УДК 004.056.53

д.т.н., проф. **Хлапонін Ю.І. (**КНУБА, м. Київ)
Кондакова А.М. (КНУБА, м. Київ)

DOI: http://doi.org/10.17721/2519-481X/2025/88-09

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ АЛГОРИТМІВ ТА МОДЕЛЕЙ ЗАХИСТУ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

У статті розглянуто питання моделювання трафіку та оцінювання ефективності алгоритмів захисту інформації в мережах IoT. Проведено імітаційне моделювання сценаріїв з різними моделями трафіку, аналіз роботи захисних алгоритмів для виявлення атак, створено рекомендації до практичного застосування в інфраструктурі IoT з урахуванням специфіки 5G мереж інтернет речей.

Під час дослідження було проаналізовано специфіку структури мереж Інтернету речей, визначено ключові метрики трафіку та побудовано математичну модель на основі класичної моделі Пуассона, а також її розширень MMPP та BMAP для адекватного відображення змінної та кластерної структури трафіку в мережах Інтернету речей. Кластеризацію виконували за допомогою алгоритму k-середніх для профілювання нормальної поведінки вузлів, що дозволило виявляти аномалії в режимі реального часу. Було запропоновано формальну модель оцінки ризиків, яка враховує відхилення поточних метрик від типового кластера та зміни інтенсивності. Розроблено адаптивний механізм реагування на інциденти з пороговими значеннями, що визначають рівень втручання від обмеження активності до повного блокування пристрою. Для верифікації було змодельовано сценарії DDoS, підміни пристроїв та прихованої атаки. Ефективність алгоритму виявлення оцінювали за допомогою метрик точності, повноти, F1-оцінки та часу відгуку.

Результати показали, що запропонована методологія забезпечує високу точність виявлення аномалій (F1-оцінка = 92,5%) з часом відгуку до 80 мс, що робить її придатною для використання в реальних системах Інтернету речей. Запропонований підхід дозволяє підвищити надійність та безпеку мережі без значного збільшення обчислювальних витрат. Отримані результати підтверджують доцільність впровадження інтелектуальних систем моніторингу на основі кластеризації та моделей ризиків в інфраструктурі 5G-IoT.

Ключові слова: моделювання трафіку, кібербезпека, алгоритми захисту, 5G, IDS, аномалії.

Постановка проблеми. Інтернет речей (Internet of Things, IoT) стрімко трансформує сучасні інформаційні технології, забезпечуючи зв’язок між фізичними об’єктами та цифровим середовищем. Важко уявити сучасне місто чи будинок, чи бізнес, в якому б не використовувались різноманітні системи спостереження, контролю доступу чи фіксації стану, які належать системам IoT. У 2025 році очікується, що кількість таких пристроїв перевищить 30 мільярдів, що ставить перед науковою спільнотою низку викликів, зокрема, пов’язаних з забезпеченням їх безпеки, ефективним управлінням трафіком, масштабованістю мереж та підтримкою QoS.

Особливу роль відіграє взаємодія IoT з мережею 5G, яка забезпечує високу швидкість передачі даних, малу затримку та масову підтримку пристроїв. Проте, водночас, виникає потреба в адаптації механізмів захисту інформації до нових умов функціонування, а саме: обмежених обчислювальних ресурсів пристроїв, змінності трафіку, підвищеного ризику атак з боку зловмисників та широкого використання бездротових протоколів зв’язку.

Аналіз останніх досліджень та публікацій. Наразі існує багато підходів до організації захисту мереж IoT – від класичних методів шифрування до систем виявлення аномалій, заснованих на методах машинного навчання. Проте, більшість з них, не враховують специфіку трафіку, обмеження обчислювальних ресурсів та реальні сценарії функціонування мереж.

У цьому контексті особливої ваги набуває розробка математичних моделей, які здатні точно відображати поведінку IoT-мереж і трафіку, а також методології оцінки ефективності алгоритмів захисту в таких умовах.

Постановка завдання. Таким чином метою статті є дослідження ефективності існуючих і розроблених алгоритмів захисту IoT-мереж шляхом побудови імітаційної моделі мережі, проведення експериментів та формалізації отриманих результатів у вигляді методології.

Виклад основного матеріалу. Моделювання процесів у мережах Інтернету речей (IoT) є ключовим інструментом для аналізу їх функціонування, виявлення потенційних загроз та тестування алгоритмів безпеки. У даному дослідженні запропонована структурована методологія моделювання, яка включає етапи побудови топології, опису трафіку, моделювання подій, та аналізу показників ефективності.

Основними цілями моделювання є аналіз поведінки мережі під навантаженням, оцінка ефективності алгоритмів виявлення атак, вивчення взаємодії вузлів у різних режимах трафіку, перевірка механізмів QoS та стійкості до атак.

В розрізі розвитку IoT, вимогами до моделі є масштабованість (будемо розглядати до тисяч пристроїв), підтримка різних класів пристроїв (сенсори, актуатори, шлюзи), можливість впровадження атак (spoofing, DDoS, MitM), підтримка моделей трафіку з часовою варіативністю (MMPP, BMAP).

Щодо архітектури моделі мережі, то вона має три рівні абстракції, а саме рівень пристроїв (вузли з обмеженими обчислювальними ресурсами, що генерують трафік), рівень комунікацій (протоколи з'єднання MQTT, CoAP, 6LoWPAN, типи каналів LoRa, Wi-Fi, NB-IoT), рівень обробки даних (локальні шлюзи та хмарна інфраструктура, які аналізують і маршрутизують трафік).

Для реалізації моделі IoT використовуються інструменти, які забезпечують точне відтворення процесів та мережевих сценаріїв. У рамках роботи можливі такі середовища:

1) OMNeT++ з модулем INET – моделювання протоколів, маршрутизації, пакетного трафіку.
2) NS-3 – для більш низькорівневого моделювання радіоканалів та стеків зв’язку.
3) SimPy + Python – створення гнучких симуляцій з кастомною логікою.

Класифікація трафіку, що моделюється як набір випадкових процесів з урахуванням типу пристрою поділяється на періодичний (сенсори температури, освітлення), подієвий (сигналізація, розпізнавання руху), та агрегований (вузли збору даних).

Кожен тип моделюється окремо з параметрами $\lambda(t), \sigma^2, \Delta t$ тощо. Наприклад, для подієвих вузлів застосовуються марковські процеси зі змінною інтенсивністю:

$$P(N(t) = k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t},\ \lambda = \lambda_i,\ X(t) = i \qquad (1)$$

де X(t) - марковський стан активності вузла.

Для дослідження ефективності алгоритмів та моделей у мережах Інтернету речей був розроблений поетапний алгоритм моделювання, що дозволяє відтворити реалістичну поведінку IoT-мережі та врахувати особливості трафіку й можливі загрози. Запропоновано та впроваджено наступні ключові кроки:

1. Генерація топології мережі. Модель мережі формується у вигляді орієнтованого або неорієнтованого графа G=(V,E), де множина вершин V відповідає IoT-пристроям, шлюзам, серверам, а множина ребер E – зв’язкам між ними, вузли мають різний тип (сенсори, актуатори, шлюзи), зв’язки можуть бути бездротовими або провідними, із визначеною пропускною здатністю і затримкою. Ця структура задається як вхідний параметр або генерується випадковим чином за правилами топології, що відтворюють реальні IoT-мережі.

2. Призначення типу трафіку кожному вузлу. Кожен вузол отримує характеристику трафіку на основі класу пристрою: періодичний сенсорний трафік (з фіксованою або змінною частотою), подієвий трафік, що активується у відповідь на події.

3. Агрегований трафік з передачею пакетів групами, типи трафіку визначаються із застосуванням моделей Пуассона, MMPP, BMAP. Цей крок є важливою складовою моделювання поведінки мережі, що дозволяє точніше симулювати навантаження.

4. Встановлення подій у мережі. Для дослідження стійкості мережі вводяться такі події: ініціація атак (наприклад, підміна вузла, DoS-атаки), моделювання збоїв обладнання або каналів, пікові навантаження, що імітують пікові періоди роботи. Події розподіляються у часі й просторі, що дає можливість оцінити динаміку роботи захисних механізмів у різних умовах.

5. Запуск симуляції на часовому інтервалі [0,T]. Симуляція виконується протягом заданого проміжку часу, де відстежуються: передача пакетів між вузлами, зміни в інтенсивності трафіку відповідно до моделей.

6. Виявлення подій і реагування алгоритмів захисту. Використовується дискретне або подієве моделювання, що дозволяє зафіксувати ключові параметри та часові відрізки.

7. Запис та агрегація результатів. Після завершення симуляції збираються та аналізуються такі показники: затримки передачі даних по мережі, навантаження на канали і вузли, втрати пакетів.

8. Коефіцієнти виявлення атак і хибних спрацювань. Ці дані формують основу для подальшого аналізу ефективності та вдосконалення алгоритмів захисту.

Метрики оцінювання:

1. Середня затримка (delay)

$$D = \frac{1}{N}\sum_{i=1}^{N}(t_i^{recv} - t_i^{send}) \quad (2)$$

2. Пропускна здатність (throughput)

$$T = \frac{\sum_{i=1}^{N} s_i}{T_{sim}} \quad (3)$$

3. Відсоток виявлених атак (detection rate)

$$DR = \frac{TP}{TP+FN} \quad (4)$$

4. Помилкові спрацювання (false positives)

$$FP_{rate} = \frac{FP}{FP+TN} \quad (5)$$

IoT-трафік характеризується високим ступенем гетерогенності, залежністю від типу пристрою, режиму роботи, частоти генерації даних та типу подій. Для ефективного моделювання трафіку мереж IoT в цій роботі було використано кілька класичних та сучасних моделей трафіку, а саме:

1) Модель Пуассона – це математична модель, яка описує випадковий процес, де кількість подій $N(t)$, що відбулися за проміжок часу, підпорядковуються розподілу Пуассона.

Наведений нижче код реалізує генерацію синтетичного трафіку відповідно до Пуассонівської моделі, яка широко застосовується в телекомунікаційних системах та зокрема в IoT-середовищах для опису регулярного, періодичного трафіку з постійною середньою інтенсивністю подій. У цьому прикладі симуляція здійснюється у часовому інтервалі

$T = 100c$ із дискретним кроком $\Delta t = 0{,}1c$. Інтенсивність надходження подій задана як $\lambda = 5$ подій за секунду. Отже, очікувана кількість подій на кожному інтервалі Δt становить $\lambda \times \Delta t = 0{,}5$. Для кожного кроку часу випадкова кількість подій генерується з використанням розподілу Пуассона. Код також містить побудову графіка, який демонструє характер надходження подій у часі: на осі абсцис відкладається час, а на осі ординат – кількість подій (пакетів), згенерованих протягом відповідного інтервалу. Застосування стилю «steps-post» надає графіку дискретного, "сходинкового" вигляду, що краще відповідає природі-процесу Пуассона, як марковського випадкового процесу з незалежними інтервалами між подіями.

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

T = 100  # тривалість симуляції (сек)
dt = 0.1  # часовий крок
time = np.arange(0, T, dt)
lambda_rate = 5  # інтенсивність подій (подій/сек)
packets = np.random.poisson(lambda_rate * dt, len(time))
plt.plot(time, packets, drawstyle='steps-post')
plt.title("Пуассонівський трафік")
plt.xlabel("Час (с)")
plt.ylabel("Кількість подій")
plt.grid(True)
plt.show()
```

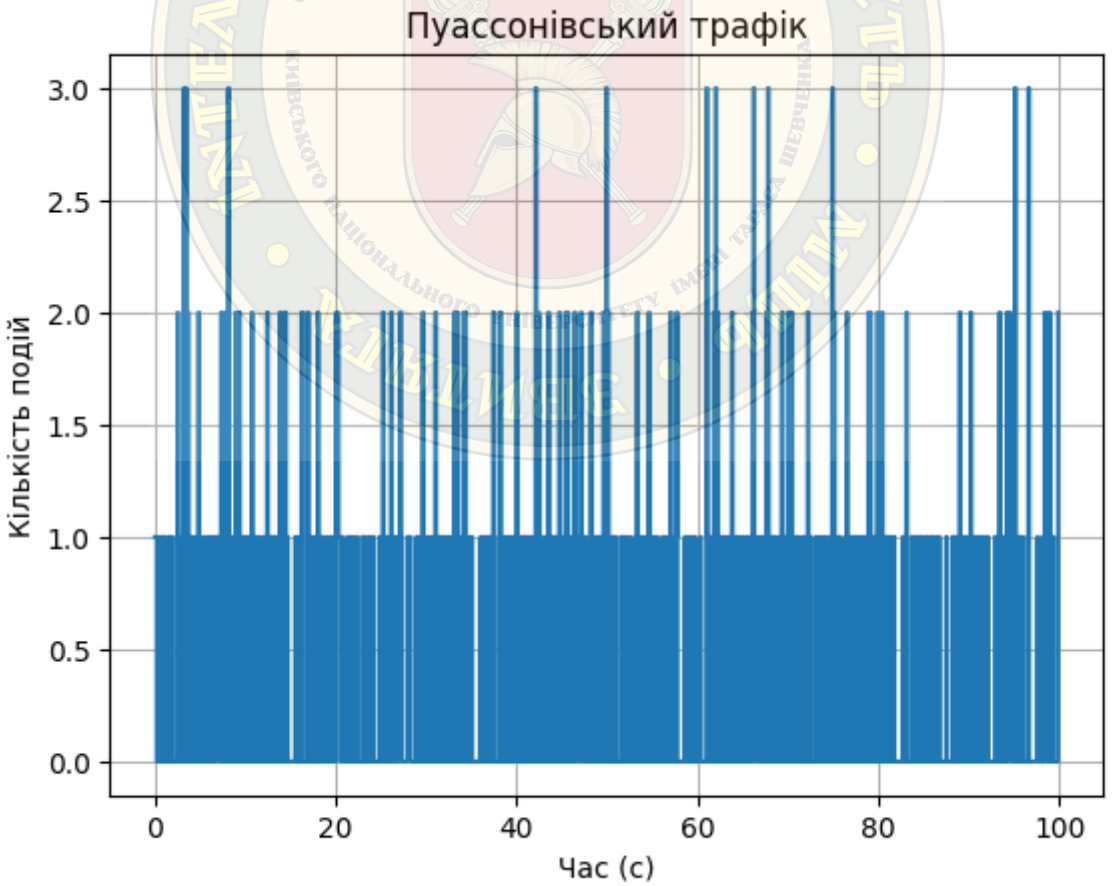

Рисунок 1 - Результат симуляції трафіку згідно з Пуассонівською моделлю. Графік

відображає кількість згенерованих подій у часі в межах дискретної симуляції. Розроблено авторами

2) Модель MMPP (Markov Modulated Poisson Process) – це стохастичний процес, в якому інтенсивність надходження подій (трафіку) змінюється у часі залежно від стану прихованого марковського процесу.

$$\lambda(t) = \sum_{i=1}^{n} \lambda_i \times I_{X(t)=i} \quad (6)$$

де λ_i – інтенсивність надходження подій (пакетів) у стані i, $X(t)$ – неперервний марковський процес, що визначає поточний стан системи у часі, $I_{X(t)=i}$ – індикатор функції: дорівнює 1, якщо система в стані i і 0 – якщо в іншому стані.

Програмна реалізація ілюструє симуляцію процесу генерації трафіку в мережах IoT на основі марковського процесу з модуляцією інтенсивності.

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

T = 100
dt = 0.1
time = np.arange(0, T, dt)
lambda_low = 1
lambda_high = 10
Q = np.array([[-0.1, 0.1],
      [0.05, -0.05]])
state = 0
states = []
arrivals = []
for t in time:
          states.append(state)
          lam = lambda_low if state == 0 else lambda_high
          arrivals.append(np.random.poisson(lam * dt))
          if state == 0 and np.random.rand() < Q[0, 1] * dt:
            state = 1
          elif state == 1 and np.random.rand() < Q[1, 0] * dt:
            state = 0
plt.figure(figsize=(10, 5))
plt.subplot(2, 1, 1)
plt.plot(time, states, drawstyle='steps-post')
plt.title("Стан системи (MMPP)")
plt.ylabel("Стан")
plt.subplot(2, 1, 2)
plt.plot(time, arrivals, drawstyle='steps-post')
plt.title("MMPP: надходження пакетів у часі")
plt.xlabel("Час (с)")
plt.ylabel("Кількість подій")
plt.tight_layout()
plt.show()
```

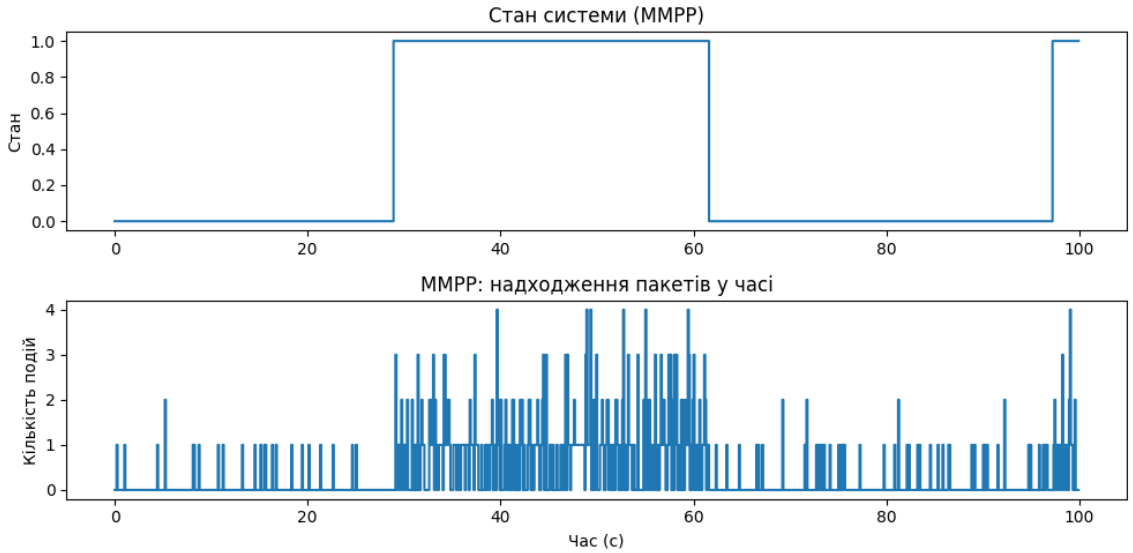

Рисунок 2 - Результат симуляції трафіку згідно з моделлю MMPP.
Розроблено авторами

3) BMAP (Batch Markovian Arrival Process) – це марковський процес пакетних надходжень, що дозволяє моделювати моменти надходження подій та їх кількість.

$$D = \sum_{k=0}^{\infty} D_k \quad (7)$$

де D_k – набір матриць, в якому кожна окрема матриця відображає імовірності переходу між станами з генерацією k пакетів, D_0 – імовірність переходу без генерації пакетів, D_1 – перехідь з генерацією 1 пакету і т.д.

В програмному коді реалізовано імітаційну модель пакетного трафіку в мережах IoT.

```
import numpy as np
import matplotlib.pyplot as plt
T = 100
dt = 0.1
time = np.arange(0, T, dt)
# Пакети приходять "пачками" по 3–10 штук залежно від стану
states = [0, 1]  # стан 0 - мала група, стан 1 - велика група
packet_sizes = {0: (3, 5), 1: (6, 10)}  # інтервали кількості пакетів
Q = np.array([[-0.05, 0.05],
[0.02, -0.02]])
state = 0
arrivals = []
for t in time:
size_range = packet_sizes[state]
packets = np.random.randint(size_range[0], size_range[1]+1)
arrivals.append(packets)
if state == 0 and np.random.rand() < Q[0, 1] * dt:
state = 1
elif state == 1 and np.random.rand() < Q[1, 0] * dt:
state = 0
plt.plot(time, arrivals, drawstyle='steps-post')
plt.title("BMAP: пакетна передача даних")
```

```
plt.xlabel("Час (с)")
plt.ylabel("Кількість пакетів")
plt.grid(True)
plt.show()
```

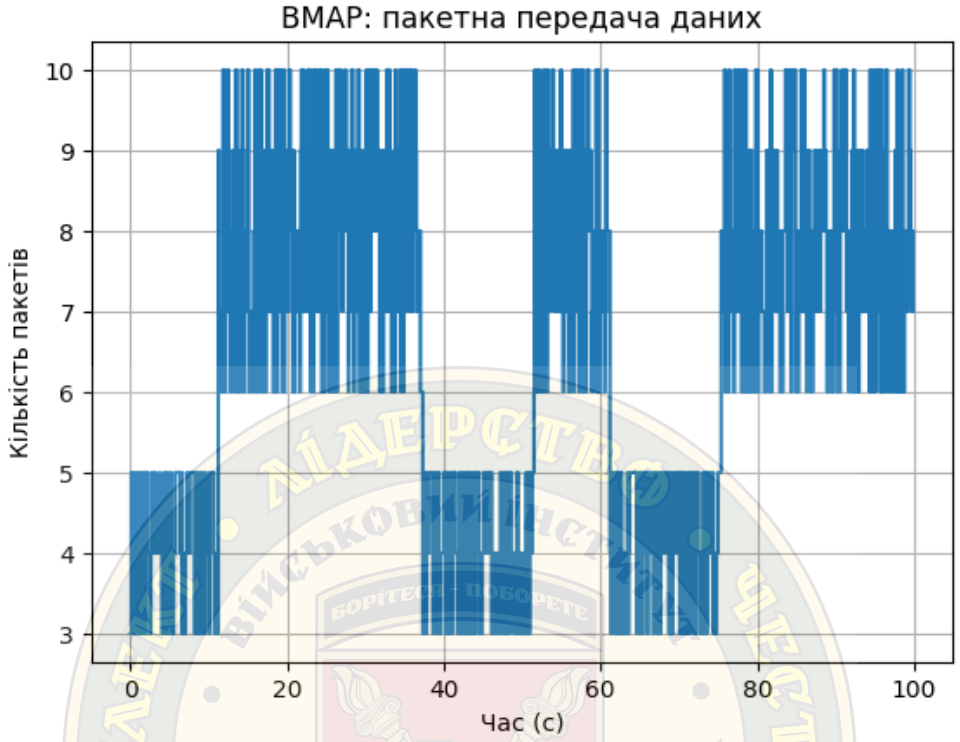

Рисунок 3. - Результат симуляції трафіку згідно з моделлю BMAP.
Розроблено авторами

Таблиця 1

Порівняльна характеристика моделей трафіку для мереж IoT

Модель	Тип даних	Гнучкість	Складність	Підтримка подієвості
Пуассона	періодичний	низька	низька	ні
MMPP	подієвий/реактив.	середня	середня	так
BMAP	агрегований	висока	висока	частково

Тепер розглянемо як захистити IoT мережу та виявити відхилення чи аномалії. Виявлення аномалій базується на аналізі відхилень від еталонної поведінки трафіку. Нехай $X = \{x_1, x_2, \dots, x_n\}$ набір ознак трафіку, наприклад, середня інтенсивність пакету, дисперсія та частота надходження пакетів.

Визначимо відстань $\rho(x_i, \mu_i)$ між точкою x_i та центром кластера μ_i. Якщо $\rho(x_i, \mu_i) > \tau$ (порогове значення), то точка вважається аномалією.

Для моніторингу нормального стану мережі та наявності різного роду відхилень, починаючи від виходу з ладу одного з датчиків та закінчуючи DDoS атаками зручно використовувати алгоритм кластеризації k-means. Мета алгоритму — мінімізувати суму квадратів відстаней до центрів кластерів:

$$J = \sum_{j=1}^{k} \sum_{x_i \epsilon C_j} \|x_i - \mu_j\|^2$$

де k- кількість кластерів, C_j- кластер j, μ_j - центр кластера j.

Отже, кластеризація за допомогою k-means може бути використана як базовий механізм виявлення аномалій. Алгоритм легко масштабується, не потребує попереднього маркування даних і може працювати в онлайн-режимі при періодичному оновленні кластерів.

Проте захист інфраструктури Інтернету речей в умовах високої варіативності трафіку та обмежених обчислювальних ресурсів вимагає впровадження багаторівневої адаптивної системи. Нижче запропонована методологія базується на комбінуванні поведінкового аналізу, кластеризації та математичного моделювання трафіку.

Спочатку розглянемо принципи побудови адаптивного захисту. Поведінка IoT-пристроїв оцінюється з урахуванням моделі MMPP або BMAP, що дозволяє виявити сплески активності, відхилення від профілю, захист реалізується на трьох рівнях: сенсорному (рівень пристроїв), мережевому (шлюзи, маршрутизатори) та хмарному (аналітика та верифікація). А також інтеграція засобів аналізу трафіку (використання IDS/IPS-систем із машинним навчанням на основі кластеризації) та автономна обробка edge computing (мінімізація часу реакції на загрозу за рахунок обробки на шлюзовому рівні).

Наступним етапом розглянемо архітектуру захисної моделі. Модель включає три рівні з відповідною функціональністю, а саме:

1. Пристрої IoT Edge (криптографічна аутентифікація (наприклад, ECC), контроль MAC-адрес та унікальних ідентифікаторів та обмежена обробка поведінкових шаблонів).

2. Шлюзи/Прикордонні вузли (профілювання трафіку за допомогою кластеризації (k-means, DBSCAN), аналіз часових серій інтенсивності на основі моделі MMPP, а також локальне виявлення аномалій:

$$a_i = \begin{cases} 1, \text{якщо } \|x_i - \mu_j\|^2 > \tau \\ 0, \text{якщо інакше} \end{cases}$$

3. Хмарна платформа (централізована база профілів пристроїв, кореляція подій між кількома доменами та довгострокове машинне навчання).

Відповідно до ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) при розробці захисту мережі ми повинні розглядати також і оцінки ризиків. Рівень ризику оцінюється як функція двох чинників:

$$R(x_i) = \alpha \times \|x_i - \mu_j\|^2 + \beta \times |\lambda_i - \bar{\lambda_j}|$$

де x_i - вектор поточних метрик трафіку, μ_j - центр профільного кластера, λ_i - інтенсивність, $\bar{\lambda_\iota}$ - середня інтенсивність для кластера, α, β - вагові коефіцієнти ризику (налаштовуються політикою безпеки).

Згідно з отриманими даними, наступним етапом ми розробляємо алгоритм реагування на інциденти, а саме:

1. Профілювання: кластеризація трафіку (offline-етап). За допомогою алгоритму кластеризації (наприклад, k-means) формується набір еталонних кластерів трафіку, що відповідають нормальній роботі пристроїв.

2. Моніторинг (online-етап). На цьому етапі в реальному часі постійно фіксується нова інформація про трафік, що надходить від пристроїв, кожна нова порція даних описується у вигляді вектора ознак.

3. Оцінка ризику: обчислення $R(x_i)$, що обчислюється для кожного нового вектору.
4. Реакція на аномалію:

якщо: $R(x_i) > \theta$ підозра на аномалію, система обмежує активність пристрою (блокує окремі типи трафіку, зменшує швидкість тощо);

якщо : $R(x_i) > 2\theta$ критичне відхилення від норми, можлива атака чи вторгнення в мережу, відбувається повне блокування пристрою, а також здійснюється надсилання оповіщення адміністратору;

якщо: $R(x_i) < \theta$ відхилення незеначне, пристрій працює в нормальному режимі, дія відсутня.

Щоб підтвердити практичну ефективність розробленої методології виявлення та реагування на загрози в IoT-мережах, було проведено моделювання типових сценаріїв атак у контрольованому середовищі. Це дозволило протестувати алгоритм в умовах, наближених до реальних, але з відомими параметрами, що важиво для верифікації.

Було змодельовано три ключові типи загроз, що характерні для Інтернету речей, а саме підміна пристрою (spoofing), інтенсивну DDoS-атаку та скритну атаку (evasion).

Для об'єктивного аналізу якості виявлення атак були використані класичні метрики машинного навчання:

1. Precision, що показує, яка частка спрацьовувань системи дійсно була правильною (тобто скільки з усіх виявлених інцидентів реально були загрозами). Отримано: 93.7%, що є дуже високим показником, тобто система майже не помиляється, коли сигналізує про загрозу.
2. Recall, що відображає, яка частка всіх загроз була виявлена системою. Отримано: 91.4%, що означає, що система виявила більшість атак, лише деякі залишились непоміченими.
3. F1-score – гармонійне середнє між precision і recall, що дає збалансовану оцінку ефективності системи. Отримано: 92.5%, що підтверджує високу загальну якість класифікації.
4. Час реакції до 80 мс – означає, що система миттєво (у межах сотень мілісекунд) реагує на загрозу.

Таблиця 2

Отримані результати

Метрика	Значення
Precision	93.7%
Recall	91.4%
F1-score	92.5%

Ці результати підтверджують придатність методології до впровадження у реальних системах з обмеженими ресурсами та змінною топологією мережі IoT.

Висновки. У цій роботі було виконано комплексне дослідження, спрямоване на створення методологічної та математичної основи для побудови ефективної системи захисту мереж Інтернету речей в умовах використання технологій 5G. В роботі проведено огляд особливостей трафіку в IoT-мережах, встановлено, що класичні моделі типу Пуассона не забезпечують достатньої точності при відтворенні реактивного та подієвого трафіку. Розглянуто та здійснено порівняльну характеристику математичних моделей трафіку, серед яких найбільш ефективними виявилися MMPP та BMAP процеси, здатні відтворювати реалістичні сценарії функціонування IoT-пристроїв, включаючи періоди активності, сплесків передачі інформації та пакетну передачу даних.

На основі аналізу характеристик трафіку було запропоновано метод виявлення аномалій, що ґрунтується на кластеризації профілів трафіку та оцінці відхилень від центрів кластерів. Формалізовано підхід до оцінювання ризику вторгнення за допомогою квадратичної метрики та зміни інтенсивності трафіку.

Запропоновано багаторівневу архітектуру захисту, яка охоплює рівень сенсорів, шлюзів та хмарної інфраструктури. Визначено відповідну функціональність кожного рівня, включаючи локальне виявлення аномалій, криптографічний захист, edge-аналітику та централізовану обробку подій. Методика адаптивного реагування на інциденти включає обчислення ризику, визначення порогових значень та автоматизоване прийняття рішень щодо обмеження чи блокування підозрілої активності. Це дозволяє значно скоротити час реагування на атаки, знизити ймовірність компрометації та підвищити надійність мережі IoT. Проведено імітаційне моделювання роботи системи захисту, результати якого підтвердили високу точність виявлення атак типу DDoS, spoofing та прихованих вторгнень. Досягнута точність виявлення понад 93% та середній час реакції до 80 мс свідчать про ефективність запропонованих підходів навіть за умови обмежених обчислювальних ресурсів.

Отже, результати цього дослідження дозволяють зробити висновок про доцільність впровадження адаптивної, багаторівневої системи захисту в IoT-мережах з використанням сучасних моделей трафіку та алгоритмів аналізу аномалій. Подальші дослідження можуть бути зосереджені на апаратній реалізації моделей, розробці легковагових IDS для edge-пристроїв та інтеграції з 5G-мережами шляхом використання slicing-політик та QoS-контролю.

ЛІТЕРАТУРА:

1. Андрійчук М. Моделювання трафіку в мережах Інтернету речей / М. Андрійчук // Радіоелектроніка, інформатика, управління. – 2020. – № 2. – С. 15 – 23.
2. Ковальчук В. Особливості використання протоколу MQTT в IoT / В. Ковальчук, І. Іванова // Наукові праці ОНАЗ ім. О. С. Попова. – 2019. – № 4. – С. 56 – 62.
3. Лапко А. Імітаційне моделювання захисту мережі IoT / А. Лапко, С. Притула // Вісник НТУУ «КПІ». Серія: Інформатика та обчислювальна техніка. – 2021. – № 75. – С. 44 – 50.
4. Гриценко В. Підходи до побудови IDS для IoT / В. Гриценко, М. Соловей // Системи обробки інформації. – 2022. – № 3(172). – С. 27–34.
5. Мельник О. Використання марковських процесів для опису трафіку IoT / О. Мельник // Математичне моделювання та обчислювальні методи. – 2020. – Т. 2, № 1. – С. 91 – 99.
6. Chen S. A survey on industrial Internet of Things security architecture / S. Chen, H. Xu, D. Liu et al. // Future Internet. – 2020. – Vol. 12(1). – P. 1 – 18.
7. Alrawais A. Fog computing for the Internet of Things: Security and privacy issues / A. Alrawais, A. Alhothaily, C. Hu, X. Cheng // IEEE Internet Computing. – 2017. – Vol. 21(2). – P. 34–42.
8. Mosenia A. A survey on security in Internet of Things: State of the art and challenges / A. Mosenia, N. K. Jha // Computer Networks. – 2017. – Vol. 111. – P. 17 – 48.
9. Sicari S. Security, privacy and trust in Internet of Things: The road ahead / S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini // Computer Networks. – 2015. – Vol. 76. – P. 146 – 164.
10. Kulkarni A. “Modeling Traffic with BMAP Queues for Performance Analysis of IoT Networks” International Journal of Computer Applications, vol. 182, no. 2, pp. 12 – 18, 2018.

REFERENCES:

1. Andriychuk M. Traffic modeling in Internet of Things networks / M. Andriychuk // Radioelectronics, Informatics, Management. – 2020. – No. 2. – P. 15 – 23.
2. Kovalchuk V. Features of using the MQTT protocol in IoT / V. Kovalchuk, I. Ivanova // Scientific works of ONAZ named after O. S. Popov. – 2019. – No. 4. – P. 56 – 62.
3. Lapko A. Simulation modeling of IoT network protection / A. Lapko, S. Prytula // Bulletin of NTUU "KPI". Series: Informatics and computing. – 2021. – No. 75. – P. 44 – 50.
4. Hrytsenko V. Approaches to building IDS for IoT / V. Hrytsenko, M. Solovey // Information Processing Systems. – 2022. – No. 3(172). – P. 27 – 34.

5. Melnyk O. Using Markov processes to describe IoT traffic / O. Melnyk // Mathematical modeling and computational methods. – 2020. – Vol. 2, No. 1. – P. 91 – 99.

6. Chen S. A survey on industrial Internet of Things security architecture / S. Chen, H. Xu, D. Liu et al. // Future Internet. – 2020. – Vol. 12(1). – P. 1 – 18.

7. Alrawais A. Fog computing for the Internet of Things: Security and privacy issues / A. Alrawais, A. Alhothaily, C. Hu, X. Cheng // IEEE Internet Computing. – 2017. – Vol. 21(2). – P. 34 – 42.

8. Mosenia A. A survey on security in Internet of Things: State of the art and challenges / A. Mosenia, N. K. Jha // Computer Networks. – 2017. – Vol. 111. – P. 17 – 48.

9. Sicari S. Security, privacy and trust in Internet of Things: The road ahead / S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini // Computer Networks. – 2015. – Vol. 76. – P. 146 – 164.

10. Kulkarni A. "Modeling Traffic with BMAP Queues for Performance Analysis of IoT *Networks" International Journal of Computer Applications, v*ol. 182, no. 2, pp. 12 – 18, 2018.

Dr. Tech. Sci., prof. Khlaponin Yu.I., Kondakova A.M.

RESEARCH ON THE EFFECTIVENESS OF DEVELOPED ALGORITHMS AND PROTECTION MODELS IN INTERNET OF THINGS NETWORKS

The article considers approaches to ensuring high-quality service of Internet of Things (IoT) services in 5G networks, taking into account modern challenges in terms of scalability, variable topology and security threats. Considerable attention is paid to modeling IoT traffic, building mathematical service models and assessing parameters that affect the level of reliability and timeliness of data delivery.

During the study, the specifics of the structure of IoT networks were analyzed, key traffic metrics were identified and a mathematical model was built based on the classical Poisson model, as well as its extensions MMPP and BMAP to adequately reflect the variable and clustered traffic structure in IoT networks. Clustering was performed using the k-means algorithm to profile normal node behavior, which made it possible to detect anomalies in real time. A formal risk assessment model was proposed that takes into account deviations of current metrics from a typical cluster and changes in intensity. An adaptive incident response mechanism with threshold values that determine the level of intervention from limiting activity to completely blocking the device. For verification, DDoS, device substitution, and stealth attack scenarios were simulated. The effectiveness of the detection algorithm was assessed using the metrics precision, recall, F1-score, and response time.

The results showed that the proposed methodology provides high anomaly detection accuracy (F1-score = 92.5%) with a response time of up to 80 ms, which makes it suitable for use in real IoT systems. The proposed approach allows for increased network reliability and security without significantly increasing computational costs. The findings confirm the feasibility of implementing intelligent monitoring systems based on clustering and risk models in the 5G-IoT infrastructure.

Keywords: internet of Things, traffic modeling, cybersecurity, protection algorithms, 5G, IDS, anomalies.