ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Кваліфікаційна робота

Тема: Методи та засоби моніторингу корпоративної комп'ютерної мережі

Виконав: ст. гр. СПзм-21-1 Гребеннік К.В. Керівник: доц. Ткачов В.М.

Activate Windows
Go to Settings to activate Windows

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

- Факультет - Навчально-науковий центр заочної форми навчання
- Кафедра - електронних обчислювальних машин
- Мета дослідження – моделі, методів і засобів аналізу та прогнозування трафіку комп’ютерних мереж, проектування комп’ютерної мережі та проведення практичних експериментів, щодо аналізу трафіку для покращення властивостей даної мережі
- Актуальність роботи – застосування вейвлет-перетвореннь для аналізу трафіку корпоративної мережі

Activate Windows
Go to Settings to activate

Моніторинг мережі

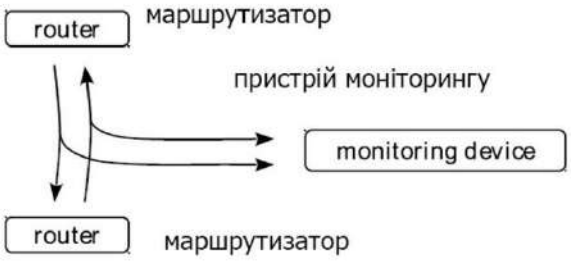
Моніторинг мережі – це використання системи, яка постійно відстежує комп'ютерну мережу на наявність повільних або несправних компонентів і сповіщає адміністратора мережі (через електронну пошту, SMS або інші сигнали тривоги) у разі збоїв або інших проблем, є підзадачею керування мережею (Network Management System)

Види моніторингу мережі:

- Активний
- Пасивний
- Комбінований

Activate Windows
Go to Settings to activate Win

Підходи моніторингу мережі



Дзеркалювання портів (Port Mirroring)
Тестовий порт доступу (Test Access Port)
Захват пакетів (Packet capture)
Зіставлення паттернів (Pattern matching DPI*)
Подієвий аналіз пакетів (Event based DPI*)
Потокове спостереження (Flow observation)
***** **DPI - Deep Packet Inspection** - докладний аналіз пакетів

Activate Windows
Go to Settings to activate Win

Порівняння підходів моніторингу мережі 1

Підхід моніторингу	Переваги і недоліки	
Дзеркалювання портів	За	-Доступне широко у комутаторах
	Проти	-Ненадійний зв'язок
Тестовий порт доступу	За	-Надійний на високих швидкостях
	Проти	-Дорогий, вимагає роз'єднання при встановленні
Захват пакетів	За	- Безперешкодний доступ до повних мережевих даних протягом аналізу
	Проти	- Переважно ручний аналіз - Не масштабується до високих швидкостей і великого розмір захоплених даних

Activate Windo
Go to Settings to act

Порівняння підходів моніторингу мережі 2

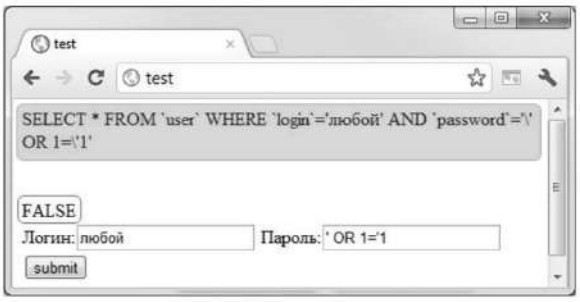
Зіставлення паттернів	За	**- Проста розробка правил виявлення** **- Добре масштабується до високих швидкостей**
	Проти	- Не всі дані можна описати шаблонами або регулярними виразами
Подієвий аналіз пакетів	За	- Добре масштабується до високих швидкостей
	Проти	- Вимагає більш складної реалізації ніж відповідність шаблону DPI - Розробка правил вимагає від розробника дізнайтеся значно більше про DPI реалізації, ніж для зіставлення шаблонів
Потокове спостереження	За	- Конфіденційність – пакетні дані не використовуються - Добре масштабується до високих швидкостей
	Проти	- Зберігає лише агреговані метадані про трафік - Обмежені можливості аналізу даних

Activate Windov
Go to Settings to acti

Методи моніторингу мережі

- Виявлення вторгнень (Intrusion Detection)
- Перегляд пакетів (Packet Sniffing)
- Сканування вразливостей (Vulnerability Scanning)
- Брандмауер моніторингу (Firewall Monitoring)
- Тестування на проникнення (Penetration Testing)

*SQL-ін'єкція відноситься до вставки мета символів SQL вводяться користувачем дані, що призводить до зміни запиту в кінцевій базі даних



Activate Windows
Go to Settings to activate

Огляд найбільш вживаних програм моніторингу комп'ютерних систем і мереж

- Ринок програмного забезпечення для моніторингу мережі настільки переповнений інструментами, що вибрати буває важко. Комплексні інструменти моніторингу мережі дають можливість керувати своїми пристроями та переконатися, що вони доступні, коли це потрібно

- Auvik, Nagios Core, Checkmk, Domotz, Zabbix
- SolarWinds Network Performance Monitor,

Activate Windows
Go to Settings to activate W

Zabbix

Zabbix – open-source система моніторингу служб і станів комп'ютерної мережі. Zabbix складається з трьох базових компонентів:

- сервера для координації виконання перевірок, формування перевірочних запитів та накопичення статистики;
- агентів для здійснення перевірок на стороні зовнішніх хостів;
- фронтенда для організації управління системою

Activate Windows
Go to Settings to activate Wind

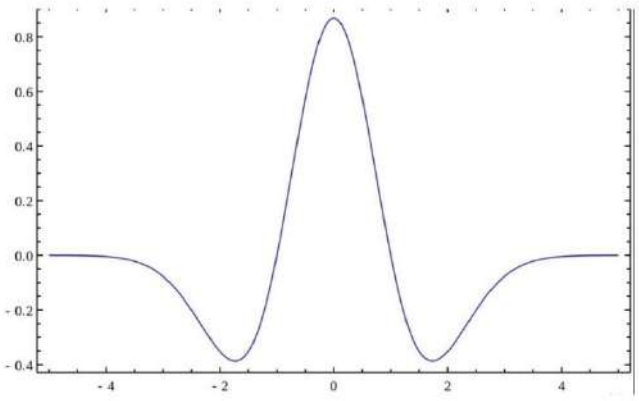
Аналіз трафіку за допомогою вейвлет перетвореннь

Виявлення подій під час вимірювання (моніторингу) комп’ютерної мережі

Виявлення вірусних «хробаків» електронної пошти за допомогою вейвлет-аналізу потоків запитів DNS

Activate Windows
Go to Settings to a

Виявлення подій під час вимірювання (моніторингу) комп'ютерної мережі



- Види вейвлет перетворення:
- DWT (Discrete wavelet transform) – дискретне вейвлет перетворення;
- CWT(Continious wavelet transform) – неперевне вейвлет перетворення;
- Графік функції вейвлет-перетворення типу «Мексиканський капелюх»

Activate Windo
Go to Settings to act

Застосування алгоритму Хаара для виявленя раптових подій

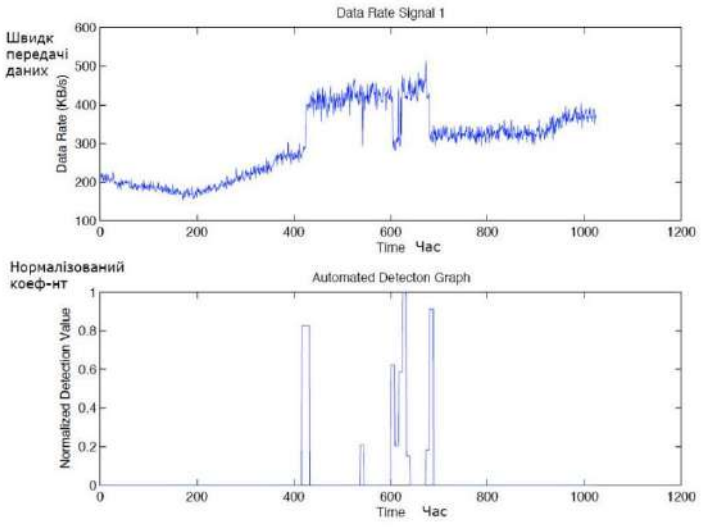
- Алгоритм Хаара заснований на вейвлеті Хаара, який в свою чергу є окремим випадком вейвлету Добеші.

- $T_{lvl} = \sigma_{lvl} \times \sqrt{2 \times log_e n}$
- $\sigma_{lvl} = \frac{median(|cDetail_{lvl}|)}{0.6745}$

Activate Windows
Go to Settings to activate Wi

Виявлення змін у сигналі при різній швидкості передачі даних

Час розрахунку алгоритму не є проблемою для онлайн реалізації алгоритму виявлення аномалії. Це тому, що коли аналіз швидкості передачі да-них або сигналу затримки, де кожна вибірка є за секунду, а достатньо кількох мілісекунд часу обробки. Для фіксування такого сигналу для 1024 точок вимірювання знадобиться 1024 секунди. Таким чином, достатньо вікна сканування приблизно 17 хвилин для повного аналізу та ви-явлення.

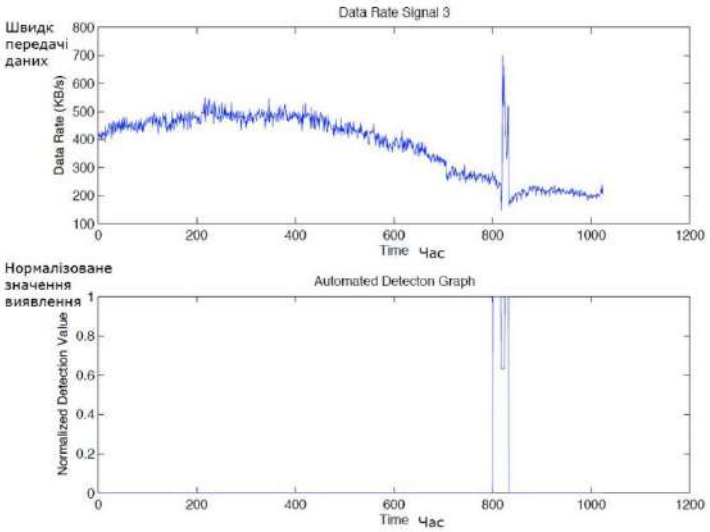


Activate Windo
Go to Settings to ac

Безперервне вейвлетне перетворення

як сума за весь час сигналу, помноженого на масштабовані, зміщені ($shift$) версії вейвлет-функції φ. Ця сума призводить до набору вейвлет-коефіцієнтів, які є функцією масштабу $scale$ та положення.

$$C_{scale,shift} = \int_{-\infty}^{\infty} f(t) \times \varphi(scale, shift, t)dt$$



Activate Windows
Go to Settings to activate V

Виявлення вірусних «хробаків» електронної пошти за допомогою вейвлет-аналізу потоків запитів DNS

- Дискретне вейвлет перетворення - Discrete Wavelet Transform (DWT)

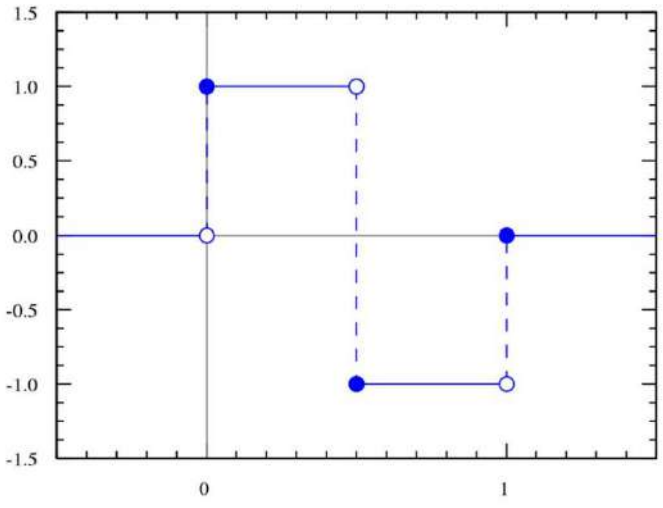
$$\int_{-\infty}^{\infty} 2^{(n+n_1)/2}\psi(2^n t - k)\psi(2^{n_1} t - k_1)\, dt = \delta_{nn1}\delta_{kk1}$$

- Тут δ_{ij} подає дельту Кронекера. Двоїста функція $\psi(t)$ – це сама $\psi(t)$.
- Вейвлетні/масштабні функції з різним масштабом *n* мають функційний взаємозв'язок оскільки:
  - $\varphi(t) = \varphi(2t) + \varphi(2t-1)$
  - $\varphi(t) = \varphi(2t) - \varphi(2t-1)$

Activate Windc
Go to Settings to ac

Візуалізація Гааровго вейвлету

У математиці Гаарів вейвлет (англ. Haar wavelet) — це послідовність перемасштабованих функцій «квадратної» форми, які разом утворюють вейвлетне сімейство або базис. Гаарову послідовність тепер визнають як перший відомий вейвлетний базис, та широко використовують як навчальний приклад



Activate Windo
Go to Settings to act

Значення μ та стандартне відхилення σ для чотирьох систем стиснення даних при значенні коеффіцієнта k=4, k=8 k=16, k=32

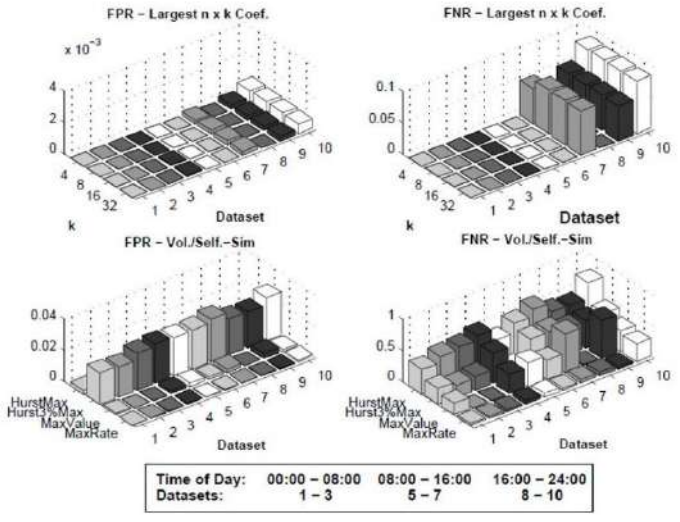
		k=4				k=8			
		C.	D.	S.	DB	C.	D.	S.	DB
FC	μ	100	93.3	97.5	92.4	100	94.8	99.5	94.2
	σ	0	13.6	3	13.4	0	11.2	1	11.1
LC	μ	100	98	98.6	95.4	100	98.8	99.1	97.5
	σ	0	2.7	2.6	10.4	0	2.1	1.9	7.5
BKC	μ	100	97.0	98	94.9	100	96.3	98.9	98.8
	σ	0	5.9	1.9	9.9	0	9.7	1.8	11.0
BCO	μ	100	97.9	98.9	97.6	100	98	99.2	97.7
	σ	0	3.8	2.3	3.8	0	3.7	1.7	3.7

		k=16				k=32			
		C.	D.	S.	DB	C.	D.	S.	DB
FC	μ	100	98.7	99.7	95.6	100	96.5	99.9	96.2
	σ	0	1.7	0.6	9.9	0	9.7	0.4	9.7
LC	μ	100	99.1	99.2	97.3	100	99	99.1	97.4
	σ	0	1.8	1.7	7.5	0	1.9	1.8	6.7
BKC	μ	100	96.1	97.9	95.6	100	96.6	98.3	95.3
	σ	0	9.6	2.8	9.6	0	8.3	1.9	8.3
BCO	μ	100	98	99.2	97.8	100	98.1	99.3	97.9
	σ	0	3.7	1.5	3.7	0	3.5	1.3	3.6

Activate Windows
Go to Settings to activate Wi

Частота хибнопозитивних (FPR) і хибнонегативних (FNR) вибірок різних поштових хробаків з різними наборами даних

метод виявлення вірусів може бути використаний для виявлення активності електронного хробака у відправника, швидше, ніж в одержувача листів домену. Це означає, що він більш ефективніший, ніж подібні методи, засновані на самоподібності вірусу або накопиченні обсягу запитів.



Activate Windo
Go to Settings to act

Висновки

- Використання вейвлет-перетворення таким чином описаний у кваліфікаційній роботі дозволяє отримати корисне подальше стиснення над конкуруючими алгоритмами без втрат, водночас забезпечуючи контрольоване погіршення сигналу. Деградація гарантує, що важливі характеристики вихідних даних зберігаються. Крім того, крім високого ступеня стиснення і хорошої реконструкції якості сигналу, було досліджено кілька факторів стисненого сигналу щоб визначити дію стиснення на них
- Представлено метод, який базується на неконтрольованому навчанні та аналіз часових рядів і використовує вейвлет-перетворення для виявлення активності електронного хробака у відправника, швидше, ніж в одержувача листів домену. Результати експериментів показують, що метод є придатний для отримання надійних поведінкових знань, які є необхідним кроком для автоматичного адаптованого коригування дії. Майбутня робота потребує вивчення ефективності методу через дані запитів DNS з інших мережевих середовищ, і можливо, замість вейвлетів використовуватимуться інші (більш актуальні) часові ряди. Крім того, є перспектива у вивченні контрзаходів, які можна активно застосовувати одноразово виявлено машину, заражену поштовим хробаком, щоб перешкодити таким атакам, як обмеження швидкості DNS-відповідей зараженим пристроєм користувача.Методика такого розрахунку і його результати можуть служити для застосування у спеціалізованому програмному забезпеченні для моніторингу мереж.

Activate Windows
Go to Settings to activate W