклад, повторне надсилання одного й того ж свідчення різними маршрутами не збільшує кількість незалежних спостережень. Крім того, групові рішення залежать від надійності джерел, своєчасності доставки та можливості одночасних порушень зв'язку між кількома учасниками. Отже, для ефективного використання кооперативних свідчень необхідно визначити критерії їх незалежності та умови, за яких сукупність локальних спостережень є достатньою для формування спільної підозри.

Окремий напрям досліджень пов'язаний із дистанційною атестацією (remote attestation), призначеною для перевірки визначених характеристик програмного стану пристрою. Протокол SEDA [4] пропонує масштабований підхід до колективної атестації вбудованих пристроїв, тоді як PADS [6] зосереджується на розподіленій атестації в умовах динамічної топології. Особливості побудови таких механізмів, їхні припущення щодо довіреної основи та обмеження застосування представлені в дослідженнях [8, 9]. Достовірність результату атестації залежить від захищеності процедури вимірювання, цілісності еталонних значень, збереження атестаційних секретів та перевірки актуальності сформованих свідчень. Важливо зазначити, що успішна атестація підтверджує відповідність лише тих компонентів програмного стану, які охоплені відповідною процедурою. Відсутність відповіді на запит не дозволяє самостійно встановити факт порушення цілісності.

Аналіз розглянутих підходів показує, що контроль присутності та перевірка програмної цілісності стосуються різних властивостей сенсорного вузла і потребують окремих критеріїв оцінки. Для механізмів, що базуються на контактній взаємодії, недостатньо визначити лише допустиму тривалість відсутності повідомлень. Результат групового контролю також залежить від кількості спостерігачів, порогу спрацьовування системи безпеки та характеру взаємозалежності між їхніми спостереженнями. Зокрема, якщо кілька учасників одночасно втрачають зв'язок, припущення про незалежність локальних повідомлень може призвести до заниження оцінки ризику хибних спрацьовувань. Підвищення порогу групового підтвердження, своєю чергою, зменшує ймовірність випадкової тривоги, але потребує участі більшої кількості доступних спостерігачів.

ФОРМАЛІЗАЦІЯ МЕРЕЖІ ТА АРХІТЕКТУРА КОНТРОЛЮ СТАНУ ВУЗЛІВ

Розглянуто мережу, яка складається з N сенсорних вузлів, де $N \geq 2$. Множина вузлів позначена як $V = \{v^1, \dots, v^N\}$. Для кожного контрольованого вузла b визначено набір із m призначених спостерігачів $S(b)$, при чому $1 \leq m < N$ кількість призначених спостерігачів може не відповідати кількості вузлів, здатних безпосередньо взаємодіяти з об'єктом контролю в конкретний момент часу. Хоча для здійснення локальних спостережень наявність базової станції не є обов'язковою, узгодження остаточного статусу пристрою та відкликання його повноважень вимагають застосування визначеної довіреної процедури.

Контроль присутності ґрунтується на отриманні достовірних підтверджень. Для цього перевіряються ідентичність джерела, цілісність повідомлення та його актуальність. Захист від повторного використання раніше сформованих свідчень забезпечується відповідними криптографічними механізмами, зокрема часовими мітками або унікальними випадковими значеннями (nonce). У разі передавання підтверджень через проміжні вузли необхідно забезпечити можливість перевірки джерела та часу формування первинного свідчення. При цьому надходження одного й того самого повідомлення різними маршрутами не вважається сукупністю незалежних спостережень і не повинно впливати на їхню кількість.

Для оцінювання можливостей та обмежень контактного контролю розглянуто три сценарії функціонування вузла. Сценарій H_0 відповідає штатній роботі пристрою, доступність якого може змінюватися внаслідок переміщення в мережі або через нестабільність радіозв'язку. Сценарій H_1^0 передбачає фізичне вилучення вузла, внаслідок чого припиняється формування нових автентифікованих підтверджень. Сценарій H_1^A охоплює випадки активної компрометації, за якої пристрій продовжує мережеву взаємодію та може використовувати чинні криптографічні облікові дані.

За умов фізичного вилучення тривала відсутність підтверджень може свідчити про можливу компрометацію вузла, проте сама по собі не є достатнім доказом. Виявлення активної компрометації становить складніше завдання, оскільки збереження мережевої активності та використання чинних

облікових даних не гарантують цілісності програмного забезпечення пристрою. Тому в таких випадках контактний контроль доцільно доповнювати механізмами перевірки програмної цілісності. Розглянуті сценарії дають змогу визначити межі застосування контактного контролю та показують, що за його результатами неможливо достовірно встановити причину недоступності вузла без залучення додаткових ознак і механізмів перевірки.

В моделі для всіх призначених спостерігачів встановлюється однакова тривалість контрольного інтервалу λ . За сценарію H_0 надходження достовірних підтверджень окремому спостерігачеві умовно описується однорідним пуассонівським процесом з інтенсивністю $\mu > 0$. Припускається, що інтенсивності надходження підтверджень для всіх спостерігачів однакові, а самі потоки є незалежними. Подібне припущення дозволяє аналітично оцінити ймовірність відсутності контакту з вузлом та формування групової тривоги. Особливо враховуються випадки одночасного порушення зв'язності, за яких результати спостережень можуть бути статистично залежними.

Загальну структуру контролю та взаємозв'язок процедур оцінювання стану вузла наведено на Рис. 1. В основу запропонованої архітектури покладено три взаємодоповнювальні механізми: контроль присутності, перевірку автентичності та дистанційну атестацію. Контроль присутності дає змогу встановити, чи надходять підтвердження в межах визначеного інтервалу, тоді як перевірка автентичності забезпечує можливість використання отриманих повідомлень як достовірних свідчень. Дистанційна атестація застосовується для перевірки визначених характеристик програмної цілісності пристрою за умови наявності необхідних довірених засобів. Результати всіх трьох процедур об'єднуються в окремому блоці, де на їх основі формуються дані для подальшого оцінювання стану контрольованого вузла.

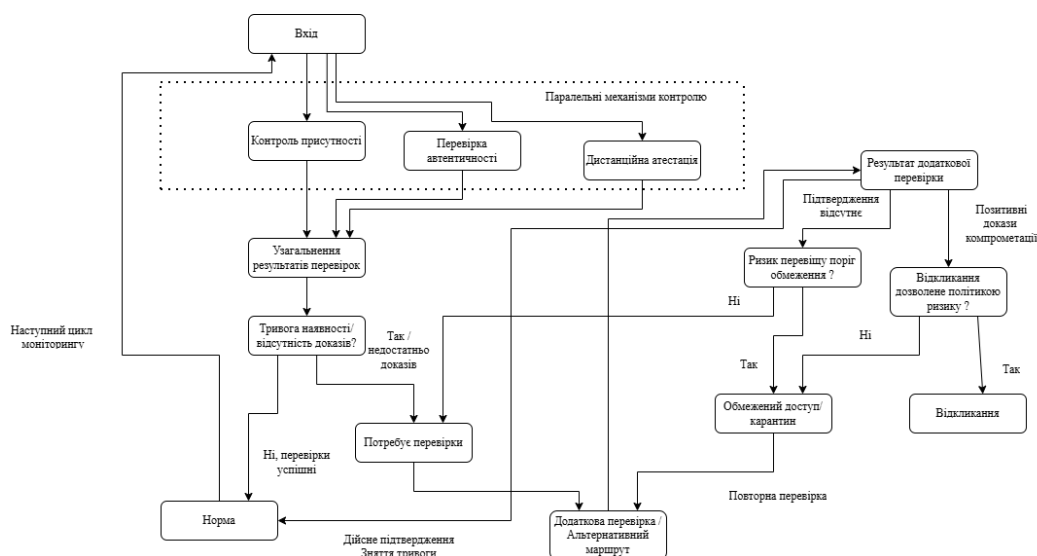


Рис. 1. Логічна архітектура багаторівневої оцінки стану вузла

Відповідно до схеми на Рис.1, результати перевірок узагальнюються для визначення підстав формування тривоги. У контактній складовій моделі для цього використовується порогове правило, за яким групова тривога формується за умови надходження щонайменше k незалежних локальних сигналів підозри від призначених спостерігачів. Якщо отримані свідчення не вказують на порушення встановлених умов контролю, вузол залишається у стані «Норма», а моніторинг продовжується в межах наступного циклу. У разі виникнення тривоги або недостатності наявних свідчень вузлу надається проміжний стан «Потребує перевірки», що передбачає проведення додаткових перевірок.

Для уточнення стану вузла може застосовуватися повторний криптографічний виклик, отримання підтвердження альтернативним маршрутом або дистанційна атестація програмного стану пристрою. На виконання цих процедур відводиться визначений часовий інтервал. Якщо протягом цього часу надходить нове достовірне підтвердження, підозра щодо недоступності вузла знімається, а пристрій повертається до звичайного режиму моніторингу. Проте відновлення контакту не гарантує відсутності активної компрометації, оскільки доступність пристрою та цілісність його програмного забезпечення оцінюються за різними критеріями.

Якщо після додаткової перевірки підтвердження так і не отримано, подальше рішення залежить від оціненого рівня ризику. На Рис.1 цей етап відображено блоком «Ризик перевищує поріг обмеження?». Якщо встановлений поріг перевищено, доступ вузла до мережевих ресурсів може бути обмежений.



зокрема шляхом переведення в режим карантину до проведення повторної перевірки. За нижчого рівня ризику перевірка продовжується без автоматичного запровадження обмежень.

Окремо розглядається випадок отримання позитивних доказів компрометації вузла. За таких умов рішення про відкликання його повноважень приймається відповідно до чинної політики безпеки та встановлених критеріїв ризику. Якщо відкликання не передбачене або не допускається, застосовується обмеження доступу чи карантин. Отже, запропонована архітектура передбачає послідовне розмежування трьох етапів: виявлення ознак можливої компрометації, уточнення стану вузла за результатами додаткових перевірок та визначення необхідних заходів реагування.

МАТЕМАТИЧНА МОДЕЛЬ КОНТРОЛЮ ПРИСУТНОСТІ

Імовірність надходження нового підтвердження. Нехай протягом інтервалу часу t , що відраховується від останнього контакту з вузлом, спостерігач отримує певну кількість достовірних підтверджень, наприклад $Z(t)$.

Якщо $Z(t)$ має пуассонівський розподіл з інтенсивністю $\mu > 0$, то відсутність нового підтвердження відповідає нульовому значенню лічильника подій.

$$P_r\{Z(t) = 0 | H_0\} = \exp(-\mu t) \quad (1)$$

$$P_r\{Z(t) \geq 1 | H_0\} = 1 - \exp(-\mu t) \quad (2)$$

Для некооперативного спостереження $\mu = \mu_d$, кооперацію допускається описати через $\mu_{ef} = \mu_d + \mu_c$ лише за додаткової умови, що нові, незалежні та справжні свідчення утворюють окремий пуассонівський потік. Повторне пересилання одного й того самого повідомлення збільшення μ не забезпечує.

$$\mu_{ef} = \mu_d + \mu_c \quad (3)$$

Вираз (1) характеризує ймовірність того, що протягом заданого часу спостерігач не отримає жодного нового підтвердження. За прийнятої пуассонівської моделі ця залежність відповідає функції виживання часу очікування до наступної події. Водночас її значення не можна безпосередньо трактувати як ймовірність захоплення чи компрометації вузла, оскільки відсутність контакту може бути спричинена також мобільністю пристрою або порушенням радіозв'язку. Побудована на основі цієї залежності аналітична крива відображає вплив інтенсивності надходження підтверджень на тривалість очікування, проте не характеризує фактичну траєкторію переміщення сенсорного вузла

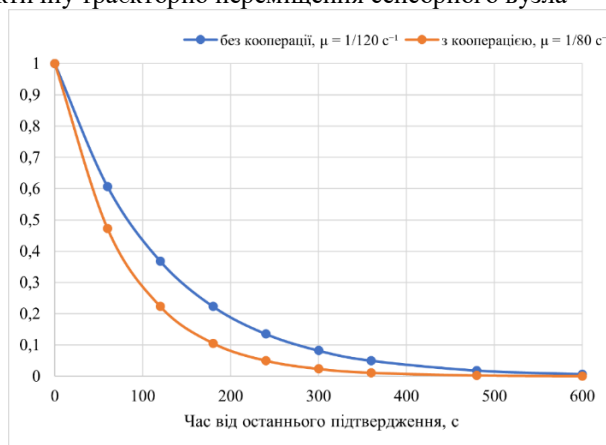


Рис. 2. Ймовірність відсутності нового підтвердження за різної інтенсивності контактів

Порогове правило k із m та ймовірність хибної тривоги. Для кожного спостерігача формується локальний індикатор $I_i(\lambda)$, який набуває значення 1, якщо впродовж λ не надійшло нового дійсного підтвердження від контролюваного вузла, і 0 в іншому випадку. Групова тривога виникає, якщо кількість індикаторів, рівних одиниці, досягає заданого порогу k . За H_0 , однакової інтенсивності μ та умовної незалежності m потоків локальна ймовірність мовчання становить $p_0 = \exp(-\mu\lambda)$.

$$A = 1\{\sum_{i=1}^m I_i(\lambda) \geq k\}. \quad (4)$$

$$p_0(\lambda) = \exp(-\mu\lambda). \quad (5)$$

$$P_{FA}(\lambda; m, k) = \sum_{i=k}^m \binom{m}{i} p_0^i (1 - p_0)^{m-i} \quad (6)$$

Для наочного представлення залежності розглядається випадок із трьома спостерігачами ($m = 3$), тому вираз (6) набуває вигляду полінома (7). Зі збільшенням λ ймовірність хибної тривоги щодо справного вузла зменшується, оскільки спостерігачі мають більше часу для отримання підтверджень. Водночас це збільшує затримку виявлення можливої недоступності вузла. Подібний вплив має підвищення порогу k : для формування групової тривоги потрібно більше незалежних сигналів підозри, що знижує ймовірність хибного спрацювання, але водночас підвищує вимоги до кількості доступних і працездатних спостерігачів. При цьому ймовірність хибної групової тривоги не слід ототожнювати з ймовірністю помилкового відкликання повноважень вузла, оскільки остаточному рішенням передусє додаткова перевірка.

$$P_{FA}(\lambda; 3, 2) = 3p_0^2 - 2p_0^3 \quad (7)$$

Припущення про незалежність спостережень не завжди відповідає реальним умовам функціонування безпроводової сенсорної мережі. Зокрема, спільні порушення радіозв'язку можуть одночасно впливати на декількох спостерігачів, спричиняючи появу залежних локальних сигналів підозри. Для врахування такого випадку розглядається сценарій, за якого з ймовірністю ρ протягом контрольного інтервалу виникає спільне порушення зв'язності, що унеможливує отримання підтверджень усіма спостерігачами. За відсутності такого порушення зберігаються припущення біноміальної моделі. Відповідну ймовірність хибної тривоги визначає наступний вираз:

$$P_{FA,c} = \rho + (1 - \rho)P_{FA}(\lambda; m, k) \quad (8)$$

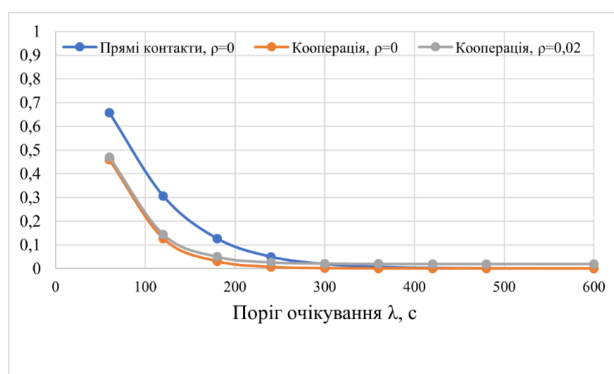


Рис. 3. Вплив кооперації та спільної недоступності каналів на ймовірність хибної тривоги

За прийнятих умов навіть істотне зменшення ймовірності хибного спрацювання в незалежній моделі не усуває ризику, пов'язаного зі спільною недоступністю каналів. У розглянутому сценарії його нижня межа визначається параметром (ρ).

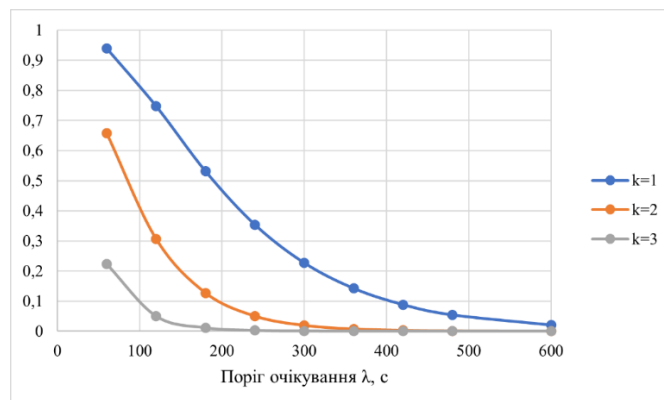


Рис. 4. Залежність ризику хибної тривоги від порогу k за фіксованих значень ($m = 3, \mu = 1/120 \text{ с}^{-1}$)

Інтерпретація групової тривоги. Відсутність підтверджень від вузла свідчить про порушення умов контактного контролю, однак не дозволяє однозначно встановити його причину. Зокрема, втрата зв'язку може бути наслідком як фізичного вилучення пристрою, так і його переміщення або тимчасової недоступності радіоканалу. Тому групову тривогу доцільно розглядати як підставу для додаткової перевірки, а не як безпосередній доказ компрометації.

Для оцінювання ймовірності компрометації необхідно враховувати, наскільки характерним є отриманий набір свідчень E для різних станів вузла. Зокрема, потрібно визначити ймовірність появи таких свідчень за умови захоплення пристрою та порівняти її з відповідною ймовірністю за нормальної роботи, включно з можливими порушеннями зв'язку.

Якщо відомі апіорна ймовірність компрометації $\pi = P(H_1)$ та умовні ймовірності отримання відповідних свідчень $L_1 = P(E|H_1), L_0 = P(E|H_0)$ для подальшого оцінювання може використовуватися формула Байєса:

$$P_r(H_1|E) = \frac{\pi L_1}{\pi L_1 + (1 - \pi) L_0} \quad (9)$$

Вираз (9) використовується для обґрунтування необхідності калібрування моделі загроз і врахування альтернативних причин втрати контакту. До отримання достатніх підтверджень результатом роботи контактної механізми має бути статус «Потребує перевірки», а не остаточний висновок про компрометацію вузла.

АЛГОРИТМ РЕАГУВАННЯ НА ПІДОЗРУ ТА ЗАХИСНІ ОБМЕЖЕННЯ

Результати порогового контролю присутності є підставою для додаткової перевірки стану вузла та визначення можливих заходів реагування. Після отримання нового підтвердження, захищеного цифровим підписом або кодом автентифікації повідомлення МАС, спостерігач перевіряє ідентифікатор відправника, цілісність і актуальність повідомлення, чинність криптографічних облікових даних та відповідність часових параметрів установленим вимогам. Для кожного контрольованого вузла фіксується час останнього достовірного підтвердження, а також зберігаються відомості, необхідні для перевірки походження. Якщо протягом визначеного інтервалу λ нове підтвердження не надходить, спостерігач формує локальний сигнал підозри. Відповідна інформація передається іншим учасникам із застосуванням механізмів захисту від підроблення, повторного використання повідомлень та надмірної частоти тривоги.

Групову тривогу формується після надходження сигналів щонайменше від k різних автентифікованих спостерігачів із загальної кількості m призначених учасників. Після досягнення цього порогу запускається процедура повторної перевірки, для виконання якої відводиться часовий інтервал δ . Залежно від характеру виявлених ознак і технічних можливостей мережі така перевірка може включати повторний криптографічний виклик, отримання підтвердження альтернативним маршрутом або дистанційну атестацію програмної цілісності пристрою. Якщо перевірка присутності завершується успішно, підозра щодо недоступності вузла знімається. Проте відновлення контакту не виключає активної компрометації, тому за наявності відповідних ознак може знадобитися додаткова перевірка програмного стану. Послідовність основних етапів контролю, переходи між станами та умови застосування захисних заходів представлено на Рис.5.

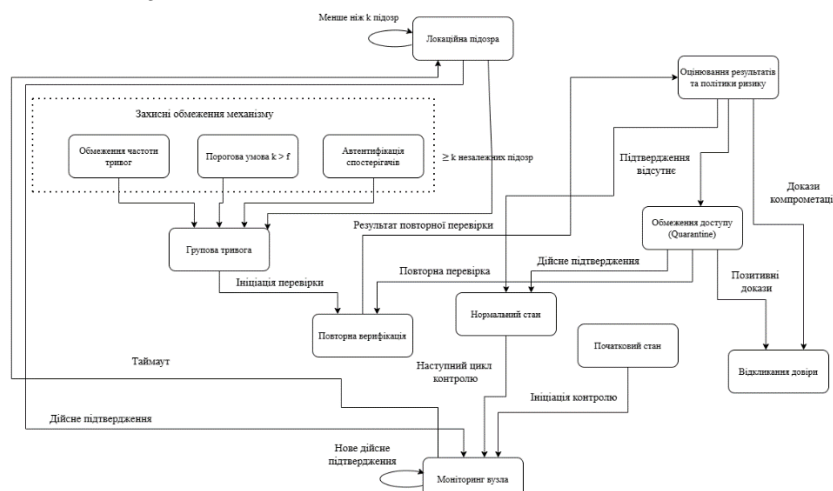


Рис. 5. Стани процедури перевірки



Як видно з Рис.5, після ініціалізації система переходить до моніторингу, під час якого реєструються достовірні підтвердження від контрольованого вузла. Якщо протягом встановленого інтервалу підтвердження не отримано, формується локальна підозра. Поки кількість таких сигналів не досягає порогу k , підстав для групової тривоги недостатньо. Після надходження необхідної кількості сигналів від різних спостерігачів проводиться повторна верифікація. Успішне підтвердження присутності дозволяє відновити звичайний режим контактного контролю за умови відсутності інших ознак порушення безпеки.

Якщо повторна перевірка не дала змоги підтвердити доступність вузла, отримані результати використовуються для оцінювання ризику та вибору подальших дій відповідно до політики безпеки мережі. Залежно від наявних свідчень може бути прийнято рішення про тимчасове обмеження доступу, переведення вузла в режим карантину з можливістю повторної перевірки або відкликання його повноважень. Останній варіант потребує достатніх підтверджених підстав, оскільки сама відсутність контакту не доводить факту компрометації. Відповідно, завершення контрольного інтервалу чи негативний результат повторної перевірки не повинні автоматично призводити до незворотного виключення вузла з мережі.

Важливим аспектом роботи є захист механізму групової тривоги від навмисного спотворення результатів спостереження. Для цього передбачено автентифікацію учасників контролю, перевірку унікальності первинних свідчень та обмеження частоти надсилання сигналів підозри.

Якщо серед m призначених спостерігачів не більш ніж f можуть діяти як візантійські учасники, виконання умови $k > f$ не дозволяє їм самостійно сформувати групову тривогу. Однак така умова не усуває ризику помилкових спрацьовувань добросовісних спостерігачів, зокрема за одночасного порушення зв'язності мережі. Крім того, успішна автентифікація повідомлення підтверджує використання відповідних криптографічних облікових даних, але не гарантує, що пристрій, який їх використовує, не був скомпрометований [18].

Для сценарію фізичного вилучення вузла можна визначити умовну верхню межу часу, необхідну для ухвалення рішення. Така оцінка ґрунтується на припущенні, що після вилучення пристрій більше не формує нових автентифікованих підтверджень, а часові мітки останніх контактів залишаються достовірними. Також необхідно, щоб щонайменше k спостерігачів могли своєчасно сформувати й передати сигнали підозри, а процедура повторної перевірки завершувалася протягом інтервалу δ . За виконання цих умов затримка ухвалення рішення обмежується співвідношенням:

$$T_d \leq \lambda + \delta + \Delta \quad (10)$$

де T_d -затримка формування підсумкового рішення від моменту фізичного вилучення вузла; λ - інтервал очікування підтвердження; δ - максимальна тривалість повторної перевірки; Δ - верхня межа додаткових затримок передавання групової тривоги, узгодження результатів та ухвалення рішення.

Наведена оцінка справедлива лише за умови, що для кожної із зазначених складових можна встановити скінченну верхню межу. Якщо мережа тривалий час залишається ізольованою, необхідна кількість спостерігачів недоступна або результати перевірки неможливо доставити до відповідного вузла прийняття рішень, гарантувати завершення процедури протягом визначеного часу неможливо.

ДОДАТКОВА АТЕСТАЦІЯ ТА ЕКСПЛУАТАЦІЙНІ ХАРАКТЕРИСТИКИ КОНТРОЛЮ

Контроль присутності не дозволяє виявити порушення програмної цілісності вузла, якщо пристрій продовжує працювати в мережі та використовує чинні криптографічні облікові дані. Для перевірки таких випадків може застосовуватися дистанційна атестація окремих компонентів. Надійність цього механізму залежить від наявності захищеного кореня довіри (root of trust), безпечного зберігання атестаційних секретів, коректності вимірювання програмного стану та можливості перевірити актуальність отриманих свідчень [4, 6, 8, 9].

Для оцінювання приймається припущення, що перевірки здійснюються відповідно до однорідного пуассонівського процесу з інтенсивністю v . При цьому кожна перевірка за наявності визначеного порушення дозволяє виявити його з умовною ймовірністю s . Якщо результати окремих перевірок незалежні, а ймовірність виявлення залишається сталою, то за властивістю проріджування пуассонівського процесу успішні виявлення утворюють окремий потік з інтенсивністю vs . За таких умов ймовірність виявлення хоча б одного порушення протягом заданого інтервалу часу T становить:

$$P_{d,att}(T) = 1 - \exp(-vsT) \quad (11)$$

Параметр s у цьому випадку відображає умовну ймовірність успішного виявлення порушення за встановлених припущень. Фактична результативність перевірки залежить від реалізації засобів захисту, складу контрольованих компонентів і характеру можливого втручання. Зокрема, компрометація кореня довіри, виконання шкідливого коду поза межами вимірюваного стану або порушення процедури формування атестаційних свідчень можуть істотно знизити ймовірність виявлення. Отже, залежність (11) застосовується лише до визначеного сценарію контролю цілісності та не характеризує всі можливі способи компрометації вузла.

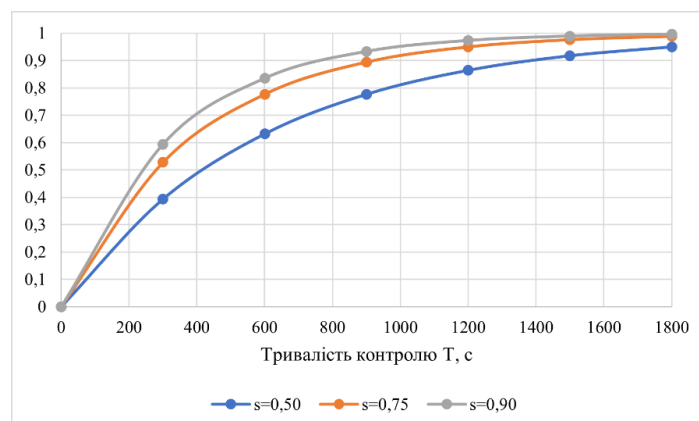


Рис. 6. Ймовірність виявлення визначеного порушення цілісності при $v=1/300 \text{ c}^{-1}$

Поряд із результативністю перевірки необхідно враховувати ресурсні обмеження сенсорних вузлів, насамперед обсяг доступної пам'яті, енергоспоживання та готовність спостерігачів до виконання контрольних функцій. Якщо кожен вузол здійснює спостереження не більш ніж за m іншими пристроями, обсяг пам'яті для зберігання поточних записів контролю зростає пропорційно кількості таких пристроїв. За умови призначення кожному з N вузлів рівно m спостерігачів сумарна кількість відповідних записів у мережі становить $O(Nm)$. Водночас наведені оцінки стосуються лише інформації про поточний стан спостережень і не враховують додаткову пам'ять, необхідну для криптографічних ключів, журналів аудиту, маршрутних таблиць, буферів повідомлень і списків відкликання.

Енергетичні витрати механізму протягом інтервалу контролю T залежать від кількості переданих і прийнятих повідомлень, виконаних криптографічних операцій та процедур дистанційної атестації. Для їх узагальненого оцінювання використовується співвідношення:

$$E(T) = n_{TX} E_{TX} + n_{RX} E_{RX} + n_{Cr} E_{Cr} + n_{ATT} E_{ATT} + E_{idle} \quad (12)$$

де n_{TX} , n_{RX} , n_{Cr} , n_{ATT} - кількість передавань, приймань, криптографічних операцій та процедур атестації відповідно; E_{TX} , E_{RX} , E_{Cr} , E_{ATT} - середні енергетичні витрати на виконання відповідних операцій; E_{idle} - витрати енергії в режимах простою або очікування. Для повідомлень різної довжини та криптографічних операцій різної складності необхідно враховувати відповідні індивідуальні витрати.

Для базового механізму періодичних повідомлень працездатності за інтервалу передавання τ і синхронізованого початку відліку кількість ініційованих повідомлень усією мережею протягом T визначається як:

$$M_{HB}(T) = N[T/\tau] \quad (13)$$

Отримана оцінка характеризує кількість повідомлень, ініційованих вузлами мережі, без урахування їх подальшого проходження через проміжні пристрої. Тому фактичне навантаження на канали зв'язку може бути більшим через багатоповову маршрутизацію, повторні передавання та додатковий обмін службовою інформацією.

Вибір параметрів λ, m, k, δ потребує узгодження кількох взаємопов'язаних характеристик: часу виявлення можливої недоступності вузла, ймовірності хибної тривоги, готовності групи спостерігачів та витрат енергії.

Залежно від вимог до мережі пріоритетом може бути зменшення енергоспоживання $E(T)$ або скорочення затримки реагування T_d за умови дотримання встановленого обмеження на ймовірність хибних спрацьовувань $P_{FA} \leq \alpha$. При цьому оптимальні значення параметрів неможливо визначити лише на основі

загальних аналітичних залежностей. Для їх обґрунтованого вибору необхідні дані про інтенсивність контактів між вузлами, стан радіоканалів, характер відмов обладнання та можливі сценарії атак.

Ще одним чинником, що впливає на роботу кооперативного механізму, є доступність спостерігачів у момент формування групової тривоги. Якщо кожен із m призначених спостерігачів незалежно від інших здатний своєчасно передати повідомлення з ймовірністю a , готовність групи визначається ймовірністю того, що необхідну інформацію зможуть доставити щонайменше k учасників. За прийнятого припущення про незалежність ця ймовірність обчислюється:

$$P_r(a; m, k) = \sum_{j=k}^m \binom{m}{j} a^j (1-a)^{m-j} \quad (14)$$

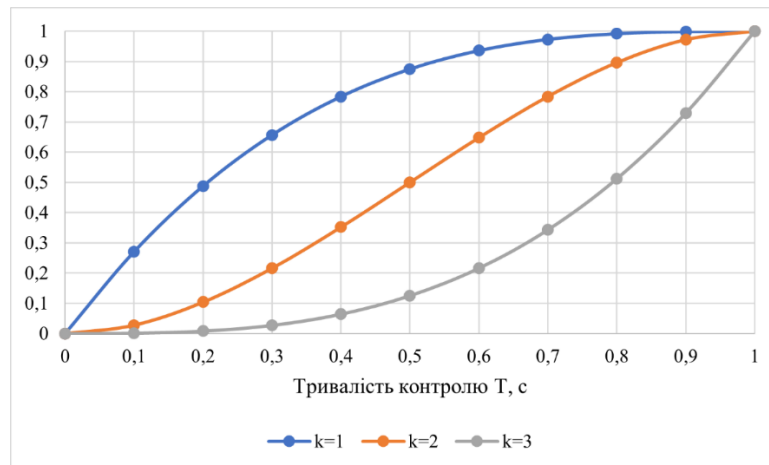


Рис. 7. Готовність групи із трьох незалежних спостерігачів за правилами $k=1, 2, 3$

Залежність (14) дозволяє оцінити готовність групи до своєчасного формування тривоги, але не визначає загальної ймовірності виявлення компрометації. Зокрема, вона не враховує достовірність первинних свідчень, можливість підроблення повідомлень і залежність між відмовами окремих спостерігачів. Тому отримані значення характеризують лише доступність механізму групового реагування за визначених умов.

Наприклад, для групи з трьох спостерігачів за ймовірності доступності кожного $a = 0,8$ готовність механізму становить 0,992 при $k = 1$, 0,896 при $k = 2$ та 0,512 при $k = 3$. Отримані значення показують, що підвищення порогу групової тривоги зменшує ймовірність своєчасного надходження необхідної кількості повідомлень. Водночас за незалежних спостережень вищий поріг дозволяє знизити ризик хибного спрацювання, оскільки для формування тривоги необхідне підтвердження від більшої кількості учасників. Таким чином, вибір порогу k має враховувати не лише вимоги до достовірності групового рішення, а й фактичну готовність спостерігачів забезпечити його формування в межах допустимого часу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі запропоновано аналітичну модель кооперативного контролю присутності вузлів безпроводової сенсорної мережі, призначену для оцінювання ймовірності хибних тривог за різних умов мережевої взаємодії. На основі пуассонівської моделі надходження підтверджень отримано залежності для визначення ймовірності відсутності нового автентифікованого повідомлення та формування групової тривоги за пороговим правилом k із m . Показано, що за умови незалежності спостережень збільшення контрольного інтервалу знижує ймовірність хибного спрацювання, але водночас подовжує час виявлення можливої недоступності вузла. Підвищення порогу групового підтвердження також зменшує ризик хибної тривоги, проте потребує більшої кількості доступних спостерігачів і може ускладнювати своєчасне формування групового рішення.

Уточнення моделі з урахуванням спільних порушень зв'язності дозволило визначити вплив залежності між локальними спостереженнями на ймовірність хибних тривог. Встановлено, що за наявності спільного розриву каналів збільшення часу очікування не усуває ризику помилкового спрацювання, нижня межа якого в прийнятій сценарній моделі визначається ймовірністю такого порушення. Додатково отримано залежність для оцінювання готовності групи спостерігачів до своєчасного формування тривоги. Ці результати дають змогу визначити взаємозв'язок між параметрами кооперативного контролю,



ймовірністю хибних спрацьовувань, затримкою реагування та доступністю учасників спостереження.

Розроблений алгоритм реагування передбачає послідовне формування локальної підозри, її групове підтвердження, повторну перевірку стану вузла та вибір захисних заходів відповідно до оціненого ризику. При цьому відсутність контакту не ототожнюється з фактом компрометації, оскільки може бути спричинена як фізичним вилученням пристрою, так і зміною його положення або порушенням радіозв'язку. Для випадків, коли скомпрометований вузол зберігає мережеву активність, розглянуто можливість застосування дистанційної атестації програмної цілісності. Отримано аналітичну залежність для оцінювання ймовірності виявлення визначеного порушення за заданої інтенсивності перевірок та їхньої умовної результативності. Також визначено основні складові витрат пам'яті й енергії, необхідні для організації розподіленого контролю.

Подальші дослідження доцільно спрямувати на уточнення моделі з урахуванням реальних розподілів міжконтактних інтервалів, статистичної залежності між спостереженнями та характеру спільних порушень зв'язності. Важливими залишаються питання стійкості групового контролю до компрометації окремих спостерігачів, вибору критеріїв тимчасової ізоляції вузлів і умов відновлення їхніх повноважень. Окремим напрямом є оцінювання ресурсних витрат на конкретних апаратних платформах та перевірка отриманих залежностей за різних сценаріїв мобільності, що дозволить уточнити межі застосування запропонованої моделі й обґрунтувати вибір параметрів контролю для практичного використання в безпроводових сенсорних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dovzhenko, N., Ivanichenko, Y., Mamchenko, S., Khvostichenko, V., & Hrechko, D. (2026). An extended model for assessing the security of cooperative establishment of secure channels in wireless sensor networks. *Cybersecurity: Education, Science, Technique*, 2(34), 744–756. <https://doi.org/10.28925/2663-4023.2026.34.1377>
2. Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2009). Mobility and cooperation to thwart node capture attacks in MANETs. *EURASIP Journal on Wireless Communications and Networking*, 2009, Article 945943. <https://doi.org/10.1155/2009/945943>
3. Dovzhenko, N., Barabash, O., Musienko, A., Ivanichenko, Y., & Krashenninnik, I. (2024). Enhancing sensor network efficiency through optimized flooding mechanism. *CEUR Workshop Proceedings*, 3654, 465–470. <https://doi.org/10.55056/ceur-ws.org/Vol-3654/short15.pdf>
4. Asokan, N., Brasser, F., Ibrahim, A., Sadeghi, A.-R., Schunter, M., Tsudik, G., & Wachsmann, C. (2015). SEDA: Scalable embedded device attestation. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)* (pp. 964–975). Association for Computing Machinery. <https://doi.org/10.1145/2810103.2813670>
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). IEEE. <https://doi.org/10.1109/SECPRI.2003.1199337>
6. Ambrosin, M., Conti, M., Lazzeretti, R., Rabbani, M. M., & Ranise, S. (2018). PADS: Practical attestation for highly dynamic swarm topologies. In *Proceedings of the 2018 International Workshop on Secure Internet of Things (SIoT)* (pp. 18–27). IEEE. <https://doi.org/10.1109/SIoT.2018.00009>
7. Dovzhenko, N., Ivanichenko, Y., & Sokolov, V. (2026). An adaptive model for cyber threat detection in IoT subsystems of data centers. *Cybersecurity: Education, Science, Technique*, 1(33), 716–727. <https://doi.org/10.28925/2663-4023.2026.33.1258>
8. Ambrosin, M., Conti, M., Lazzeretti, R., Rabbani, M. M., & Ranise, S. (2020). Collective remote attestation at the Internet of Things scale: State-of-the-art and future challenges. *IEEE Communications Surveys & Tutorials*, 22(4), 2447–2461. <https://doi.org/10.1109/COMST.2020.3008879>
9. Ankergård, S. F. J. J., Dushku, E., & Dragoni, N. (2021). State-of-the-art software-based remote attestation: Opportunities and open issues for Internet of Things. *Sensors*, 21(5), Article 1598. <https://doi.org/10.3390/s21051598>
10. Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2020). *IoT device cybersecurity capability core baseline* (NIST Interagency/Internal Report 8259A). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259A>
11. Openko, P., Dovzhenko, N., Orikhovskiy, 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>



12. Fagan, M., Megas, K., Cuthill, B., Marron, J., & Hoehn, B. (2026). *Foundational cybersecurity activities for IoT product manufacturers* (NIST Interagency/Internal Report 8259, Revision 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259r1>
13. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance in 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>
14. 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. <https://doi.org/10.1007/s12083-025-02194-3>
15. Chandra, T. D., & Toueg, S. (1996). Unreliable failure detectors for reliable distributed systems. *Journal of the ACM*, 43(2), 225–267. <https://doi.org/10.1145/226643.226647>
16. Chen, W., Toueg, S., & Aguilera, M. K. (2002). On the quality of service of failure detectors. *IEEE Transactions on Computers*, 51(5), 561–580. <https://doi.org/10.1109/TC.2002.1004595>
17. Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 49–63). IEEE. <https://doi.org/10.1109/SP.2005.8>
18. Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3), 382–401. <https://doi.org/10.1145/357172.357176>

**Nadiia M. Dovzhenko**

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

Yevhen V. 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

Roman V. Kyrychok

PhD, Associate Professor,
Associate Professor of the Department of Information and Cyber
Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9919-9691
r.kyrychok@kubg.edu.ua

**ANALYTICAL MODEL FOR ASSESSING INDICATORS OF NODE COMPROMISE IN WIRELESS
SENSOR NETWORKS**

Abstract. The development of wireless sensor networks and their increasing use in modern monitoring systems have created a need for improved mechanisms to detect potential node compromise, particularly under conditions of limited computational resources, unstable communication links, and the risk of physical node capture. Conventional presence-monitoring mechanisms based on periodic heartbeat messages cannot reliably distinguish between node unavailability caused by normal network conditions and violations of its software or hardware integrity. This paper proposes an analytical model for assessing indicators of potential node compromise based on threshold-based presence monitoring involving m designated observers and a $k - out - of - m$ decision rule. Assuming that independent authenticated confirmations arrive according to a Poisson process, analytical expressions are derived to estimate the probability of receiving no new confirmation and the probability of triggering a false group alarm. These expressions account for the contact arrival rate, the duration of the observation interval, and the cooperation threshold. The model is extended to incorporate correlated connectivity disruptions and observer availability. In addition, the decision-making procedure is refined by introducing a re-verification stage for suspicious nodes, while remote attestation is considered as an additional mechanism for detecting software integrity violations. The analytical results demonstrate how the probability of false alarms depends on contact patterns, the degree of cooperation, and correlated connectivity disruptions. It is shown that increasing the group confirmation threshold reduces the probability of false alarms but simultaneously decreases the likelihood of timely alarm generation. The derived relationships provide a theoretical basis for selecting the parameters of potential node compromise detection mechanisms while accounting for the operational characteristics of wireless sensor networks.

Keywords: wireless sensor network, Internet of Things (IoT), WSN, protection, node capture, node compromise, mobility, cooperation, alarm, security, reliability, probabilistic model.

REFERENCES

1. Dovzhenko, N., Ivanichenko, Y., Mamchenko, S., Khvostichenko, V., & Hrechko, D. (2026). An extended model for assessing the security of cooperative establishment of secure channels in wireless sensor networks. *Cybersecurity: Education, Science, Technique*, 2(34), 744–756. <https://doi.org/10.28925/2663-4023.2026.34.1377>



2. Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2009). Mobility and cooperation to thwart node capture attacks in MANETs. *EURASIP Journal on Wireless Communications and Networking*, 2009, Article 945943. <https://doi.org/10.1155/2009/945943>
3. Dovzhenko, N., Barabash, O., Musienko, A., Ivanichenko, Y., & Krashenninnik, I. (2024). Enhancing sensor network efficiency through optimized flooding mechanism. *CEUR Workshop Proceedings*, 3654, 465–470. <https://doi.org/10.55056/ceur-ws.org/Vol-3654/short15.pdf>
4. Asokan, N., Brasser, F., Ibrahim, A., Sadeghi, A.-R., Schunter, M., Tsudik, G., & Wachsmann, C. (2015). SEDA: Scalable embedded device attestation. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)* (pp. 964–975). Association for Computing Machinery. <https://doi.org/10.1145/2810103.2813670>
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). IEEE. <https://doi.org/10.1109/SECPRI.2003.1199337>
6. Ambrosin, M., Conti, M., Lazzeretti, R., Rabbani, M. M., & Ranise, S. (2018). PADS: Practical attestation for highly dynamic swarm topologies. In *Proceedings of the 2018 International Workshop on Secure Internet of Things (SIoT)* (pp. 18–27). IEEE. <https://doi.org/10.1109/SIoT.2018.00009>
7. Dovzhenko, N., Ivanichenko, Y., & Sokolov, V. (2026). An adaptive model for cyber threat detection in IoT subsystems of data centers. *Cybersecurity: Education, Science, Technique*, 1(33), 716–727. <https://doi.org/10.28925/2663-4023.2026.33.1258>
8. Ambrosin, M., Conti, M., Lazzeretti, R., Rabbani, M. M., & Ranise, S. (2020). Collective remote attestation at the Internet of Things scale: State-of-the-art and future challenges. *IEEE Communications Surveys & Tutorials*, 22(4), 2447–2461. <https://doi.org/10.1109/COMST.2020.3008879>
9. Ankergård, S. F. J. J., Dushku, E., & Dragoni, N. (2021). State-of-the-art software-based remote attestation: Opportunities and open issues for Internet of Things. *Sensors*, 21(5), Article 1598. <https://doi.org/10.3390/s21051598>
10. Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2020). *IoT device cybersecurity capability core baseline* (NIST Interagency/Internal Report 8259A). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259A>
11. Openko, P., Dovzhenko, N., Orikhovskiy, 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>
12. Fagan, M., Megas, K., Cuthill, B., Marron, J., & Hoehn, B. (2026). *Foundational cybersecurity activities for IoT product manufacturers* (NIST Interagency/Internal Report 8259, Revision 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259r1>
13. Dovzhenko, N., Ivanichenko, Y., Skladannyi, P., & Ausheva, N. (2024). Integration of security and fault tolerance in 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>
14. 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. <https://doi.org/10.1007/s12083-025-02194-3>
15. Chandra, T. D., & Toueg, S. (1996). Unreliable failure detectors for reliable distributed systems. *Journal of the ACM*, 43(2), 225–267. <https://doi.org/10.1145/226643.226647>
16. Chen, W., Toueg, S., & Aguilera, M. K. (2002). On the quality of service of failure detectors. *IEEE Transactions on Computers*, 51(5), 561–580. <https://doi.org/10.1109/TC.2002.1004595>
17. Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 49–63). IEEE. <https://doi.org/10.1109/SP.2005.8>
18. Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3), 382–401. <https://doi.org/10.1145/357172.357176>

Отримано редакцією журналу / Received: 21.08.26

Прорецензовано / Revised: 30.08.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.