ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки

Методи моніторингу трафіка в корпоративній мережі

Кваліфікаційна робота

Виконав:
ст. гр. СПм-22-2
Лукірін Ю.М.

Керівник:
проф. Міхаль О.П.

Мета та завдання кваліфікаційної роботи 2

Метою кваліфікаційної роботи є аналіз методів моніторингу трафіка, методів ідентифікації трафіка та удосконалення технологій передачі трафіка за рахунок підвищення якості кластеризації та класифікації трафіка.

Об'єкт дослідження: трафік в корпоративних комп'ютерних мережах з пакетною комутацією.

Завдання:

- аналіз стану сучасних корпоративних мереж із пакетною комутацією щодо застосовуваних методів моніторингу, ідентифікації та моделей трафіку, технологій та протоколів передачі інформації;
- аналіз алгоритмів класифікації трафіку протоколів, що використовуються у корпоративних телекомунікаційних мережах;
- аналіз існуючих методів та моделей аналізу мережних пакетів, враховучи особливості передачі данних по мережі (втрата окремих пакетів, стиснення і шифрування даних, вкладене тунелювання);
- розробка програмних засобів моніторингу корпоративної мережі з використанням досліджених моделей та методів.

Моніторинг корпоративної комп'ютерної мережі 3

Існуючі рівні для програмних засобів аналізу трафіка 4

Виділення і розбір заголовків протоколів в пакеті 5

Схема ідентифікації трафіка для завдання моніторингу 6

Існуючі методи ідентифікації трафіка корпоративної мережі з пакетною комутацією

7

- Байєсовський метод.
- Методи з урахуванням фільтра Калмана
- Нейронні мережі та самонавчальні системи
- Методи, що базуються на детермінованих процесах
- Методи на основі процесів із модуляцією

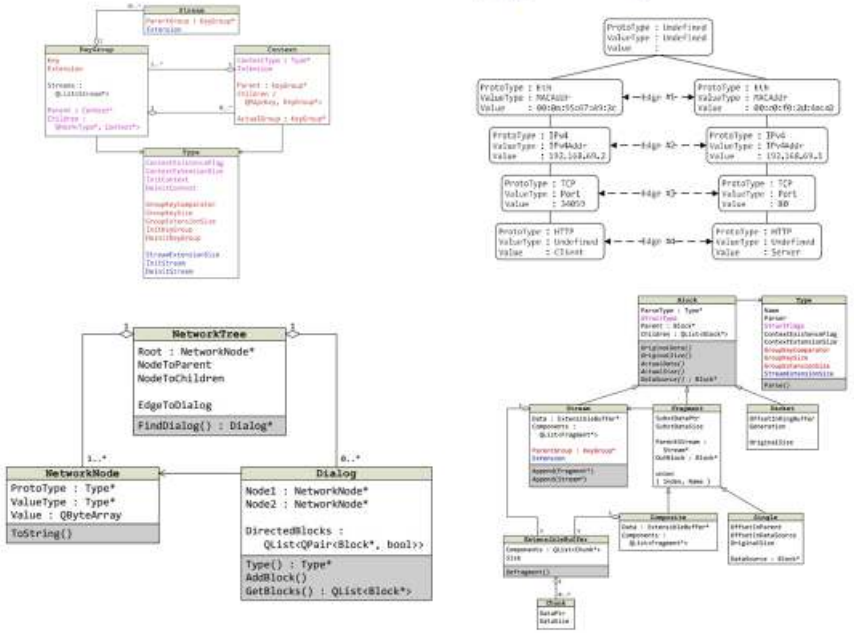
Модель мережної взаємодії між двома застосунками

8

$$Packet^i = <Control^i, Payload^i> , i = 1 \dots N$$

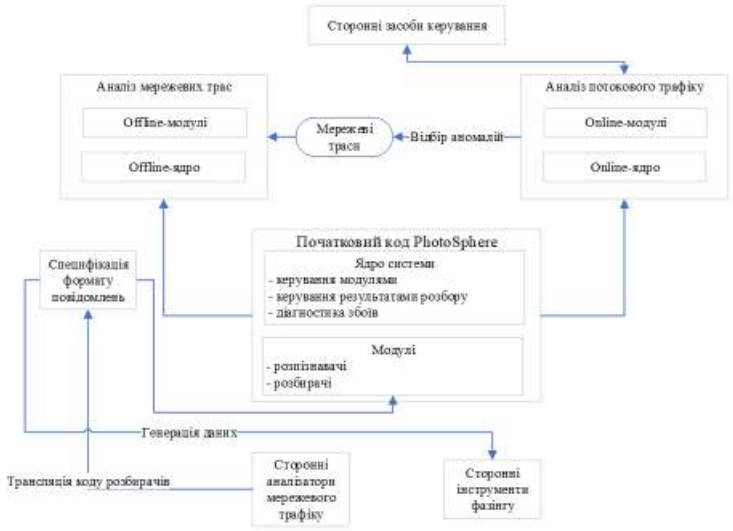
Сутності моделю. Дерево мережі

9



Програмні засоби моніторингу трафіка мережі. Схема взаємодії програмних модулів

10



API для розробки модулів розбору та модулів побудови

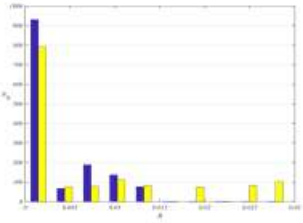
11

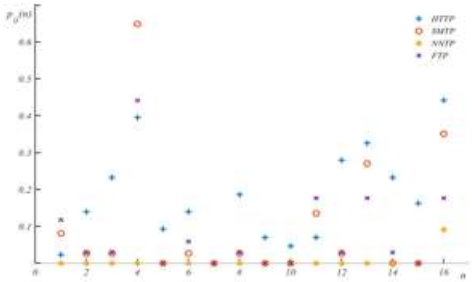
Ім'я функції	Опис
createBuffer	Створити буфер
completeBuffer	Зберегти буфер до файлу
bufferAppend	Додати дані блока в буфер у відповідності до заданого формату

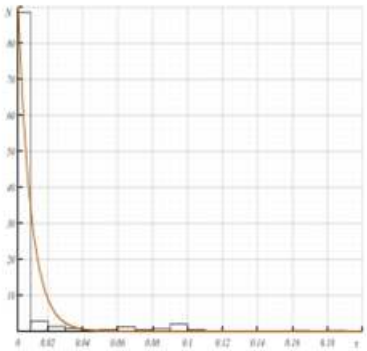
Ім'я функції	Опис
Операції над блоками	
processSingle	Створити та розібрати single-блок
processComposite	Створити та розібрати composite-блок
createStream	Створити блок-потік
completeStream	Виконати розбір блоку-потоку
streamAppend	Додати дані блока в блок-потік
Керування станом розбору	
contextExtension	Отримати дані розширення активного контексту
activateKeyGroup	Активувати в рамках поточного контекста групу
keyGroupExtension	Отримати дані розширення активної групи з ключем
setSrcDst	Активувати відправника та отримувача
Реєстрація розбирачів і розпізнавачів	
regType	Зареєструвати тип
regRecognizer	Зареєструвати розпізнавач
getType	Отримати тип, який зареєстрований в іншому модулі
Журнал повідомлень	

Результати роботи

12

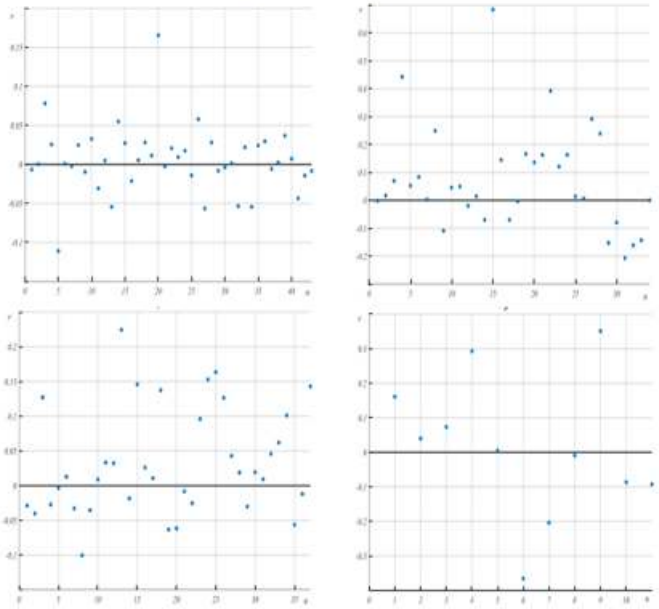






Результати роботи

13



Висновки

14

В ході виконання кваліфікаційної роботи проведено аналіз методів моніторингу трафіка, методів ідентифікації трафіка та удосконалення технологій передачі трафіка за рахунок підвищення якості кластеризації та класифікації трафіка. Проаналізовано стан сучасних корпоративних мереж із пакетною комутацією щодо застосовуваних методів ідентифікації та моделей трафіку, технологій та протоколів передачі інформації. Також проведено аналіз алгоритмів класифікації трафіку протоколів, що використовуються у корпоративних телекомунікаційних мережах. Запропонована архітектура програмних засобів поглибленого моніторингу мережевого трафіка, що дозволяє розробляти і налагоджувати модулі підтримки протоколів на попередньо збереженому трафіку і згодом використовувати ці модулі в реальному режимі часу. Розроблені та реалізовано програмні засоби для проведення моніторингу корпоративної мережі.

ДОДАТОК Б

Тези доповіді

Problems of Informatization: the eleventh international scientific and technical conference

МЕТОДИ МОНІТОРИНГУ ТРАФІКА В КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Лукірін Ю.М., Климова І.М.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасному світі, де організації стають все більш залежними від інформаційних систем, методи та засоби моніторингу трафіка в корпоративних мережах стають критично важливими. Здатність відстежувати, аналізувати та реагувати на аномалії в мережевому трафіку може бути ключем до захисту інформації та забезпечення надійності мережі [1]. Протоколи моніторингу дозволяють адміністраторам отримувати детальну інформацію про стан мережевих пристроїв, трафіку та загальний стан мережі. Аналізатор трафіку є інструментом, який допомагає спеціалістам отримувати деталізовану інформацію про діяльність в мережі. Аналізатор трафіку захоплює пакети даних, які передаються через мережевий інтерфейс, і дозволяє користувачеві переглядати, аналізувати та інтерпретувати ці дані. Захоплені пакети можуть бути вивчені в реальному часі або збережені для подальшого аналізу.

Метою доповіді є аналіз існуючих методів моніторингу трафіка в корпоративних комп'ютерних мережах, протоколів моніторингу та аналізаторів трафіку. В доповіді наводяться результати досліджень. Проведений аналіз даних методів показав, що методи моніторингу на основі протоколів використовують протоколи, такі як SNMP, для збору даних про стан пристроїв та використання мережі; протоколи NetFlow та sFlow забезпечують збір даних про потоки трафіка, що дозволяє аналізувати великі обсяги трафіка та визначати джерела та призначення конкретних потоків. В окремих випадках також використовується пакетне захоплення, що дозволяє аналізувати великі обсяги трафіка. Аналізатори трафіку, в свою чергу, застосовуються для діагностики проблем в мережі, забезпечують безпеку мережі (виявлення підозрілого або зловмисного трафіку [2]), а також для моніторингу використання пропускної спроможності, що допомогає ідентифікувати проблеми з завантаженістю мережі та планувати розширення мережевої інфраструктури. В зв'язку з цим чинності набувають методи обробки та фільтрації зображень в комп'ютерних системах, засновані на використанні сучасних методів глибинного навчання. Моніторинг трафіку в корпоративних мережах є невід'ємною частиною сучасного управління IT. За допомогою правильних методів та інструментів компанії можуть забезпечити надійність, продуктивність та безпеку своїх мережевих ресурсів.

Список літератури

1. Li, X., Bian, F., Crovella, M., Diot, C., Govindan, R., Iannaccone, G., and Lakhina, A. (2006). Detection and identification of network anomalies using sketch subspaces. **IMC 2006**, p. 147–152.

2. Ayres, P. E., Sun, H., Chao, H. J., and Lau, W. C. (2006). Alpi: A DDOS defense system for high-speed networks. IEEE Journal on selected areas in communications, 24(10):1864-1876.

Рисунок Б.1 – Наукова публікація