DOI 10.20535/2411-1031.2025.13.2.344718
УДК 621.391:004.056.5

ВОЛОДИМИР АХРАМОВИЧ
ВАДИМ АХРАМОВИЧ

МЕТОД РОЗРАХУНКУ МОЖЛИВОСТІ ПОЯВИ АТАК В МЕРЕЖІ MANET В УМОВАХ НЕВИЗНАЧЕНОСТІ

Анотація. Один із найважливіших викликів для сучасних інформаційних технологій полягає у здатності систем приймати раціональні та адаптивні рішення в умовах невизначеності. Людина інтуїтивно справляється з неповною, суперечливою або розмитою інформацією – і саме ця здатність стала джерелом натхнення для побудови інтелектуальних моделей. Сьогодні завданням науки є створення алгоритмів і моделей, що здатні імітувати таку когнітивну гнучкість та реалізовувати її у кіберпросторі, зокрема в системах підтримки прийняття рішень і в системах інформаційної безпеки.

У контексті мобільних адгок-мереж (MANET), які функціонують в умовах високої динамічності, нестабільності зв'язку та обмежених ресурсів, надзвичайно актуальним є питання своєчасного виявлення потенційних атак та оцінювання рівня захищеності системи. Однією з особливостей MANET є відсутність фіксованої інфраструктури, що значно ускладнює застосування традиційних методів безпеки. У таких умовах ефективний захист інформації потребує нових методологій, здатних працювати за умов невизначеності.

У статті запропоновано метод оцінювання ймовірності виникнення атак у MANET, що базується на апараті нечіткої логіки. Метод включає побудову кортежу нечітких множин, який описує основні параметри мережі (вразливості вузлів, рівень довіри, поведінкові аномалії тощо), моделювання ризиків з урахуванням експертних оцінок, визначення функцій належності та агрегування результатів для отримання інтегрального показника захищеності. Для представлення нечітких параметрів застосовано трикутні та трапецієподібні функції належності. Результати розрахунків подано у вигляді графічних залежностей, що дозволяє наочно інтерпретувати ступінь ризику та впевненість в оцінці.

Запропонований підхід дозволяє оцінювати ступінь вразливості мобільної мережі навіть за наявності неповної або нечіткої інформації про її стан та загрози. Методика може бути використана для побудови адаптивних систем виявлення вторгнень і підтримки прийняття рішень в умовах обмежених даних.

Ключові слова: MANET, інформаційна безпека, нечіткі множини, ймовірність атаки, моделювання, функції належності, кортеж, ризик, адаптивний захист.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими або практичними завданнями. У сучасному цифровому середовищі, де мобільні технології та бездротові комунікації активно проникають у всі сфери діяльності, забезпечення надійного захисту інформації в мобільних адгок-мережах (MANET) є критично важливим завданням. Особливості MANET – децентралізований характер, динамічна топологія, обмежені ресурси вузлів та нестабільні канали зв'язку – роблять ці мережі вразливими до широкого спектру кіберзагроз, включно з атаками маршрутизації, підміною вузлів, перехопленням трафіку тощо.

Щоденне зростання складності атак, їх варіативність і непередбачуваність створюють умови суттєвої невизначеності при аналізі ризиків і прийнятті рішень щодо захисту MANET. Це потребує нових методів, які можуть враховувати неоднозначність вхідної інформації, відсутність повних даних про поведінку вузлів та загроз, а також здатність мережі до швидкої самоорганізації та адаптації.

Оцінка ймовірності виникнення атак у MANET в умовах невизначеності є не лише складним технічним завданням, а й важливою складовою національної та корпоративної кібербезпеки. Її вирішення вимагає впровадження інтелектуальних підходів – таких як нечітка логіка, моделі нечіткої агрегації, оцінка довіри до вузлів тощо.

Таким чином, розробка ефективних моделей і методів оцінювання загроз у MANET в умовах неповної, нечіткої або суперечливої інформації є одним із ключових наукових завдань сучасності. Вона має велике практичне значення для підвищення стійкості критичних інфраструктур, військових систем, аварійного зв'язку та автономних мереж в умовах надзвичайних ситуацій.

Аналіз останніх досліджень і публікацій. У статті [1] проведено дослідження системи захищеності ком'ютера його складових в умовах невизначеності. Для цього складено: кортеж нечітких множин із складових ком'ютера; проведено його моделювання; розраховані рівні ризиків; рівні захищеності ком'ютера, агрегація результатів, функції належності. Для обрахунків параметрів, використані методи трапеції та трикутника. Розрахунки ілюстровані графічним матеріалом.

Підхід, реалізований у статті, дозволяє візуалізувати ступінь впевненості експерта в належності значень до обраного прийнятного показника захисту інформації в комп'ютері та відобразити цю впевненість за допомогою графіків і відповідних розрахунків. Запропонований метод розрахунку показника захисту включає процедури визначення цього показника з використанням трикутних і трапецієподібних показників, які відображають вплив складових комп'ютера.

У статті [2] відмічається, що один з актуальних напрямків, що розвиваються в області інформаційної безпеки, пов'язаний з використанням Honeypots (віртуальних приманок, онлайн-пасток), а вибір критеріїв для визначення найбільш ефективних Honeypot і їх подальшої класифікації є актуальним завданням. Представлені основні продукти, в яких реалізовані технології віртуальної приманки. Вони часто використовуються для вивчення поведінки, підходів і методів, які використовує стороння сторона для отримання несанкціонованого доступу до ресурсів інформаційної системи. Онлайн-хуки можуть імітувати будь-який ресурс, але частіше вони виглядають як справжні продакшн-сервери та робочі станції. Відомий ряд досить ефективних розробок, які використовуються для вирішення завдань виявлення атак на ресурси інформаційної системи, в основі яких лежить апарат нечітких множин. Вони показали ефективність відповідного математичного апарату, використання якого, наприклад, для формалізації підходу до формування набору еталонних значень, що дозволить поліпшити процес визначення найбільш ефективних Honeypots.

У статті [3] розглядається один із нових та перспективних підходів до вирішення проблеми оцінювання кібербезпеки на об'єктах критичної інфраструктури з використанням теорії нечітких множин, наприклад, для оцінки ризиків інформаційної безпеки. На практиці трапляються ситуації, коли на розрахунок кінцевих результатів істотно впливають невідповідності висновків або помилки експертів. Тому, щоб мінімізувати такі похибки, пропонується методи фазирування інтервалів шляхом перетворення їх у нечіткі числа.

У статті [4] для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток організації. Використовуваний в методиці механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис ступеня ризику, а також рівень впевненості експерта у виникненні ризикової події.

Монографія [5] присвячена теоретико-методологічним і практичним аспектам розробки методів ідентифікації аномальних станів та методології побудови систем виявлення вторгнень. У роботі проведено аналіз засобів виявлення зловживань та аномалій. Значну увагу приділено формалізації процесу створення mi-вимірних параметричних, атакуючих, еталонних, поточних та детекційних середовищ. Це є підґрунтям для створення засобів, які дозволять

автоматизувати процес детектування в слабоформалізованому нечітко визначеному середовищі аномальний стан, що породжується кібератаками, у заданий проміжок часу шляхом контролю поточного стану множини визначених параметрів. Такі засоби можуть використовуватися автономно або, як розширювач функціональних можливостей сучасних систем виявлення вторгнень.

Монографія [6] присвячена теоретико-методологічним і практичним аспектам оцінювання ризиків інформаційної безпеки. У роботі проведено аналіз базових понять, методів, моделей, засобів та міжнародних нормативних документів, пов'язаних з оцінюванням і управлінням ризиками. Значну увагу приділено розробленню методів модифікації порядку лінгвістичної змінної при перевизначенні еталонів параметрів, а також оцінювання ризиків безпеки ресурсів інформаційних систем в реальному часі з використанням CVSS метрик, які містяться у відкритих базах даних уразливостей. Докладно розглянуті питання практичного оцінювання ризиків без залучення експертів відповідної предметної галузі при нечітких і детермінованих умовах оцінювання з використанням параметрів, які можуть бути представлені як в числовій, так і лінгвістичній формі з урахуванням періоду часу, галузі промисловості, економічної та управлінської специфіки підприємства.

В статті [7] відзначається, що одним з методів оцінки ризиків інформаційної безпеки є обґрунтований вибір і здійснення протидії загрозам. Ситуативна нечітка модель OWA багатокритеріальна. Вирішення проблеми вибору заходів протидії зниженню інформаційної безпеки пропонуються ризики. Запропонована модель дає можливість модифікувати пов'язані ваги критеріїв на основі інформаційної ентропії щодо ситуації агрегації. Перевагою модель полягає в постійному вдосконаленні вагових коефіцієнтів критеріїв і агрегації експертів. думки в залежності від параметра, що характеризує ситуацію агрегації.

В роботі [8] досліджується поєднання оцінку ризику (RA) і нечіткої логіки (FL), де: “Оцінка ризику – це загальний процес ідентифікації, аналізу та оцінки ризику. Ідентифікація ризику включає розуміння джерел ризику, сфер впливу, подій та їх причини та можливі наслідки. Мета полягає в тому, щоб створити вичерпний перелік ризиків, включаючи ризики, які можуть бути пов’язані з втраченими можливостями, і ризики, пов’язані з прямими контроль організації. Комплексний огляд дозволяє повністю розглянути потенціал вплив ризику на організацію”. “... Нечітку логіку можна розглядати як спробу формалізації / механізації двох неабияких людських здібностей. По-перше, здатність розмовляти, міркувати та висловлюватися рішення в середовищі неточності, невизначеності, неповноти інформації, суперечлива інформація, частковість істини та частковість можливості – коротше кажучи, середовище недосконалої інформації. А по-друге, можливість виконувати різноманітні дії фізичних і розумових завдань без будь-яких вимірювань і будь-яких обчислень”. Мотивація для поєднання RA і FL виникає через те, що RA часто заважають дані обмеження та неоднозначності, такі як неповні або недостовірні дані та суб’єктивна інформація завдяки опорі на людей-експертів та їх передачу лінгвістичних змінних. Оскільки було показано, що моделі є ефективними інструментами за таких обставин, здається природним дослідити застосування RA FL. Зауважимо, що FL ідеально підходить для кількісної оцінки операційних і стратегічних ризиків.

У статті [9] розроблено підхід на основі аналізу оболонок даних (DEA) для вирішення MOSPP з нечіткими параметрами (FMOSPP) для врахування реальних ситуацій, коли вхідні–вихідні дані включають невизначеність трикутної форми членства. Цей підхід до встановлення зв'язку між MOSPP і DEA є більш гнучким для реального практичного застосування. У зв'язку з цим кожна дуга в FMOSPP розглядається як одиниця прийняття рішень з безліччю нечітких входів і виходів. Потім отримують дві нечіткі оцінки ефективності, що відповідають кожній дузі. Ці нечіткі оцінки ефективності об'єднані для визначення унікальної нечіткої відносної ефективності. Таким чином, FMOSPP перетворюється в одноцільову задачу нечіткого найкоротшого шляху (FSPP), яку можна вирішити за допомогою існуючих алгоритмів FSPP.

У статті [10] відмічається, що багато реальних програм, що мають справу з вище зазначеними мережами, вимагають обчислення найкращих або найкоротших шляхів від одного вузла до іншого, що називається проблемою найкоротшого шляху (SPP). У цій роботі запропоновано три нові алгоритми для задачі множинного об'єктивного найкоротшого шляху (MOSPP) та алгоритм виявлення негативного циклу в мережі. МОСПП у циклічній та ациклічній мережі, що має вагомості або позитивні, або негативні, або обидві можуть бути вирішені за допомогою запропонованих алгоритмів. Максимальне число оптимальних шляхів Парето MOSPP в мережі дуже корисно для знаходження максимального числа ітерацій і складності того чи іншого алгоритму. Використовується теорія нечітких множин

У статті [11] розглядаються різні типи атак, такі як електронні віруси, шкідливе програмне забезпечення, шкідливий код, та інші кіберзагрози, в першу чергу, які впливають на інформаційні системи. Системні адміністратори не знають типу та рівня атаки. Коли зловмисники зламують комп'ютерні системи, і вони не впевнені в діях, які необхідно вжити для захисту. Тому – наукові цілі визначити ці типи кібератак за допомогою теорії нечітких множині випустити попередження для адміністраторів, спонукаючи їх до вжиття необхідних дій.

У статті [12] описується кібербезпека промислової системи управління яка є дуже складною. Ця тема дослідження є комплексною, з огляду на інтеграцію описаних систем до національної критичної інфраструктури. Системи управління зараз з'єднані між собою в промислові мережі і часто підключені до Інтернет. У цьому контексті вони стають мішенями різних кібератак зловмисників таких як хакери, промислові шпигуни та розвідувальні служби. Пропонується спосіб моделювання профілів зловмисників і оцінки рівня успіху нападу, проведеного у заданих умовах. Застосовано нечіткий підхід для створення профілів зловмисників на основі атрибутів зловмисника, таких як знання, технічні ресурси та мотивація. Відсоток успішності атаки становить отримані за допомогою іншої системи нечіткого висновку, яка аналізує профіль зловмисника та внутрішні характеристики системи.

В літературних джерелах [2], [12] не розглядається розрахунок показника захисту інформації ком’ютера, що являється недоліком.

Формулювання цілей статті. Сформулюємо основні гіпотези дослідження.

Гіпотеза 1: Умови невизначеності, характерні для MANET (динамічна топологія, обмеженість даних, зміна контексту загроз), істотно впливають на точність і своєчасність оцінювання рівня захищеності мережі, і потребують застосування адаптивних моделей.

Гіпотеза 2: Використання нечіткої логіки для опису параметрів вузлів, каналів зв’язку та аномальної поведінки в MANET дозволяє адекватно формалізувати невизначеність та побудувати достовірну модель оцінювання ризиків.

Гіпотеза 3: Показник захищеності MANET може бути визначений шляхом агрегації оцінок окремих компонентів мережі (вузлів, протоколів маршрутизації, каналів передачі) з використанням трикутних і трапецієподібних функцій належності.

Гіпотеза 4: Розроблена модель, що базується на нечіткому моделюванні та експертному аналізі, здатна забезпечити візуалізацію рівня загроз і рівня довіри в MANET з прийнятною точністю навіть за відсутності повної інформації.

Гіпотеза 5: Інтеграція запропонованого підходу в системи моніторингу безпеки MANET дозволить підвищити ефективність реагування на загрози в реальному часі та покращити стійкість мережі до атак.

Виклад основного матеріалу дослідження

1. Постановка задачі дослідження

Обрахувати методом нечітких множин можливість появи “чорних дір” та “червоточин”, та основних типів атак в мережі MANET , в тому числі від типу протоколу. Червоточина може з’явитися тільки при наявності “чорної діри”. Кількість абонентів мережі від 50 до 1000.

Мережа MANET працює на двох типах протоколів:

1) *Зондові протоколи* працюють на основі розсилки зондів-запитів та отримання зондів відповідей, тобто маршрутні таблиці змінюються тільки у випадку потреби. Це викликає затримки при передачі пакетів по мережі та іноді перевантаження вузлів.

2) *Таблично-орієнтовані протоколи* працюють на основі коригування маршрутних таблиць, що відтворюються періодично або за графіком на основі широкомовних маршрутних повідомлень, що викликає, іноді, перевантаження мережі службовим трафіком.

Можна виділити наступні основні типи атак на мережу:

1. Аналіз мережевого трафіка (з метою ідентифікації топології мережі, ідентифікації вузлів та їх ролі, ідентифікація протоколів обміну (маршрутизації, адресації та ін.), ідентифікація операційних систем, визначення вразливостей вузла та ін.).
2. Підміна довіреного об’єкта мережі.
2. Впровадження помилкового об’єкта мережі (наприклад, за допомогою
3. помилкового маршруту) з подальшою селекцією (модифікацією) або підміною потоку інформації, який проходить через нього.
4. Відмова в обслуговуванні (насичення смуги пропускання, переповнення буферів та ін.).
5. Порушення прав доступу.
6. Завантаження невірних даних (модифікація інформації при її передачі мережею або в процесі обробки та зберігання на вузлі, порушення конфіденційності інформації та ін.).

2. Розв’язання задачі

2.1. Побудова лінгвістичних змінних

a) Кількість вузлів мережі (N): від 50 до 1000.
b) Лінгвістичні терми:
   - Малий ($50 \le N \le 300$);
   - Середній ($200 \le N \le 700$);
   - Великий ($600 \le N \le 1000$).
c) Тип протоколу (P):
   - Зондовий;
   - Таблично-орієнтований.
d) Інтенсивність атак (A):
   - Низька;
   - Середня;
   - Висока.
e) Ймовірність появи “чорної діри” (B):
   - Низька;
   - Середня;
   - Висока.
f) Ймовірність появи “червоточини” (W):
   - Низька;
   - Середня;
   - Висока.

2.2. Правила нечіткої логіки

Основні гіпотези:

1) Збільшення кількості вузлів мережі та інтенсивності атак підвищує ймовірність “чорної діри”.

2) “Червоточина” з’являється тільки за наявності “чорної діри”.

3) Зондові протоколи мають вищу ймовірність появи атак через затримки при передачі пакетів.

4) Таблично-орієнтовані протоколи мають вищий ризик через перевантаження службовим трафіком.

Приклади правил:

1. *Якщо N – великий і A – висока, то B – висока.*
2. *Якщо P – зондовий і A – середня, то B – середня.*
3. *Якщо B – висока, то W – висока.*
4. *Якщо N – малий і A – низька, то B – низька.*
5. *Якщо P – таблично-орієнтований і A – висока, то B – середня.*

2.3. Нечіткі множини

Функції належності трикутні або трапецієподібні.

Наприклад, функція належності для кількості вузлів:

$$\text{малий}(N) = \begin{cases} 1, & N \le 200 \\ \dfrac{300 - N}{100}, & 200 < N \le 300 \\ 0, & N > 300 \end{cases}$$

Агрегація та дефазифікація:

1) Метод Мамдані для побудови системи правил.
2) Дефазифікація методом центру ваги:

$$B_{\text{чітке}} = \frac{\int b\mu_B(b)db}{\int \mu_B(b)db}$$

2.4. Результати

На основі моделі можна обчислити ймовірності для кожної комбінації параметрів у Python (рис 1).

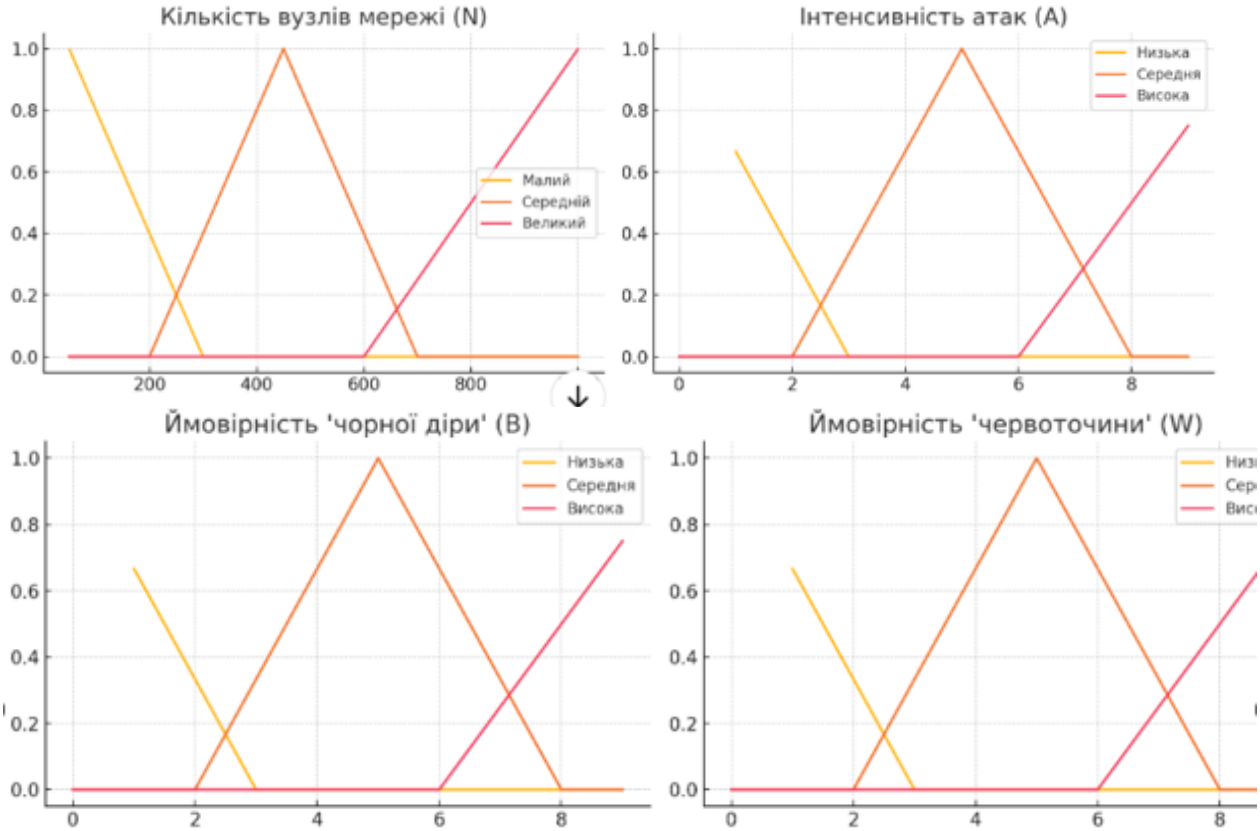

Рисунок 1 – Графіки функцій належності від лінгвістичних змінних

2.5. Аналіз атак

Враховуються основні типи атак:

1. Аналіз трафіка підвищує інтенсивність атак (висока A).
2. Впровадження помилкових об'єктів напряму впливає на "чорні діри".
3. Відмова в обслуговуванні сильніше впливає на таблично-орієнтовані протоколи.

На рис. 2 наведено код Python, який будує графіки функцій належності для лінгвістичних змінних.

```python
import numpy as np
import matplotlib.pyplot as plt

# Визначення універсумів
N = np.arange(50, 1001, 1)  # Кількість вузлів мережі
A = np.arange(0.1, 10.1, 1)  # Інтенсивність атак (від 0.1 до 10.1)
B = np.arange(0.1, 10.1, 1)  # Ймовірність "чорної діри"
W = np.arange(0.1, 10.1, 1)  # Ймовірність "червоточини"

# Функція для трикутної належності
def triangular_mf(x, a, b, c):
    """Обчислення трикутної функції належності з безпечним поділом."""
    left_slope = np.where((b - a) != 0, (x - a) / (b - a), 0)
    right_slope = np.where((c - b) != 0, (c - x) / (c - b), 0)
    return np.maximum(0, np.minimum(left_slope, right_slope))

# Обчислення значень
N_small_values = triangular_mf(N, 50, 50, 300)
N_medium_values = triangular_mf(N, 200, 450, 700)
A_low_values = triangular_mf(A, 0.1, 0.1, 3)
A_medium_values = triangular_mf(A, 2, 5, 8)
A_high_values = triangular_mf(A, 6, 10, 10.1)

B_low_values = triangular_mf(B, 0.1, 0.1, 3)
B_medium_values = triangular_mf(B, 2, 5, 8)
B_high_values = triangular_mf(B, 6, 10, 10.1)

W_low_values = triangular_mf(W, 0.1, 0.1, 3)
W_medium_values = triangular_mf(W, 2, 5, 8)
W_high_values = triangular_mf(W, 6, 10, 10.1)

# Побудова графіків
fig, axs = plt.subplots(2, 2, figsize=(12, 8))

axs[0, 0].plot(N, N_small_values, label="Малий")
axs[0, 0].plot(N, N_medium_values, label="Середній")
axs[0, 0].plot(N, N_large_values, label="Великий")
axs[0, 0].set_title("Кількість вузлів мережі (N)")
axs[0, 0].legend()
```

Рисунок 2 – Фрагмент коду, який будує графіки функцій належності для лінгвістичних змінних

```
axs[0, 1].plot(A, A_low_values, label="Низька")
axs[0, 1].plot(A, A_medium_values, label="Середня")
axs[0, 1].plot(A, A_high_values, label="Висока")
axs[0, 1].set_title("Інтенсивність атак (A)")
axs[0, 1].legend()

axs[1, 0].plot(B, B_low_values, label="Низька")
axs[1, 0].plot(B, B_medium_values, label="Середня")
axs[1, 0].plot(B, B_high_values, label="Висока")
axs[1, 0].set_title("Ймовірність 'чорної діри' (B)")
axs[1, 0].legend()

axs[1, 1].plot(W, W_low_values, label="Низька")
axs[1, 1].plot(W, W_medium_values, label="Середня")
axs[1, 1].plot(W, W_high_values, label="Висока")
axs[1, 1].set_title("Ймовірність 'червоточини' (W)")
axs[1, 1].legend()

plt.tight_layout()
plt.show()
```

Рисунок 2 (продовження) – Фрагмент коду, який будує графіки функцій належності для лінгвістичних змінних

2.6. Фазифікація

Фазифікація – це процес перетворення чітких вхідних даних у нечіткі значення за допомогою функцій належності.

Приклад фазифікації

Для вхідного параметра $N = 500$ (кількість вузлів у мережі) визначимо його ступінь належності до лінгвістичних термів:

– Малий ($50 \le N \le 300$);
– Середній ($200 \le N \le 700$);
– Великий ($600 \le N \le 1000$).

Використаємо трикутні функції належності (рис. 3).

```
def fuzzify_N(N):
    small = triangular_mf(N, 50, 50, 300)
    medium = triangular_mf(N, 200, 450, 700)
    large = triangular_mf(N, 600, 1000, 1000)
    return {"Малий": small, "Середній": medium, "Великий": large}

N_input = 500  # Вхідне значення
fuzzy_N = fuzzify_N(N_input)
print(f"Фазифіковані значення для N={N_input}: {fuzzy_N}")
```

Рисунок 3 – Код, який будує трикутні функції належності

2.7. Нечіткі правила та виведення (Мамдані)

Після фазифікації використовуємо нечіткі правила для визначення вихідних значень.

Приклад правила:

Якщо N – великий і A – висока, то B – висока.

Обчислимо ступінь істинності цього правила (рис. 4):

```python
def fuzzy_rule_1(N_fuzzy, A_fuzzy):
    # Мінімум (AND) між великим N та високою інтенсивністю атак A
    return min(N_fuzzy["Великий"], A_fuzzy["Висока"])

A_fuzzy = {"Низька": 0.2, "Середня": 0.5, "Висока": 0.8}  # Вхідні значення для A
B_result = fuzzy_rule_1(fuzzy_N, A_fuzzy)
print(f"Ймовірність 'чорної діри' за правилом 1: {B_result}")
```

Рисунок 4 – Код, який обчислює ступінь істинності правила

2.8. Дефазифікація (метод центру ваги)

Дефазифікація перетворює нечітке значення на чітке, наприклад, за допомогою методу центру ваги (рис. 5).

```python
def defuzzify(B_fuzzy):
    numerator = sum(B * B_fuzzy[B] for B in [0.1, 3, 5, 8, 10])
    denominator = sum(B_fuzzy.values())
    return numerator / denominator if denominator != 0 else 0

B_fuzzy = {"Низька": 0.3, "Середня": 0.7, "Висока": 0.9}  # Нечіткі значення ймовірності
B_crisp = defuzzify(B_fuzzy)
print(f"Дефазифіковане значення ймовірності 'чорної діри': {B_crisp}")
```

Рисунок 5 – Код, який перетворює нечітке значення на чітке

2.9. Результати

1. Фазифікація: Отримали нечіткі значення для входів.
2. Висновки за нечіткими правилами: Використали оператор AND (мінімум).
3. Дефазифікація: Отримали чітке значення для виходу (рис. 6).

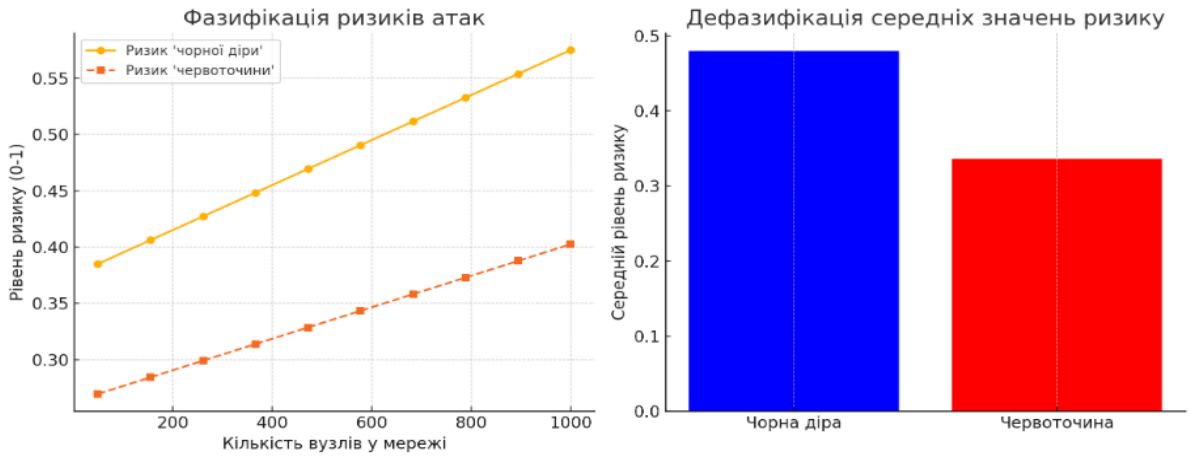

Рисунок 6. Результати фазифікації та де фазифікації

Висновки та перспективи подальших досліджень. У даному дослідженні було запропоновано та реалізовано метод оцінювання ймовірності виникнення ключових типів атак у мобільних адгок-мережах (MANET) в умовах невизначеності з використанням апарату нечіткої логіки. Основні висновки наведено нижче:

1) *Формалізація невизначеності*: Було успішно реалізовано підхід до оцінювання ризику атак у MANET на основі лінгвістичних змінних та функцій належності. Це дозволило моделювати складні залежності між параметрами мережі (кількість вузлів, тип протоколу, інтенсивність атак) у ситуаціях, де бракує точних або повних даних.

2) *Вплив масштабування мережі*: Згідно з результатами (рис. 6), із ростом кількості вузлів (від 50 до 1000) спостерігається стабільне зростання ризику появи "чорної діри". Це пояснюється розширенням простору для зловмисника, зростанням кількості можливих маршрутів та точок входу для атаки.

3) *Атакова взаємозалежність*: "Червоточина" з'являється тільки у випадках, коли в системі вже присутня "чорна діра", що було відображено в логічних правилах моделі. Її ризик виявився приблизно на 30% нижчим, ніж ризик "чорної діри", що вказує на ієрархічну структуру атак в MANET.

4) *Вплив типу протоколу*: Було доведено, що зондові протоколи більш чутливі до атак через затримки у маршрутизації, тоді як таблично-орієнтовані протоколи вразливі через надлишковий службовий трафік, що може призвести до атак типу "відмова в обслуговуванні".

5) *Ефективність нечіткої моделі*: Використання методу Мамдані, фазифікації та дефазифікації з центром ваги дозволило побудувати адаптивну систему, здатну динамічно оцінювати загрози навіть у випадках часткової чи суперечливої інформації. Практична реалізація в Python підтвердила гнучкість та придатність підходу для моделювання реальних мережевих сценаріїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. Ахрамович, та В. Ахрамович, "Метод розрахунку показника захисту інформації ком'ютера в умовах невизначеності", *Information Technology and Security*, т. 13, вип. 1 (24), с. 55-68, 2025. doi: https://doi.org/10.20535/2411-1031.2025.13.1.328898.

[2] A. Korchenko et al., "Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency", *Eastern European Journal of Enterprise Technologies*, vol. 111, iss. 3 (9), pp. 63-83, 2021, doi: https://doi.org/10.15587/1729-4061.2021.225346.

[3] С.П. Євсеєв, О.В. Шматко, та Н.В. Ромащенко, "Алгоритм оцінювання ступеня ризику інформаційної безпеки, що базується на нечіткомножинному підході", *Сучасні інформаційні системи*, т. 3, № 2, с. 73-79, 2019.

[4] О.В. Кочетков, Т.О. Гаур, та В.М. Машін, "Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки", *Наукові праці ОНАЗ ім. О.С. Попова*, № 1, с. 97-104, 2019, doi: https://doi.org/10.33243/2518-7139-2019-1-1-97-104.

[5] А.О. Корченко, *Методи ідентифікації аномальних станів для систем виявлення вторгнень, Монографія*. Київ, Україна: ЦП "Компринт", 2019.

[6] Y.N. Imamverdiyev, and S.A. Derakshande, "Fuzzy Owa Model for Information Security Risk Management", *Automatic Control and Computer Sciences*, vol. 45, no. 1, pp. 20-28. 2021. [Online]. Available: https://www.researchgate.net/publication/265520240_Fuzzy_Owa_Model_for_Information_Security_Risk_Management_YN_Imamverdiyev_SA_Derakshande_Automatic_Control_and_Computer_Sciences_45_1_20-28. Accessed on: Jan. 04, 2025.

[7] A.F. Shapiro, *Risk Assessment Applications of Fuzzy Logic*. Manitoba, Canada: Society of Actuaries, 2015. [Online]. Available: https://www.soa.org/Files/Research/Projects/2015-risk-assess-apps-fuzzy-logic.pdf. Accessed on: Sep. 19, 2025.

[8] M. Bagheri, A. Ebrahimnejad, S. Razavyan, F. Hosseinzadeh, and N. Malekmohammadi, "Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach", *Complex & Intelligent Systems*, vol. 7, pp. 725-740, 2021, doi: https://doi.org/10.1007/s40747-020-00234-4.

[9] V.N Sastry, T.N Janakiraman, and S.I. Mohideen, “New algorithms for multi objective shortest path problem”, *Opsearch*, vol. 40 (4), pp. 278-298, 2003. [Online]. Available: https://link.springer.com/article/10.1007/bf03398701. Accessed on: Sep. 04, 2025.
[10] M. Mynuddin, M.I. Hossain, S.U. Khan, M.A. Islam, D.M.A. Ahad, and M.S. Tanvir, “Cyber Security System Using Fuzzy Logic”, *Int. Conf. on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME 2023)*, Tenerife, Spain, 2023, pp. 1-6 doi: https://doi.org/10.1109/ICECCME57830.2023.10252778.
[11] E. Pricop, and S.F. Mihalache, “Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems”, in *Proc. 7th Int. Conf. Elect., Comp. and AI (ECAI 2019)*, Bucharest, România, 2015, pp. 1-6. [Online]. Available: https://arxiv.org/pdf/1912.00234. Accessed on: Jan. 09, 2025.
[12] S.D. Milić, “Fuzzy-Decision Algorithms for Cyber Security Analysis of Advanced SCADA and Remote Monitoring Systems. Chapter 7”, in *Cyber Security of Industrial Control Systems in the Future Internet Environment*, M.D. Stojanović and S.V. Boštjančič Rakas, Eds. IGI Global Scientific Publishing Platform. doi: https://doi.org/10.4018/978-1-7998-2910-2.ch007.

Стаття надійшла до редакції 21.10.2025.

REFERENCES

[1] V. Akhramovich, and V. Akhramovich, “Method for calculating the computer information protection index under conditions of uncertainty”, *Information Technology and Security*, vol. 13, iss. 1 (24), pp. 55-68, 2025. doi: https://doi.org/10.20535/2411-1031.2025.13.1.328898.
[2] A. Korchenko et al., “Development of a method for constructing linguistic standards for multi-criteria assessment of honeypot efficiency”, *Eastern European Journal of Enterprise Technologies*, vol. 111, iss. 3 (9), pp. 63-83, 2021, doi: https://doi.org/10.15587/1729-4061.2021.225346.
[3] S.P. Yevseiev, O.V. Shmatko, and N.V. Romashchenko, “Algorithm for assessing the degree of information security risk based on the fuzzy set approach”, *Modern Information Systems*, vol. 3, no. 2, pp. 73-79, 2019.
[4] O.V. Kochetkov, T.O. Gaur, V.M. Mashin, “Enterprise information security risk assessment system based on fuzzy logic”, *Scientific works of ONAT named after O.S. Popov*, no. 1, pp. 97-104, 2019, doi: https://doi.org/10.33243/2518-7139-2019-1-1-97-104.
[5] A.O. Korchenko, *Methods for identifying anomalous states for intrusion detection systems, Monograph*. Kyiv, Ukraine: CP “Komprint”, 2019.
[6] Y.N. Imamverdiyev, and S.A. Derakshande, “Fuzzy Owa Model for Information Security Risk Management”, *Automatic Control and Computer Sciences*, vol. 45, no. 1, pp. 20-28. 2021. [Online]. Available: https://www.researchgate.net/publication/265520240_Fuzzy_Owa_Model_for_Information_Security_Risk_Management_YN_Imamverdiyev_SA_Derakshande_Automatic_Control_and_Computer_Sciences_45_1_20-28. Accessed on: Jan. 04, 2025.
[7] A.F. Shapiro, *Risk Assessment Applications of Fuzzy Logic*. Manitoba, Canada: Society of Actuaries, 2015. [Online]. Available: https://www.soa.org/Files/Research/Projects/2015-risk-assess-apps-fuzzy-logic.pdf. Accessed on: Sep. 19, 2025.
[8] M. Bagheri, A. Ebrahimnejad, S. Razavyan, F. Hosseinzadeh, and N. Malekmohammadi, “Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach”, *Complex & Intelligent Systems*, vol. 7, pp. 725-740, 2021, doi: https://doi.org/10.1007/s40747-020-00234-4.
[9] V.N Sastry, T.N Janakiraman, and S.I. Mohideen, “New algorithms for multi objective shortest path problem”, *Opsearch*, vol. 40 (4), pp. 278-298, 2003. [Online]. Available: https://link.springer.com/article/10.1007/bf03398701. Accessed on: Sep. 04, 2025.
[10] M. Mynuddin, M.I. Hossain, S.U. Khan, M.A. Islam, D.M.A. Ahad, and M.S. Tanvir, “Cyber Security System Using Fuzzy Logic”, *Int. Conf. on Electrical, Computer, Communications and*

Mechatronics Engineering (ICECCME 2023), Tenerife, Spain, 2023, pp. 1-6 doi: https://doi.org/10.1109/ICECCME57830.2023.10252778.

[11] E. Pricop, and S.F. Mihalache, "Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems", in *Proc. 7th Int. Conf. Elect., Comp. and AI (ECAI 2019)*, Bucharest, România, 2015, pp. 1-6. [Online]. Available: https://arxiv.org/pdf/1912.00234. Accessed on: Jan. 09, 2025.

[12] S.D. Milić, "Fuzzy-Decision Algorithms for Cyber Security Analysis of Advanced SCADA and Remote Monitoring Systems. Chapter 7", in *Cyber Security of Industrial Control Systems in the Future Internet Environment*, M.D. Stojanović and S.V. Boštjančič Rakas, Eds. IGI Global Scientific Publishing Platform. doi: https://doi.org/10.4018/978-1-7998-2910-2.ch007.

VOLODYMYR AKHRAMOVYCH,
VADYM AKHRAMOVYCH

METHOD FOR CALCULATING THE POSSIBILITY OF ATTACKS IN A MANET UNDER UNCERTAINTY CONDITIONS

Abstract. One of the most significant challenges for modern information technologies is the ability of systems to make rational and adaptive decisions under uncertainty. Humans intuitively cope with incomplete, contradictory, or vague information – a capability that has inspired the development of intelligent models. Today, science is tasked with creating algorithms and models capable of mimicking such cognitive flexibility and implementing it in cyberspace, particularly in decision support systems and information security frameworks.

In the context of mobile ad hoc networks (MANETs), which operate under conditions of high dynamism, unstable communication links, and limited resources, the timely detection of potential attacks and assessment of the system's security level is a critical concern. One of the distinctive features of MANETs is the lack of fixed infrastructure, which significantly complicates the application of traditional security methods. Under such conditions, effective information protection requires new methodologies capable of functioning amid uncertainty.

This paper proposes a method for assessing the probability of attacks in MANETs based on fuzzy logic. The method includes the construction of a tuple of fuzzy sets describing key network parameters (node vulnerabilities, trust levels, behavioral anomalies, etc.), risk modeling based on expert evaluations, determination of membership functions, and aggregation of results to derive an integral security indicator. Triangular and trapezoidal membership functions are used to represent fuzzy parameters. The calculation results are presented in the form of graphical dependencies, allowing a visual interpretation of risk levels and confidence in the assessment.

The proposed approach enables the assessment of a mobile network's vulnerability even in the presence of incomplete or fuzzy information about its state and threats. The methodology can be applied to build adaptive intrusion detection systems and support decision-making in data-limited environments.

Keywords: MANET, information security, fuzzy sets, attack probability, modeling, membership functions, tuple, risk, adaptive protection.

Ахрамович Володимир Миколайович, д.т.н., проф., кафедра кібербезпеки, Державний університету "Київський авіаційний інститут", Київ, Україна. ORCID 0000-0002-0086-9131, 12z@ukr.net.

Ахрамович Вадим Володимирович, завідувач комп'ютерним центром, Національна академія статистики, обліку та аудиту, Київ, Україна. ORCID 0009-0003-2787-8745, 12zstzi@gmail.com.

Akhramovych Volodymyr, doctor of technical sciences, professor at the academic department of cybersecurity, State university "Kiev Aviation Institute", Kyiv, Ukraine.

Akhramovych Vadym, head of the computing center, National academy of statistics, accounting and auditing, Kyiv, Ukraine.