



Система виявлення вторгнень для віртуалізації мережевих функцій

Intrusion Detection System for NFV

Автор: студент II курсу, групи КА-83мн Галета П.О.
Науковий керівник: к.ф.-м.н, доц. Шубенкова І.А.

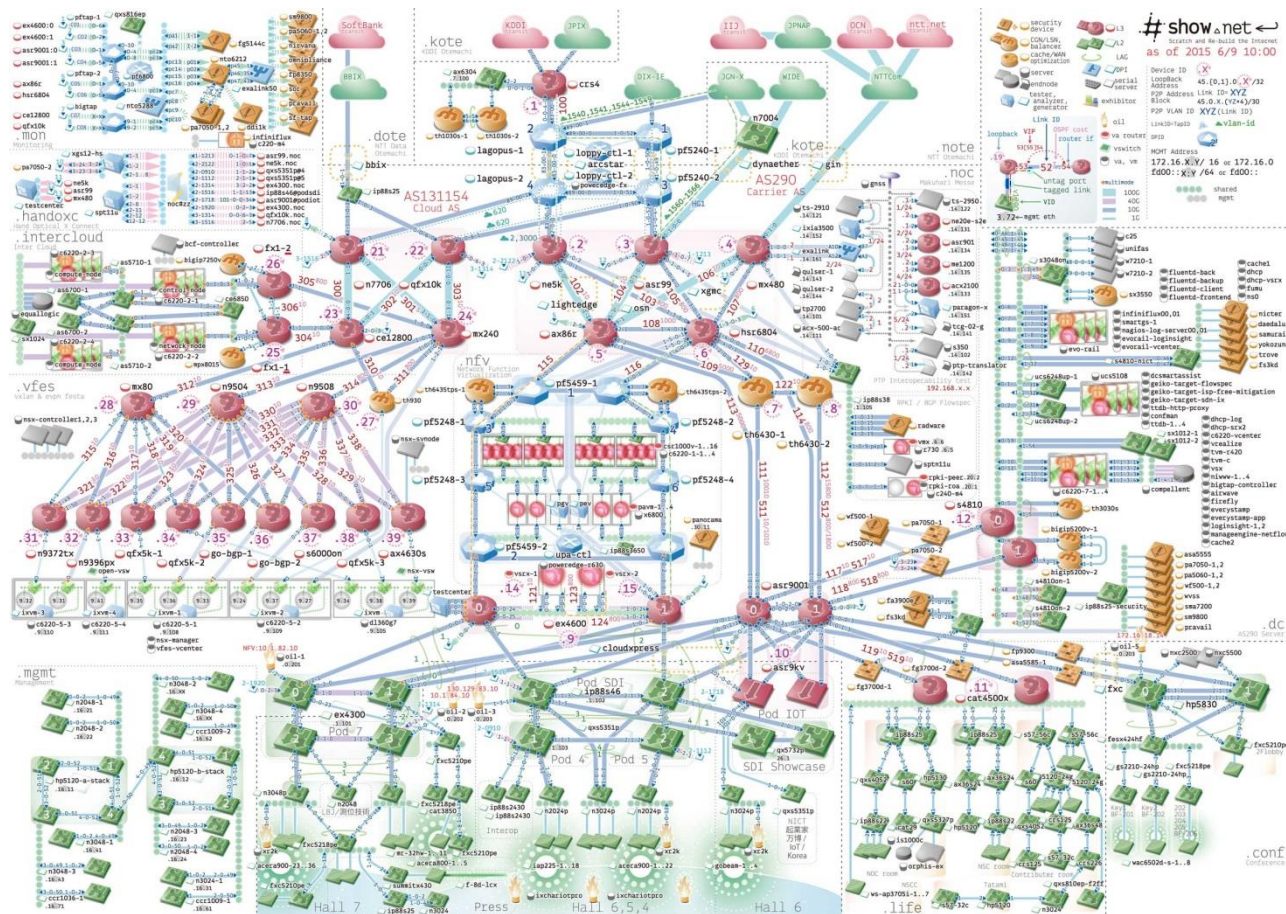
- **Об'єкт дослідження:** віртуалізація мережевих функцій
- **Предмет дослідження:** методи виявлення мережевих атак, що можуть бути використані при віртуалізації мережевих функцій
- **Методи:** моделювання загроз, навчання без вчителя

Завдання

- Аналіз віртуалізації мережевих функцій та інформаційної безпеки віртулізованих мереж.
- Аналіз методів виявлення мережевих атак
- Створення системи розпізнавання вторгнень

Проблеми корпоративних мереж

Enterprise network problems



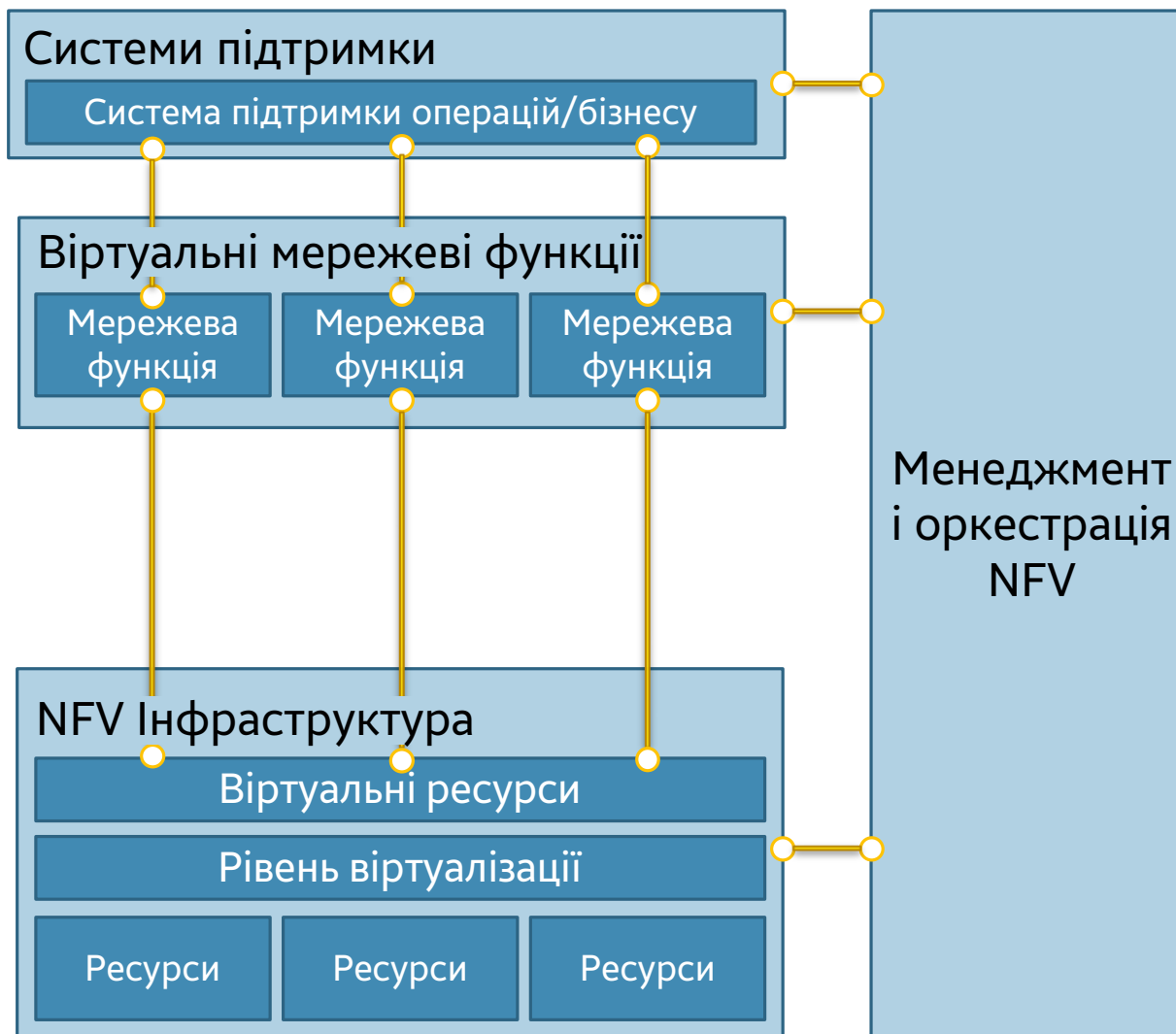
Складність в управлінні

Складність в оновленні

Неефективне використання ресурсів

Віртуалізація мережевих функцій

Network Function Virtualization



Інвестиції в NFV

Investments in NFV



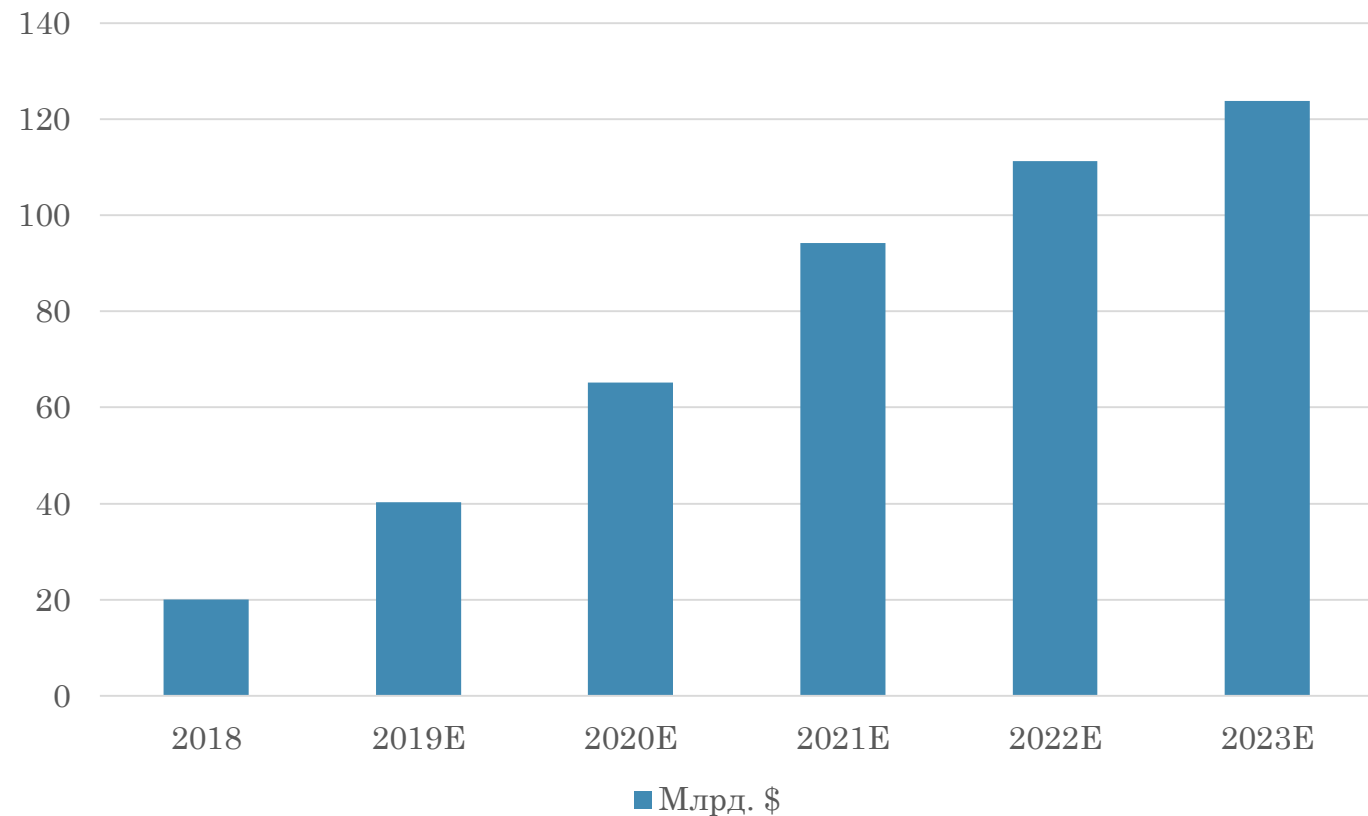
NFV Інфографіка

NFV Infographic



Компаніям, що зацікавлені в NFV належить 70% від усієї галузі

Спрогнозовані інвестиції в NFV



Переваги та проблеми NFV

NFV Advantages & Current problems

Автоматизація

Відкриті стандарти

Гнучкість

Нові сценарії

NFV

Швидкодія

Взаємодія

Захищеність



Безпека в NFV

NFV Security



Помилки у політиках та їх дотриманні
Помилки при життєвому циклі розробки

Cryptography &
Hardening

IAM

Втрата даних та витік інформації

Незахищені інтерфейси

Внутрішня загроза

Вразливості гіпервізора

Невірна композиція сервісів

Атаки на обладнання

Атаки на площину управління

Вразливості в віртуальних машинах

Вразливості в програмному забезпеченні VNF

Мережеві атаки

DOS/DDOS атаки

IDS

Network Isolation

Вразливості викликані проблемами з сумісністю

Спільні ресурси

Системи виявлення вторгнень

Intrusion Detection Systems



- Вузьке місце в мережі
- Обмежена інформація

Мережеві

Сигнатурні

- Не може розпізнати нову атаку
- Необхідність у сигнатурах

IDS

- Не бачить всієї мережі
- Пізня стадія детектування

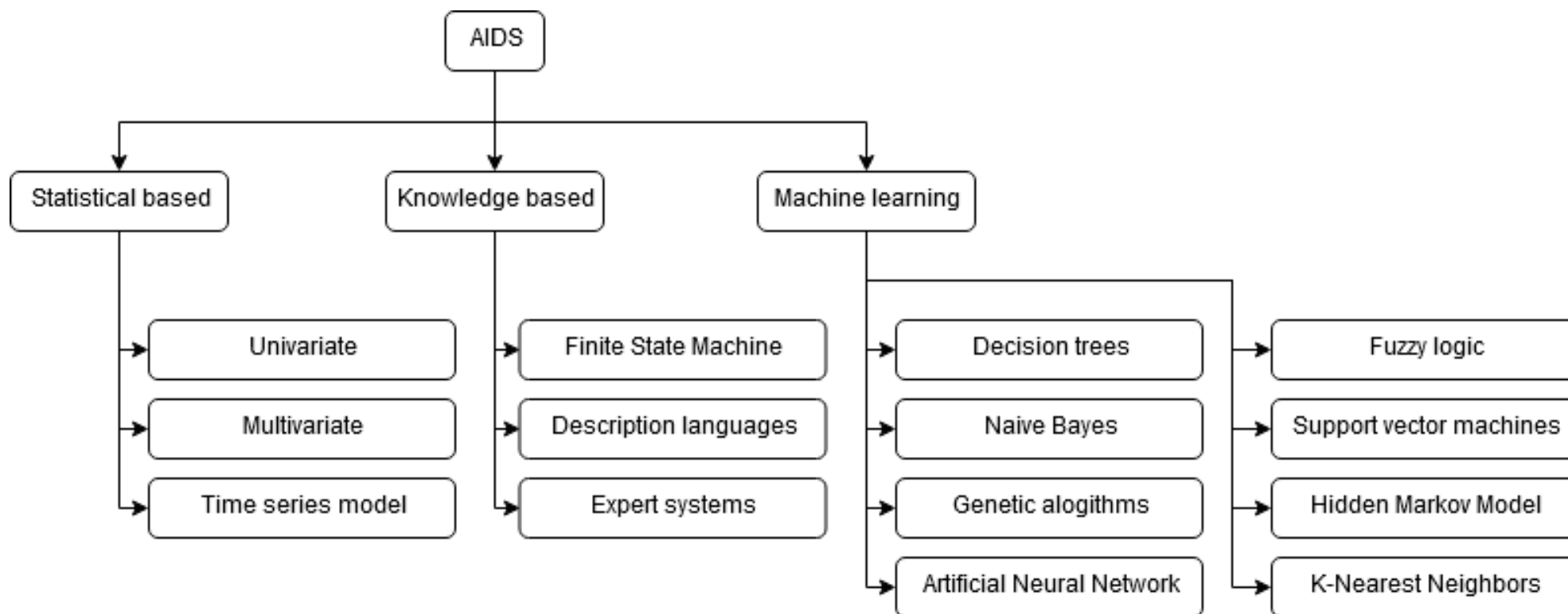
Хостові

Поведінкові

- Помилкові тривоги
- Динамічна середа

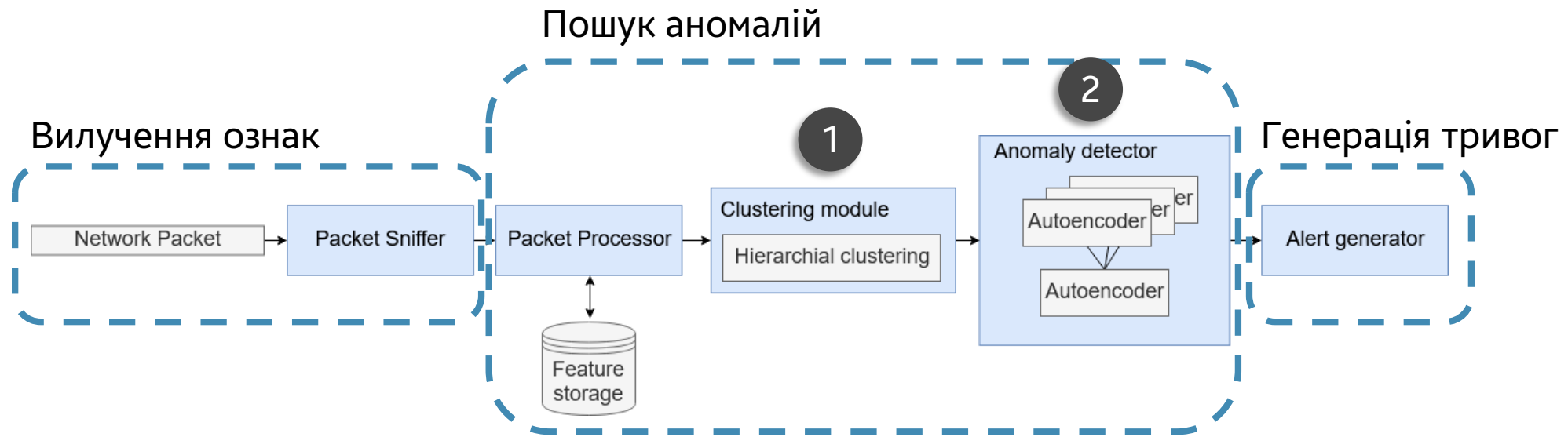
Поведінкові системи виявлення

Anomaly-based Intrusion Detection Systems



Архітектура системи

System architecture



Перший етап навчання (~10 тис.)

Другий етап навчання (~80 тис.)

Функціонування

Конструювання ознак

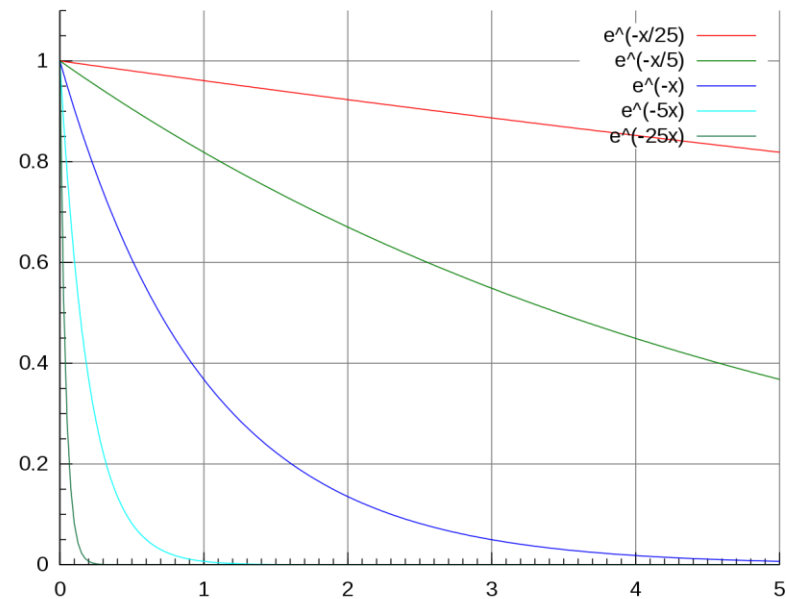
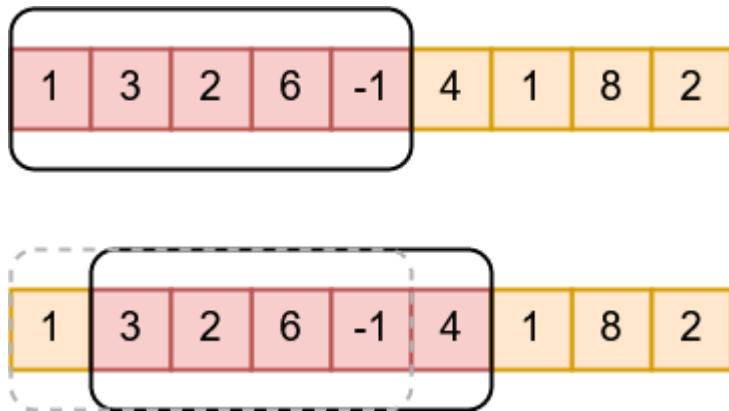
Feature engineering

IP_1
 IP_1, IP_2
 $IP_1, IP_2, port_1, port_2$

1 sec

n sec

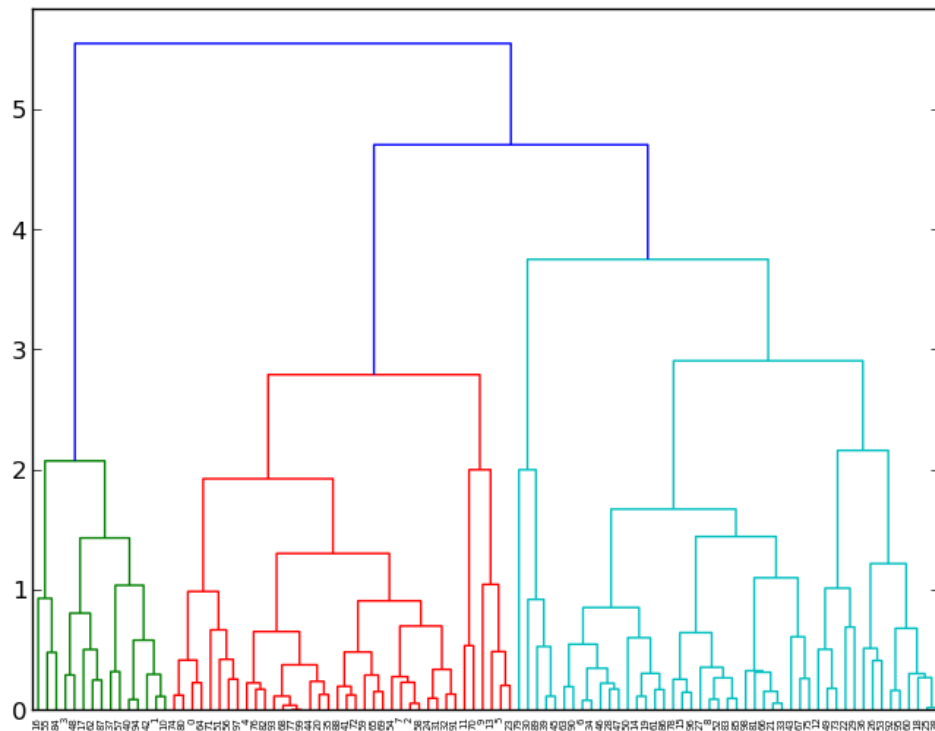
Mean, Standard deviation, Covariance, etc.



Виявлення аномалій

Anomaly detection

- 1
- 3
- 2
- 6
- 1
- 4
- 1
- 8
- 2



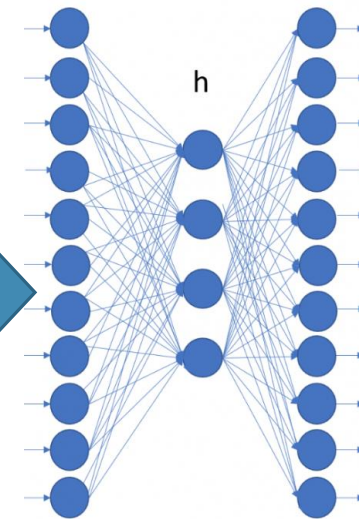
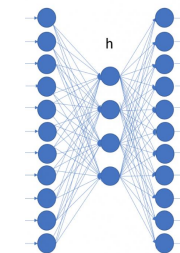
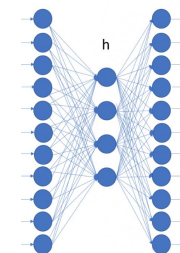
- 1
- 3
- 2



- 6
- 1
- 4
- 1

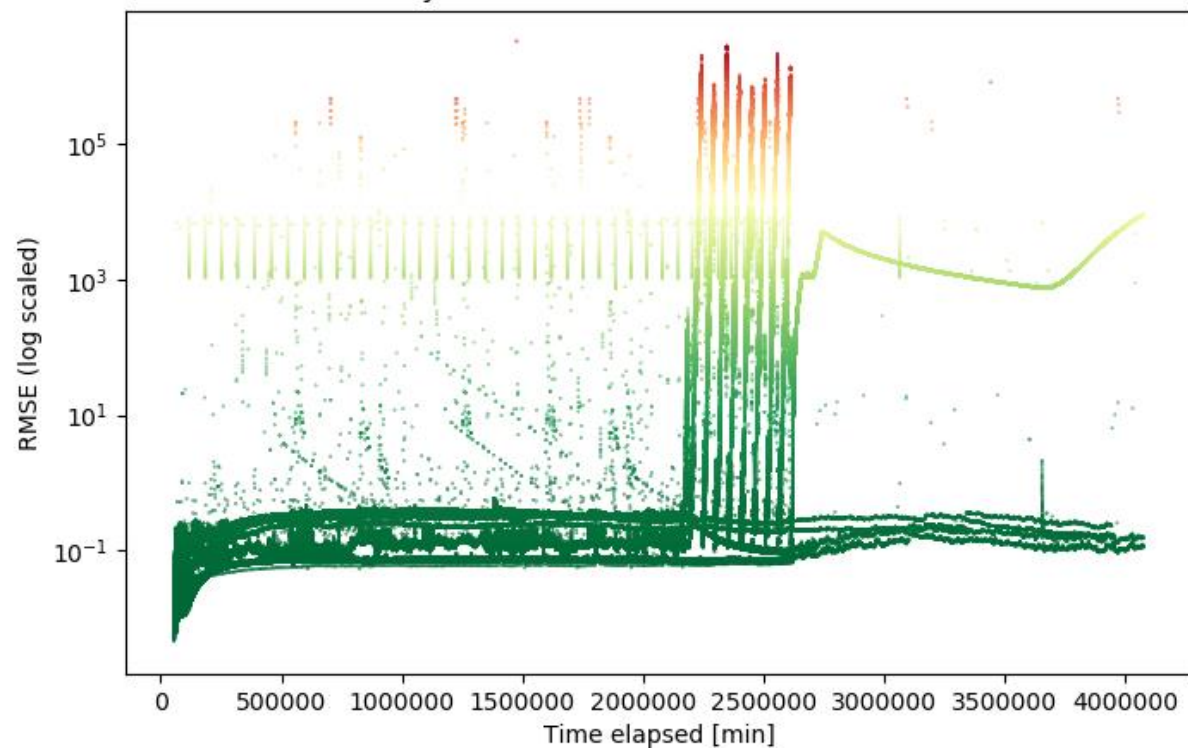


- 8
- 2



Тестування системи

System Evaluation



Швидкість при навчанні	8300 pps
Швидкість при роботі	11000 pps
Максимальне використання процесора	100%
Максимальне використання пам'яті	80Mb
Атака	AUC
DoS	0.953
Nmap scan	0.931
Fuzzing	0.991
Botnet	0.957
MitM	0.892
Flooding	0.991
Середнє	0.952

Висновки

- Проведено аналіз віртуалізації мережевих функцій та інформаційної безпеки віртулізованих мереж.
- Проведено аналіз методів виявлення мережевих атак
- Створено систему розпізнавання вторгнень

Дякую за увагу

