**Міністерство освіти і науки України**
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету )
Кафедра кібербезпеки
(повна назва кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Методи та засоби захисту інформації системи «розумний дім»

Виконав: студент VI курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Лесишин Т.І. (прізвище та ініціали)

Керівник (підпис) Баран І.О. (прізвище та ініціали)

Нормоконтроль (підпис) Лечаченко Т.А. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) Боднарчук І.О. (прізвище та ініціали)

Тернопіль - 2023

Міністерство освіти і науки України
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

# ЗАВДАННЯ
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Лесишину Тарасу Івановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби захисту інформації системи «розумний дім»

Керівник роботи Баран Ігор Олегович., к.т.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «16» 11 2023 року № _

2. Термін подання студентом завершеної роботи 25.12.2023р.

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналіз предметної області. 1.1 Аналітичний огляд. 1.2 Опис атаки FATS. 1.3 Безпека розумного будинку. 1.4 Конфіденційність розумного будинку. 2. Теоретична частина. 2.1 Атаки бічного каналу. 2.2 Вразливості розумних систем. 2.3 Категорії атак бічного каналу 2.4 Атака з відсмоктування даних з розумного будинку. 2.5 Стратегії захисту приватності від атаки FATS. 2.6 Техніка введення пакетів зі затримкою. 2.7 Метод ін'єкції фальшивих пакетів 2.8 Гібридні техніки. 3. Практична частина. 3.1 Методи захисту сигналів в мережевому Трафіку 3.2 Показники EDR та TPR. 4. Безпека життєдіяльності, основи охорони праці. 4.1 Основи охорони праці. 4.2 Безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титулка. 2. Актуальність. 3. Мета, задачі дослідження. 4. Атака FATS.
5. Аналіз методів захисту. 6,7,8. Дослідження кожного методу.
9. Запропонований аналог. 10. Результати проведеного дослідження

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Основи охорони праці | Осухівська Г.М., зав. каф. КС | | |
| Безпека життєдіяльності | Стручок В.С., ст. викладач каф. ОХ | | |

7. Дата видачі завдання 16.11.2023р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Ознайомлення з завданням до кваліфікаційної роботи | 16.11 – 16.11 | *Виконано* |
| 2. | Підбір джерел про методи захисту системи «Розумний | | |
| | Дім» | 17.11 – 20.11 | *Виконано* |
| 3. | Опрацювання джерел про методи захисту системи | | |
| | «Розумний Дім» | 21.11 – 23.11 | *Виконано* |
| 4. | Виконання дослідження щодо методів захисту системи | | |
| | «Розумний Дім» | 24.11 – 27.11 | *Виконано* |
| 5. | Підготовка матеріалу | 28.11 – 30.11 | *Виконано* |
| 6. | Оформлення розділу «Аналіз предметної області» | 01.12 – 03.12 | *Виконано* |
| 7. | Оформлення розділу «Теоретична частина» | 04.12 – 06.12 | *Виконано* |
| 8. | Оформлення розділу «Практична частина» | 07.12 – 09.12 | *Виконано* |
| 9. | Виконання завдання до підрозділу «Безпека | | |
| | життєдіяльності, основи хорони праці» | 10.11 – 12.12 | *Виконано* |
| 10. | Оформлення кваліфікаційної роботи | 12.12 – 13.12 | *Виконано* |
| 11. | Нормоконтроль | 18.12 – 19.12 | *Виконано* |
| 12. | Перевірка на плагіат | 18.12 – 19.12 | *Виконано* |
| 13. | Попередній захист кваліфікаційної роботи | | |
| 14. | Захист кваліфікаційної роботи | 26.12 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Студент _____ Лесишин Т.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Баран І.О.
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

Методи та засоби захисту інформації системи «розумний дім» // Лесишин Тарас Іванович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм–61 // Тернопіль, 2023 // С. – 69, рис. – 16, табл. – 1, слайдів – 11 .

Ключові слова: IOT, РОЗУМНИЙ ДІМ, FATS, РОЗУМНІ СИСТЕМИ, МЕТОДИ ЗАХИСТУ, EDR, TRP

Кваліфікаційна робота присвячена застосуванню методів захисту системи «розумний дім» від атак по типу FATS.

У першому розділі проведено теоретичний аналіз аспектів системи розумного дому та принципів її роботи. А також описаний принцип роботи атаки FATS.

У другому розділі наведені вразливості розумних систем, а також інші методи та техніки можливих атак. Наведені стратегії захисту від атаки FATS.

У третьому розділі розглядається основні методи захисту ConstRate, ProbRate, FitProbRate, SDASL. Продемонстровані принципи роботи цих методів, а також ефективність їх протидії атакам FATS.

# ANNOTATION

Methods and Means of information protection of the «Smart Home» system // Lesyshyn Taras // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2023 // P. - 69, Fig. - 16, Table – 1, Slides – 11.

Keywords: IOT, SMART HOME, FATS, SMART SYSTEMS, PROTECTION METHODS, EDR, TRP

The qualifying work is dedicated to the application of protection methods for the "smart home" system against side-channel attacks and FATS attacks.

The first section provides a theoretical analysis of aspects of the smart home system and its operating principles. Additionally, it describes the working principle of the FATS attack.

The second section outlines vulnerabilities in the smart systems, as well as other methods and techniques of potential attacks. It presents strategies for protecting against FATS attacks.

The third section explores the main protection methods: ConstRate, ProbRate, FitProbRate, SDASL. The working principles of these methods are discussed, along with their effectiveness in countering FATS attacks.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

FATS – fingerprint and timing-based snooping

SCA – side-channel attack

IoT – Internet of Things

AI – Artificial intelligence

ADL – Activities of Daily Living

SPA – simple power analysis

DPA – differential power analysis

CMDS – classical non-parametric multi-dimensional scaling

LDA – linear discriminant analysis

WSN – wireless network systems

SDASL – sample data and supervised learning

RF – radio frequencies

TPR – true positive rate

EDR – event detection rate

AAM – actual activity mimicking

# ЗМІСТ

# ВСТУП

Актуальність теми. В останні роки технології розумного будинку здобули значну популярність серед користувачів, завдяки важливим досягненням у розвитку їхніх основних компонентів, таких як сенсори та процесори. Ці компоненти стали широко поширеними в різних галузях і водночас стали більш доступними. Незважаючи на ці досягнення, системи, засновані на Інтернеті речей, виявилися вразливими до витоків даних, що породжує серйозні проблеми конфіденційності. Цей аспект пробуджує зацікавленість дослідників у пошуку безпечних рішень для вирішення цього виклику.

Актуальність даної теми обумовлена в контексті зростаючого використання технологій розумного будинку, дослідження методів захисту від атак, зокрема FATS, має велике значення для забезпечення безпеки та конфіденційності користувачів.

Мета дослідження: дослідити методи захисту розумних систем.

В роботі поставлено та розв’язано наступні задачі:

– проаналізувати стан та тренди розвитку даного напряму;
– виконати огляд можливостей створення захищених умов;
– провести огляд регулювання спорідненості захищеної системи із навколишнім середовищем;
– дослідити способи проведення атак;
– створити моделі захисту.

Об’єкт дослідження: розумні системи та IoT.

Предмет дослідження: методи та засоби захисту розумних систем.

Методи дослідження: наукові роботи українських та зарубіжних вчених за темою дослідження.

Наукова новизна отриманих результатів:

– досліджено основні методи рівномірного розподілу сигналів у мережевому трафіку і продемонстровано принцип роботи;
– запропоновано підхід, для покращення ефективності даних методів.

Практичне значення одержаних результатів. Результати проведеного дослідження можуть бути використані в реальних будинках з розумними системами для покращення захисту.

Апробація. Результати дослідження апробовано на XI науково- технічній конференції «Інформаційні моделі, системи та технології» у вигляді опублікованих тез.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається з вступу, 4 розділів, висновків, списку використаної літератури. Обсяг роботи: пояснювальна записка – 69 арк. формату А4, графічна частина – 11 слайдів, додатки – 1 арк. формату А4.

# 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

## 1.1 Аналітичний огляд

Розумний будинок - це концепція, яка існує протягом кількох десятиліть [1 - 3] і обіцяє технологічно вдосконалене житло для підвищення якості домашнього життя мешканців. У останні роки, завдяки появі та стрімкому розвитку IoT та рішень машинного інтелекту, ця технологія далі розвивалася від віддалено керованого або автоматизованого будинку до більш реалістичного, розумного будинку. Сучасні розумні будинки на основі IoT надають різноманітні послуги для підвищення зручності та контролю мешканців над своїми будівлями, комбінуючи кілька інтелектуальних пристроїв. Деякі з пропонованих переваг поточних розумних будинків включають управління та обслуговування в галузі: температури [4], обстановки освітлення [5], споживання енергії [6], внутрішнього спостереження [7], ризиків безпеки [8], таких як випадки пожежі [9], фізичної безпеки [10], вторгнень, та моніторингу здоров'я для літніх людей, дітей та домашніх улюбленців [11]. Однак використання наведених послуг не є абсолютно безпечним для користувачів; наприклад, існує ризик порушення конфіденційності.

Системи IoT великою мірою залежать від бездротових рішень у комунікації. Оскільки домашня мережа несе значний обсяг особистої інформації мешканців, будь-який випадок витоку даних може бути катастрофою для користувачів, наприклад, несанкціоноване розголошення стилю життя, стану здоров'я, політичних поглядів та фінансового становища [12, 13]. У багатьох випадках потенційні збитки від випадку витоку даних в розумному будинку можуть бути складними для компенсації, якщо не неможливими. Тому зростання обурення щодо конфіденційності розумних будинків стимулює дослідників шукати відповідні рішення для зменшення цього ризику. У цій роботі коротко розглянуто загрози від атак шпигунства за допомогою бокового каналу сигналу, а потім головним чином зосереджено на атаці FATS, щоб дослідити останні спроби та досягнення у вирішенні цієї проблеми та існуючі прогалини в

дослідженнях.

Завдяки стандартам індустрії та зростаючій конкуренції між виробниками розумних пристроїв, вартість та доступність цих технологій постійно збільшуються. Це сприяє більш широкому поширенню розумних будинків серед різних соціальних груп. Нові функції та можливості постійно додаються до розумних систем, що робить їх більш адаптивними та зручними для кінцевих користувачів.

Однією з перспективних галузей розвитку розумних будинків є їх інтеграція в міську інфраструктуру, що дозволить створити концепцію "розумного міста". Взаємодія між розумними будинками, транспортними системами, комунальними службами та іншими складовими міського середовища може призвести до покращення якості життя мешканців та оптимізації використання міських ресурсів.

Невпинний розвиток розумних технологій також ставить перед собою завдання забезпечення високого рівня кібербезпеки. Велика кількість підключених пристроїв та обмін даними потребує ефективних заходів для захисту від потенційних кіберзагроз.

Розумні будинки є не лише символом сучасних технологій, але й важливим етапом у вдосконаленні нашого повсякденного життя. Вони стають більш доступними та інтегрованими, пропонуючи нові можливості для комфорту, безпеки та раціонального використання ресурсів.

## 1.2 Опис атак FATS

Приватність даних в сучасних інтелектуальних будинках стає все більш важливою, оскільки жителі активно діляться інформацією про свої щоденні звички через велику кількість вбудованих сенсорів. Ці дані обробляються інтелектуальними системами для адаптації роботи під потреби мешканців. Проте цей потік інформації може стати предметом використання зловмисниками для виявлення особистих деталей життя мешканців.

Приватність, у контексті інтелектуальних будинків, визначається як право

особи на утримання особистого життя та інформації в таємниці, доступній лише обмеженій кількості осіб. Це право закріплено законом у більшості країн і захищається від порушень, таких як нелегальне слідкування чи несанкціонований доступ.

Мотивація для порушення приватності може бути різноманітною, включаючи комерційні вигоди і особисті ворожбиті. Навіть уряди можуть порушувати приватність громадян через нелегальне слідкування. Такий сценарій підкреслює необхідність зміцнення захисту приватності в інтелектуальних будинках.

Атаки, такі як FATS, базовані на аналізі відбитків і часу, становлять серйозний ризик. Системи виявлення вторгнень часто неефективні в цьому випадку через пасивний характер атаки. Атакуючі можуть непомітно збирати дані, і жертвам важко вчасно реагувати на цю загрозу.

Шифрування не завжди допомагає, оскільки атака здійснюється з врахуванням контекстуальних аспектів бездротових передач. У світлі цих викликів важливо розробляти надійні та активні механізми захисту в інтелектуальних будинках. Такі механізми мають забезпечувати ефективний захист інформації користувачів, зберігаючи баланс між конфіденційністю та зручністю використання системи.

SCA є важливою проблемою для безпеки систем, оскільки зловмисники можуть використовувати пристрої без повного контролю над ними, не маючи доступу до вихідних кодів, вмісту комунікацій або деталей функціональності системи. Розглянемо різні аспекти SCA, включаючи фізичні аспекти, відповіді системи та контекстуальні дані, пов'язані з бездротовою комунікацією розумного пристрою. Ці аспекти формують різнорідні ресурси для отримання критичної інформації з систем.

Атака FATS є однією з атак SCA, використовуючи підслуховування випромінюваних сигналів для створення уявлення про внутрішні дії мешканців. Це пасивне порушення конфіденційності, що ставить жертв у складну ситуацію, оскільки вони не можуть виявити атаку під час проведення. Отримані дані можуть використовуватися для шантажу чи продажу третім сторонам.

Для подолання ризиків атак FATS дослідники розробляють активні стратегії оборони для саботування роботи атаки, оскільки блокування їх повністю неможливо. Одна з основних стратегій - приховування бездротових шаблонів трафіку фактичних подій та затуманювання кореляцій між передачами. Це включає введення вимушеної випадкової затримки перед передачею пакета та внесення фіктивних пакетів в трафік мережі.

Розробка механізму збереження конфіденційності для розумних будинків проти атак FATS стикається з численними викликами. Важливо забезпечити оптимальний баланс між конфіденційністю, затримкою системи та енергетичними вимогами. Багато існуючих рішень мають недоліки в ефективності відносно споживання енергії та часу реакції системи.

Звітування про фактичні події із затримкою може впливати на якість обслуговування, а введення фіктивних пакетів може призвести до зайвого споживання енергетичних ресурсів системи. Таким чином, пошук ефективних рішень, які враховують усі аспекти, є важливим напрямком досліджень у сфері кібербезпеки розумних будинків.

## 1.3 Безпека розумного будинку

Розумний будинок – це не просто житлова будівля; це технологічно оснащений простір, де велика кількість взаємопов’язаних розумних систем створює унікальне житлове середовище. Ці вбудовані системи пропонують користувачам передові цифрові послуги, які полегшують їхнє життя та роблять його більш комфортним і ефективним. Переваги розумного будинку охоплюють різноманітні аспекти, починаючи від дистанційного моніторингу стану здоров'я і закінчуючи інтелектуальним управлінням комунальними послугами та високорівневим відеоспостереженням за безпекою [14, 15].

Швидка еволюція технологій, таких як IoT, AI та бездротові рішення зв'язку, відкриває безмежні можливості для розумних будинків та робить їх особливо привабливими для сучасних користувачів. Розробка датчиків та виконавчих пристроїв Інтернету речей стає важливим компонентом цього

технологічного революційного розвитку, роблячи їх більш вартісними та універсальними у різних областях застосування [16, 17].

Поліпшені бездротові протоколи відіграють важливу роль у розвитку розумних будинків. Вони пропонують легкі рішення з більш широким охопленням сигналу, кращою стабільністю та надійністю з'єднання, меншим попитом на енергію та більш жорсткими заходами безпеки [18].

Машинне навчання відіграє важливу роль у розробці різноманітних рішень для розумних будинків. Це охоплює створення чат-ботів [19], автоматизованих відеоаналізаторів для систем відеоспостереження [20], систем виявлення аномалій [21] і технологій інтелектуальної взаємодії комп'ютера і людини [22].

Незважаючи на беззаперечні переваги, які розумні будинки можуть принести, вони також породжують обурення, особливо у зв'язку з питаннями інформаційної безпеки та конфіденційності. Через схильність до можливого витоку особистих даних, розумні будинки можуть стати об'єктом серйозних наслідків для користувачів [23, 24].

У всій своїй сучасній славі розумний будинок, однак, викликає серйозні питання щодо інформаційної безпеки та приватності. Велика кількість взаємодіючих систем створює потенційні точки вразливості, які можуть бути використані для несанкціонованого доступу та витоку конфіденційної інформації.

Щоб забезпечити високий рівень захисту, необхідно вдосконалювати методи шифрування, контролю доступу та моніторингу систем. Також важливо враховувати питання етики та визначати прозорі політики щодо використання та зберігання даних користувачів.

Розумні будинки можуть стати ключовим елементом сучасної інфраструктури, проте їх успішне впровадження вимагає уважного вивчення та вирішення всіх аспектів, пов'язаних із забезпеченням безпеки, захистом приватності та створенням надійних і стійких до атак систем. Тільки таким чином розумні будинки зможуть відкривати нові можливості для користувачів, забезпечуючи сучасне та безпечне житло..

На рисунку 1.1 представлена схематична картинка інтелектуального

будинку та його різноманітних застосувань. Це включає в себе інтеграцію розумних систем у кожен аспект побуту, починаючи від автоматизованого управління освітленням та закінчуючи системами енергозбереження та контролю клімату.

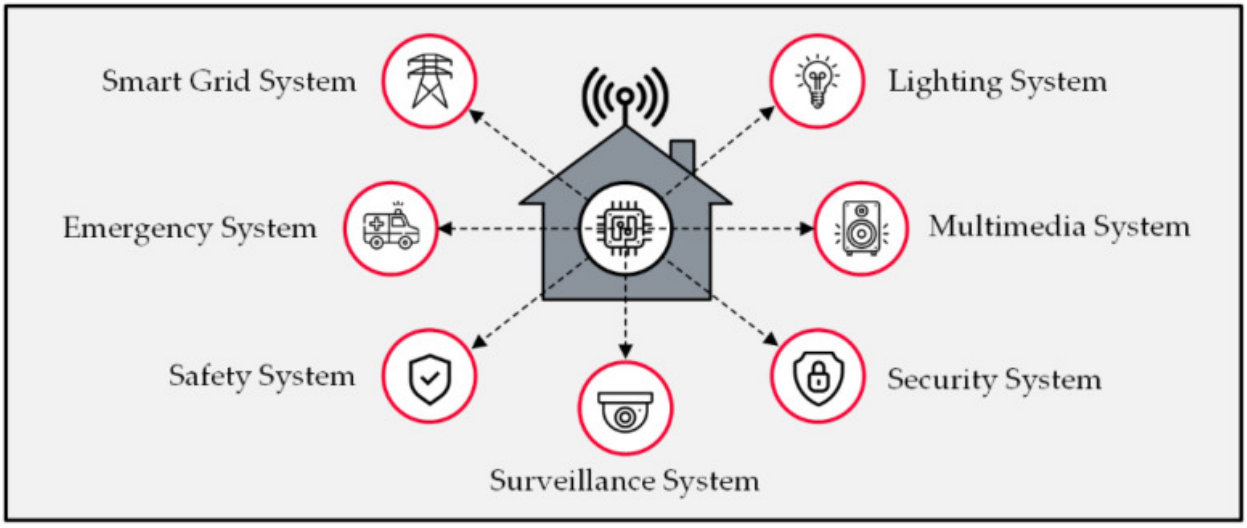


Рисунок 1.1 – Підсистеми розумного будинку

## 1.4 Конфіденційність розумного будинку

Загрози конфіденційності, пов'язані з розумними будинками, входять до категорії найбільших ризиків, які необхідно вирішувати для забезпечення надійності та захисту особистої інформації користувачів. Однак варто враховувати, що наявність різноманітних кібератак може призвести до серйозного компрометування функціональності систем розумного будинку. Забезпечення безпеки особистих даних мешканців є невід'ємною частиною розвитку та прийняття таких технологій.

Дані, що передаються через бездротову мережу IoT, можна розділити на дві основні категорії: системні дані та дані користувачів. Для забезпечення відповідного рівня безпеки необхідно приділяти увагу кожній з цих категорій. Системні дані можуть містити критичну інформацію про функціонування та стан

розумного будинку, тому важливо забезпечити їх конфіденційність.

З іншого боку, дані користувачів є особистими та приватними, що вимагає не лише конфіденційності, але й захисту приватності. Розробники та постачальники розумних систем повинні вживати ефективних заходів для захисту особистих даних мешканців та забезпечення їхньої непорушності.

Отже, вирішення проблем конфіденційності та безпеки в розумних будинках передбачає комплексний підхід, який включає в себе технічні заходи, політики захисту даних та свідоме відношення до проблем кібербезпеки від усіх учасників цього процесу.

### 1.4.1 Конфіденційність даних

Конфіденційність в бездротових системах виходить на перший план як надзвичайно важливий аспект, оскільки вона передбачає належне приховування вмісту пакетів даних, які включають у себе керуючі повідомлення або інформацію про функціональність розумних пристроїв, та запобігання несанкціонованому доступу зловмисників [20]. Використання криптографічних методів є загальним і відомим способом захисту цих повідомлень в системі IoT. Складність передових методів шифрування ставить серйозний виклик перед атакуючими, які постійно намагаються знайти секретні ключі для розкриття змісту та забезпечення того, що інформація системи залишається недоступною тим, хто не має дозволу [21].

З іншого боку, недоліком методів шифрування є те, що вони залишають незахищеними контекстуальні дані мережевих повідомлень. Тут йдеться про ідентифікацію, місцезнаходження та час активності розумного пристрою. Цей вид інформації надає значний ресурс зловмисникам для отримання критичної інформації про систему, яка може бути навіть ціннішою, ніж сам вміст.

Для вдосконалення захисту конфіденційності в бездротових системах необхідно продовжувати розробку та вдосконалення методів захисту, які охоплюють не лише захист вмісту, але й контекстуальних даних. Ще одним можливим шляхом розв'язання цього завдання є використання додаткових

заходів, таких як анонімізація чи шифрування контекстуальних даних. Це допомагає забезпечити повний обсяг конфіденційності в бездротових мережах Інтернету речей.

Такий комплексний підхід передбачає дослідження та впровадження інтегрованих стратегій захисту конфіденційності, що є невід'ємною частиною безпеки в сучасних розумних системах передачі даних. Застосування цих вдосконалених методів враховує різноманітні потреби в складних системах бездротового обміну інформацією, гарантуючи високий рівень захисту та конфіденційності для всіх користувачів.

Додатково, слід враховувати аспекти безпеки, пов'язані із зовнішніми атаками на систему IoT. Наприклад, атаки FATS можуть стати серйозною загрозою, оскільки зловмисники можуть використовувати пристрої без повного контролю над ними, не маючи доступу до вихідних кодів, вмісту комунікацій або деталей функціональності системи.

Розробка механізму збереження конфіденційності для розумних будинків проти атак FATS стикається з численними викликами. Важливо забезпечити оптимальний баланс між конфіденційністю, затримкою системи та енергетичними вимогами. Багато існуючих рішень мають недоліки в ефективності відносно споживання енергії та часу реакції системи.

Звітування про фактичні події із затримкою може впливати на якість обслуговування, а введення фіктивних пакетів може призвести до зайвого споживання енергетичних ресурсів системи. Таким чином, пошук ефективних рішень, які враховують усі аспекти, є важливим напрямком досліджень у сфері кібербезпеки розумних будинків.

Специфіка безпеки в інтелектуальних будинках доповнюється питаннями приватності даних, які є важливим елементом розгляду в контексті розумних систем. Жителі інтелектуальних будинків активно діляться інформацією про свої щоденні звички через вбудовані сенсори, спостерігаючи за їхньою активністю. Це створює потік даних, який може стати об'єктом для зловмисників та порушити приватність жителів.

### 1.4.2 Приватність даних

Приватність даних у сучасних інтелектуальних будинках стає необхідністю, оскільки велика кількість вбудованих сенсорів дозволяє системам відстежувати та аналізувати різноманітні аспекти життя мешканців. Захист особистої інформації стає важливим завданням для того, щоб уникнути порушення приватності та недозволеного доступу до особистих даних.

Концепція приватності полягає у визнанні права особи на утримання особистого життя та інформації в таємниці, доступній лише обмеженому колу осіб. Це право закріплено законом у більшості країн і забезпечується для захисту від незаконного слідкування чи несанкціонованого доступу до особистих даних.

Мотивація для порушення приватності може мати різні вектори, включаючи комерційні переваги та особисті ворожбиті мотивації. Навіть урядові органи можуть використовувати нелегальні методи слідкування, порушуючи приватність громадян. Це визначає необхідність посилення заходів захисту приватності в інтелектуальних будинках.

Певні види атак, наприклад, атаки, що базуються на аналізі відбитків і часу (FATS), можуть становити серйозний ризик для конфіденційності. Системи виявлення вторгнень можуть бути неефективними у випадках пасивних атак, коли зловмисники непомітно збирають дані, і потерпілі важко вчасно реагувати на цю загрозу. Навіть шифрування не завжди є достатнім, оскільки атаки враховують контекст бездротових передач.

Приватність даних особливо актуальна у випадку інтелектуальних будинків, де жителі активно діляться інформацією про свої щоденні звички через вбудовані сенсори. Інтелектуальні системи використовують ці дані для адаптації своєї роботи під потреби мешканців, але цей потік інформації може стати об'єктом для зловмисників та порушити приватність користувачів [26].

Розгортання систем інтелектуальних будинків пов'язане з викликами щодо захисту конфіденційності. Проте, розумні технології можуть бути використані для розробки механізмів, які забезпечують безпеку та конфіденційність.

Важливо розглядати приватність як призначений для захисту та розвивати інноваційні рішення для забезпечення високого рівня безпеки особистих даних.

Для забезпечення високого рівня захисту, необхідно розглядати технології шифрування, вдосконалення методів аутентифікації та розглядати можливості обмеження доступу до особистих даних. Застосування принципів "за замовчуванням конфіденційно" і "прозорий захист приватності" може допомогти зміцнити захист в інтелектуальних будинках.

Окрім технічних заходів, важливо проводити освіту серед користувачів щодо питань кібербезпеки та захисту приватності. Висвітлення можливих ризиків та навчання правилам безпеки може покращити свідомість користувачів і зробити їх менш вразливими до соціально інженерних атак.

Усі ці заходи повинні вписуватися в розвиток сучасних стандартів безпеки та політик конфіденційності, а також враховувати законодавство, яке регулює збір та обробку особистих даних. Забезпечення приватності в інтелектуальних будинках - це складне завдання, що вимагає спільних зусиль розробників, виробників, законодавців та користувачів для створення безпечного та надійного середовища.

У зв'язку з цим важливо постійно розробляти та вдосконалювати надійні та активні механізми захисту в інтелектуальних будинках. Ці механізми повинні забезпечити ефективний захист інформації користувачів, утримуючи баланс між конфіденційністю та зручністю використання системи. На рисунку 1.2 відображено різницю між конфіденційністю та приватністю, враховуючи різні типи даних.

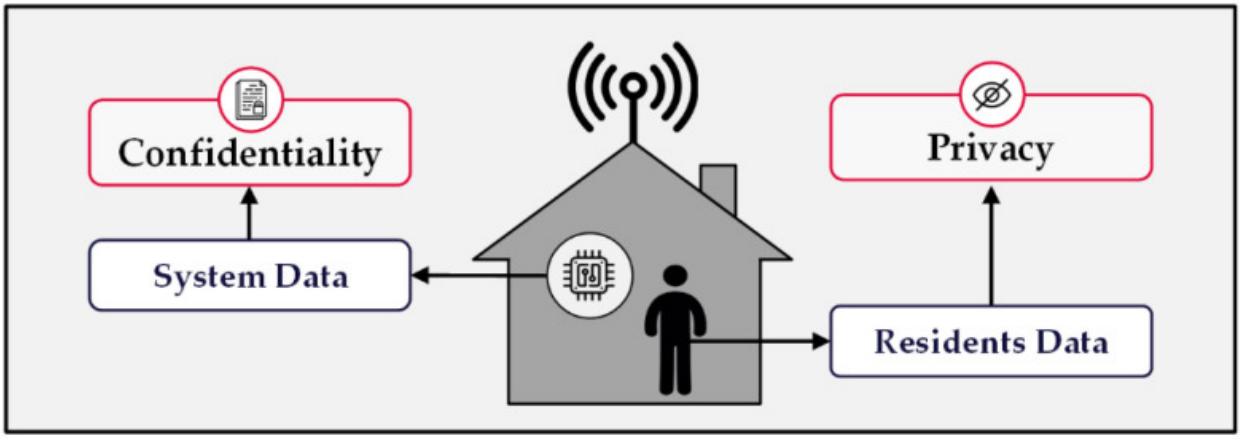


Рисунок 1.2 – Типи даних та пов'язані з ними заходи безпеки

## 1.5 ВИСНОВОК ДО РОЗДІЛУ І

У цьому розділі було розглянуто застосування Інтернету речей та розумного дому, наведені його основні підсистеми розумного дому.

Також були проаналізовані загрози конфіденційності та можливі ризики, проаналізовано безпеку розумного будинку.

Описаний один з можливих ризиків, а саме атака FATS.

# 2 ТЕОРЕТИЧНА ЧАСТИНА

## 2.1 Атаки бічного каналу

Проведення атаки бічного каналу означає використання фізичних аспектів пристрою для виявлення пов'язаної з ним критичної інформації. Основне припущення в атаках бічного каналу полягає в тому, що дані постійно витікають; отже, зловмисники мають можливості зловживати системою [25].

Атаки бічного каналу поділяються на активні та пасивні. Активні атаки бічного каналу потребують фізичного доступу до цільового пристрою/системи або фізичної близькості. Прикладом активної атаки бічного каналу є атака аналізу несправностей, в якій хакери вводять заздалегідь визначені входи та спостерігають за реакцією системи; через цей процес вони мають намір виявити, як пристрій працює. Іншим прикладом є аналіз звуків, вироблених пристроєм, та виявлення їх кореляції з функціональністю системи, що більше застосовується до систем із механічними виконавчими пристроями.

Пасивні атаки бічного каналу не виявляються потерпілими під час атаки. Вони тихо використовують зовнішні аспекти пристрою. Наприклад, атака прослуховування дистанційно прослуховує мережевий трафік і захоплює передані пакети даних для подальшого аналізу. Навіть якщо захоплені пакети були зашифровані, зловмисники можуть витягти цінну інформацію з контекстуальних аспектів сигналів, що несуть ці пакети даних.

Відповідним рішенням для подолання ризику пасивних атак бічного каналу є використання активних методів захисту для запобігання зловмисникам інтерпретувати викрадені пакети [7].

Для захисту від атак бічного каналу важливо розглядати фізичні та програмні аспекти безпеки пристроїв та систем. Фізичні заходи можуть включати в себе захист від фізичного доступу, екранування пристроїв від електромагнітного випромінювання, а також використання антивірусів та програм для виявлення вторгнень.

У світлі зростання кількості підключених пристроїв і розвитку Інтернету

речей, захист від атак бічного каналу стає критично важливим завданням. Здатність адекватно реагувати на ці виклики і вдосконалювати методи захисту буде визначальним чинником для забезпечення безпеки пристроїв та конфіденційності користувачів.

## 2.2 Вразливості розумних систем

Типовий розумний пристрій, розроблений для розумного будинку, зазвичай має кілька стандартних будівельних блоків, таких як процесор, порти введення/виведення, диск для зберігання даних, модулі бездротового зв'язку (Wi-Fi, Bluetooth та ін.), блок живлення та, в залежності від застосування пристрою, групу сенсорів та виконавчих пристроїв. Для атакуючих, які використовують атаки бічного каналу, кожен компонент пристрою може виявити цінні дані. Таким чином, протягом останніх десятиліть було розроблено численні правопорушні техніки для вторгнення в різні аспекти розумних пристроїв [27 - 29].

SPA і DPA – це методи атак, спрямовані на виявлення конфіденційної інформації, таких як ключі шифрування, через аналіз споживаної енергії пристрою під час його роботи. Ці атаки особливо актуальні для блоків живлення, оскільки зловмисники можуть використовувати витікання енергії для отримання важливих даних.

Атаки на бездротові комунікації систем полягають у зловживанні часового та трафікового аналізу передачі даних через бездротові канали, такі як Wi-Fi та Bluetooth. Зловмисники можуть отримати доступ до конфіденційної інформації, моніторингу чи навіть модифікації передачі даних.

Атака на порти введення/виведення через аналіз несправностей може включати в себе введення зловмисних даних або витікання інформації через ці порти. Захист від цих атак включає фізичні та програмні заходи безпеки.

Акустичний та електромагнітний аналіз використовують витікання звукових чи електромагнітних сигналів, що генеруються пристроєм під час його роботи. Зловмисники можуть використовувати ці витоки для отримання

інформації про внутрішні процеси пристрою.

Загальна стратегія захисту передбачає використання фізичних засобів безпеки, вдосконалення криптографічних методів шифрування, застосування заходів контролю доступу та моніторингу мережі для виявлення підозрілих активностей. Продовження досліджень у цій області є ключовим для розробки більш ефективних методів захисту розумних пристроїв та систем Інтернету речей.

Як показано на рисунку 2.1, кожна вбудована одиниця в пристрої стикається щонайменше з відповідною атакою. Простий аналіз потужності (SPA) та диференційний аналіз потужності (DPA) - це дві атаки, які загрожують системі через блок живлення.

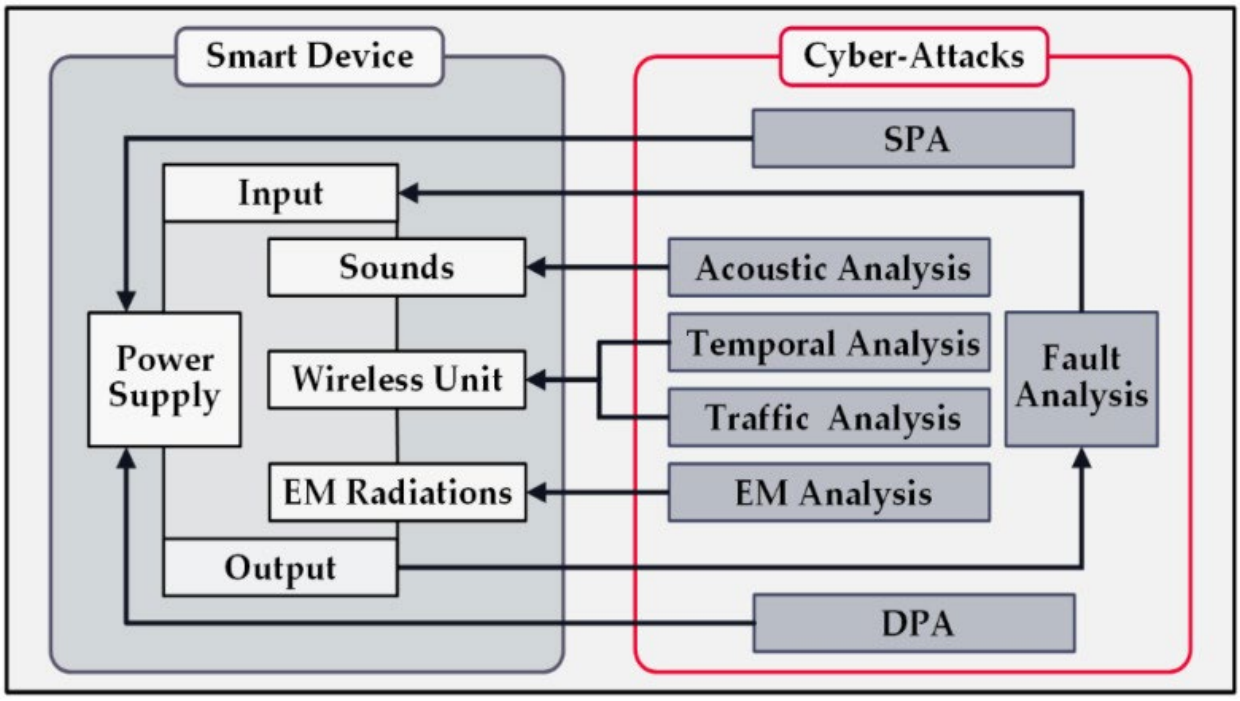


Рисунок 2.1 – Схема атак на смарт-пристрої

## 2.3 Категорії атак бічного каналу

Атаки бічного каналу поділяються на три класи з точки зору фізичної

безпеки: інвазивні, напівінвазивні та неінвазивні. Інвазивна атака фізично маніпулює цільовим пристроєм, що в більшості випадків призводить до його знищення. Пошкодження компонентів для вивчення їх функцій та проведення хімічних експериментів - це приклади цього класу атак бічного каналу. Так само напівінвазивні атаки бічного каналу потребують фізичних маніпуляцій, але не розбирають пристрої - наприклад, відкриття корпусу для отримання прямого доступу до плати або розбирання деяких частин.

З іншого боку, неінвазивні атаки бічного каналу лише використовують доступну інформацію через порти даних, зовнішні кабелі живлення, бездротові комунікації, випромінювання електромагнітних хвиль або вироблені звуки. Ці елементи надають цінні контекстні дані про систему та її функціональність [30]. Рисунок 2.2 демонструє таксономію атак бічного каналу.

Неінвазивні атаки бічного каналу можуть бути особливо тонкими і ефективними, оскільки вони використовують доступні зовнішні джерела для отримання інформації про пристрій без фізичного втручання. До цих атак відносять аналіз електромагнітних випромінювань, перехоплення інфрачервоних сигналів, аналіз звукових сигналів та інші методи. Їхній успіх залежить від точності та чутливості вимірювального обладнання, а також від того, наскільки система захисту пристрою може утруднити або заважати збору цієї інформації.

Таксономія атак бічного каналу на рисунку 2.2 дає загальний огляд класів атак та підкреслює різноманітність методів, які можуть бути використані зловмисниками. Захист від таких атак вимагає інтегрованого підходу, включаючи фізичні заходи безпеки, криптографічні методи та програмні заходи контролю доступу.

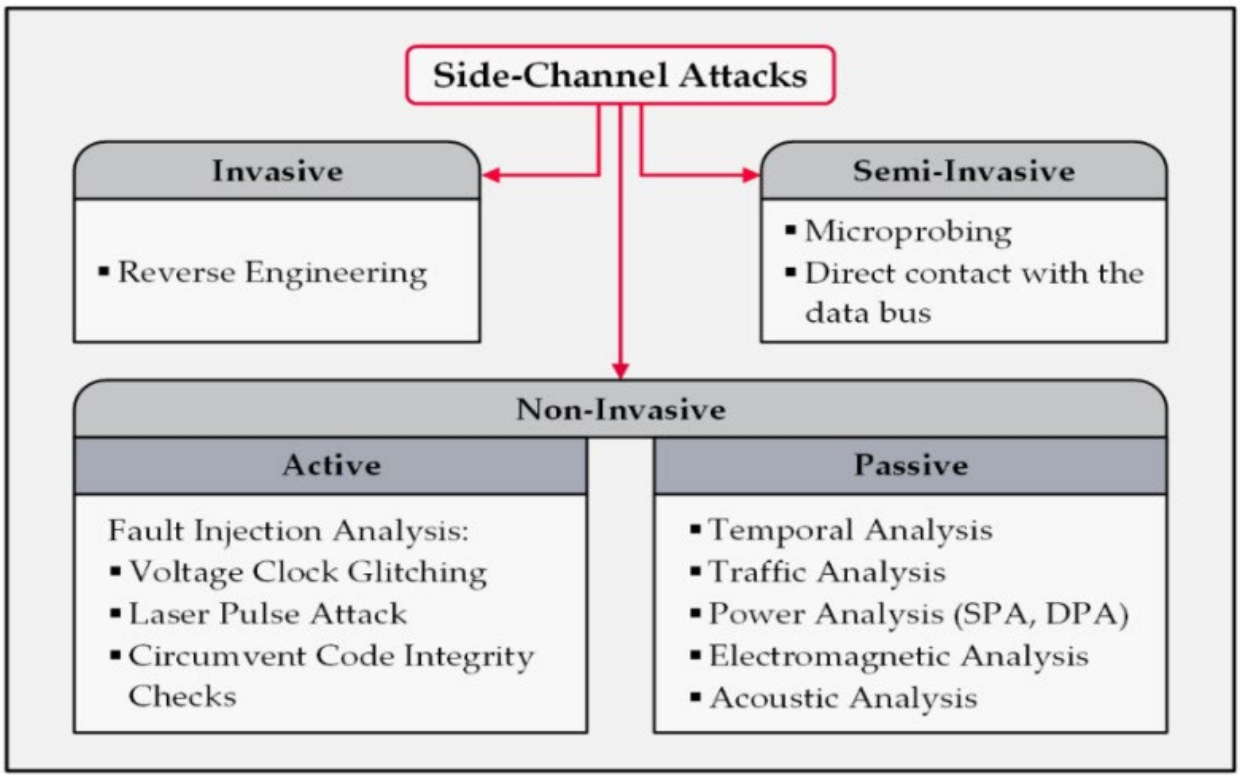


Рисунок 2.2 – Таксономія атак бічного каналу

Аналіз енергоспоживання та диференційний аналіз енергоспоживання - це дві техніки, які використовуються для виявлення чутливої інформації в пристроях за допомогою вивчення їхнього використання енергії [31].

SPA: Спостерігає за змінами споживання енергії пристрою під час виконання різних алгоритмів і виявляє серії патернів, які можна корелювати з конкретними діями. Зловмисники намагаються зіставити ці вилучені патерни з відомими алгоритмами для визначення функції пристрою. Наприклад, цей метод може розрізняти методи шифрування, оскільки їх вимоги до енергії різні. Слід відзначити, що випадкові сплески струму та шуми є викликами, які обмежують ефективність цього підходу [32].

DPA: Це вдосконалений метод аналізу потужності, який використовує статистичні підходи для виправлення помилок. Цей метод спостерігає за споживанням енергії пристрою для виявлення ключа шифрування. Основна відмінність між методами DPA і SPA полягає в тому, що метод DPA аналізує споживання енергії пристрою для двох типів операцій - некриптографічних та криптографічних; потім порівнює результати для виявлення критичної

інформації системи. DPA - це потужний інструмент, який загрожує всім видам апаратного забезпечення, захищеного криптографічними підходами [33, 34].

Аналіз несправностей: Це підхід, при якому зловмисник вводить різні види несправностей у розумний пристрій і досліджує результати системи. Деякі приклади фізичних маніпуляцій з обладнанням - підвищення температури пристрою, направлення лазерного променя з певною частотою та введення штучних входів для збільшення ймовірності зіткнення сигналів [35].

Електромагнітний аналіз: Використовує випромінену потужність випромінювання пристроїв, захищених криптографічними підходами, під час виконання процесів шифрування та дешифрування для виявлення кореляції між електромагнітним випромінюванням та шифротекстом. Ця атака не вимагає непосередньої близькості атакуючої системи до цільового пристрою, залежно від потужності обладнання для прийому випромінення, що робить її підходящою для віддаленого виконання.

Акустичний аналіз: Використовує вироблені звуки (шуми) електромеханічних компонентів пристрою як вхідні дані та намагається отримати конфіденційну інформацію системи за допомогою аналізу акустичних коливань. Переваги цієї атаки - здатність алгоритму атаки точно розрізняти слабо відмінні звуки та його використання відносно простого обладнання, такого як цифровий пристрій запису звуку чи смартфон [36 - 38].

Аналіз часу: Зосереджується на часових даних, пов'язаних із бездротовими передачами сигналів системи. Атака спрямована на виявлення тимчасових кореляцій у мережевому трафіку та розпізнавання патернів, що розкривають критичну інформацію про поведінку системи. Цей злочинний підхід є відповідним варіантом для атакуючого, який має глобальний огляд над комунікаціями системи, особливо якщо йому цікава контекстна інформація системи [39].

Аналіз трафіку: Включає широкий спектр опцій для дослідження мережевого трафіку системи. Цей підхід головним чином фокусується на переданих пакетах даних через бездротову мережу. Кількість пакетів, асоційовані відбитки сигналів пакетів та кореляція між пакетами, які

передаються з різних пристроїв, є цінними контекстними даними для зловмисника при визначенні відправника, отримувача та їхніх місць [40].

## 2.4 Атака з відсмоктування даних з розумного будинку

Через їх пасивний характер, кібератаки на основі прослуховування є однією з найважливіших загроз кіберфізичним системам. Тим не менше, було розроблено кілька криптографічних рішень для захисту вмісту комунікацій. Підклас цих атак спрямований на контекстні дані системи, тому методи шифрування стають неактуальними для забезпечення безпеки даних системи при зіткненні з такими загрозами. У цій статті ми розглядаємо атаку такого роду, відому як атака на основі сліду та вимірювання часу (FATS) [41]. Ця атака починається з прослуховування сигналів, що випромінюються з розумного будинку, знаходячись в неподалік від будинку в межах бездротової мережі будинку (наприклад, в будинку сусіда), навіть коли всі пакети даних зашифровані. Потім алгоритм атаки аналізує зібрані пакети даних на основі їх відбитків сигналу та відміток часу, щоб виявити повсякденні дії жертв. Ця ситуація є яскравим прикладом порушення приватності.

Вкрадені дані з домашньої мережі можуть містити чутливу інформацію про спосіб життя мешканців, політичні погляди, фінансовий стан, особисті умови здоров'я, сексуальну поведінку, розклади, вибори покупок та інше. Таким чином, зловмисник буде здатний запускати подальші серйозні атаки на шкоду своїм жертвам, використовуючи цю інформацію. Приклади можливих ризиків включають шантаж, продаж інформації третій стороні, тероризм, дифамацію та державний слід.

Реалізація атак FATS складається з декількох рівнів, в яких відбувається поєднання технік машинного навчання, таких як класифікація, кластеризація та відповідність на основі ознак. Атака кластеризує зафіксовані сигнали на основі їх відбитків радіо та намагається знайти взаємозв'язки між відмітками часу передачі пакетів даних. Зрештою алгоритм визначає підключені пристрої, кімнати та події вдома; з цього моменту хакер отримує несанкціонований доступ

до моніторингу розумного будинку. Чотири рівні цієї атаки виглядають наступним чином:

– Рівень 0 визначає розумні пристрої за їх унікальними радіо підписами. Відбиток передачі даних - це набір ознак форми RF-хвилі, які розрізняють джерело сигналів, навіть якщо відправники сигналів мають подібного виробника та модель. Атака визначає основні події, такі як зайнятість дому або сон, на цьому етапі.

– Рівень 1 кластеризує визначені вузли, досліджуючи інтервали часу між передачами сигналів. Припущення полягає в тому, що пристрої, які фізично розташовані близько один до одного, активуються приблизно в один і той же час. Таким чином, сформовані кластери представляють собою або місцезнаходження їхніх членів, наприклад, кімната, або їх призначення, наприклад, приготування їжі.

– Рівень 2 виконує кластеризацію з етикетуванням, використовуючи витягнуті ознаки з сформованих кластерів. Зверніть увагу, що цей процес надає пріоритет логічній категоризації, а не місцям розташування пристроїв. Наприклад, пральна машина буде відзначена як подія прання, хоча вона може знаходитися в кухні чи підвалі.

– Рівень 3 проводить ще один раунд класифікації, в якому алгоритм атаки використовує витягнуті вектори ознак кластерів вузлів та навчальні дані для позначення цих кластерів як пристроїв. Наприклад, навчена модель атаки очікує, що плита буде в кухні; тому вона перевіряє кластери, розташовані в кластері кухні з вектором ознак плити, витягнутим з фактичного набору даних. У разі відповідності невідомий кластер пристрою визначається як плита.

Процедура атаки FATS поєднує кілька статистичних і технік машинного навчання для виявлення ідентичностей кімнат, пристроїв та подій. Спочатку вона кластеризує записи на основі відбитків радіо. Потім, використовуючи пов'язані мітки часу, вона створює тимчасову матрицю, що представляє близькість у часі між передачами. Далі вона перетворює тимчасову матрицю в метричну матрицю відстаней, використовуючи алгоритм найкоротшого шляху Дейкстри [42]. Застосовується класичне багатовимірне масштабування без параметрів (CMDS),

щоб створити матрицю позицій на основі матриці відстаней [43]. Нарешті, алгоритм [44] кластеризації K-mean групує кластери пристроїв, які часово корелюють. На рисунку 2.3 показана операційна діаграма атак FATS.

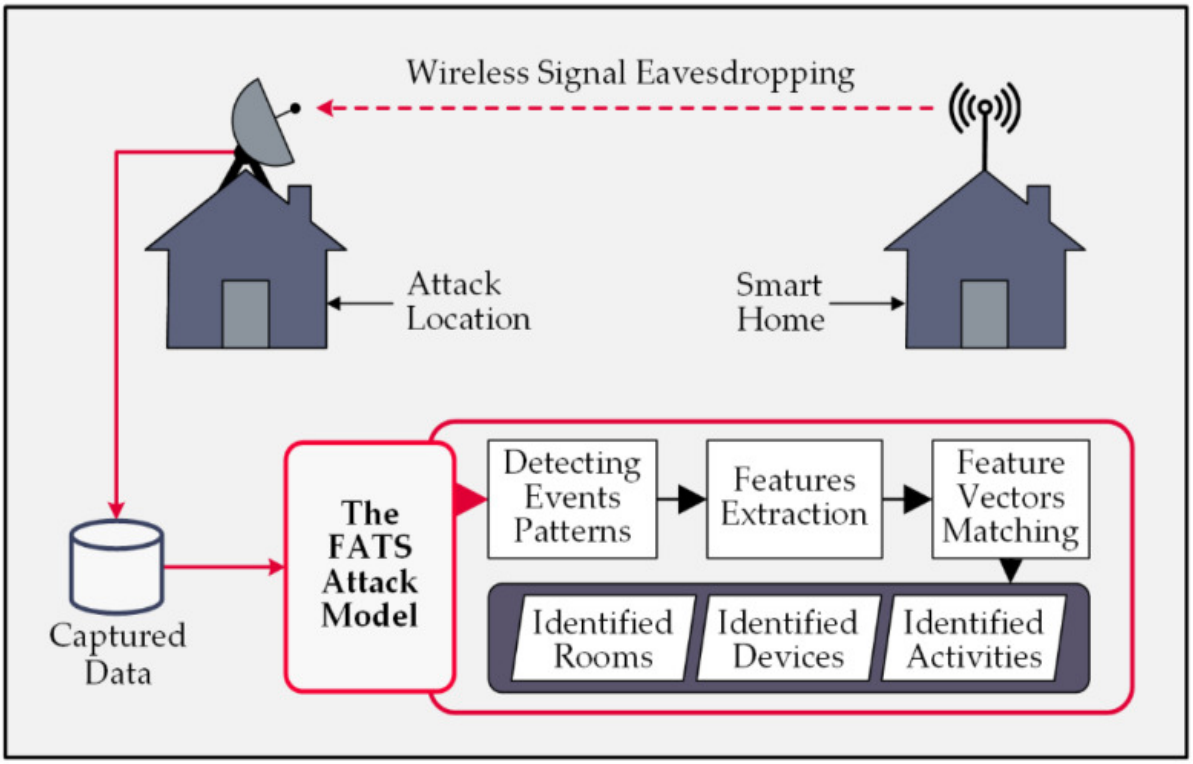


Рисунок 2.3 – Операційна діаграма атак FATS

Атака перетворює введення в геопросторову інформацію пристроїв. Потім вона намагається ідентифікувати пристрої, кімнати та події, порівнюючи вектори ознак, які були створені для невідомих кластерів, із відомими векторами для своєї моделі за допомогою деяких класифікаторів. В результаті вона успішно порушує приватність мешканців, не розгадуючи секретний ключ шифрування. На рисунку 2.4 подано докладніші відомості про внутрішні процеси атак FATS.

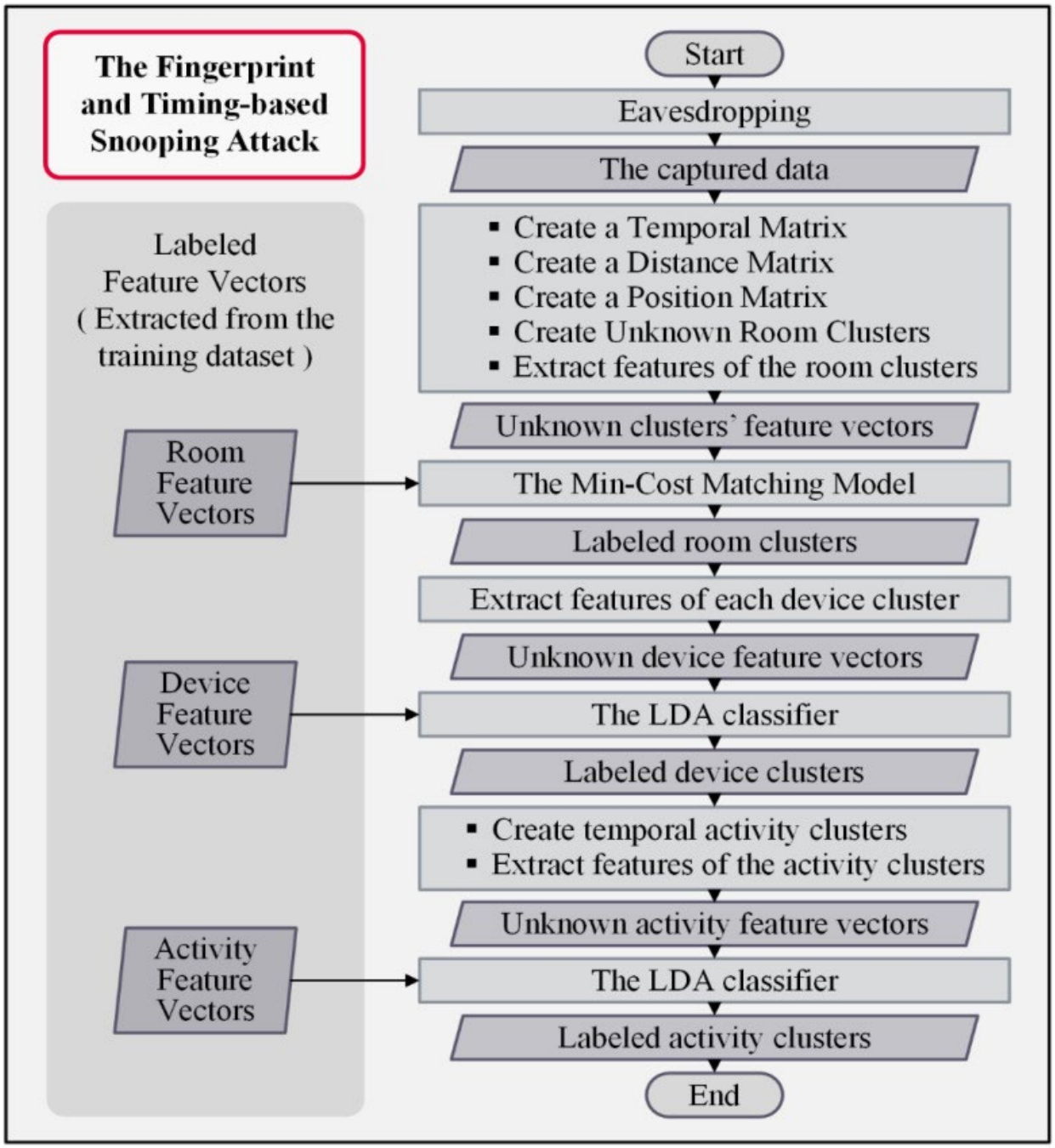


Рисунок 2.4 – Приклад внутрішніх процесів атак FATS

Атака позначає кластери кімнат на наступному рівні, обчислюючи максимальне мінімальне вартісне двостороннє відображення [45]; критичні функції для процесу відповідності - це кількість передач на день з кімнати, загальна кількість передач протягом дня та вночі, медіанний інтервал між передачами в межах кімнати та медіанна довжина кластерів часової активності. У наступному процесі атака ідентифікує пристрої, витягуючи ознаки пристроїв,

а потім порівнює їх із відомими векторами ознак для навченої моделі; це завдання виконується з використанням класифікатора стандартного LDA [46] . Після цього створення кластерів часової активності в кожному кластері пристроїв призводить до створення кількох векторів ознак активності. Ці функції - це час початку, тривалість та кількість передач кожним пристроєм. Вдруге класифікатор LDA виконує завдання відповідності на невідомих векторах ознак активності, щоб пов'язати їх із позначеним вектором моделі атаки. В кінцевому підсумку атака розкриває ідентичність всіх кімнат, пристроїв та активностей зловмиснику; потім вони можуть відстежувати всі домашні активності та отримувати особисту інформацію мешканців.

## 2.5 Стратегії захисту приватності від атаки FATS

Дослідження запропонованих методів, розроблених для захисту розумних будинків від атак FATS, показують, що дослідники випробували різні стратегії оборони, і в деяких випадках вони досягли значного покращення рівня конфіденційності. Хоча збереження конфіденційності - це основна мета кожного запропонованого рішення, наслідки використаних підходів для інших параметрів системи важливі.

Наприклад, рішення, які накладають затримку на комунікації системи, зменшують якість обслуговування; цей побічний ефект особливо неприпустимий для кількох систем дому, чутливих до затримок, таких як системи виявлення пожежі та падіння літніх людей. Крім того, вимоги до енергії методів повинні бути обґрунтованими. Підходящим рішенням повинен бути оптимальний баланс між трьома системними параметрами, а саме рівнем конфіденційності, затримкою у комунікаціях та споживанням енергії.

Ускладнення механізму розпізнавання зразків у атаках FATS - головна ідея оборонних стратегій для зменшення ризику витоку даних; для цього переважний підхід - це омана сигнального трафіку бездротової мережі розумного будинку. Оскільки основою алгоритму атаки є пошук тимчасових кореляцій між переданими сигналами, маніпулювання фактичними зразками підриває

продуктивність атаки.

Стратегії розробки захисного методу можна розділити на дві категорії. У першій категорії рішення відкладають відправку пакетів даних. Тривалість затримок випадково визначається; отже, атака матиме складність у визначенні реальних часових кореляцій між переданими сигналами. З іншого боку, методи другої категорії випадково вводять деякі фальшиві пакети у мережевий трафік, і характеристики цих імітаційних пакетів ідентичні фактичним; отже, атака не може їх розрізнити. В результаті точність атаки FATS зменшується, оскільки для зловмисника буде складно правильно розуміти фактичні події, які відбуваються в будинку.

Ці стратегії є важливим кроком у забезпеченні безпеки розумних будинків, проте дослідники продовжують вдосконалювати методи та шукати оптимальні рішення, які б дозволили ефективно боротися із загрозами атак FATS, не пожертвуючи іншими параметрами функціональності та продуктивності систем.

## 2.6 Техніка введення пакетів зі затримкою

Тимчасова маніпуляція сигнальним трафіком є ключовою стратегією в захисті від атак FATS, оскільки вона включає в себе зміну реальних часових кореляцій сигналів, що передаються пристроями, спільно повідомляючими про події. Цей підхід використовує алгоритм генератора випадкових інтервалів для затримки передачі пакетів на випадковий час. Головна ідея полягає в тому, що пристрої, які співпрацюють при повідомленні про подію, відправляють свої повідомлення приблизно в один і той же час. Змінюючи цей час, стратегія ускладнює завдання атакуючого, що намагається виявити реальні патерни активності, і зменшує точність атаки.

Однак важливо враховувати, що недолік цієї стратегії полягає в ексцесивній затримці, яку вона може накласти на комунікацію системи. Деякі підсистеми розумного будинку, зокрема системи моніторингу охорони здоров'я, можуть бути чутливими до затримок, оскільки затримані комунікації можуть суттєво впливати на їхню часову реакцію, що є критичним для їхньої

ефективності.

На рисунку 2.5 наведено конкретний приклад використання відстроченої стратегії повідомлення, де патерни активності 1 та 2 розкидані в часі з метою ускладнення завдання атакуючому фіксувати їх як активність за механізмом виявлення патернів подій атаки. Важливо відзначити, що пакети даних зашифровані та містять інформацію, яка дозволяє центральному контролеру розібратися в тому, як вони дійсно взаємодіють між собою. Ця стратегія, хоча і ефективна у запобіганні атакам FATS, може мати свої обмеження, особливо в ситуаціях, де чутливість до затримок є критичною для деяких систем розумного будинку.

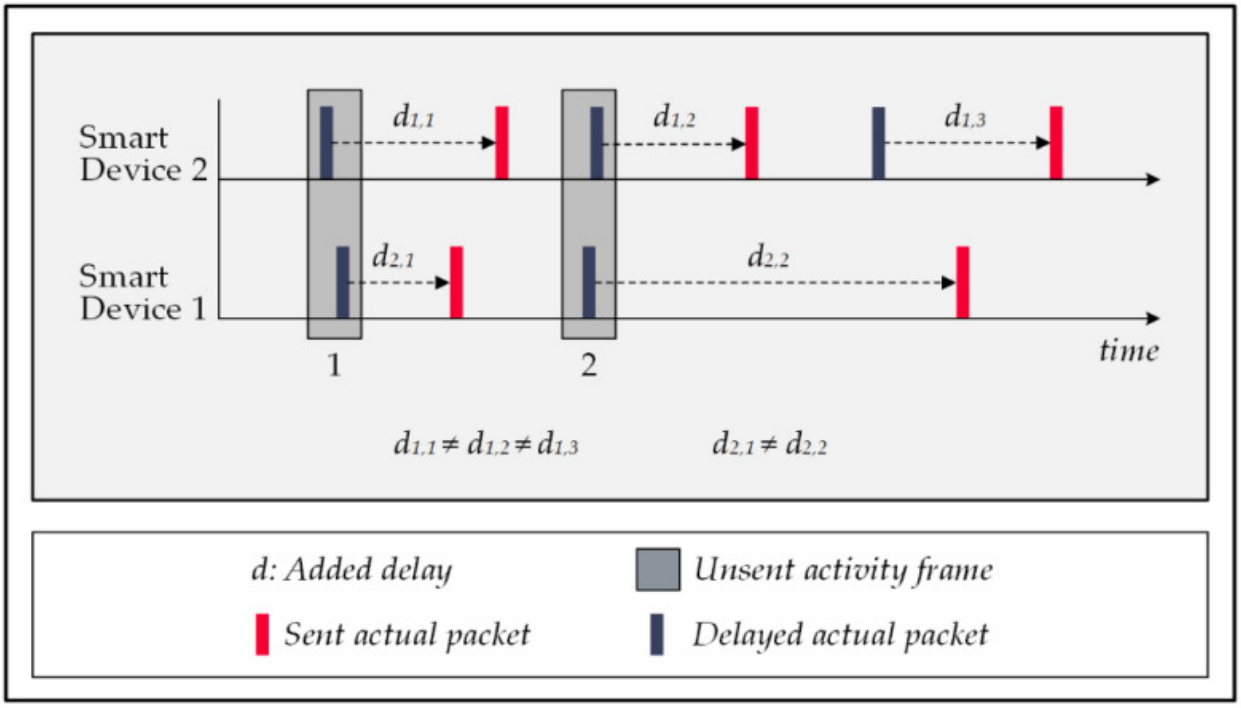


Рисунок 2.5 – Сигнальний трафік

## 2.7 Метод ін'єкції фальшивих пакетів

Введення серії фальшивих пакетів даних у безпровідний трафік будинку представляє собою альтернативний підхід для обману атаки FATS. За цією

стратегією система видає команди розумним пристроям для генерації випадкової кількості пакетів даних, ідентичних реальним, та їх передачі випадковими інтервалами. Підроблені повідомлення зашифровані, обмежуючи їх розрізнення від легітимних пакетів.

Цей метод призводить до того, що атака включає фальшиві пакети в свої процеси виявлення патернів, і ця помилка призводить до неправильних висновків алгоритму атаки. Неточність результатів може виникнути внаслідок невдачі атаки виявити патерни реальних подій, представляючи випадки неправдивих негативів. Також можливо виникнення ситуацій, коли атака виявляє події, які ніколи не відбувалися, утворюючи випадки неправдивих позитивів. Обидві ці помилки суттєво впливають на правильність атаки та здатність алгоритму атаки до адекватного реагування на реальні умови.

На рисунку 2.6 зображено схематичний вигляд мережевого трафіку, де атака сформувала шість рамок активності. Рамки 1 та 5 є правильними виявленнями, рамка 6 - хибним позитивом, що представляє невірно виявлену подію, а рамки 2 та 3 - невиявленими подіями атакою, показуючи складність коректного розпізнавання дійсних подій в умовах впровадження фальшивих даних [48].

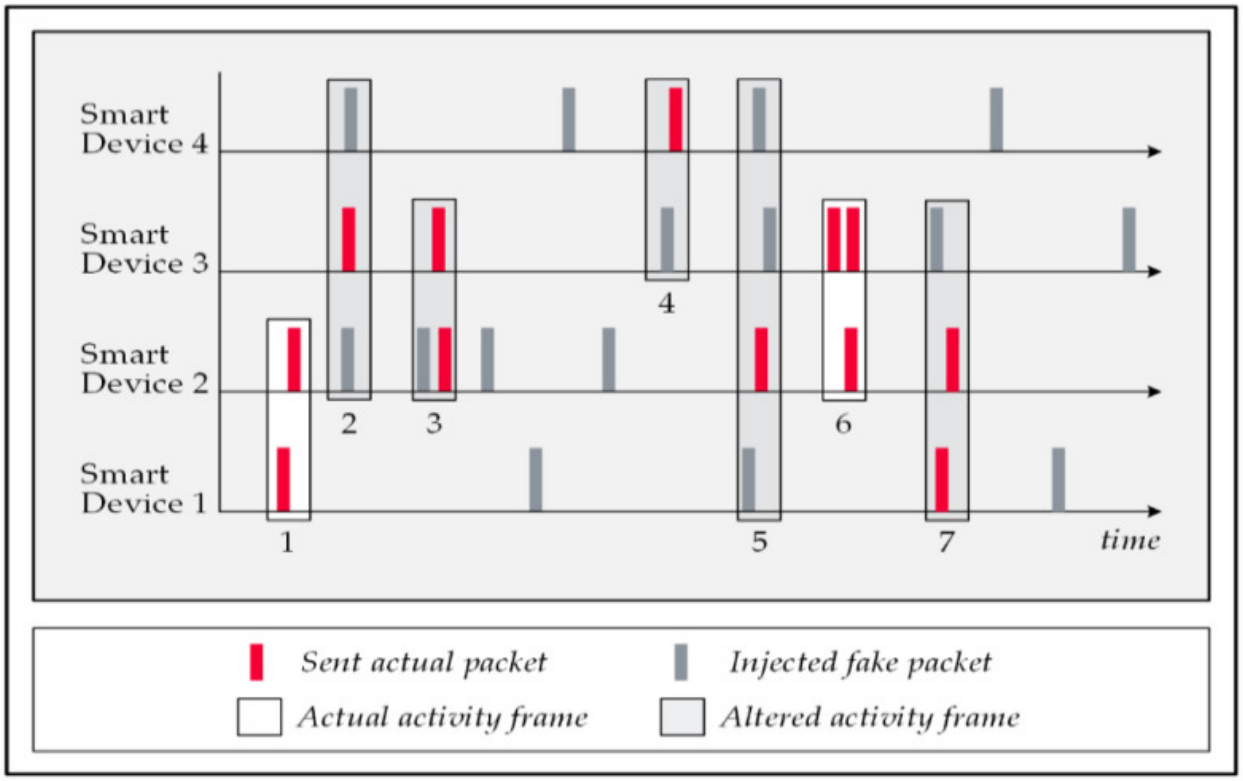


Рисунок 2.6 – Схематичний вигляд мережевого трафіку

## 2.8 Гібридні техніки

Як зображено на рисунку 2.7, комбінування попередніх стратегій захисту в один метод дозволяє об'єднати їхні захисні переваги. У даному прикладі трафіку рамка 1 представляє реальну подію, але атака не може її виявити через змінений час передачі пакетів даних. З іншого боку, атака визнає рамки 2, 3 та 4 як ймовірні реальні активності, в усіх них були внесені фальшиві пакети, які обдурювали атаку; отже, жодна з них не відповідала б жодній відомій активності за навчальним моделюванням [49, 50].

Цей підхід до захисту від атак FATS використовує комплексне поєднання вже розглянутих стратегій, максимізуючи важливі характеристики кожної з них. Комбінування інтринсичних та екструзичних методів призводить до вдосконаленого захисту, зменшуючи ефективність атак та забезпечуючи надійний рівень конфіденційності.

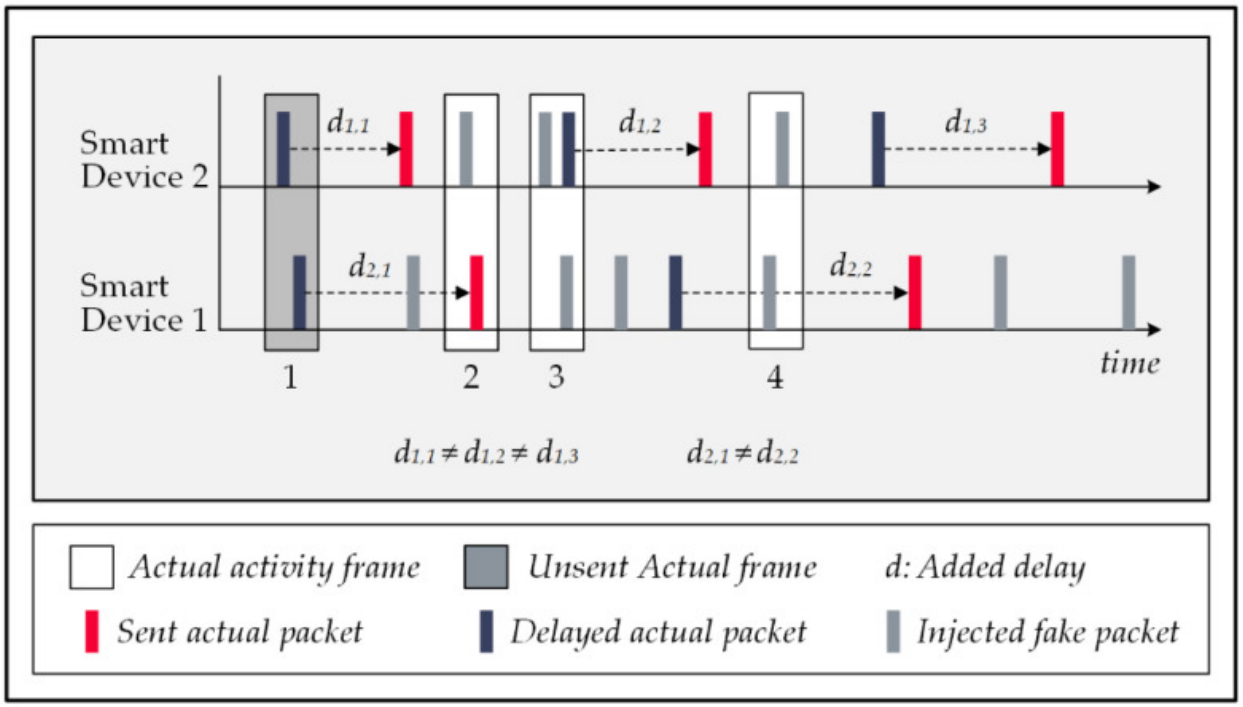


Рисунок 2.7 – Приклад впровадження фальшивих пакетів

## 2.9 ВИСНОВОК ДО РОЗДІЛУ II

У цьому розділі був проведений аналіз основних вразливостей та загроз у системі розумного будинку.

Були проаналізовані рівні загроз та методи підвищення захисту у системі розумного будинку.

Були розглянуті стратегії захисту від атаки FATS.

# 3 ПРАКТИЧНА ЧАСТИНА

## 3.1 Методи захисту сигналів в мережевому трафіку

В інформаційно-технічній епохі, де цифрові технології проникають у всі аспекти нашого життя, забезпечення конфіденційності та безпеки даних стає найбільш актуальним завданням. Особливу увагу привертає проблема захисту розумних будинків від атак, таких як FATS. Серед різноманітних методів і стратегій оборони велика увага приділяється підходу, відомому як "ConstRate".

Метод базується на тимчасовій координації передачі даних розумних пристроїв для унеможливлення атак FATS. Кожен пристрій визначає фіксовані інтервали передачі даних, роблячи процес передачі менш передбачуваним для потенційних зловмисників. Мета цього дослідження - ретельно оцінити ефективність та вивчити його вплив на реакцію системи та енергоефективність.

Важливо відзначити деякі переваги цього методу. Рівномірний розподіл сигналів у мережевому трафіку ускладнює атаки, спрямовані на часові кореляції, тим самим забезпечуючи певний рівень захисту. Проте, слід враховувати обмеження, такі як випадковий вибір інтервалів очікування, що може впливати на час реакції системи та енергоспоживання.

У цьому дослідженні метою є знаходження оптимального балансу між забезпеченням конфіденційності та врахуванням обмежень часу та енергії. Розглядаючи принципи схеми "ConstRate", шукаємо ефективні стратегії для розумних будинків, забезпечуючи їхню високу функціональність та надійний захист від атак.

Аналіз результатів мого дослідження свідчить про рівномірний розподіл сигналів як перевагу методу. Це важливий аспект, що ускладнює задачу зловмисників у виявленні часових кореляцій. Однак треба ураховувати імовірні недоліки, такі як випадковий вибір інтервалів, які можуть вплинути на час реакції та споживання енергії.

Завдяки розгляду схеми та її застосуванню в розумних будинках, моя робота спрямована на розвиток наукового підґрунтя для створення ефективних

та захищених від сучасних загроз рішень в галузі розумних технологій.

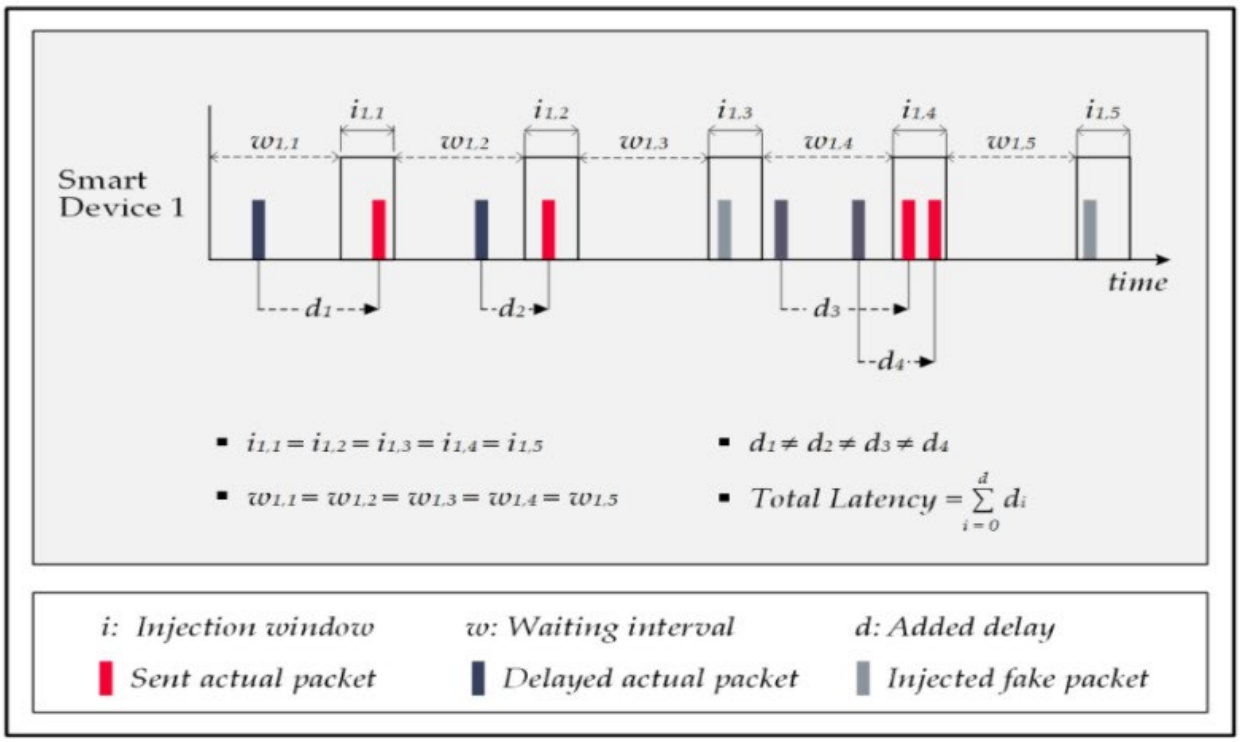


Рисунок 3.1 – Схема ConstRate

В останні роки конфіденційність та безпека даних у WSN та IoT стали предметом широкого вивчення. Моя зацікавленість у цій темі поглибилася, особливо оглядаючи аспекти анонімності джерел, перехоплення даних та атаки впровадження хибних даних у розумних будинках.

Згідно моїх висновків, схема "ConstRate" має переваги у рівномірному розподілі сигналів у мережевому трафіку, ускладнюючи виявлення часових кореляцій для атак. Проте, важливо враховувати його недоліки, такі як випадковий вибір інтервалів очікування, що може впливати на час реакції системи та енергоспоживання.

Розглядаючи недоліки схеми, бачимо підхід, який був запропонований у схемі "ProbRate". Тут інтервали очікування формуються за допомогою експоненційного розподілу, де кожен випадковий інтервал має свій унікальний розподіл. Цей метод спирається на те, що інтервали стають коротшими з часом,

сприяючи скороченню затримок передачі пакетів та зменшенню загальної затримки в системі.

Вважаю, що ця схема може забезпечити високий рівень конфіденційності для розумних будинків, навіть у випадках атак FATS. Її основна перевага полягає в тому, що непередбачуваність інтервалів, визначених експоненційним розподілом, ускладнює завдання атакуючих та сприяє ефективному зменшенню можливостей атак визначити необхідні часові взаємозв'язки.

Також, необхідно зазначити, що метод відкриває можливості для майже ідеального рівня конфіденційності в розумних будинках. Ілюстрація на рисунку 3.2 ілюструє, як ця схема впливає на мережевий трафік, приховуючи фактичні шаблони та забезпечуючи високий рівень безпеки.

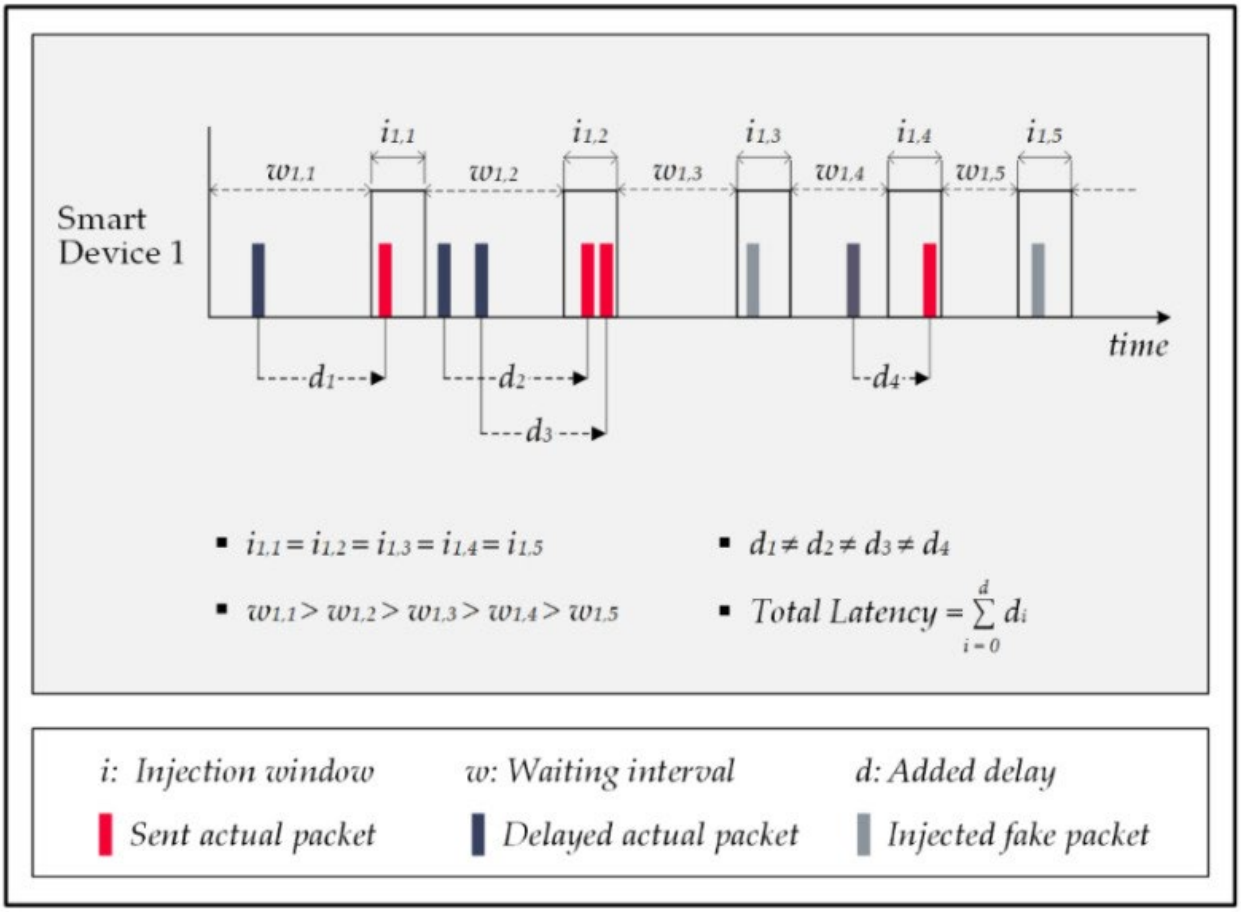


Рисунок 3.2 – Схема ProbRate

Хоча схема "ProbRate" зменшує затримки, вона не усуває загальної затримки системи. Факт залишається в тому, що це питання є проблематичним для систем, чутливих до затримок, у розумних будинках. Крім того, зменшуючи час очікування для введення пакетів, збільшується кількість вікон для введення, що підвищує ймовірність введення фальшивих повідомлень; отже, споживання енергії системи зростає.

Схема "FitProbRate" (FPR) - це інший підхід до збереження конфіденційності в розумному будинку у випадку атак FATS [40]. Ця схема є вдосконаленою версією схеми "ProbRate"; таким чином, система визначає інтервали очікування на основі експоненційного розподілу, аналогічно попередньому методу. Крім того, схема FPR використовує тест Андерсона-Дарлінга [61], щоб забезпечити, що кожен обраний інтервал належить множині значень експоненційного розподілу. Крім того, цей підхід контролює відхилення між виміряними середніми значеннями вибірки та фактичним середнім значенням визначеного розподілу, щоб уникнути значущої різниці між ними. Крім того, схема надає пріоритет пересиланню фактичних пакетів якнайшвидше; отже, система відправляє пакет даних після найкоротшого часу очікування, який вписується у заданий розподіл, і перепланує введення підготовленого фальшивого пакета на наступне вікно введення. В результаті використаної стратегії інтервали очікування поступово скорочуються, а вікна введення наближаються одне до одного, зменшуючи загальну затримку.

Під час аналізу отриманих результатів відзначемо, що системна затримка у схемі "FitProbRate" становить лише одну десяту частину системної затримки у схемі "ProbRate". Це свідчить про помітне поліпшення в аспекті підтримки якості обслуговування в розумному будинку. Однак важливо також відзначити, що запропонований метод не вирішує питання енергетичного навантаження.

У даній схемі розумні пристрої повинні вводити щонайменше один фіктивний пакет в кожне вікно, що порожнє від фактичних повідомлень, з метою розгойдання алгоритму розпізнавання шаблонів атаки. Як невдачливий наслідок, протягом тривалого періоду тиші, наприклад, вночі, система витрачає значну кількість енергії на введення зайвих фальшивих пакетів, оскільки відсутні

фактичні шаблони для приховування. Крім того, аналогічно попереднім схемам, кількість введених фальшивих пакетів залишається необмеженою випадковою величиною, що негативно впливає на енергоефективність схеми. На рисунку 3.3 показано зразок маніпулювання шаблонами трафіку за допомогою схеми "FitProbRate". У цьому прикладі фактичний пакет зсунувся з третього інтервалу очікування на третє вікно введення, і система перепланувала введення підготовленого фальшивого пакета для цього вікна на четверте вікно введення.

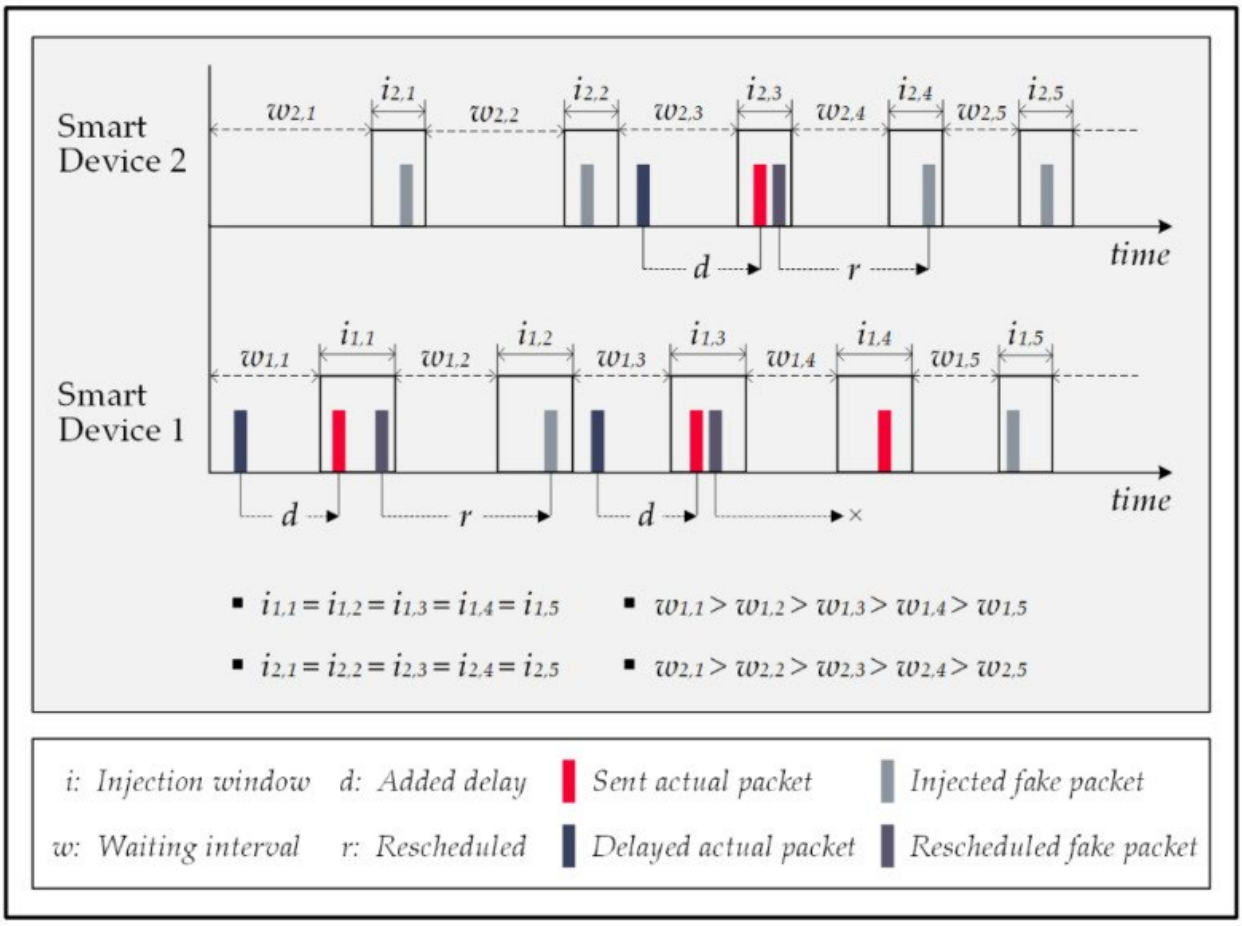


Рисунок 3.3 – Схема FitProbRate

Також розглянемо ще один метод [52], що відрізняється від попередніх схем, що головним чином базувались на використанні статистичних розподілів. У цьому підході механізм захисту аналізує поведінкову семантику подій вдома та навчається приймати рішення на основі історичних записів вдома. Основна

мета полягає в передбаченні ймовірності виникнення реальних подій. Таким чином, система може навмисно впроваджувати фальшиві пакети для втручання в реальний потік сигналів, змінюючи патерни активності та понижуючи точність виявлення подій атакою FATS.

Незважаючи на те, що цей метод зменшує енергоспоживання системи, він не вирішує проблему додаткової затримки, оскільки передача пакетів даних повинна відбуватися в заздалегідь визначених вікнах введення. Крім того, успішність методу сильно залежить від точності його передбачень. Неправильне передбачення призводить до марно витраченої енергії на передачу фіктивних повідомлень.

На рисунку 3.4 показано модель руху, захищену методом поведінкової семантики подій для збереження конфіденційності інформації вдома. Однак атака FATS виявила три рамки активності. Вона не може ідентифікувати жодні події, оскільки виявлені рамки не відповідають жодному з відомих патернів активності атаки. У першому та третьому вікнах введення метод захисту вірно передбачив виникнення подій; таким чином, втручання фальшивих пакетів, введених іншими пристроями, зробили модель руху нерозпізнаваною для атаки. Прогноз подій для другого вікна введення був невірним; в результаті введені фальшиві пакети не сприяли приховуванню домашніх подій, і енергія була витрачена марно.

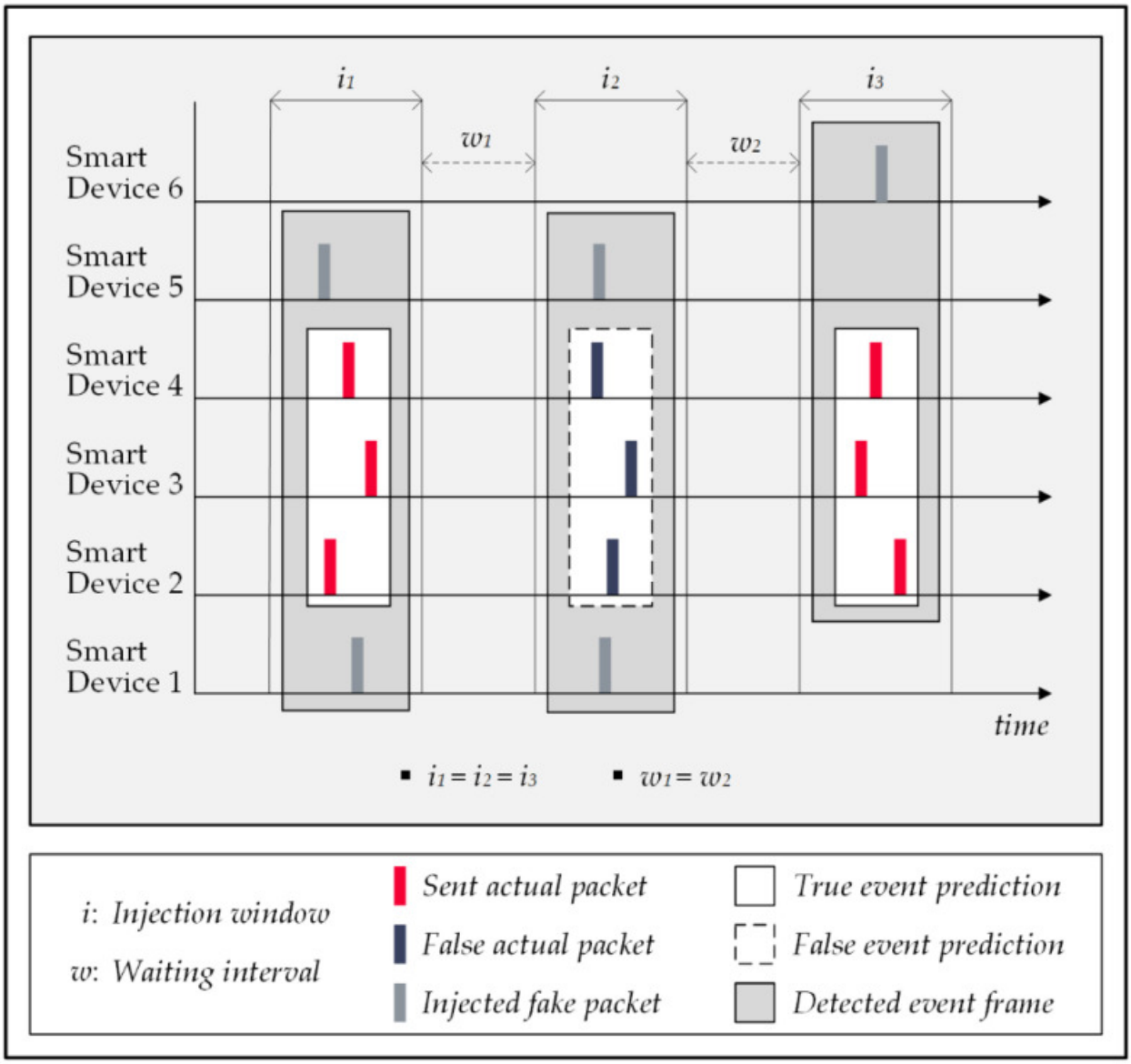


Рисунок 3.4 – Модель руху захисту конфіденційної інформації

Проблема затримки в методі захисту конфіденційності значно зменшується за допомогою адаптивного методу реального часу [53], відомого як метод аналізу вибіркових даних та навчання з учителем (SDASL). Цей підхід використовує техніки навчання з учителем для подолання ризику атак FATS в розумному будинку. Метод має низьку затримку, високу адаптивність і забезпечує задовільний рівень конфіденційності.

В цій схемі центральний контролер періодично обчислює параметри прийняття рішень для кожного розумного пристрою. Застосовується алгоритм логістичної регресії для визначення, чи потрібно пристрою висилати фальшивий

пакет даних. Метод складається з двох фаз: аналізу вибіркових даних та навчання з учителем. На першому етапі визначається FDR, що вказує на схожість частотних ставок у вибірковому наборі даних та фальшивих повідомленнях. Далі FDR використовується для оновлення розумних пристроїв.

На другому етапі застосовується модель навчання з учителем для збору, маркування та оновлення параметрів моделі навчання. Кожен пристрій отримує копію кінцевої моделі прогнозування. Функція логістичної регресії приймає рішення за вхідними даними у реальному часі, визначаючи необхідність введення фальшивого пакету. Схема передбачає часту комунікацію між центральним контролером та розумними пристроями.

Метод SDASL зменшує точність атаки FATS на 30% після 13 днів тренування, що вказує на 70% рівень конфіденційності для будинку. Втрата конфіденційності є меншою порівняно із статистичними методами, але вирішує проблему затримок при введенні. З енергетичної точки зору, за результатами, для кожного фактичного пакета даних вводиться 13 фальшивих пакетів, що означає, що енергозатрати методу SDASL більше, ніж у незахищеного будинку.

В контексті новаторського концепту для протидії атакам FATS, введеної в метод SDASL, запропоновано стратегію колективного введення фіктивних пакетів. Ця ідея полягає в масовому введенні фальшивих пакетів для імітації реальної домашньої активності. Навіть якщо ці випадкові введення не втручаються в реальний шаблон, вони можуть обдурити атаку та запобігти витратам енергії. На рисунку 3.5 показано огляд впливу цього методу на мережевий трафік та ефективність атаки.

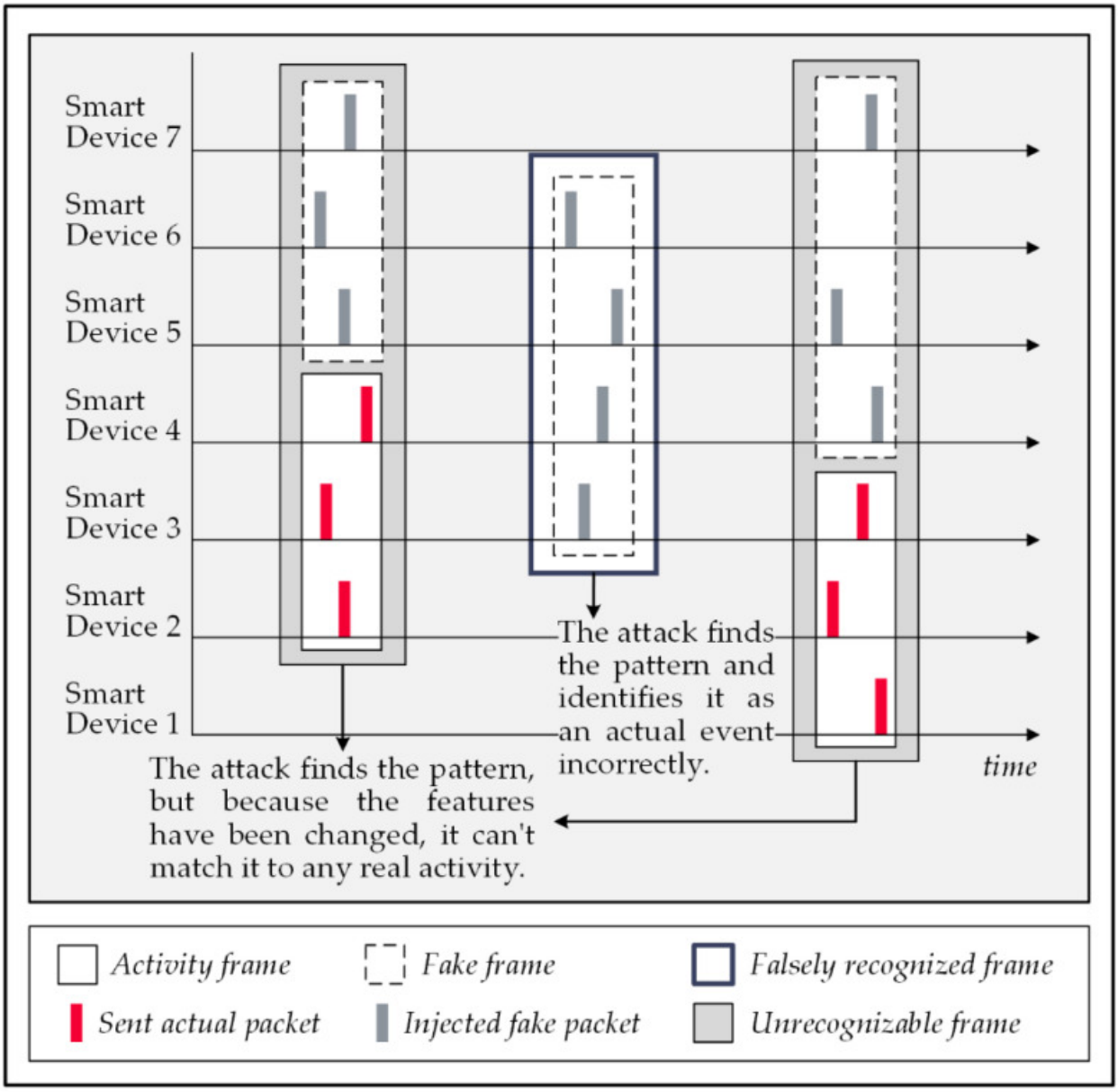


Рисунок 3.5 – Мережевий трафік під час атаки

Подання атакою фальшивих подій збільшує TPR; таким чином, ефективно знижується точність атаки. Цей підхід відомий як метод AAM і надає найоптимальніший баланс для трійці захисту конфіденційності, затримок у комунікаціях та споживання енергії.

У цьому рішенні політика негайного пересилання фактичного пакета даних усуває проблему затримки. Більше того, це поліпшує рівень конфіденційності, обманюючи атаку FATS інформувати про нереальні події, що зменшує TPR моделі атаки. Крім того, незважаючи на випадковість введення, цей метод

збільшує шанс перекриття фальшивих та фактичних паттернів активності, використовуючи ймовірнісно-заснований механізм, який спрямовує введення на періоди дня з вищою ймовірністю фактичних подій. Ця стратегія підвищує рівень конфіденційності, ефективніше використовує ресурси енергії та відповідає вимозі нульової затримки для питань якості обслуговування. Метод імітації реальної активності здійснюється шляхом створення фальшивих подій, які імітують активність користувача чи реальні події в системі розумного будинку. Такий підхід дозволяє збільшити кількість фальшивих паттернів активності, приховуючи фактичні зміни в системі.

Однією з ключових переваг методу AAM є його здатність ефективно знижувати TPR, що є критичним параметром для оцінки точності атаки. Принцип дії полягає в тому, що штучно створені фальшиві події надають атакуючій системі невірні дані, спрямовуючи її на неправильні висновки. Це робить атаку менш ефективною та забезпечує більш високий рівень конфіденційності для розумного будинку.

Додатковою перевагою методу AAM є його спроможність працювати з мінімальними затримками. Відправлення фактичних подій негайно без будь-яких штучних затримок сприяє забезпеченню нульової затримки в комунікаціях системи. Це особливо важливо для виключно чутливих до затримок систем, таких як системи безпеки чи системи моніторингу стану здоров'я.

Ще однією ключовою особливістю методу AAM є його спроможність ефективно використовувати ресурси енергії. Введення фальшивих подій на підставі ймовірнісно-заснованого механізму, що спрямовує їх на періоди дня з вищою ймовірністю фактичних подій, дозволяє оптимізувати використання енергії системи. Ця стратегія допомагає уникнути надмірного використання енергії на створення фальшивих подій та забезпечує ефективне функціонування системи.

У підсумку, метод AAM представляє собою обгрунтований та оптимальний підхід для забезпечення безпеки та конфіденційності в системах розумного будинку. Він успішно поєднує в собі зниження затримок у комунікаціях, ефективне використання енергії та зменшення TPR, що робить

його ефективним та економічно вигідним рішенням для широкого спектру застосувань в цьому сегменті технологій.

## 3.2 Показники EDR та TPR

Збереження конфіденційності розумних будинків - це критична вимога, яку слід задовольняти для уникнення непередбачених наслідків можливих витоків даних. Атаки FATS ефективно дозволяють зловмисникам дізнатися про приватні аспекти життя мешканців розумного будинку, пов'язані з їхньою домашньою активністю. Основні характеристики цієї атаки можна узагальнити наступним чином:

Ця атака виконується пасивно; отже, вона не виявляється під час періоду атаки. Атака витягує інформацію з контекстуальних даних комунікацій будинку; таким чином, методи шифрування не можуть їй протистояти. Даний зловмисний алгоритм потребує мінімум вхідних даних, включаючи відбитки сигналів та мітки часу передачі; отже, ускладнено блокування йому доступу до цих даних.

Враховуючи всі вищезазначені обставини і враховуючи те, що атаку неможливо зупинити, очевидно, що зменшення ризику цієї загрози вимагає впровадження проактивного рішення забезпечення захисту, щоб гарантувати, що патерни трафіку витоку даних будуть змінені таким чином, що зловмисний алгоритм не зможе їх точно інтерпретувати.

Моє дослідження існуючих методів захисту показує, що основна тактика в цих підходах полягає в максимізації затемнення мережевого трафіку для виклику ускладнень у здатності атаки визначати патерни. Я вважаю за розумне припустити, що низька ефективність атаки у виявленні патернів активності викликає проблеми на наступних етапах. Ця мета досягається за допомогою технік, таких як тимчасова маніпуляція переданими сигналами або введення випадкових фальшивих пакетів даних, обидві ефективно змінюють патерни трафіку. Тим не менш, цей досягнений результат супроводжується витратами для системи, які виражаються як затримки в комунікаціях або енергетичні накладні витрати.

Варто відзначити, що приватність дому має обернений зв'язок з точністю атаки; отже, будь-яке зниження точності атаки означає відповідний приріст приватності. Два основні показники для обчислення точності атаки – це EDR та TPR [44]. EDR вказує на частку правильно виявлених домашніх подій серед всіх фактичних активностей. Наприклад, виявлення 75 фактичних подій в домі, в якому відбулося 100 активностей, дає EDR 75%. Крім того, TPR вказує на відсоток правильності звіту. Наприклад, в результаті списку, що містить 100 позначених подій, якщо 60 пунктів є помилковими, TPR буде 40%. Зрештою, точність атаки - це добуток EDR і TPR. Таким чином, точність атаки за вищезазначеними прикладами становить 33,75%.

Моє дослідження наголошує на зниженні EDR атаки як своєї основної мети. Я вважаю, що логіка за цим вибором виглядає просто, але ефективно; якщо атака не виявляє події, вона не може їх ідентифікувати. Результати кількох рецензованих схем захисту підтримують цей аргумент, такі як схеми "ConstRate", "ProbeRate" та "FitProbRate", які забезпечують майже ідеальну конфіденційність для домашніх систем. Однак я вважаю, що ігнорування недоліків цих рішень може бути вартим. Ці підходи змінюють часові кореляції переданих сигналів, затримуючи їх пересилання, що означає неприйнятні затримки в реальному часі для послуг дому. Ця проблема впливає на час реакції систем, чутливих до затримок, і шкодить їх ефективності. Прикладами можуть бути випадки, такі як падіння літньої людини, виявлення пожежі, яке вимагає негайного повідомлення, або, в більш простому випадку, пізнє виконання розумних замків, що може створити незручності для користувачів.

Крім того, приховання фактичних активностей і шаблонів трафіку вимагає введення численних фальшивих пакетів; кількість цих введень не є детермінованою для відповіді на вимогу випадковості в процедурах захисту. Результати показали, що для забезпечення відповідної конфіденційності кількість фальшивих пакетів в рази перевищує кількість фактичних пакетів. У цьому відношенні позначення FVR вказує на співвідношення фальшивих пакетів до фактичних. Оскільки передача обох типів пакетів споживає енергетичні ресурси однаково, енергетичні накладання системи можуть бути значущими, що

підриває доступність рішень. У відміну від інших методів, метод імітації фактичної діяльності спрямовується на TPR для зменшення точності атаки. На відміну від інших, які намагаються приховати шаблони трафіку фактичних подій, цей метод спонукає атаку виявляти активності якнайбільше. Таким чином, це надає можливість внести більше фальшивих шаблонів активності в кінцевий результат атаки, що зменшує TPR. Введення меншої кількості фальшивих пакетів знижує витрати енергії системи та усуває затримки в бездротовому зв'язку, що є перевагами цього методу порівняно з іншими рішеннями. Загалом, критичним показником для оцінки методу захисту конфіденційності є обставини компромісу між наданим рівнем конфіденційності, викликаною затримкою та споживаною енергією рішення. Метод буде ідеальним, якщо він максимізує рівень конфіденційності, утримуючи два інші фактори на як найнижчому рівні. На рисунку 3.6 зображено взаємозв'язок між параметрами конфіденційності, затримки та енергоспоживання, зазначеними вище.

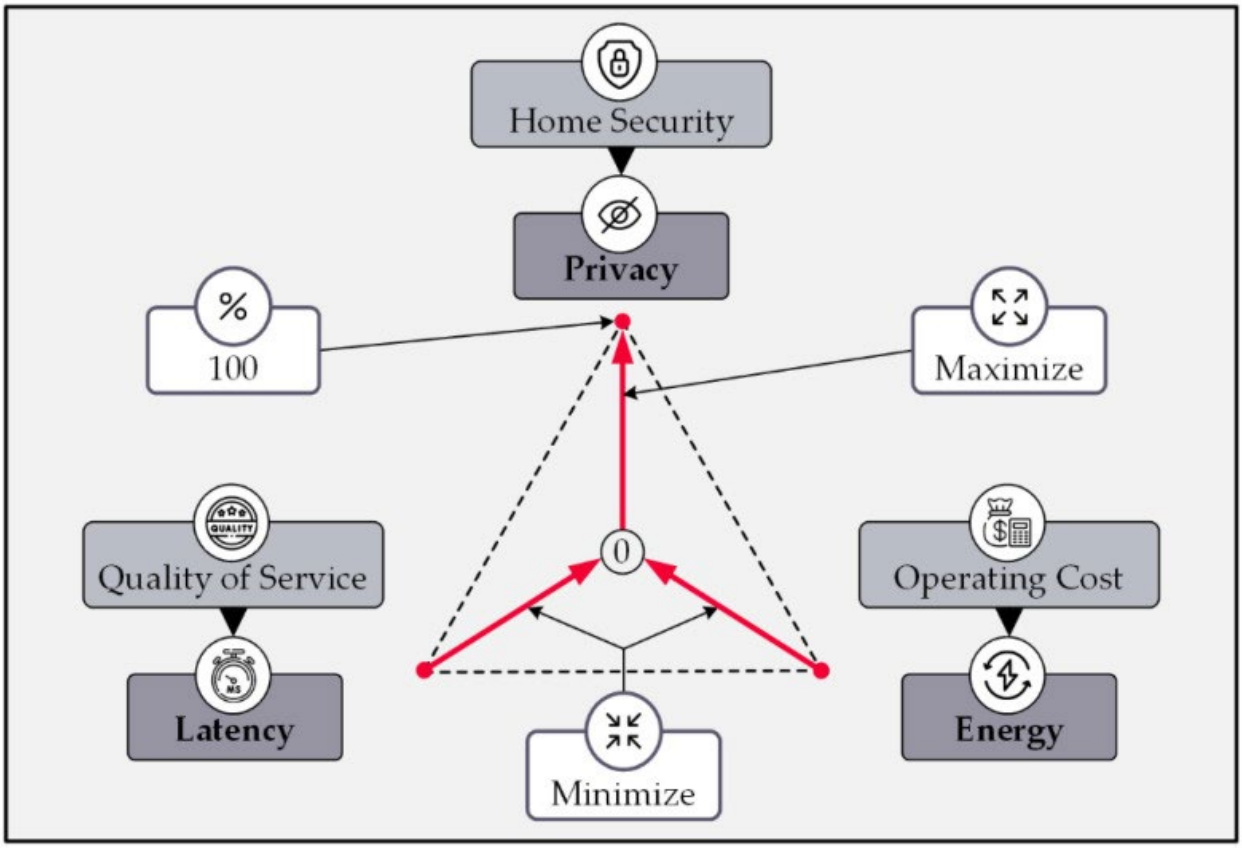


Рисунок 3.6 – Схема взаємозв’язку між параметрами конфіденційності, затримки та енергоспоживання

Перше обґрунтування необхідності урахування цього компромісу полягає в наявності чутливих до затримок системних підсистем розумного будинку, які повинні відповідати високим вимогам до якості обслуговування. Ця чутливість може виявитися критичною для ефективності різних служб, таких як системи моніторингу охорони здоров'я чи аварійного повідомлення. Друге обґрунтування випливає з непередбачуваного збільшення операційних витрат, спричиненого масштабним енергетичним навантаженням, що виникає внаслідок додаткових затримок у передачі даних.

Таблиця 3.1 узагальнює різні методи захисту конфіденційності з точки зору їхніх захисних підходів і порівнює їх продуктивність за триадою параметрів: рівень конфіденційності, затримка комунікації системи та споживання енергії. Доцільно відзначити, що кожен метод має свої переваги та обмеження. Наприклад, схема ConstRate, яка забезпечує рівномірний розподіл сигналів у мережевому трафіку, ускладнює виявлення часових кореляцій для атак, але може призвести до ексцесивної затримки. З іншого боку, схема ProbRate, базована на експоненційному розподілі інтервалів очікування, може зменшити затримки, але вимагає додаткових ресурсів та уваги до регулювання параметрів розподілу.

Ураховуючи потреби систем розумного будинку, де важливо забезпечити швидку реакцію на події та зберігати конфіденційність даних, обрання оптимального методу захисту є завданням, яке вимагає балансу між цими факторами. Результати та аналіз методів, які надає таблиця, допомагають визначити та підкреслити переваги та обмеження кожного підходу для подальшого вдосконалення та оптимізації систем безпеки розумних будинків.

Таблиця 3.1 – Методи захисту конфіденційності

| **Методи захисту** | **Концепція вирішення** | **Метрики ефективності** | | |
|---|---|---|---|---|
| | | **Конфіденційність** | **Затримка** | **Енергоспоживання** |
| ConstRate | Випадкове введення фальшивих пакетів зі сталими інтервалами | Висока | Дуже висока | Дуже високе |
| ProbRate | Випадкове введення фальшивих пакетів із експоненційним скороченням інтервалів | Висока | Висока | Дуже високе |
| FitProbRate | Випадкове введення фальшивих пакетів із експоненційним скороченням інтервалів | Висока | Висока | Дуже високе |
| Поведінковий семантичний аналіз | Випадкове введення фальшивих пакетів із використанням найближчих експоненційних інтервалів для фактичного передавання | Середня | Середня | Високе |
| SDASL | Адаптивне введення фальшивих пакетів | Середня | Середня | Високе |
| Міміка фактичної активності | Випадкове введення фальшивих активностей | Висока | Низька | Середнє |

## 3.3 ВИСНОВОК ДО РОЗДІЛУ III

У цьому розділі були розглянуті методи захисту від атаки FATS. А саме проаналізовані такі схеми як ConstRate, ProbeRate та FitProbRate, які забезпечують майже ідеальну конфіденційність для домашніх систем, і допомагають визначити та підкреслити переваги та обмеження кожного підходу для подальшого вдосконалення та оптимізації систем безпеки розумних будинків.

# 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

## 4.1 Основи охорони праці

Метою кваліфікаційної роботи магістра є дослідження методів захисту інформації системи “Розумний Дім”. Оскільки, проведення моніторингу та використання системи передбачає використання комп’ютерної техніки, зокрема ПК, то обов’язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників, в тому числі і фахівців з підвищення ефективності контролю доступу в приміщення, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [51]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». Згідно вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог:

Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення,

обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним. Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні

з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

Важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у ДБН В.2.5-28:2018. Організація робочого місця фахівця із моніторингу безпеки повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».

## 4.2 Безпека в надзвичайних ситуаціях

### 4.2.1 Міжнародний тероризм

Терор (лат. terror – страх, жах) – має ознаку «усувати», «закривати». Ця обставина і визначає терор як особливу форму політичного насильства, що характеризується жорстокістю, цілеспрямованістю й уявленою ефективністю. Ці особливості визначили широке використання терору упродовж людської історії як засобу політичної боротьби в інтересах держави, організацій чи окремих угруповань. Безпосередньо сам факт привселюдної страти кримінальних чи політичних злодіїв, чи процес «аутодафе» в період середньовікової інквізиції, є класичною формою терору в інтересах держави чи католицької церкви.

Правовою основою боротьби з міжнародним тероризмом є «Декларація про заходи для ліквідації міжнародного тероризму», що затверджена на 49-й сесії Генеральної асамблеї ООН (резолюція 49/60 від 9 грудня 1994 р.)

Цей документ встановлює принципи відносин світової спільноти і програму заходів з метою ліквідації такого огидного суспільного явища, як міжнародний тероризм, а також встановлює подальше співробітництво між державами для ліквідації будь-яких форм і проявів терористичної діяльності. Характерним для розвитку світової спільноти є те, що наявність лідера

(провідної країни чи провідної сили) народжує відповідну реакцію – формування нижчого за рангом (рівнем) іншого лідера (іншої країни чи іншої провідної сили).

Міжнародний тероризм, створюючи свій плацдарм, може викликати кризи (системні) в світовій, моральній, політичній, економічній системі відносин і зруйнувати та усунути всі передумови розвитку світової спільноти. В Україні, за даними служби безпеки, за останні два роки скоєно понад 560 злочинів терористичного характеру, внаслідок цього 90 осіб (із них 15 представників владних структур) загинуло.

В Україні зростає активність міжнародних терористичних організацій, насамперед із країн Ближнього Сходу («Хезболах», «Абу Ніджаль», «Хамас», «Брати мусульмани»), які прагнуть використати територію України для транзиту своїх бойовиків до країн західної Європи, підготовки терористичних акцій.

Головними принципами попередження та боротьби з міжнародним тероризмом має стати постійне удосконалення відповідної законодавчої бази, співробітництво з правоохоронними організаціями, консолідація з іншими країнами й організація напрямів запобігань поширенню будь-яких терористичних організацій і угруповань.

Терористичний акт не має безпосередніх можливостей досягнення оголошеної кінцевої мети і звичайно складається з таких елементів: насильницька дія у різноманітних її формах, політичний мотив в основі здійснення самого терористичного акту; сам акт спрямовано проти осіб, організацій, націй, національностей і меншин, державних інститутів чи їх представників з метою їх залякування чи виконання окремих вимог. Терор щодо націй, етнічної, расової чи релігійної групи, що здійснюється для її повного чи часткового усунення, розглядається світовою спільнотою вже як

акт геноциду.

Варіанти комбінацій за спрямованістю суб'єкт—об'єкт здійснення терористичного акту багатоспрямовані, тому важко дати універсальне визначення «терору». Проте деякі критерії певної класифікації можна встановити:

індивідуальний, організований терор і терор як політика держави;

терор як метод внутрішньополітичної боротьби і терористичні акти міжнародного характеру.

### 4.2.2 Структура системи БЖД

Поняття «життєдіяльність» стосується тільки людини. Людина живе і працює в безпосередньому зв'язку з навколишнім середовищем.

Життєдіяльність (ЖД) – це складна фізіологічна система, яка має назву «система ЖД».

Системою називають сукупність взаємозв'язаних елементів, функціонування яких спрямоване на досягнення певної загальної мети.

Система ЖД складається із взаємопов'язаних елементів: життя, діяльності людини, навколишнього середовища, – і має підтримувати комфортне та безпечне існування людини, забезпечити сталий розвиток людства [52].

Розглянемо характеристики елементів системи ЖД.

Життя – це форма існування матерії, яка характеризується обміном речовин, здатністю до розмноження і розвитку, вмінням пристосовуватись до навколишнього середовища.

Людина – вища форма розвитку живої матерії, і її існування – дуже складний процес, що не тільки підтримує її фізіологічний стан, але й задовольняє духовні потреби. Крім того, на життя людини суттєво впливають умови проживання та праці, медичний догляд і багато інших факторів, що виникають завдяки діяльності самих людей.

Діяльність – це специфічна форма ставлення людей до навколишнього середовища та одне до одного, яка має задовольняти потреби та інтереси людини. Це соціальна категорія, нерозривно зв'язана із суспільством. Тільки завдяки діяльності людини створено всі блага, які має людство.

Однією із специфічних форм діяльності людини є праця – перша й основна умова існування людини (людства).

Праця – цілеспрямована діяльність людини, у процесі якої вона впливає на природу і використовує її з метою виробництва матеріальних та інших благ, необхідних для задоволення своїх потреб.

Потреби – це необхідність для людини того, що забезпечує її існування і самозабезпечення (фізіологічне, матеріальне, соціальне, духовне та ін.).

Навколишнє середовище (довкілля) або середовище існування – це все, що оточує людину впродовж її життя. Навколишнє середовище, у свою чергу, поділяють на такі види:

– природне середовище;

– штучне середовище. Природне середовище (біосфера) – це частина Землі і простору навколо неї, де зосереджено все живе. Біосфера включає:

– атмосферу (газоподібна частина);

– гідросферу (рідка водна частина);

– літосферу (тверда частина).

На ЖД людей найбільше впливає частина біосфери від поверхні Землі вглиб на 15–20 км і до висоти 20–22 км, де починається озоновий шар. Природне середовище є джерелом природних ресурсів для існування людини: повітря, води, деревини, корисних копалин, ґрунту та ін.

Штучне середовище – це складова довкілля, створена людством за тривалий час його існування. Штучне середовище умовно можна поділити на два види:

– виробниче середовище;

– побутове середовище.

Виробничим називають середовище, в якому людина реалізує свою трудову діяльність (підприємства, установи, навчальні заклади тощо).

Побутовим є середовище, де люди мешкають або проводять вільний час. Воно охоплює сукупність житлових будинків, комунально-побутових об’єктів, місця відпочинку та ін.

Організм людини може нормально функціонувати тільки тоді, коли умови (параметри) зовнішнього середовища відповідають оптимальним. Якщо умови середовища змінюються, стають несприятливими, то на протидію їм організм

людини включає спеціальні механізми, які зберігають постійність параметрів внутрішнього середовища (всередині організму) чи змінюють їх у межах допустимого.

Можливість функціонування організму в середовищі, параметри якого постійно змінюються, забезпечується завдяки механізму, який називають адаптацією. Адаптація (лат. adapto – пристосування) – динамічний процес пристосування організму до мінливих умов зовнішнього середовища, який спостерігається в будь-якому виді діяльності щоразу, коли виникають значні зміни в системі «людина – середовище».

Адаптація може бути фізіологічною, психологічною, соціальною. Отже, для функціонування системи ЖД середовище має обов'язково відповідати природним параметрам. Відхилення можливі в межах допустимого, коли організм людини здатний адаптуватися, захистити себе, підтримувати існування. Усе, що існує за цими межами, становить загрозу життю, тому виникає потреба захисту ЖД людей.

Отже, безпека – важлива складова системи ЖД. Розглядаючи систему ЖД як взаємодію людей з навколишнім середовищем, слід зауважити, що вона завжди підпорядкована певним принципам, правилам, умовам життя, природним умовам, традиціям тощо.

Система ЖД має такі характерні ознаки:

– її функціонування підпорядковане об'єктивним законам природи;

– це динамічна система, яка розвивається, удосконалюється, пристосовується до змін умов існування;

– тяжіє до сталого розвитку, вживаючи заходів захисту від упливу негативних факторів. Основні принципи забезпечення ЖД такі:

– своєчасність, достатність, якість забезпечення людей необхідними для життя засобами високої якості і заходами в потрібний час у належній кількості;

– безпека ЖД (захист ЖД від упливу негативних факторів, що виникають унаслідок як природних явищ, так і діяльності людей).

Рівень реалізації цих принципів значною мірою залежить від способів забезпечення ЖД. Виходячи із сказаного, можна визначити такі головні способи забезпечення ЖД:

1. Організація ефективної трудової діяльності людей в суспільстві з максимальним залученням усіх ресурсів (створення робочих місць, упровадження високопродуктивного виробництва і технологій, нормування праці тощо).

2. Організація та удосконалення освіти і підготовка кадрів, розвиток науки відповідно до вимог часу.

3. Розвиток сфери послуг (комунальних, транспортних, торговельних, побутових і т. ін.).

4. Розширення мережі культурних, спортивних, розважальних установ.

5. Проведення заходів щодо збереження здоров’я людей (диспансеризація, оздоровлення, кваліфіковане медичне обслуговування і лікування, санітарно-епідеміологічний стан).

6. Розроблення законодавчих і нормативно-правових актів із забезпечення прав, свобод і захисту людей і суспільства в цілому.

Залежно від того, якою мірою реалізуються принципи та способи забезпечення ЖД, визначається рівень життя людей окремих країн і загальний розвиток людства.

# ВИСНОВКИ

У кваліфікаційній роботі розглянуто основні стратегії боротьби з атаками FATS.

На підставі моїх досліджень було виявлено, що основні стратегії захисту, на яких ґрунтуються існуючі рішення, включають тимчасову маніпуляцію сигнальним трафіком, введення фальшивих патернів у трафік або комбінацію цих технік.

– розглянуто та описано одну з основних вразливостей розумних систем, а саме атаку FATS;

– продемонстровано роботу схеми ConstRate;

– продемонстровано роботу схеми ProbRate;

– продемонстровано роботу схеми FitProbRate;

– для порівняльного аналізу у роботі порівнюється ефективність цих трьох методів та принципи захисту від атаки FATS;

– проведено порівняльний аналіз цих трьох підходів до виявлення найбільш ефективного з них. Виявлено їх відносні переваги та недоліки.

Подальший розвиток цієї роботи полягає в удосконаленні даних методів.

# ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Jiang L., Liu D.-Y., Yang B. Smart home research. pp. 659–663. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/1382266 (дата звернення 08.11.2023).

2. Robles R.J., Kim T.-H. Applications, systems and methods in smart home technology. [Електронний ресурс] Режим доступа: https://scholar.google.com/scholar_lookup?journal=Int.+J.+Adv.+Sci.+Technol.&title=Applications,+systems+and+methods+in+smart+home+technology:+A+Review&author=R.J.+Robles&author=T.-H.+Kim&volume=15&publication_year=2010&pages=37-48& (дата звернення 08.11.2023).

3. Stojkoska B.L.R., Trivodaliev K.V. A review of Internet of Things for smart home: Challenges and solutions. [Електронний ресурс] Режим доступа: https://www.sciencedirect.com/science/article/abs/pii/S095965261631589X (дата звернення 08.11.2023).

4. Mowad M.A.E.-L., Fathy A., Hafez A. Smart home automated control system using android application and microcontroller. [Електронний ресурс] Режим доступа: https://scholar.google.com/scholar_lookup?journal=Int.+J.+Sci.+Eng.+Res.&title=Smart+home+automated+control+system+using+android+application+and+microcontroller&author=M.A.E.-L.+Mowad&author=A.+Fathy&author=A.+Hafez&volume=5&publication_year=2014&pages=935-939& (дата звернення 08.11.2023).

5. Tang S., Kalavally V., Ng K.Y., Parkkinen J. Development of a prototype smart home intelligent lighting control architecture using sensors onboard a mobile computing system. [Електронний ресурс] Режим доступа: https://www.sciencedirect.com/science/article/abs/pii/S0378778816319971 (дата звернення 08.11.2023).

6. Shirani F., Groves C., Henwood K., Pidgeon N., Roberts E. ‘I’m the smart meter’: Perceptions of smart technology amongst vulnerable

consumers. [Електронний ресурс] Режим доступа: https://www.sciencedirect.com/science/article/abs/pii/S0301421520303724 (дата звернення 08.11.2023).

7. Abrishamchi M.A.N., Cheok A.D., Abdullah A.H., Bielawski K.S. In-Home Surveillance Systems and Privacy Considerations for Malaysians. [Електронний ресурс] Режим доступа: https://ijic.utm.my/index.php/ijic/article/view/198 (дата звернення 08.11.2023).

8. Kumar K., Sen N., Azid S., Mehta U. A fuzzy decision in smart fire and home security system. [Електронний ресурс] Режим доступа: https://www.sciencedirect.com/science/article/pii/S1877050917302296 (дата звернення 08.11.2023).

9. Heartfield R., Loukas G., Budimir S., Bezemskij A., Fontaine J.R., Filippoupolitis A., Roesch E. A taxonomy of cyber-physical threats and impact in the smart home. [Електронний ресурс] Режим доступа: https://www.sciencedirect.com/science/article/abs/pii/S0167404818304875 (дата звернення 08.11.2023).

10. Anthi E., Williams L., Słowińska M., Theodorakopoulos G., Burnap P. A supervised intrusion detection system for smart home IoT devices. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/8753563 (дата звернення 08.11.2023).

11. Mshali H., Lemlouma T., Moloney M., Magoni D. A survey on health monitoring systems for health smart homes. [Електронний ресурс] Режим доступа: https://www.sciencedirect.com/science/article/abs/pii/S0169814117300082 (дата звернення 08.11.2023).

12. Gerber N., Reinheimer B., Volkamer M. Home sweet home? [Електронний ресурс] Режим доступа: https://spice.luddy.indiana.edu/files/2018/07/wssp2018-paper2.pdf (дата звернення 08.11.2023).

13. Zeng E., Mare S., Roesner F. End user security and privacy concerns with smart homes. pp. 65–80. [Електронний ресурс] Режим доступа:

https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng (дата звернення 08.11.2023).

14. Hamdan Y.B. Smart home environment future challenges and issues. [Електронний ресурс] Режим доступа: https://scholar.google.com/scholar_lookup?journal=J.+Electron.&title=Smart+home+environment+future+challenges+and+issues-a+survey&author=Y.B.+Hamdan&volume=3&publication_year=2021&pages=239-246& (дата звернення 08.11.2023).

15. Zheng S., Apthorpe N., Chetty M., Feamster N. User perceptions of smart home IoT privacy. [Електронний ресурс] Режим доступа: https://dl.acm.org/doi/abs/10.1145/3274469 (дата звернення 08.11.2023).

16. Al-Sarawi S., Anbar M., Alieyan K., Alzubaidi M. Internet of Things (IoT) communication protocols. pp. 685–690. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/8079928 (дата звернення 08.11.2023).

17. Stiller B., Schiller E., Schmitt C., Ziegler S., James M. *Handbook of Internet-of-Things*. [Електронний ресурс] Режим доступа: https://link.springer.com/book/10.1007/978-3-030-23983-1 (дата звернення 20.02.2022).

18. Elkhodr M., Shahrestani S., Cheung H. Emerging wireless technologies in the internet of things. [Електронний ресурс] Режим доступа: https://arxiv.org/abs/1611.00861 (дата звернення 08.11.2023).

19. Adamopoulou E., Moussiades L. Chatbots: History, technology, and applications. [Електронний ресурс] Режим доступа: https://www.sciencedirect.com/science/article/pii/S2666827020300062 (дата звернення 08.11.2023).

20. Costin A. Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. pp. 45–54. [Електронний ресурс] Режим доступа: https://dl.acm.org/doi/abs/10.1145/2995289.2995290 (дата звернення 08.11.2023).

21. Kang M. *Prognostics and Health Management of Electronics: Fundamentals, Machine Learning, and the Internet of Things*. [Електронний ресурс] Режим доступа: https://scholar.google.com/scholar_lookup?title=Prognostics+and+Health+Management+of+Electronics:+Fundamentals,+Machine+Learning,+and+the+Internet+of+Things&author=M.+Kang&publication_year=2018& (дата звернення 08.11.2023).

22. Xu W. Toward human-centered AI: A perspective from human-computer interaction. [Електронний ресурс] Режим доступа: https://dl.acm.org/doi/fullHtml/10.1145/3328485 (дата звернення 08.11.2023).

23. Vojković G., Milenković M., Katulić T. IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security. [Електронний ресурс] Режим доступа: https://hrcak.srce.hr/ojs/index.php/bsr/article/view/12916 (дата звернення 08.11.2023).

24. Dasgupta A., Gill A.Q., Hussain F. *Internet of Things (IoT) for Automated and Smart Applications*. p. 9. [Електронний ресурс] Режим доступа: https://hrcak.srce.hr/ojs/index.php/bsr/article/view/12916 (дата звернення 08.11.2023).

25. Boerman S.C., Kruikemeier S., Zuiderveen Borgesius F.J. Exploring motivations for online privacy protection behavior: Insights from panel data. [Електронний ресурс] Режим доступа: https://journals.sagepub.com/doi/full/10.1177/0093650218800915 (дата звернення 15.11.2023).

26. van der Sloot B. Where is the harm in a privacy violation. [Електронний ресурс] Режим доступа: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec8&div=38&id=&page= (дата звернення 15.11.2023).

27. Fafoutis X., Marchegiani L., Papadopoulos G.Z., Piechocki R., Tryfonas T., Oikonomou G. Privacy leakage of physical activity levels in wireless embedded wearable systems. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/7792352 (дата звернення 15.11.2023).

28. Davis B.D., Mason J.C., Anwar M. Vulnerability studies and security postures of IoT devices: A smart home case study. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/9050664 (дата звернення 15.11.2023).

29. Shouran Z., Ashari A., Priyambodo T. Internet of things (IoT) of smart home: Privacy and security. [Електронний ресурс] Режим доступа: https://www.researchgate.net/profile/Zaied-Shouran/publication/331133954_Internet_of_Things_IoT_of_Smart_Home_Privacy_and_Security/links/5c692af14585156b57016c66/Internet-of-Things-IoT-of-Smart-Home-Privacy-and-Security.pdf (дата звернення 15.11.2023).

30. Mai K. *Introduction to Hardware Security and Trust*. p. 175–194. [Електронний ресурс] Режим доступа: https://books.google.com.ua/books?hl=uk&lr=&id=bNiw9448FeIC&oi=fnd&pg=PR3&ots=r37zPcYVow&sig=z7znxSGLSEzews0frkDGPe29JFQ&redir_esc=y#v=onepage&q&f=false (дата звернення 15.11.2023).

31. Лесишин Т.І. Методи та засоби захисту системи «розумний дім»: матеріали наук-тех. конф., м. Тернопіль, 13-14 груд. 2023 р. С. 75.

32. Conti M., Nati M., Rotundo E., Spolaor R. Mind the plug! laptop-user recognition through power consumption. pp. 37–44. [Електронний ресурс] Режим доступа: https://dl.acm.org/doi/abs/10.1145/2899007.2899009 (дата звернення 15.11.2023).

33. Kocher P., Jaffe J., Jun B., Rohatgi P. *Introduction to differential power analysis*. [Електронний ресурс] Режим доступа: https://link.springer.com/article/10.1007/s13389-011-0006-y (дата звернення 15.11.2023).

34. Kocher P., Jaffe J., Jun B. *Introduction to Differential Power Analysis and Related Attacks*. [Електронний ресурс] Режим доступа: https://www.rambus.com/wp-content/uploads/2015/08/DPATechInfo.pdf (дата звернення 15.11.2023).

35. Li Y., Chen M., Wang J. Introduction to side-channel attacks and fault attacks. pp. 573–575. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/7522801 (дата звернення 15.11.2023).

36. Deepa G., SriTeja G., Venkateswarlu S. An overview of acoustic side-channel attack. [Електронний ресурс] Режим доступа: https://web.archive.org/web/20180409221150id_/http://www.ijcscn.com/Documents/Volumes/vol3issue1/ijcscn2013030103.pdf (дата звернення 15.11.2023).

37. Backes M., Dürmuth M., Gerling S., Pinkal M., Sporleder C. Acoustic {Side-Channel} Attacks on Printers. [Електронний ресурс] Режим доступа: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Backes.pdf (дата звернення 04.12.2023).

38. Cheng P., Bagci I.E., Roedig U., Yan J. SonarSnoop: Active acoustic side-channel attacks. [Електронний ресурс] Режим доступа: https://link.springer.com/article/10.1007/s10207-019-00449-8 (дата звернення 04.12.2023).

39. Alias Y.F., Isa M.A.M., Hashim H. Timing Attack: An Analysis of Preliminary Data. [Електронний ресурс] Режим доступа: https://jtec.utem.edu.my/jtec/article/view/1774 (дата звернення 04.12.2023).

40. Joshi M., Hadi T.H. A review of network traffic analysis and prediction techniques. [Електронний ресурс] Режим доступа: https://arxiv.org/abs/1507.05722 (дата звернення 04.12.2023).

41. Srinivasan V., Stankovic J., Whitehouse K. Protecting your daily in-home activity information from a wireless snooping attack. pp. 202–211. [Електронний ресурс] Режим доступа: https://dl.acm.org/doi/abs/10.1145/1409635.1409663 (дата звернення 04.12.2023).

42. Noto M., Sato H. A method for the shortest path search by extended Dijkstra algorithm. pp. 2316–2320. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/886462 (дата звернення 04.12.2023).

43. Saeed N., Nam H., Haq M.I.U., Muhammad Saqib D.B. A survey on multidimensional scaling. [Електронний ресурс] Режим доступа: https://dl.acm.org/doi/abs/10.1145/3178155 (дата звернення 04.12.2023).

44. Teknomo K. K-means clustering tutorial. [Електронний ресурс] Режим доступа: https://scholar.google.com/scholar_lookup?journal=Medicine&title=K-means+clustering+tutorial&author=K.+Teknomo&volume=100&publication_year=2006&pages=3& (дата звернення 04.12.2023).

45. Roughgarden T. A Second Course in Algorithms. Режим доступа: http://web.archive.org/web/20200212164159/http://timroughgarden.org/w16/l/l5.pdf (дата звернення 04.12.2023).

46. Balakrishnama S., Ganapathiraju A., Picone J. Linear discriminant analysis for signal processing problems. pp. 78–81. [Електронний ресурс] Режим доступа: https://ieeexplore.ieee.org/abstract/document/766096 (дата звернення 04.12.2023).

47. Yang Y., Shao M., Zhu S., Cao G. Towards statistically strong source anonymity for sensor networks. [Електронний ресурс] Режим доступа: https://dl.acm.org/doi/abs/10.1145/2480730.2480737 (дата звернення 04.12.2023).

48. Park H., Park T., Son S.H. A comparative study of privacy protection methods for smart home environments. [Електронний ресурс] Режим доступа: https://gvpress.com/journals/IJSH/vol7_no2/8.pdf (дата звернення 04.12.2023).

49. Park H., Basaran C., Park T., Son S.H. Energy-efficient privacy protection for smart home environments using behavioral semantics. [Електронний ресурс] Режим доступа: https://www.mdpi.com/1424-8220/14/9/16235 (дата звернення 04.12.2023).

50. He J., Xiao Q., He P., Pathan M.S. An adaptive privacy protection method for smart home environments using supervised learning. [Електронний ресурс] Режим доступа: https://www.mdpi.com/1999-5903/9/1/7 (дата звернення 04.12.2023).

51. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень. [Електронний ресурс]. Режим доступа: https://zakon.rada.gov.ua/rada/show/va042282-99#Text.

52. Стручок В.С. Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання / В.С.Стручок. — Тернопіль:

ФОП Паляниця В. А., 2022. — 156 с.

Додаток А

**УДК 62-503.5**
**Т.І. Лесишин**
Тернопільський національний технічний університет імені Івана Пулюя, Україна

## МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ СИСТЕМИ “РОЗУМНИЙ ДІМ”

**T.I. Lesyshyn**

## METHODS AND MEANS OF INFORMATION PROTECTION OF THE “SMART HOME” SYSTEM

Розумні будинки, які використовують технологію Інтернету речей, надають унікальні можливості для автоматизації завдань та покращення зручності у нашому повсякденному житті. Зростання популярності цих технологій неухильно викликає занепокоєння щодо кібербезпеки та конфіденційності. Потреба в удосконаленні систем шифрування та розробці нових стратегій безпеки виникає з потенційної загрози витоку цінної інформації через бездротові сигнали. Важливість міцного криптографічного захисту, а також врахування факторів, таких як тимчасове маніпулювання трафіком та випадковість, підкреслюється сучасними атаками, такими як "шпигунство на основі FATS".

У сучасній ері передових технологій розумні пристрої стикаються з серйозним ризиком витоку конфіденційності та безпеки через появу атак бічного каналу. Зловмисники можуть використовувати систему через переконання в постійному витоку даних, що становить основу для цих атак. Дослідження пасивних та активних атак бічного каналу виявляє слабкості, які існують у стандартних компонентах розумних пристроїв.

Аналіз енергоспоживання та диференційний аналіз енергоспоживання - це дві техніки, які використовуються для виявлення чутливої інформації в пристроях за допомогою вивчення їхнього використання енергії. Спостерігаючи коливання у використанні енергії, можливо виявити тенденції та розрізняти алгоритми, в той час як SPA має здатність визначати техніки шифрування. Диференційний аналіз енергоспоживання є вдосконаленим підходом, який використовує статистичні методи для виправлення помилок та визначення ключів шифрування з більшою точністю.

Система знаходиться під загрозою фізичних маніпуляцій та розголошення інформації альтернативними каналами через аналіз помилок, електромагнітних характеристик та звукових характеристик. Дослідження часу та аналіз трафіку підкреслює використання інформації, пов'язаної з часом, та передачі сигналів для виявлення закономірностей та важливої інформації. Хакери можуть аналізувати комунікації системи та визначати її функціональність через ці атаки.

Сучасні дослідження в галузі безпеки розумного дому в бездротових мережах спрямовані на покращення конфіденційності та зменшення загальних затримок за допомогою використання вдосконалених схем захисту від атак FATS. Схема ConstRate, яка визначає послідовність вікон виконання для розподілу сигналів у мережевому трафіку, стала ефективним інструментом для оптимізації конфіденційності. Покращена схема ProbRate, заснована на експоненційному розподілі інтервалів очікування, дозволяє зберігати конфіденційність при зменшенні часових затримок. З свого боку, схема FitProbRate (FPR) використовує тест Андерсона-Дарлінга та пріоритетизацію фактичних пакетів для ефективного зменшення затримок системи.