

**Партика Ольга Олександрівна**

кандидат фізико-математичних наук, доцент,

доцент кафедри захисту інформації

Національний університет «Львівська політехніка», Львів, Україна

ORCID: 0000-0002-3086-3160

olha.o.mykhailova@lpnu.ua

**ЗАХИСТ РЕПУТАЦІЙНОГО МЕХАНІЗМУ БЕЗДРОТОВОЇ МЕРЕЖІ ВІД ПОМИЛКОВИХ
ООНОВЛЕНЬ ЗА НАЯВНОСТІ СКОМПРОМЕТОВАНИХ ВУЗЛІВ НА ОСНОВІ ТИПІЗОВАНОГО
ПРАВИЛА k - z - N**

Анотація. У бездротових мережах репутація вузла часто оновлюється шляхом порівняння його локального повідомлення з глобальним рішенням центру злиття. Якщо частина вузлів скомпрометована або мережа має неповне покриття, таке рішення не завжди є надійним еталоном: правильне повідомлення чесного вузла може не збігтися з глобальним результатом і спричинити необґрунтоване зниження його довіри. У роботі запропоновано типізоване подання результату правила k - z - N , яке не змінює бінарного рішення, але додатково розрізняє однозначний кворум, подвійний кворум, недосягнутий кворум, брак покриття та відсутність даних. Оновлення репутації виконується лише у випадках, коли сформовано однозначний кворум H_1 або H_0 . Коректність реалізації перевірено повним перебором 15 309 пар «конфігурація–квота». Експериментально порівняно класичне оновлення, фільтрацію за покриттям, двостороннє кворумне правило, байєсівські варіанти та бета-репутацію із забуванням. У базовому сценарії використовувались $N=7$, $k=4$, два скомпрометовані вузли та апіорна ймовірність H_1 , рівна 0,5. За $p_A=0,5$ класичне правило давало близько 34% несправедливих штрафів чесних вузлів, фільтрація за покриттям — близько 28%, а типізоване правило — 1,9%. Різниця середньої довіри між чесними та скомпрометованими вузлами становила близько 0,59. Абляційний аналіз показав, що за $k=4$ цей результат відтворюється простішим двостороннім кворумним правилом, тоді як за $k=3$ повна типологія дає невеликий додатковий ефект. Одержані результати показують, що врахування структури глобального рішення дає змогу зменшити кількість помилкових штрафів чесних вузлів без зміни базового правила k - z - N . Практично це означає, що центр злиття може відмовитися від оновлення репутації в раундах, де глобальний результат сформовано за недостатньої або суперечливої підтримки, не змінюючи при цьому самого алгоритму прийняття рішення.

Ключові слова: кібербезпека; бездротові мережі; компрометація вузлів; візантійська атака; оцінювання довіри; репутація вузлів; правило k - z - N ; злиття рішень.

ВСТУП

Постановка проблеми. У бездротовій мережі центр злиття може приймати рішення за повідомленнями багатьох вузлів. Якщо частина вузлів скомпрометована, атакувальник може змінювати їхні повідомлення і впливати не лише на поточне рішення, а й на подальшу репутацію учасників. Проблема виникає, коли глобальне рішення автоматично вважається правильним еталоном. За неповного покриття або суперечливих голосів такий еталон може бути хибним, і чесний вузол отримає негативне оновлення без фактичної помилки.

У цій роботі захищається саме етап оновлення довіри. Базове рішення k - z - N не змінюється. Додатково фіксується, як саме воно було отримане: за однозначного кворуму, за конфлікту двох кворумів, за недосягнутого кворуму, через брак покриття або за повної відсутності даних. Така інформація використовується як додаткова умова перед зміною репутації вузла.

Правило k - z - N є простим способом об'єднання локальних рішень [1]: глобальне H_1 формується, якщо його підтримали щонайменше k джерел; інакше повертається H_0 . Більш складні схеми, зокрема правило Чейра–Варшні [2], враховують характеристики локальних детекторів. Проте після отримання одного бінарного результату втрачається інформація про те, чи було рішення підтримане достатньою кількістю надійних повідомлень.

Для бездротових і сенсорних мереж це особливо важливо. Вузол може не мати зв'язку, не бачити



потрібну область або не отримати достатньо якісний сигнал. Під час виявлення безпілотних платформ [3] чи у V2X-коридорах [4] відсутність повідомлення не є еквівалентом голосу H_0 . Якщо її трактувати як негативне свідчення, репутаційний механізм починає карати чесні вузли за обмеження покриття.

У задачах кібербезпеки доцільно розрізняти дві причини розбіжності: природну невизначеність мережі та навмисне спотворення повідомлень. Перша виникає через покриття, втрати або різні умови спостереження; друга є наслідком компрометації вузла. У моделях візантійських атак скомпрометований вузол може навмисно передавати хибне локальне рішення [5, 6]. Якщо обидві ситуації обробляти однаково, механізм довіри сам стає об'єктом атаки.

Основне питання роботи полягає в тому, чи можна зменшити помилкове покарання чесних вузлів, якщо перед оновленням їхньої репутації враховувати структуру кворумного рішення?

Аналіз останніх досліджень і публікацій. Дослідження візантійських атак у розподіленому виявленні показують, що скомпрометовані вузли можуть істотно зміщувати результат злиття [5, 6]. Для протидії цьому використовують механізми довіри та репутації, зокрема у бездротових ad hoc і сенсорних мережах [29, 30], а також моделі конфліктних думок у суб'єктивній логіці [31, 32]. Спільна проблема цих підходів полягає в якості еталона, за яким оновлюється довіра.

Окремий клас робіт присвячений неповним і суперечливим свідченням. Теорія Демпстера-Шафера та її модифікації описують конфлікт, невизначеність і перерозподіл конфліктної маси [7–17]. У цій статті цей апарат використовується лише для формального розрізнення двох ситуацій: «джерела суперечать одне одному» і «даних недостатньо». Нове правило комбінування мас не пропонується.

Міри конфлікту [18–22] дають змогу оцінити силу розбіжності між джерелами, але сам конфлікт не показує, який саме вузол є скомпрометованим. Для репутаційного механізму важливо також відрізнити неправдиве повідомлення від нерелевантного або відсутнього спостереження [23, 24].

У схемах цензурування сенсорів мовчання може бути інформативним [26]. У цій роботі прийнято простішу семантику: A означає відсутність придатного локального свідчення. Такий стан не вважається голосом за H_0 і не повинен автоматично погіршувати репутацію вузла. Підходи відкритого світу [27, 28] тут не розглядаються.

Квотні правила та оператори злиття можуть допускати суперечливий результат [25], однак питання використання структури такого результату саме для захисту оновлення репутації вузлів вивчено значно менше. Ця задача розглядається далі.

Таблиця 1

Порівняння підходів, пов'язаних із конфліктом свідчень і квотними рішеннями

Родина правил	Де опиняється конфлікт	Зв'язок із правилом k-з-N	Чи розрізняються недосягнутий кворум і брак покриття
Правило Демпстера [7]	усувається нормалізацією; за повного конфлікту нормалізація неможлива		ні
Трансферабельна модель переконань [10]	залишається на $\emptyset$		ні, одна маса $m(\emptyset)$
Правило Ягера [11]	переноситься на θ		ні
Правило Дюбуа-Прада [12]	на об'єднання суперечливих елементів		ні
Усереднення з вагами достовірності [15, 16]	усувається до комбінування		ні
Збереження конфлікту як тривоги [17]	зберігається на $\emptyset$		ні
«Принаймні r із N релевантні» [24]	вибір гіпотези про поведінку джерел	збігається для категоричних голосів у спеціальному випадку	не виділено



Родина правил	Де опиняється конфлікт	Зв'язок із правилом k-3-N	Чи розрізняються недосягнутий кворум і брак покриття
Квотне злиття переконань [25]	допускається суперечливий результат	аналогічна квотна структура на рівні інтерпретацій	ні
Суб'єктивна логіка [31, 32]	окрема міра; злита думка її не містить		ні

Мета статті. Метою роботи є розроблення та перевірка механізму захищеного оновлення довіри до вузлів бездротової мережі за наявності скомпрометованих джерел. Для цього результат правила k-3-N доповнюється типом стану, а оновлення репутації виконується лише тоді, коли глобальне рішення має достатньо надійну структуру.

Модель загроз

Розглядається централізована бездротова система з центром злиття. Частина вузлів може бути скомпрометована, але атакувальник не контролює сам центр і не змінює параметри k , P_D або P_{FA} . У базовому сценарії активний скомпрометований вузол інвертує своє локальне рішення. Додатково перевіряється стратегія постійного H_0 . Мета атаки, впливати на глобальне рішення та, через нього, на репутацію чесних вузлів. Утримання A саме по собі атакою не вважається: воно може виникати через відсутність покриття або придатного спостереження.

МАТЕМАТИЧНА МОДЕЛЬ ТА МЕТОД ДОСЛІДЖЕННЯ

Вхідні повідомлення

У кожному раунді вузол передає одне з трьох повідомлень: H_1 , H_0 або A . H_1 та H_0 є локальними рішеннями, а A означає, що вузол не має придатного свідчення. Для подальших обчислень достатньо знати кількість повідомлень кожного типу:

$$c = (n_1, n_0, n_A), \quad n_1 + n_0 + n_A = N, \quad (1)$$

де n_1 — кількість голосів H_1 ; n_0 — кількість голосів H_0 ; n_A — кількість утримань; $n_{eff} = n_1 + n_0$ — кількість активних повідомлень. У межах прийнятої моделі A не прирівнюється ані до H_0 , ані до H_1 .

$$\delta_k(c) = \begin{cases} H_1, & n_1 \geq k, \\ H_0, & n_1 < k. \end{cases} \quad (2)$$

Класичне правило k-3-N формує тривогу, якщо $\geq k$. Інакше повертається. Саме це рішення надалі використовується як базове; типізація його не змінює.

Тип стану кворумного рішення

Для загального випадку використовуються квоти k_1 для H_1 та k_0 для H_0 . Спочатку визначається, яка з гіпотез уже набрала необхідний кворум:

$$C(c) = \{H_1: n_1 \geq k_1\} \cup \{H_0: n_0 \geq k_0\}. \quad (3)$$

Далі перевіряється, чи могла б гіпотеза досягти кворуму, якби утримані вузли надали активні повідомлення:

$$P(c) = \{H_1: n_1 + n_A \geq k_1\} \cup \{H_0: n_0 + n_A \geq k_0\}. \quad (4)$$

На цій основі виділяються п'ять змістовних ситуацій: однозначний кворум H_1 або H_0 , подвійний кворум (ПК), недосягнутий кворум (НК), брак покриття (БП) та відсутність даних (ВД). Для механізму довіри ці ситуації мають різне значення.

НК означає, що активних голосів достатньо, але жодна сторона не набрала своєї квоти. БП означає інше: активних повідомлень недостатньо для надійного рішення. ВД є граничним випадком, коли всі вузли утрималися.



$$\sigma(c) = \begin{cases} \text{ВД}, & n_{\text{eff}} = 0, \\ \text{ПК}, & C(c) = \emptyset, \\ H_1, & C(c) = \{H_1\}, \\ H_0, & C(c) = \{H_0\}, \\ \text{БП}, & C(c) = \emptyset, 0 < n_{\text{eff}} < \min(k_1, k_0), \\ \text{НК}, & C(c) = \emptyset, n_{\text{eff}} \geq \min(k_1, k_0). \end{cases} \quad (5)$$

$$R(c) = 1\{C(c) = \emptyset, P(c) \neq \emptyset\}.$$

Індикатор $R(c)=1$ означає, що жодна гіпотеза ще не досягла своєї квоти, але принаймні одна з них залишається досяжною з урахуванням наявних утримань. Показник використовується лише для опису структури невизначеного стану.

Бінарна проєкція визначена так само, як у класичному правилі k-з-N:

$$\pi(\sigma) = H_1 \Leftrightarrow \sigma \in \{H_1, \text{ПК}\} \quad (6)$$

Після типізації застосовується та сама бінарна проєкція, що й у класичному правилі k-з-N. Отже, запропоноване подання не змінює алгоритму виявлення, а використовується для визначення доцільності подальшого оновлення репутації вузлів.

Оцінювання конфлікту

Додатково використовується проста міра конфлікту між активними голосами, частка пар вузлів, що підтримують різні гіпотези:

$$C_{\text{pair}} = \frac{n_1 n_0}{\binom{n_{\text{eff}}}{2}}, \quad \tilde{C}_{\text{pair}} = \frac{C_{\text{pair}}}{C_{\text{max}}(n_{\text{eff}})}, \quad C_{\text{max}}(n) = \frac{\lfloor n/2 \rfloor \lfloor n/2 \rfloor}{\binom{n}{2}}, \quad n_{\text{eff}} \geq 2. \quad (7)$$

Показник характеризує ступінь розбіжності між активними повідомленнями. Він не використовується для безпосереднього визначення скомпрометованого вузла або як окреме правило блокування.

Властивості подання

Властивість 1. Типізація не змінює результату правила k-з-N: глобальне рішення формується тоді і тільки тоді, коли $\geq k$. Це забезпечує сумісність із базовою схемою злиття рішень.

Властивість 2. Для категоричних повідомлень множина $C(c)$ описує вже досягнуті квоти, а $P(c)$ — квоти, які ще можуть бути досягнуті за сприятливого розподілу утримань. Таке розбиття є спеціальним поданням результату квотного правила для категоричних свідчень і не розглядається як нове загальне правило комбінування.

Якщо кількість активних вузлів менша за квоту, фіксується стан БП або ВД. Якщо активних вузлів достатньо, але кворум не сформовано, виникає НК. Тому відсутність кворуму сама по собі не свідчить про помилкову поведінку окремого вузла.

Властивість 3. За відсутності утримань подвійний кворум ПК досяжний тоді і тільки тоді, коли $k_1 + k_0 \leq N$. Недосягнутий кворум НК досяжний тоді і тільки тоді, коли $k_1 + k_0 \geq N + 2$. Ці умови перевірено для всіх 49 пар (k_1, k_0) при $N=7$.

Для симетричних квот за малих значень k можливе виникнення подвійного кворуму, а за великих значень k — недосягнутого кворуму. Наявність утримань збільшує кількість невизначених станів.

Властивість 4. Утримання A не є еквівалентним голосу або . Для заміни $A \rightarrow$ бінарне рішення не змінилося в жодній із 15 309 перевірок, однак типізований стан змінився у 8 337 випадках. Вони відповідають 118 унікальним парам «вектор лічильників–квота» та 28 різним векторам лічильників. Для заміни $A \rightarrow$ типізований стан також змінився у 8 337 випадках, а бінарне рішення — у 5 103 випадках.

Властивість 5. За ієрархічного об'єднання необхідно передавати лічильники голосів, а не лише локальні мітки станів, оскільки однакові локальні мітки можуть після об'єднання приводити до різних глобальних результатів.

Властивість 6. Для бінарних категоричних повідомлень C_{pair} збігається із середньою попарною відстанню Жуссельма. У роботі ця рівність використовується як додаткова перевірка правильності реалізації.

Властивість 7. Для однорідних незалежних джерел імовірність активного позитивного повідомлення дорівнює $q=(1-p_A)p$, де $p=P_D$ за H_1 і $p=P_{FA}$ за H_0 . Тоді $n_1 \sim \text{Bin}(N, q)$, а класична ймовірність тривоги дорівнює сумі ймовірностей станів H_1 і ПК. Ця рівність використовується як перевірка узгодженості реалізації.



$$P(H_1) + P(\text{ПК}) = \sum_{j=k}^N \binom{N}{j} q^j (1-q)^{N-j}. \quad (8)$$

Типізоване правило оновлення довіри

Типізоване правило оновлення визначено так. Для активного вузла репутація оновлюється лише у станах $\sigma(c) \in \{H_1, H_0\}$; у станах ПК, НК, БП і ВД оновлення пропускається. Еталонним рішенням у типізованому правилі є класична бінарна проєкція δ_k . Отже, типізація не змінює рішення k-з-N, а лише визначає, чи дозволено використовувати його для зміни репутації.

$$\Lambda(\sigma) = \frac{P(\sigma|H_1)}{P(\sigma|H_0)}. \quad (9)$$

Окремо досліджувалась інформативність стану БП щодо істинної гіпотези. За однакових імовірностей утримання для H_1 і H_0 цей стан не надає переваги жодній з гіпотез. Якщо ймовірність утримання залежить від гіпотези, стан БП може містити додаткову інформацію.

$$P(\text{БП} | H_j) = \sum_{m=1}^{k-1} C(N, m) (1 - p_{A,j})^m p_{A,j}^{N-m}$$

Наприклад, за $N=7$ і $k=4$ різні ймовірності утримання для H_1 та H_0 істотно змінюють відношення правдоподібності стану БП. Це вказує на необхідність окремого оцінювання параметрів покриття для конкретної мережі.

$$t_i = \frac{r_i + 1}{r_i + s_i + 2} \quad (10)$$

Довіру вузла оцінювали за бета-репутацією [33]: $t_i = (r_i + 1) / (r_i + s_i + 2)$, де r_i і s_i — накопичені позитивні та негативні оновлення. Для активного вузла r_i збільшується на одиницю, якщо його локальне рішення збігається з еталоном, інакше на одиницю збільшується s_i ; для А оновлення не виконується. Частка несправедливих штрафів (ЧНШ) визначається як відношення кількості негативних оновлень чесних активних вузлів, локальний голос яких відповідав істинній гіпотезі, до кількості таких чесних правильних голосів, для яких відповідне правило фактично виконало оновлення.

Контрольні правила визначено так: класичне правило оновлює кожне активне повідомлення за еталоном; фільтрація за покриттям виконує оновлення лише за $\geq k$; двостороннє кворумне правило — лише за $\geq k$. Для цих трьох правил і для типізованого правила еталоном є.

Байєсівське правило використовує знак логарифмічного відношення правдоподібностей LLR як еталон і виконує оновлення в кожному активному спостереженні. За апіорної ймовірності та однакової для обох гіпотез: $\text{LLR} = \ln(\cdot) + \ln[(1-)/(1-)]$. Байєсівське правило з порогом упевненості виконує оновлення лише за $\cdot$, що відповідає апостеріорній ймовірності не менше 0,95 для однієї з гіпотез. У варіанті із забуванням перед кожним новим оновленням застосовується $\leftarrow \lambda$, $\leftarrow \lambda$ з $\lambda = 0,98$, після чого використовується класичний еталон.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

Експериментальне дослідження проводилось у два етапи. На першому етапі повним перебором перевірено реалізацію типізованих станів для $N=7$ та всіх значень $k=1, \dots, 7$. Загалом проаналізовано 15 309 пар «конфігурація-квота».

На другому етапі виконано моделювання атаки на репутаційний механізм. Оцінювали частоту помилкового штрафування чесних вузлів та ступінь розділення рівнів довіри до чесних і скомпрометованих вузлів після серії раундів.

У базовій конфігурації прийнято $P_D=0,80$, $P_{FA}=0,05$, $p_A=0,30$ та $P(H_1) = 0,5$. Для відтворюваності результатів використано фіксоване зерно генератора 20261010. Байєсівський контрольний варіант використовував номінальні характеристики чесного локального детектора і не враховував частку скомпрометованих вузлів явно.

Основний сценарій містив $N=7$ вузлів, з яких $B=2$ були скомпрометованими; $k=4$, $T=500$ раундів. Кожен вузол, у тому числі скомпрометований, утримувався з однаковою ймовірністю p_A . Якщо скомпрометований вузол був активним, він інвертував локальне рішення. Для кожного значення p_A виконано 300 незалежних прогонів і визначено 95% довірчі інтервали.



Порівнювали такі показники: різницю середньої довіри Δt між чесними та скомпрометованими вузлами; AUC після 30 раундів, де позитивним класом вважали чесні вузли, а оцінкою — t_i ; частку несправедливих штрафів (ЧНШ); частку активних спостережень, за якими правило виконало оновлення; частку негативних оновлень скомпрометованих вузлів.

Таблиця 2

Результати повної перевірки реалізації формальних властивостей ($N = 7$)

№	Властивість	Результат	Обсяг перевірки
1	Точне зведення до правила k -з- N	виконано	15 309 пар
2	Узгодженість множин $C(c)$ і $P(c)$ з категоричним квотним правилом	виконано	15 309 пар
3	Умови досяжності станів ПК і НК	виконано	49 пар (k_1, k_0)
4	Утримання не еквівалентне голосу H_0 за типізованим станом	рішення не змінилося в жодній парі; стан змінився у 8 337 випадках	15 309 пар
5	Стани некомпозиційні; лічильники композиційні	116 неоднозначних із 494 пар міток (k , розмір кластера, стан А, стан В)	усі k та розбиття на кластери
6	C_{pair} = середня попарна відстань Жуссельма для категоричних бінарних свідчень	виконано	15 204 пари з $n_{eff} \geq 2$
7	$P(\sigma=)+P(\sigma=ПК)$ = біноміальна ймовірність тривоги	виконано	усі $k = 1, \dots, 7$

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Перевірка типізації та приклади

Повний перебір підтвердив коректність реалізації. Заміна А на H_0 не змінює класичного рішення k -з- N , однак у багатьох випадках змінює структурний стан. Отже, однакове глобальне рішення H_0 може бути отримане за різної структури вхідних повідомлень.

Заміна А $\rightarrow$ змінила типізований стан у 8 337 перевірях. На рівні унікальних конфігурацій це 118 пар «вектор лічильників–квота», що охоплюють 28 різних векторів лічильників. Виявлено п'ять типів переходів: БП $\rightarrow$, БП $\rightarrow$ НК, $\rightarrow$ ПК, НК $\rightarrow$ та ВД $\rightarrow$.

Для репутаційної системи це означає, що вузол без достатнього покриття не повинен оцінюватися так само, як активний вузол, повідомлення якого суперечить прийнятому рішення.

Таблиця 3

Приклади типізованих станів для $N = 7$

Параметри	Стан	$C(c)$	$P(c)$	Проекція	C_{pair}
$k = 3; (7, 0, 0)$	H_1	$\{H_1\}$	$\{H_1\}$	H_1	0,00
$k = 3; (4, 3, 0)$	ПК	$\emptyset$	$\emptyset$	H_1	0,57
$k = 5; (4, 3, 0)$	НК	$\emptyset$	$\emptyset$	H_0	0,57
$k = 4; (4, 2, 1)$	H_1	$\{H_1\}$	$\{H_1\}$	H_1	0,53
$k = 4; (3, 3, 1)$	НК	$\emptyset$	$\emptyset$	H_0	0,60
$k = 4; (3, 0, 4)$	БП	$\emptyset$	$\emptyset$	H_0	0,00
$k = 4; (0, 0, 7)$	ВД	$\emptyset$	$\emptyset$	H_0	-

Для конфігурації (3,3,1) за $k=4$ шість вузлів передають активні, але суперечливі голоси, а одне повідомлення відсутнє. У такому випадку глобальне рішення H_0 має обмежену придатність як еталон для оцінювання окремих вузлів.

Для конфігурації (3,0,4) за $k=4$ три активні вузли підтримують H_1 , а між їхніми повідомленнями

немає конфлікту. Однак кворум не досягається, і класичне правило повертає H_0 . Якщо це H_0 безумовно використовувати як еталон, правильні активні вузли можуть одержати негативне оновлення лише через недостатню кількість повідомлень.

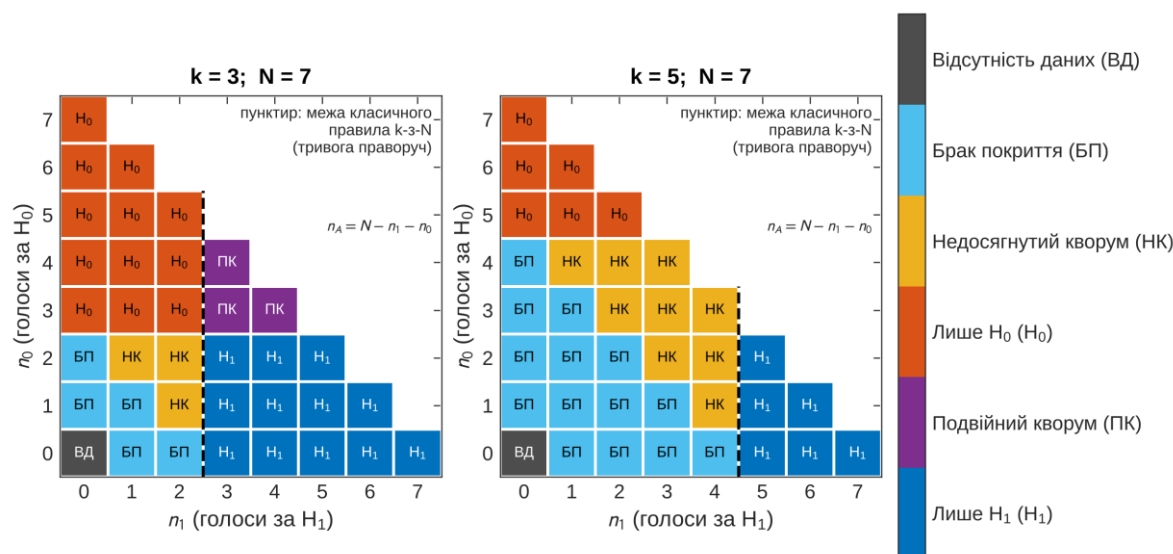


Рис. 1. Типізовані стани в площині (n_1, n_0) для $N=7$ і квот $k=3$ (ліворуч) та $k=5$ (праворуч); НК, недосягнутий кворум; пунктир, межа класичного правила $k-3-N$

На рис. 1 показано, що однаковому бінарному результату можуть відповідати різні структурні стани. Саме ця інформація використовується під час прийняття рішення щодо оновлення довіри.

Як часто виникають небезпечні для репутації стани

За базових параметрів і $k=4$ ймовірність правильної тривоги становить близько 0,63. Значна частина пропусків при цьому пов'язана не з активною підтримкою H_0 , а з недосягнутим кворумом або браком покриття.

За H_1 лише близько 2,5% пропусків відповідають активному стану H_0 . Решта припадає на НК, БП або ВД. Тому використання кожного глобального H_0 як безумовного еталона для оновлення репутації може приводити до помилкових штрафів.

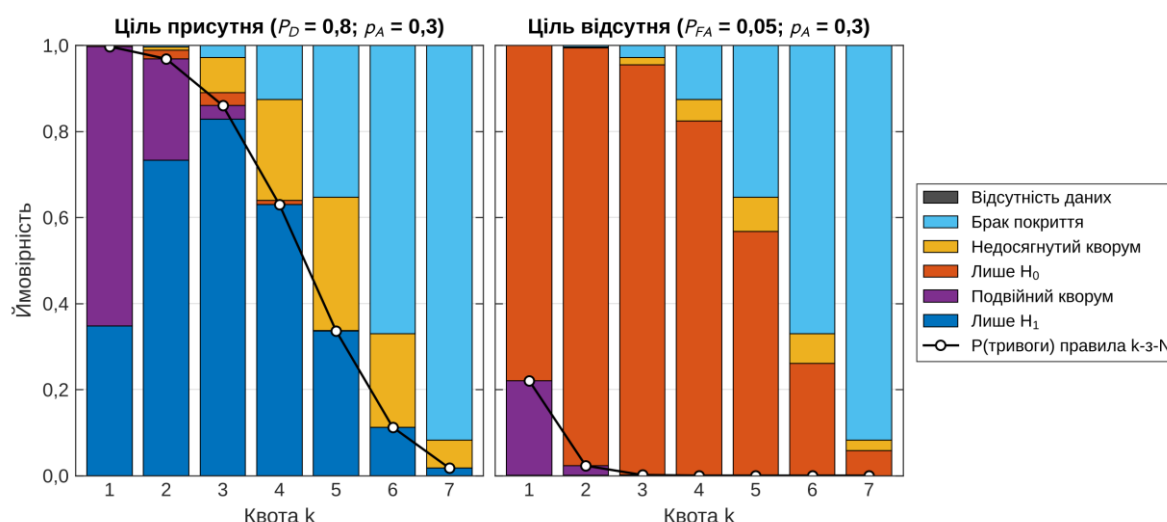


Рис. 2. Ймовірності типізованих станів залежно від квоти k за присутності (ліворуч) і відсутності (праворуч) цілі; $N=7$, $P_D=0,8$, $P_{FA}=0,05$, $p_A=0,3$

Відношення правдоподібності станів (9) наведено в табл. 4.



Таблиця 4

Відношення правдоподібності $\Lambda(\sigma)$ типізованих станів ($N = 7, P_D = 0,8, P_{FA} = 0,05, p_A = 0,3$)

k	H_1	ПК	H_0	НК	БП
1	$1,4 \cdot 10^3$	2,9	0,0038	-	-
2	$8,3 \cdot 10^2$	11	0,020	3,4	1,0
3	$1,6 \cdot 10^3$	38	0,031	4,8	1,0
4	$1,3 \cdot 10^4$	-	0,011	4,7	1,0
5	$3,2 \cdot 10^5$	-	0,0016	3,9	1,0
6	$9,0 \cdot 10^6$	-	$1,8 \cdot 10^{-4}$	3,1	1,0
7	$2,7 \cdot 10^8$	-	$1,8 \cdot 10^{-5}$	2,6	1,0

Примітка. «-», стан недосяжний за даної квоти. Для стану ВД $\Lambda = 1$ за всіх k.

Дані табл. 4 свідчать, що типізовані стани мають різну інформативність. За однакової ймовірності утримання для H_1 та H_0 стан БП є нейтральним, тоді як НК у базовому сценарії частіше виникає за H_1 . Отже, два однакові бінарні рішення H_0 можуть мати різну інформаційну цінність.

Тому під час оновлення репутації доцільно враховувати не лише кінцеве рішення H_0/H_1 , а й структуру голосів, за якої це рішення було отримане.

На рис. 3 показано, що зі зростанням p_A збільшується частка пропусків, пов'язаних з недостатньою кількістю активних повідомлень. Для розріджених або нестабільних мереж це підвищує імовірність помилкового штрафування чесних вузлів.

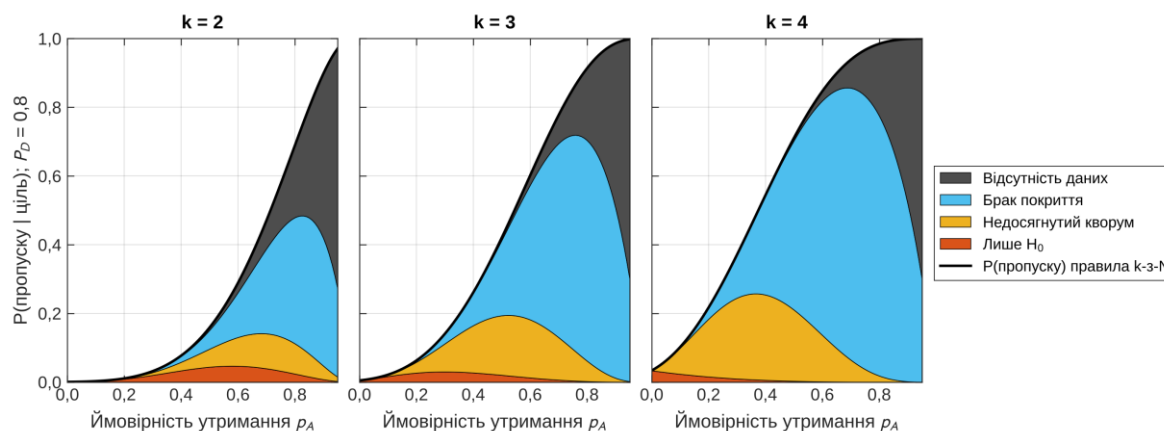


Рис. 3. Розклад імовірності пропуску класичного правила k-з-N за станами H_0 , НК, БП і ВД залежно від p_A для $k=2,3,4$; $N=7$, $P_D=0,8$

Таблиця 5

Частка пропусків класичного правила, зумовлених браком покриття (стани БП і ВД), %; $N = 7, P_D = 0,8$

k	$p_A = 0,1$	$p_A = 0,3$	$p_A = 0,5$	$p_A = 0,7$
1	0,1	6,8	27,9	56,2
2	0,2	12,0	39,4	70,1
3	0,8	20,5	54,0	83,3
4	2,7	34,0	70,4	93,1
5	8,3	53,2	85,6	98,2
6	23,9	75,5	95,6	99,7
7	58,0	93,4	99,4	100,0



За $k=4$ частка пропусків, пов'язаних лише зі станами БП і ВД, зростає приблизно з 34% при $p_A=0,3$ до 70% при $p_A=0,5$. Якщо врахувати також НК, загальний вплив утримань і недостатньої кількості активних голосів є ще більшим. Це обґрунтовує введення додаткової умови перед оновленням репутації.

Вплив на репутацію чесних і скомпрометованих вузлів

Основний експеримент був спрямований на оцінювання частоти помилкового штрафування чесних вузлів під час атаки. За $k=4$ типізоване правило збігається з двостороннім кворумним правилом, тому цей сценарій відображає насамперед ефект відмови від оновлення довіри за недостатньо обґрунтованого глобального рішення.

Таблиця 6

Порівняння правил оновлення довіри ($N=7$, $k=4$, два скомпрометовані вузли, $T=500$, 300 прогонів; «Байєс» у таблиці означає правило без порогу впевненості)

p_A	Правило	Δt , 95% ДІ	AUC ₃₀	ЧНШ, %, 95% ДІ	Частка оновлень
0,1	класичне	0,566 [0,563; 0,568]	1,000	11,0 [10,9; 11,2]	1,000
0,1	покриття	0,566 [0,564; 0,569]	1,000	11,0 [10,9; 11,1]	0,999
0,1	Байєс без порогу	0,547 [0,544; 0,550]	1,000	10,5 [10,4; 10,7]	1,000
0,1	забування	0,543 [0,536; 0,550]	1,000	11,0 [10,9; 11,2]	1,000
0,1	типізоване	0,665 [0,663; 0,668]	1,000	4,9 [4,8; 5,0]	0,861
0,3	класичне	0,388 [0,384; 0,392]	0,987	23,0 [22,8; 23,2]	1,000
0,3	покриття	0,407 [0,403; 0,411]	0,989	21,2 [21,0; 21,4]	0,929
0,3	Байєс без порогу	0,406 [0,403; 0,410]	0,992	14,8 [14,6; 15,0]	1,000
0,3	забування	0,365 [0,357; 0,373]	0,986	23,0 [22,8; 23,2]	1,000
0,3	типізоване	0,660 [0,656; 0,663]	0,999	3,1 [3,0; 3,2]	0,531
0,5	класичне	0,249 [0,245; 0,253]	0,913	34,3 [34,1; 34,6]	1,000
0,5	покриття	0,300 [0,294; 0,306]	0,897	28,4 [28,1; 28,7]	0,657
0,5	Байєс без порогу	0,304 [0,300; 0,308]	0,935	15,8 [15,6; 15,9]	1,000
0,5	забування	0,231 [0,221; 0,240]	0,910	34,3 [34,1; 34,6]	1,000
0,5	типізоване	0,585 [0,578; 0,592]	0,946	1,9 [1,8; 2,1]	0,240

За $p_A=0,5$ класичне оновлення приводить приблизно до 34% несправедливих штрафів правильних голосів чесних вузлів. Фільтрація лише за кількістю активних вузлів знижує цей показник до 28%, байєсівське правило — до 16%, а типізоване правило — до 1,9%. Основний ефект, таким чином, полягає у зменшенні кількості помилкових оновлень репутації.

Різниця середньої довіри між чесними та скомпрометованими вузлами при цьому становить

приблизно 0,59. Це покращує їх подальше розділення за рівнем довіри. Застосування забування історії не усуває причину помилкового оновлення, оскільки не змінює глобального еталона.

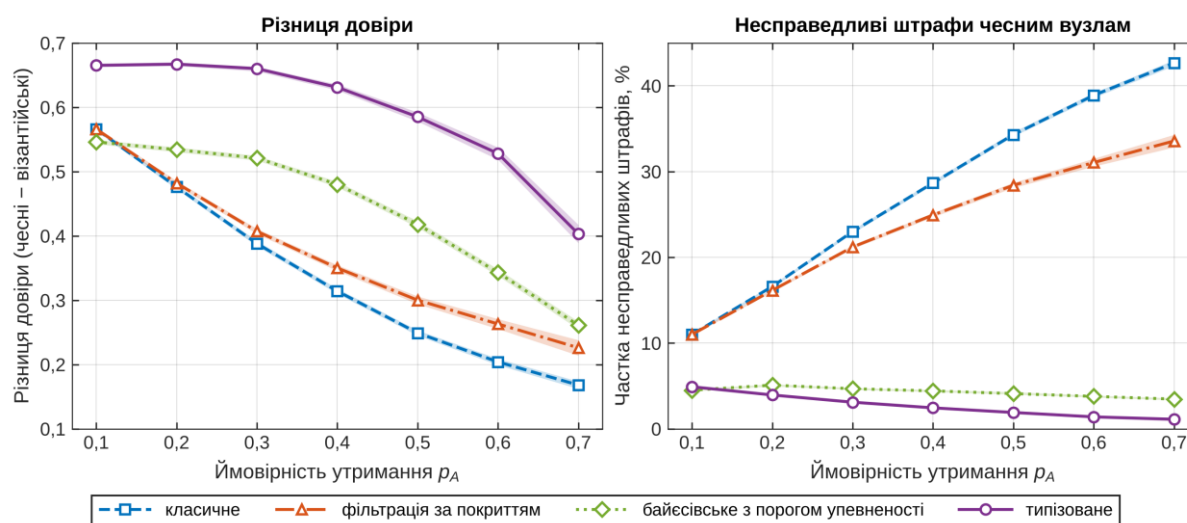


Рис. 4. Різниця довіри (ліворуч) і частка несправедливих штрафів (праворуч) залежно від p_A ; $N=7$, $k=4$, $B=2$, $T=500$, 300 прогонів; смуги — 95% ДІ.

На рисунку байєсівське правило подано з порогом упевненості $|LLR| \geq \ln 19$. Для $k=4$ типізоване правило збігається з двостороннім кворумним правилом, тому його крива окремо не наводиться.

На рис. 4 наведено співвідношення між точністю оновлення та його частотою. Типізоване правило забезпечує найменшу частку несправедливих штрафів, але оновлює репутацію лише приблизно у чверті активних спостережень. Байєсівське правило з порогом упевненості виконує оновлення частіше, але має більшу частку помилкових штрафів.

Перевірка стійкості результатів

У додаткових сценаріях змінювали кількість вузлів, частку скомпрометованих учасників, характеристики локального детектора та ймовірність утримання. Для табл. 7 використано окрему серію моделювання з $T=400$ та 200 незалежними прогонами. Тому значення $S2$ і $S6$ не повинні точно збігатися з відповідними рядками табл. 6, де $T=500$ і 300 прогонів.

Таблиця 7

Аналіз чутливості: фільтрація за покриттям і типізоване оновлення ($T=400$, 200 прогонів)

Сценарій	Параметри	Δt , за покриттям	Δt , типізоване	ЧНШ, за покриттям, %	ЧНШ, типізоване, %
S1	$N=5$, $B=1$, $k=3$; $P_D=0,8$, $P_{FA}=0,05$, $p_A=0,3$	0,486 [0,480; 0,491]	0,682 [0,677; 0,687]	14,3 [14,0; 14,5]	2,2 [2,1; 2,3]
S2	$N=7$, $B=2$, $k=4$; $P_D=0,8$, $P_{FA}=0,05$, $p_A=0,3$	0,413 [0,408; 0,418]	0,661 [0,655; 0,666]	20,8 [20,5; 21,0]	3,0 [2,9; 3,1]
S3	$N=9$, $B=2$, $k=5$; $P_D=0,8$, $P_{FA}=0,05$, $p_A=0,3$	0,441 [0,436; 0,447]	0,725 [0,720; 0,729]	19,3 [19,0; 19,6]	1,1 [1,1; 1,2]
S4	$N=7$, $B=2$, $k=4$; $P_D=0,7$, $P_{FA}=0,1$, $p_A=0,3$	0,332 [0,327; 0,337]	0,467 [0,461; 0,473]	23,3 [23,1; 23,6]	6,2 [6,0; 6,4]
S5	$N=7$, $B=2$, $k=4$; $P_D=0,9$, $P_{FA}=0,02$, $p_A=0,3$	0,504 [0,499; 0,510]	0,843 [0,840; 0,846]	18,3 [18,1; 18,6]	0,9 [0,8; 0,9]



Сценарій	Параметри	Δt , за покриттям	Δt , типізоване	ЧНШ, за покриттям, %	ЧНШ, типізоване, %
S6	$N=7, B=2, k=4;$ $P_D=0,8, P_{FA}=0,05,$ $p_A=0,5$	0,298 [0,291; 0,305]	0,592 [0,583; 0,601]	28,7 [28,3; 29,1]	1,8 [1,6; 1,9]

У всіх шести сценаріях типізоване правило забезпечувало більшу різницю довіри та меншу частку несправедливих штрафів, ніж проста фільтрація за покриттям. Абсолютні значення показників залежали від параметрів мережі, тому вибір порогів потребує окремого налаштування.

Абляція та сильніші атаки

Для відокремлення внеску повної типології від простішого кворумного обмеження проведено абляційний аналіз. За $k=4$ типізоване правило і двостороннє кворумне правило еквівалентні. За $k=3$, коли можливий подвійний кворум, повна типологія дає невеликий додатковий ефект. Окремо розглянуто сценарій із трьома скомпрометованими вузлами та стратегію постійного H_0 .

Таблиця 8

Абляція та додаткові контрольні сценарії ($N=7, T=500, 300$ прогонів)

Сценарій	Правило	Δt	ЧНШ, %	Частка оновлень	Негативні оновлення скомпрометованих, %
$k=4, p_A=0,5$	двостороннє кворумне	0,585 [0,578; 0,592]	1,9 [1,8; 2,1]	0,240	65,3
$k=4, p_A=0,5$	типізоване	0,585 [0,578; 0,592]	1,9 [1,8; 2,1]	0,240	65,3
$k=4, p_A=0,5$	байєсівське з порогом	0,418 [0,413; 0,423]	4,1 [4,0; 4,3]	0,525	52,0
$k=3, p_A=0,5$	двостороннє кворумне	0,549 [0,544; 0,554]	5,6 [5,5; 5,7]	0,614	65,4
$k=3, p_A=0,5$	типізоване	0,562 [0,557; 0,566]	4,9 [4,8; 5,0]	0,591	65,5
стале $H_0, p_A=0,3$	типізоване	0,138 [0,135; 0,141]	3,4 [3,3; 3,5]	0,662	21,2
стале $H_0, p_A=0,3$	байєсівське з порогом	0,311 [0,308; 0,313]	0,45 [0,43; 0,47]	0,836	38,0
$B=3/7, p_A=0,3$	типізоване	0,363 [0,358; 0,368]	14,3 [14,1; 14,6]	0,384	51,6

Результати табл. 8 визначають межі застосування запропонованого підходу. За стратегії постійного H_0 байєсівське правило з порогом упевненості має кращі показники, ніж типізоване правило. Отже, запропонований підхід призначений для зменшення кількості помилкових оновлень репутації і не розглядається як універсальний метод виявлення візантійської поведінки.

ОБГОВОРЕННЯ

Одержані результати стосуються безпеки репутаційного механізму і не передбачають зміни самого правила k -з- N . Якщо глобальне рішення безумовно використовується як еталон, неповне покриття та повідомлення скомпрометованих вузлів можуть спричинити помилкове зниження довіри до чесних учасників.

Запропонований підхід не визначає конкретного атакувальника, а лише обмежує використання недостатньо надійного глобального рішення під час оновлення репутації. Для ідентифікації окремого



зловмисного вузла необхідні додаткові ознаки, зокрема історія поведінки, фізична узгодженість вимірювань, просторові обмеження або припущення щодо чесної більшості.

У прийнятій моделі А означає відсутність придатного спостереження, а не прихований негативний голос. Стратегічне утримання атакувальника в експериментах не моделювалось. Тому отримані висновки не поширюються на атаку, за якої скомпрометовані вузли навмисно створюють неоднозначні стани і тим самим «заморожують» оновлення репутації.

Типізований стан може бути реалізований між модулем злиття рішень і модулем репутації. Така реалізація не потребує зміни локальних детекторів і не впливає на основне рішення щодо події, а лише визначає можливість використання цього рішення для оновлення довіри.

Результати для сильніших атак показують обмеженість захисного ефекту. За збільшення частки скомпрометованих вузлів або використання ними стратегії постійного H_0 різниця довіри зменшується, а частка несправедливих штрафів зростає. Це узгоджується з тим, що в базовій моделі поведінка атакувальника явно не оцінюється.

До основних обмежень дослідження належать бінарна постановка, однорідність і незалежність джерел, фіксовані характеристики локального детектора та однакова ймовірність утримання для H_1 і H_0 . Окремий контрольний сценарій $B=0$ у цій роботі не виконувався, тому внесок природних утримань і внесок компрометації у величину несправедливих штрафів не розділено експериментально. Такий контроль доцільно включити до подальшого дослідження.

Подальші дослідження доцільно спрямувати на аналіз стратегічного утримання, on-off атак, змови вузлів, глушіння, залежних помилок і гетерогенних джерел. Окремої уваги потребує обмеження тривалих періодів без оновлення репутації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі розглянуто спосіб оновлення довіри до вузлів бездротової мережі за наявності скомпрометованих джерел. На відміну від класичного підходу, глобальне рішення k -з- N не використовується безумовно як еталон для зміни репутації.

Глобальний результат доповнюється типом стану: однозначний кворум, подвійний кворум, недосягнутий кворум, брак покриття або відсутність даних. Наукова новизна полягає у використанні цієї структурної інформації як умови оновлення довіри, а не у введенні нового загального правила комбінування свідчень.

У базовому сценарії з двома скомпрометованими вузлами типізоване правило зменшило частку несправедливих штрафів чесних вузлів до 1,9% і забезпечило різницю довіри між чесними та скомпрометованими вузлами близько 0,59. Абляційний аналіз показав, що за $k=4$ такий ефект забезпечується також двостороннім кворумним правилом, а повна типологія дає додатковий результат лише за конфігурацій, у яких можливий подвійний кворум.

Одержані результати свідчать, що врахування структури глобального рішення дає змогу зменшити кількість помилкових оновлень репутації. Такий підхід є найбільш доцільним для розріджених бездротових мереж, де відсутність повідомлення часто зумовлена особливостями покриття, а не зловмисною поведінкою.

Подальші дослідження передбачають аналіз стратегічного мовчання, on-off атак, змови вузлів, глушіння, залежних джерел та адаптивного вибору порогів оновлення довіри.

ДЕКЛАРАЦІЯ ЩОДО ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ

Під час підготовки рукопису ChatGPT (OpenAI, GPT-5.6) і Claude (Anthropic) використовувалися для мовного та структурного редагування та допоміжної перевірки коду. Числові результати отримано за програмним кодом експериментів; рисунки побудовано засобами Python на основі одержаних даних. Остаточні результати й висновки перевірені автором.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Varshney, P. K. (1997). Distributed detection and data fusion. Springer. <https://doi.org/10.1007/978-1-4612-1904-0>
2. Chair, Z., & Varshney, P. K. (1986). Optimal data fusion in multiple sensor detection systems. IEEE Transactions on Aerospace and Electronic Systems, AES-22(1), 98–101. <https://doi.org/10.1109/TAES.1986.310699>
3. Svanström, F., Alonso-Fernandez, F., & Englund, C. (2022). Drone detection and tracking in real-time by



- fusion of different sensing modalities. *Drones*, 6(11), 317. <https://doi.org/10.3390/drones6110317>
4. Partyka, O., Imoize, A. L., & Li, C.-T. (2026). Cooperative V2X-based UAV detection in rural transportation corridors. *Drones*, 10(2), 153. <https://doi.org/10.3390/drones10020153>
 5. Marano, S., Matta, V., & Tong, L. (2009). Distributed detection in the presence of Byzantine attacks. *IEEE Transactions on Signal Processing*, 57(1), 16–29. <https://doi.org/10.1109/TSP.2008.2007335>
 6. Rawat, A. S., Anand, P., Chen, H., & Varshney, P. K. (2011). Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks. *IEEE Transactions on Signal Processing*, 59(2), 774–786. <https://doi.org/10.1109/TSP.2010.2091277>
 7. Dempster, A. P. (1967). Upper and lower probabilities induced by a multivalued mapping. *The Annals of Mathematical Statistics*, 38(2), 325–339. <https://doi.org/10.1214/aoms/1177698950>
 8. Shafer, G. (1976). *A mathematical theory of evidence*. Princeton University Press.
 9. Zadeh, L. A. (1986). A simple view of the Dempster-Shafer theory of evidence and its implication for the rule of combination. *AI Magazine*, 7(2), 85–90. <https://doi.org/10.1609/aimag.v7i2.542>
 10. Smets, P., & Kennes, R. (1994). The transferable belief model. *Artificial Intelligence*, 66(2), 191–234. [https://doi.org/10.1016/0004-3702\(94\)90026-4](https://doi.org/10.1016/0004-3702(94)90026-4)
 11. Yager, R. R. (1987). On the Dempster-Shafer framework and new combination rules. *Information Sciences*, 41(2), 93–137. [https://doi.org/10.1016/0020-0255\(87\)90007-7](https://doi.org/10.1016/0020-0255(87)90007-7)
 12. Dubois, D., & Prade, H. (1988). Representation and combination of uncertainty with belief functions and possibility measures. *Computational Intelligence*, 4(3), 244–264. <https://doi.org/10.1111/j.1467-8640.1988.tb00279.x>
 13. Lefèvre, E., Colot, O., & Vannoorenberghe, P. (2002). Belief function combination and conflict management. *Information Fusion*, 3(2), 149–162. [https://doi.org/10.1016/S1566-2535\(02\)00053-2](https://doi.org/10.1016/S1566-2535(02)00053-2)
 14. Dubois, D., Liu, W., Ma, J., & Prade, H. (2016). The basic principles of uncertain information fusion. An organised review of merging rules in different representation frameworks. *Information Fusion*, 32, 12–39. <https://doi.org/10.1016/j.inffus.2016.02.006>
 15. Murphy, C. K. (2000). Combining belief functions when evidence conflicts. *Decision Support Systems*, 29(1), 1–9. [https://doi.org/10.1016/S0167-9236\(99\)00084-6](https://doi.org/10.1016/S0167-9236(99)00084-6)
 16. Xiao, F. (2019). Multi-sensor data fusion based on the belief divergence measure of evidences and the belief entropy. *Information Fusion*, 46, 23–32. <https://doi.org/10.1016/j.inffus.2018.04.003>
 17. Lefèvre, E., & Elouedi, Z. (2013). How to preserve the conflict as an alarm in the combination of belief functions? *Decision Support Systems*, 56, 326–333. <https://doi.org/10.1016/j.dss.2013.06.012>
 18. Liu, W. (2006). Analyzing the degree of conflict among belief functions. *Artificial Intelligence*, 170(11), 909–924. <https://doi.org/10.1016/j.artint.2006.05.002>
 19. Jousselme, A.-L., Grenier, D., & Bossé, É. (2001). A new distance between two bodies of evidence. *Information Fusion*, 2(2), 91–101. [https://doi.org/10.1016/S1566-2535\(01\)00026-4](https://doi.org/10.1016/S1566-2535(01)00026-4)
 20. Martin, A., Jousselme, A.-L., & Osswald, C. (2008). Conflict measure for the discounting operation on belief functions. *Proceedings of the 11th International Conference on Information Fusion (FUSION 2008)*, Cologne, Germany. <https://doi.org/10.1109/ICIF.2008.4632320>
 21. Mercier, D., Quost, B., & Denœux, T. (2008). Refined modeling of sensor reliability in the belief function framework using contextual discounting. *Information Fusion*, 9(2), 246–258. <https://doi.org/10.1016/j.inffus.2006.08.001>
 22. Destercke, S., & Burger, T. (2013). Toward an axiomatic definition of conflict between belief functions. *IEEE Transactions on Cybernetics*, 43(2), 585–596. <https://doi.org/10.1109/TSMCB.2012.2212703>
 23. Pichon, F., Dubois, D., & Denœux, T. (2012). Relevance and truthfulness in information correction and fusion. *International Journal of Approximate Reasoning*, 53(2), 159–175. <https://doi.org/10.1016/j.ijar.2011.02.006>
 24. Pichon, F., Destercke, S., & Burger, T. (2015). A consistency-specificity trade-off to select source behavior in information fusion. *IEEE Transactions on Cybernetics*, 45(4), 598–609. <https://doi.org/10.1109/TCYB.2014.2331800>
 25. Everaere, P., Konieczny, S., & Marquis, P. (2010). Disjunctive merging: Quota and Gmin merging operators. *Artificial Intelligence*, 174(12–13), 824–849. <https://doi.org/10.1016/j.artint.2010.05.001>
 26. Rago, C., Willett, P., & Bar-Shalom, Y. (1996). Censoring sensors: A low-communication-rate scheme for distributed detection. *IEEE Transactions on Aerospace and Electronic Systems*, 32(2), 554–568. <https://doi.org/10.1109/7.489500>
 27. Deng, Y. (2015). Generalized evidence theory. *Applied Intelligence*, 43(3), 530–543. <https://doi.org/10.1007/s10489-015-0661-2>
 28. Skau, E., Armstrong, C., Truong, D. P., Gerts, D., & Sentz, K. (2023). Open world Dempster-Shafer using complementary sets. *Proceedings of the Thirteenth International Symposium on Imprecise Probability:*



- Theories and Applications, PMLR, 215, 438–449. <https://proceedings.mlr.press/v215/skau23a.html>
29. Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J.-P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. *IEEE INFOCOM* 2008, 1238–1246. <https://doi.org/10.1109/INFOCOM.2008.180>
30. Zhang, W., Zhu, S., Tang, J., & Xiong, N. (2018). A novel trust management scheme based on Dempster-Shafer evidence theory for malicious nodes detection in wireless sensor networks. *The Journal of Supercomputing*, 74(4), 1779–1801. <https://doi.org/10.1007/s11227-017-2150-3>
31. Jøsang, A. (2016). *Subjective logic: A formalism for reasoning under uncertainty*. Springer. <https://doi.org/10.1007/978-3-319-42337-1>
32. Jøsang, A., Ivanovska, M., & Muller, T. (2015). Trust revision for conflicting sources. 18th International Conference on Information Fusion (FUSION 2015), 550–557. IEEE. <https://isif.org/media/trust-revision-conflicting-sources>
33. Jøsang, A., & Ismail, R. (2002). The beta reputation system. *Proceedings of the 15th Bled Electronic Commerce Conference*, Bled, Slovenia. [https://domino.fov.um.si/proceedings.nsf/Proceedings/D9E48B66F32A7DFFC1256E9F00355B37/\\$File/josang.pdf](https://domino.fov.um.si/proceedings.nsf/Proceedings/D9E48B66F32A7DFFC1256E9F00355B37/$File/josang.pdf)

**Olha Partyka**

PhD in Physics and Mathematics, Associate Professor,
Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-3086-3160
olha.o.mykhailova@lpnu.ua

**PROTECTION OF THE WIRELESS-NETWORK REPUTATION MECHANISM AGAINST
ERRONEOUS UPDATES IN THE PRESENCE OF COMPROMISED NODES USING A TYPED k-
OUT-OF-N RULE**

Abstract. In wireless networks, node reputation is often updated by comparing a local report with the global fusion decision. When some nodes are compromised or network coverage is incomplete, the global decision is not always a reliable reference: a correct report from an honest node may disagree with it and lead to an unjustified decrease in trust. This paper proposes a typed representation of the k-out-of-N outcome that preserves the original binary decision while distinguishing a single quorum, a double quorum, an unreach quorum, insufficient coverage, and the absence of data. Reputation is updated only when a single H_1 or H_0 quorum is obtained. The implementation was verified by exhaustive enumeration of 15,309 configuration–quota pairs. Classical updating, coverage filtering, a two-sided quorum rule, Bayesian variants, and beta reputation with forgetting were compared experimentally. The base scenario used $N=7$, $k=4$, two compromised nodes, and a prior probability of H_1 equal to 0.5. At an abstention probability of 0.5, classical updating produced about 34% unjust penalties of honest nodes, coverage filtering about 28%, whereas typed updating reduced this value to 1.9%. The mean trust difference between honest and compromised nodes was about 0.59. Ablation analysis showed that for $k=4$ the same result is reproduced by a simpler two-sided quorum rule, while for $k=3$ the full typology provides a small additional gain. The results show that accounting for the structure of the global decision can reduce false penalties of honest nodes without changing the underlying k-out-of-N rule. In practical terms, the fusion center can skip reputation updates in rounds where the global result is supported by insufficient or conflicting evidence while leaving the decision rule itself unchanged.

Keywords: cybersecurity; trust assessment; wireless networks; k-out-of-N rule; Byzantine attack; compromised node; reputation mechanism; quota decision.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Varshney, P. K. (1997). Distributed detection and data fusion. Springer. <https://doi.org/10.1007/978-1-4612-1904-0>
2. Chair, Z., & Varshney, P. K. (1986). Optimal data fusion in multiple sensor detection systems. *IEEE Transactions on Aerospace and Electronic Systems*, AES-22(1), 98–101. <https://doi.org/10.1109/TAES.1986.310699>
3. Svanström, F., Alonso-Fernandez, F., & Englund, C. (2022). Drone detection and tracking in real-time by fusion of different sensing modalities. *Drones*, 6(11), 317. <https://doi.org/10.3390/drones6110317>
4. Partyka, O., Imoize, A. L., & Li, C.-T. (2026). Cooperative V2X-based UAV detection in rural transportation corridors. *Drones*, 10(2), 153. <https://doi.org/10.3390/drones10020153>
5. Marano, S., Matta, V., & Tong, L. (2009). Distributed detection in the presence of Byzantine attacks. *IEEE Transactions on Signal Processing*, 57(1), 16–29. <https://doi.org/10.1109/TSP.2008.2007335>
6. Rawat, A. S., Anand, P., Chen, H., & Varshney, P. K. (2011). Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks. *IEEE Transactions on Signal Processing*, 59(2), 774–786. <https://doi.org/10.1109/TSP.2010.2091277>
7. Dempster, A. P. (1967). Upper and lower probabilities induced by a multivalued mapping. *The Annals of Mathematical Statistics*, 38(2), 325–339. <https://doi.org/10.1214/aoms/1177698950>
8. Shafer, G. (1976). A mathematical theory of evidence. Princeton University Press.
9. Zadeh, L. A. (1986). A simple view of the Dempster-Shafer theory of evidence and its implication for the rule of combination. *AI Magazine*, 7(2), 85–90. <https://doi.org/10.1609/aimag.v7i2.542>
10. Smets, P., & Kennes, R. (1994). The transferable belief model. *Artificial Intelligence*, 66(2), 191–234. [https://doi.org/10.1016/0004-3702\(94\)90026-4](https://doi.org/10.1016/0004-3702(94)90026-4)
11. Yager, R. R. (1987). On the Dempster-Shafer framework and new combination rules. *Information Sciences*, 41(2), 93–137. [https://doi.org/10.1016/0020-0255\(87\)90007-7](https://doi.org/10.1016/0020-0255(87)90007-7)
12. Dubois, D., & Prade, H. (1988). Representation and combination of uncertainty with belief functions and possibility measures. *Computational Intelligence*, 4(3), 244–264. <https://doi.org/10.1111/j.1467-8640.1988.tb00279.x>
13. Lefèvre, E., Colot, O., & Vannoorenberghe, P. (2002). Belief function combination and conflict management.



- Information Fusion, 3(2), 149–162. [https://doi.org/10.1016/S1566-2535\(02\)00053-2](https://doi.org/10.1016/S1566-2535(02)00053-2)
14. Dubois, D., Liu, W., Ma, J., & Prade, H. (2016). The basic principles of uncertain information fusion. An organised review of merging rules in different representation frameworks. *Information Fusion*, 32, 12–39. <https://doi.org/10.1016/j.inffus.2016.02.006>
 15. Murphy, C. K. (2000). Combining belief functions when evidence conflicts. *Decision Support Systems*, 29(1), 1–9. [https://doi.org/10.1016/S0167-9236\(99\)00084-6](https://doi.org/10.1016/S0167-9236(99)00084-6)
 16. Xiao, F. (2019). Multi-sensor data fusion based on the belief divergence measure of evidences and the belief entropy. *Information Fusion*, 46, 23–32. <https://doi.org/10.1016/j.inffus.2018.04.003>
 17. Lefèvre, E., & Elouedi, Z. (2013). How to preserve the conflict as an alarm in the combination of belief functions? *Decision Support Systems*, 56, 326–333. <https://doi.org/10.1016/j.dss.2013.06.012>
 18. Liu, W. (2006). Analyzing the degree of conflict among belief functions. *Artificial Intelligence*, 170(11), 909–924. <https://doi.org/10.1016/j.artint.2006.05.002>
 19. Jousselme, A.-L., Grenier, D., & Bossé, É. (2001). A new distance between two bodies of evidence. *Information Fusion*, 2(2), 91–101. [https://doi.org/10.1016/S1566-2535\(01\)00026-4](https://doi.org/10.1016/S1566-2535(01)00026-4)
 20. Martin, A., Jousselme, A.-L., & Osswald, C. (2008). Conflict measure for the discounting operation on belief functions. *Proceedings of the 11th International Conference on Information Fusion (FUSION 2008)*, Cologne, Germany. <https://doi.org/10.1109/ICIF.2008.4632320>
 21. Mercier, D., Quost, B., & Denœux, T. (2008). Refined modeling of sensor reliability in the belief function framework using contextual discounting. *Information Fusion*, 9(2), 246–258. <https://doi.org/10.1016/j.inffus.2006.08.001>
 22. Destercke, S., & Burger, T. (2013). Toward an axiomatic definition of conflict between belief functions. *IEEE Transactions on Cybernetics*, 43(2), 585–596. <https://doi.org/10.1109/TSMCB.2012.2212703>
 23. Pichon, F., Dubois, D., & Denœux, T. (2012). Relevance and truthfulness in information correction and fusion. *International Journal of Approximate Reasoning*, 53(2), 159–175. <https://doi.org/10.1016/j.ijar.2011.02.006>
 24. Pichon, F., Destercke, S., & Burger, T. (2015). A consistency-specificity trade-off to select source behavior in information fusion. *IEEE Transactions on Cybernetics*, 45(4), 598–609. <https://doi.org/10.1109/TCYB.2014.2331800>
 25. Everaere, P., Konieczny, S., & Marquis, P. (2010). Disjunctive merging: Quota and Gmin merging operators. *Artificial Intelligence*, 174(12–13), 824–849. <https://doi.org/10.1016/j.artint.2010.05.001>
 26. Rago, C., Willett, P., & Bar-Shalom, Y. (1996). Censoring sensors: A low-communication-rate scheme for distributed detection. *IEEE Transactions on Aerospace and Electronic Systems*, 32(2), 554–568. <https://doi.org/10.1109/7.489500>
 27. Deng, Y. (2015). Generalized evidence theory. *Applied Intelligence*, 43(3), 530–543. <https://doi.org/10.1007/s10489-015-0661-2>
 28. Skau, E., Armstrong, C., Truong, D. P., Gerts, D., & Sentz, K. (2023). Open world Dempster-Shafer using complementary sets. *Proceedings of the Thirteenth International Symposium on Imprecise Probability: Theories and Applications*, PMLR, 215, 438–449. <https://proceedings.mlr.press/v215/skau23a.html>
 29. Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J.-P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. *IEEE INFOCOM 2008*, 1238–1246. <https://doi.org/10.1109/INFOCOM.2008.180>
 30. Zhang, W., Zhu, S., Tang, J., & Xiong, N. (2018). A novel trust management scheme based on Dempster-Shafer evidence theory for malicious nodes detection in wireless sensor networks. *The Journal of Supercomputing*, 74(4), 1779–1801. <https://doi.org/10.1007/s11227-017-2150-3>
 31. Jøsang, A. (2016). *Subjective logic: A formalism for reasoning under uncertainty*. Springer. <https://doi.org/10.1007/978-3-319-42337-1>
 32. Jøsang, A., Ivanovska, M., & Muller, T. (2015). Trust revision for conflicting sources. *18th International Conference on Information Fusion (FUSION 2015)*, 550–557. IEEE. <https://isif.org/media/trust-revision-conflicting-sources>
 33. Jøsang, A., & Ismail, R. (2002). The beta reputation system. *Proceedings of the 15th Bled Electronic Commerce Conference*, Bled, Slovenia. [https://domino.fov.um.si/proceedings.nsf/Proceedings/D9E48B66F32A7DFFC1256E9F00355B37/\\$File/josang.pdf](https://domino.fov.um.si/proceedings.nsf/Proceedings/D9E48B66F32A7DFFC1256E9F00355B37/$File/josang.pdf)

Отримано редакцією журналу / Received: 11.09.26

Прорецензовано / Revised: 24.09.26

Схвалено до друку / Accepted: 26.10.26



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