УДК 007.52 004.724.4 519.688

К.С. ДЄЄВ, Ю.В. БОЙКО
Київський національний університет імені Тараса Шевченка

АНАЛІЗ МЕТРИК ЯКОСТІ ОБСЛУГОВУВАННЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ В ЗАЛЕЖНОСТІ ВІД ХАРАКТЕРИСТИК IP ВЗАЄМОДІЇ

Інтерес до методів глибокого аналізу пакетів з кожним роком зростає. Акцент в напрямку розвитку комп'ютерних мереж ставиться в підвищенні їх інтелектуальності. Створення оптимальної, з точки зору обчислювальної потужності, системи класифікації є першочерговою задачею розробників програмного забезпечення та дослідників. В статті розглянуто алгоритм мінімізації наборів правил класифікації мережевих пакетів. Описані метрики можуть бути використані для створення гнучких політик в системах контролю якості обслуговування в мережах операторів, використовуючи рівень додатків як ідентифікатор. Особливістю запропонованого алгоритму є повна його пристосовність до різних типів мереж та сервісних потоків, можлива параметризація та налаштування в залежності від наявної апаратної платформи.

Ключові слова: Глибокий аналіз пакетів, аналіз трафіку, якість обслуговування, регулярні вирази.

K.S. DIEIEV, YU. V. BOYKO
Taras Shevchenko national university of Kyiv

COMPUTER NETWORK QUALITY OF SERVICE METRICS ANALYSIS DEPENDING ON CHARACTERISTICS OF IP INTERACTIONS

Increasing interest to deep packet inspection methods continue growth every year. Direction of computer networking development is placed tight to improvement awareness of internal intelligence. One of the primary goal of application developers and scientists is creation powerful and efficient in terms of computing resources classifying system. This document consider algorithm which primary purpose minimizing rule-base sets for packet analysis. Reviewed metrics could be used for flexible quality of service management in service provider network using application layer as a reference. The benefit of proposed algorithm are it applicability to different networks and service flows and embedded availability for fine-tuning dependent on available hardware platform.

Keywords: *Deep packet inspection, traffic analysis, quality of service, regular expression.*

Вступ

Глибокий аналіз пакетів (DPI, Deep Packet Inspection) відіграє важливу роль у створенні новітніх мережевих сервісів. Побудова мереж за принципом розрізнення типів додатків, що взаємодіють між собою, приносить суттєві переваги в управлінні та контролі мереж операторського класу. Використання інтелектуальних апаратно-програмних платформ аналізу мережевої взаємодії відкриває для оператора можливість впливати на інформаційні потоки в його мережі не лише з використанням стандартних мережевих реквізитів, а й за допомогою сервіс-орієнтованих правил та політик (AAN, Application Aware Network).

Створення таких мереж дозволяє гарантувати високий рівень обслуговування для різних типів користувачів у той же час збільшуючи ефективну завантаженість каналів зв'язку оператора. Так як все більше Інтернет сервісів мігрують до хмарного сховища та використовують архітектурний підхід що сприяє децентралізації обміну даними, важливим фактором є необхідність створення систем аналізу, які б дозволяли виявляти вказану взаємодію. Маючи можливість ідентифікувати такі інформаційні потоки оператор послуг має додатковий важіль впливу на користувачів свого сервісу – з'являється можливість додатково тарифікувати вказані взаємодії, застосовувати для них окремі політики чи взагалі обмежувати їх використання окремим групам користувачів. Використання методу вивчення навантаження пакетів даних, яке ґрунтується на вивчені відповідності інформаційного потоку відомим сигнатурам складає базис систем глибокого аналізу пакетів. Термін «глибокий» використовується стосовно відносного зміщення полів ідентифікації в відповідному пакеті даних. Мається на увазі, що відбувається перевірка параметрів які збережені поза фіксованими заголовками рівнів 2-4 моделі OSI.

В роботі розглядаються методи опису метрик сигнатур для аналізу. Створений алгоритм дозволяє оптимізувати процес створення правил з регулярних виразів зменшуючи загальних час необхідний для їх обробки та обсяги пам'яті для збереження таблиці станів скінченного автомата (DFA, Deterministic finite automaton), тобто мінімізуючи їх.

1. Постановка проблеми.

З ростом вимог до якості обслуговування (QoS, Quality of Service) в сучасних комп`ютерних мережах, що розвиваються відповідно до концепції побудови сервіс-орієнтованих мереж наступного покоління все більше уваги приділяється засобам аналізу IP-пакетів. Причина цього полягає в тому, що функціонал DiffServ, заснований на пріоритетній обробці пакетів на вузлах мережі (Node) здатний підвищити рівень QoS на окремих елементах мережі, в той час як саме виявлення сервісних потоків є окремою задачею спеціалізованих аналізаторів мережевої взаємодії. Інструментом впливу на політики в домені маршрутизації можуть ґрунтуватися не лише на стандартних значеннях мережевих заголовків пакетів даних. Таким чином, технології аналізу вийшли за рамки простого пошуку виділених полів за

стандартним зміщенням. Це є основною концепції QoS маршрутизації або сегментного вибору маршруту(Segment Routing), що визначає напрямок розвитку моделей сервіс-орієнтованих мереж, методів, а в подальшому й повноцінних алгоритмів і протоколів маршрутизації. Зважаючи на актуальність завдань QoS з точки зору теорії та практики, вченими і виробниками мережевого обладнання запропоновано низку різнопланових рішень, що відрізняються ступенем моніторингу стану, обчислювальною складністю, рівнем гарантій щодо якості обслуговування, а загалом - передбачуваною областю застосування. У зв'язку з цим метою даної статті є огляд технологічних і теоретичних рішень в області маршрутизації на основі типу сервісу та гарантування якості обслуговування, порівняння їх переваг і недоліків, а також визначення найбільш перспективних шляхів розвитку даного напрямку сучасних телекомунікацій.

Класифікація трафіку є важливим елементом комп'ютерних мереж з різними прикладами застосувань, наприклад, управлінням смугою передачі чи пріоритезації окремих додатків, виявлення підозрілих мережевих активностей. Існує декілька категорій методів класифікації трафіку. Аналіз взаємодії на основі номерів стандартних портів є найбільш відомим та простим, він є досить ефективним для ідентифікації додатків, що не приховують свого існування та взаємодіють за наперед визначеним алгоритмом. Будучи застосованим до взаємодії точка-точка він, однак, не показує такого результату, оскільки така взаємодія часто відбувається з використанням нестандартних портів, номери яких змінюються за випадковим принципом.

Функціональні методи, зокрема, ті які виділяють та дозволяють ідентифікувати взаємодію засновуючись на понятті потоку, можуть використовуватися для виявлення взаємодії окремих типів протоколів (HTTP, пошта, деякі типи P2P взаємодій) мають обмежену продуктивність та не можуть застосовуватись до протоколів з невідомим (захищеним) каналом передачі (HTTPS, SSH). Більш того вони потребують постійного оновлення наборів правил для ідентифікації і мають підвищений рівень хибних спрацювань.

Методи глибокого аналізу пакетів (DPI, Deep Packet Inspection)[1] є найточнішими, оскільки, проводять прямий аналіз корисного навантаження пакетів даних. Більш того вони дозволяють проводити поведінковий аналіз взаємодії, а також враховувати розміри повідомлень окремих потоків, навіть якщо сама взаємодія зашифрована. Ці методи використовують набір сигнатур протоколів для класифікації трафіку. Використовуючи набори регулярних виразів при аналізі корисного навантаження можлива ідентифікації конкретного протоколу, також вони можуть використовувати дану інформацію як уточнення до класифікації за номерами портів. Незважаючи на високий рівень точності, методи аналізу по DPI мають два головних недоліки:

- підтримувати підписи(сигнатури) ідентифікованих додатків в актуальному стані досить складно, автоматизація цієї задачі виходить за рамки пакетної класифікації. Таким чином, адаптація до тимчасових змін в існуючих протоколах відбувається вкрай складно.
- навіть для методів які дозволяють автоматичне створення сигнатур, регулярні вирази отримані в результаті є досить складними. Перевірка відповідності корисного навантаження потоку даних за цими правилами займає дуже багато часу або вимагає непомірно великого простору в пам'яті, що унеможливлює роботу таких систем в режимі реального часу при високих швидкостях взаємодії.

2. Огляд існуючих методів та підходів.

Задача проведення ефективної класифікації мережевої взаємодії розглядається в наукових колах з моменту появи у вільному доступі спеціалізованих бібліотек для спрощення процедури аналізу. Найбільш розповсюдженим представником є проект nDPI[2]. Основою створення даного програмного продукту є низка робіт в області статистичного аналізу мережевої взаємодії [3-6, 8]. Не вдаючись у деталі, основною проблемою є мінімізація кількості станів скінченного автомата який використовується при аналізі регулярних співвідношень в мережевих IP пакетах.

Методи глибокого аналізу пакетів (DPI) загалом є складними і потребують багато часу, але при цьому є найточнішими. Однією з проблем цих підходів, виключаючи складність, є відносно сильна залежність від ручного створення сигнатур (термів).

Для вирішення цих проблем використовують спрощену систему класифікації [3]. Розглянемо її підхід на прикладі реалізації бібліотеки CUTE [4]. Бібліотека представляє собою систему класифікації з використанням спрощеної системи сигнатур. Замість використання складних і довгих регулярних виразів для ідентифікації протоколу, CUTE опирається на набір попередньо підготовлених термів. Це деякий компроміс між точністю розпізнання та швидкістю роботи. Практичні експерименти показали достатній рівень точності для більшості застосувань, звичайно, дещо збільшилася кількість некласифікованих протоколів. Тестування проводилося з використанням реального трафіку сервіс провайдера і в загальному показало, що ймовірність ідентифікації у випадку помірної (до 15 %) кількості зашифрованого трафіку знаходиться в межах 0,90-0,95.

CUTE автоматично вилучає зважені терми для різних протоколів з тестових перехоплених даних. В залежності від цих зважених термів програма за спеціальним алгоритмом оцінює схожість кожного потоку та відповідність до деякого протоколу, після чого відбувається класифікація потоку. Зазначена властивість надає методу високої ефективності навіть при захопленні декількох початкових байт з кожного потоку або у випадку асиметричності обміну відносно точки моніторингу. Встановивши параметр максимального зміщення у 100 байт можна говорити про точність розпізнання порядку 90 %. Асиметричні або неповні

потоки даних є частим явищем в мережі оператора. Це пояснюється найчастіше наявністю декількох зовнішніх каналів Інтернет і відповідним балансуванням вхідного в мережу трафіку. Збільшуючи кількість термів можна досягти подальшого збільшення точності ціною зниження ефективності. Остаточне рішення щодо достатнього рівня точності має прийматися в кожному окремому випадку з огляду на цілі, які прагне досягти оператор.

Загалом, вказані підходи призводять до суттєвого покращення характеристик класифікатора. Автоматичність самого методу гарантує відсутність створення помилкових регулярних виразів, наявність терму в потоці даних не залежить від порядку розташування термів в пам'яті, тобто гарантується постійна швидкість опрацювання вхідних даних.

3. Аналіз запропонованого методу.

Створення сигнатур і підтримка їх в актуальному стані є затратною задачею, статично скомпоновані сигнатури протоколів втрачають з часом свою точність, це відбувається за рахунок постійного розвитку мережевого стеку протоколів та вдосконаленні схем взаємодії. Запропонованій метод автоматичного створення сигнатур є ідеологічним продовженням техніки LCS (Longest Common Subsequence) [5], що проводить синтез регулярного виразу, який може використовуватися як сигнатура. Інакше кажучи, метод намагається виявити найбільш оптимальний регулярний вираз для пошуку збігу в мережевому потоці для подальшої класифікації.

Розглянемо кроки необхідні для створення терму. Спочатку з кожного мережевого пакету довжиною l байт обирається терм деякої довжини t байт, який зустрічається доволі часто в інформаційному потоці (з частотою y). Враховуючи той факт, що навантаження головним чином містить ключовий терм на початку, для їх відділення будемо використовувати символ « | ». Його ми будемо додавати на початку терму. Наприклад розглянемо трафік HTTP , який містить запит GET. Перед початком запиту GET напишемо « | », тобто отримаємо «| GET». Наступним кроком буде додавання вагових коефіцієнтів до кожного окремого терму. Використаємо для цього вагову функцію (1). Більшу вагу ми надаємо термам які є унікальними для деякого досліджуваного протоколу. Тобто, терми що зустрічаються в багатьох протоколах отримують меншу вагу, є менш цікавими для класифікації:

$$W_t^p = \begin{cases} \left(\dfrac{f_t^p}{\sum_{p \in P} f_t^p} \right)^r & f_t^p \geq T \\ 0 & f_t^p < T \end{cases} \quad (1)$$

Параметри p, P, T є набором всіх протоколів, конкретним протоколом та конкретним термом відповідно. Більш того, f_t^p та W_t^p відповідно, означають частоту та вагу терму t в протоколі p. Параметри T і r є параметрами цієї вагової функції. Для всіх унікальних термів функція набуває значення (1).

Останнім кроком є безпосередня класифікація мережевих потоків. Класифікатор слідуючи алгоритму шукає в пакетному навантаженні терми в залежності від їх вагового коефіцієнту. Відповідність потоку до деякого протоколу характеризується середньою вагою термів, що були знайдені в навантаженні. Потім, обирається протокол з найбільшою схожістю. Практичні результати аналізу показали, що використання такого принципу є оптимальним з точки зору об'ємів необхідної оперативної пам'яті.

Алгоритм має два вхідні параметри:

- f - корисне навантаження;
- r набір - процентних зважених термів кожного з відомих протоколів;

Параметр W є вихідним і описується набором значень описаним у формулі (2).

$$W = \{W_{p_1}, W_{p_2}, ..., W_{p_m}\} \quad (2)$$

Використання тільки основних термів підвищує точність і ефективність методу, оскільки, поза розглядом залишаються терми що були отримані внаслідок помилок передачі чи з пошкоджених пакетів. Використання простого текстового пошуку виконано з метою спрощення розуміння алгоритму та може бути замінено на більш ефективні техніки пошуку, наприклад Aho-Corasick [6].

Лістинг алгоритму наведено на рисунку 1.

Перевірка роботи алгоритму відбувалася наступним чином:

- було зібрано два набори пакетів над якими проводилися тести; Механізм перехоплення описано в [7]. Формат перехоплених даних PCAP. Такий вибір зроблений завдяки широкому розповсюдженню вказаної бібліотеки, а також наявності програмних пакетів для аналізу статистичних розподілів внутрішніх параметрів навантаження [8];
- перший набір використовувався для попереднього створення термів за якими було проведено аналіз, мінімізація кількості станів проводилася згідно алгоритму наведеному на рисунку 1;.
- другий набір даних виступав в ролі тестової мережевої взаємодії. Слід зазначити що з розгляду попередньо вилучалися потоки даних протоколів взаємодії, що не були присутні в першому наборі (трейсі).

```
Вхід: f
Вхід: W
Результат: p
max ⟵ -1
p ⟵ ∅
for W_p ∈ W do
    sum ⟵ 0; count ⟵ 0;
    for (t,w) ∈ W_p do
        if f contain t then
            sum ⟵ sum + w; count ⟵ count + 1;
    if max = sum/count then
        p ⟵ p;
    else if max < sum/count then
            p ⟵ p;
            max = sum/count;
return p;
```

Рис. 1. Алгоритм класифікації на основі зважених термів

Така особливість проведення тестування гарантує мінімізацію хибних спрацювань за рахунок виключення протоколів які не можуть бути розпізнані через їх відсутність в таблиці станів. Використовуючи те саме місце збору пакетів та невеликий проміжок часу між захопленнями, можна звести до мінімуму вказане явище.

Перший експеримент було виконано для перевірки справедливості твердження щодо взаємозалежності параметра r та точності класифікації (рис. 2).

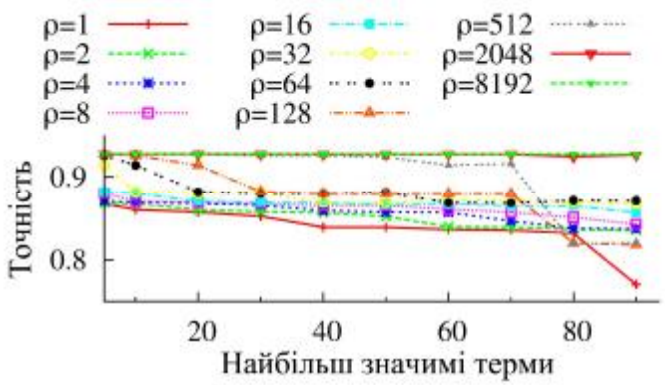

Рис. 2. Залежність точності класифікації від кількості термів (r ~ 0.8 ÷ 0.9).

r Існує явна залежність між r та точністю: чим більше r, тим більш унікальні терми, і тим точнішою є класифікація. Кожному значенню r відповідає якесь значення зваженого параметра . Вибір точності на рівні 0.9 зумовлено практичною значимістю такого рівня, так як більшість комерційних систем аналізу не можуть гарантувати більшої точності. З точки зору практичності і можливості застосування це рішення є обґрунтованим.

В експерименті ми використовували перші 256 байт для класифікації потоку. Вибір граничного значення зміщення в основному залежить від профілю трафіку мережі оператора та протоколів що домінують в ній. Провівши аналіз наборів даних для аналізу, було встановлено що середній розмір пакета складає t = 980 байт, тому значення граничної довжини терму l було обрано на рівні 256 байт. У попередній роботі [3] було перевірено гіпотезу щодо можливості проведення класифікації за заголовками IP-пакетів, тому використовуючи перші 256 – 40 байт можна визначити більшість протоколів. Більш складні

протоколи типу P2P (DHT, BtSync) потребують складнішого процесу аналізу та будуть по можливості розглянуті в наступних роботах на тему аналізу мережевих аномалій. Однією з переваг класифікації по перевірці неповного навантаження є висока швидкодія вказаного методу. Провівши оптимізацію мережевого стеку апаратно-програмного комплексу під керуванням системи LINUX (Debian), а, зокрема, встановивши об'єктивні розміри вхідних черг та оптимізувавши виконання додатку аналізатора з прив'язкою кожного з потоків до окремого ядра, можна отримати пропускну здатність до 10Гбіт/с. Загалом більш коректною буде оцінка з точки зору кількості проаналізованих пакетів за одиницю часу (pps, packet per second), оскільки на кожен отриманий пакет необхідно реагувати перериванням. Тому є сенс використовувати поллінг (polling) [9] або методи DMA (Direct Memory Access), що й використано в роботі.

Сформулюємо критерій стосовно унікальності терму, який буде використовуватися для пошуку збігу в деякому мережевому протоколі. Слід зазначити, що унікальних термів може бути не більше ніж T. З цього випливає умова:

(-) Умова унікальності (3) має зберігатися в наборі L термів протоколу P_i, якщо буде існувати хоча б один терм t, який не буде входити до L^I набору термів для пошуку збігів в інших протоколах, тобто

$$\forall P_{j(j\neq i)} \nexists L^I \in L\left(P_j\right), t \in L^I \text{ ,таке що, } \forall L \in L\left(P_i\right), \exists t \in L \quad (3)$$

Хоча умова (3) на перший погляд виглядає досить строгою, але перевірка практичним підходом показала, що більшість протоколів відповідають їй. Виняток складають протоколи, внутрішня організація яких відповідає принципу overlay (DHT, BtSync), але як вже зазначалося вище, дані протоколи виключені з аналізу зараз. Щоб оптимізувати кількість значимих термів з максимальною ефективністю, виключимо зі списку термів терм t з наступними властивостями:

$$\exists L \in L\left(P_j\right), L^I \in L\left(P_{j(i\neq j)}\right) t \in L \wedge t \in L^I \quad (4)$$

Маючи хоча б один унікальний терм, кожен набір термів буде містити один або більше термів після виключення (оптимізації). Таким чином можемо сформулювати умову пошуку збігу в мережевому трафіку P_j з точністю $1/T$ визначення протоколу P:

$$\forall P_i, P_{j\neq i}, L \in L\left(P_i\right) \text{ тоді і тільки тоді, коли } \left(y \otimes P\left(L\right) | y \in P_j\right) < T \quad (5)$$

Схожий за своїм принципом результат був отриманий у роботі Keralapura [10], але там мова йшла про застосування методу мінімізації правил для систем виявлення вторгнень, з метою зменшення розміру таблиці що містить CAM-структуру ACE (Access List Entry).

Алгоритм має назву MHSP (Minimum Hitting-Set for Protocols), своєю природою він має складність порядку $O\left(|P|^2\right)$. Новизна запропонованого в роботі алгоритму полягає у постановці додаткової умови стосовно граничної довжини t аналізованого пакета та вибір його оптимального значення.

4. Висновки.

Використання методу глибокого аналізу мережевих пакетів за допомогою представлення регулярних виразів у формі термів з їх подальшою оптимізацією має як переваги так і недоліки. Серйозною перевагою є можливість виконання коду аналізатора на доступному апаратному забезпеченні, необхідно лише виконати оптимізацію налаштувань у відповідності до сервісного профілю мережі оператора. Як саме визначати цей профіль було детально розглянуто в роботі [7] та багатьох інших. Вказана оптимізація дозволяє досліджувати інформаційні потоки на швидкостях до 10Гбіт/с. Практичне застосування дана технологія має у випадку бажання оператора впливати на потоки даних у своїй мережі базуючись не на звичайних мережевих параметрах, а на більш інтелектуальних сервісних моделях взаємодії додатків. Останнім часом цей напрямок набув суттєвого розвитку та прискорення в колах виробників комерційного мережевого програмно-апаратного продукту.

Основним недоліком розглянутої системи є неможливість поки що повноцінно аналізувати деякий прошарок протоколів P2P через особливості їх реалізації. У подальшому планується продовжити роботу з надання підтримки для цих додатків та інтеграції розглянутої системи в комплекс відкритого програмного аналізатора комп'ютерних мереж OpenDPI[11].

Література

1. F. Constantinou Identifying Known and Unknown Peer-to-Peer Traffic / F. Constantinou, P. Mavrommatis // Proc. of Fifth IEEE International Symposium on Network Computing and Applications. – 2006. – С. 93–102

2. T. Bujlow Comparison of Deep Packet Inspection (DPI) Tools for Traffic Classification / T. Bujlow, V. Carela-Espacol, P. Barlet-Ros // Technical Report, Version 3. – 2013. – С. 78-92.

3. Дєєв К. С. Аналіз методів та засобів реалізації пакетної фільтрації для глибокого аналізу мережевих пакетів / К. С. Дєєв // Вісник Вінницького політехнічного інституту. – 2014. – №6. – С. 84-90.

4. P. Haffner Automate construction of application signatures / P. Haffner, S. Sen, O. Spatscheck, D. Wang. //Proc. of the 2005 ACM SIGCOMM workshop on Mining network data., 2005. – С. 202.

5. D. Zuev Traffic Classification Using a Statistical Approach. Passive And Active Network Measurement / D. Zuev, A. Moore //6th International Workshop. – 2005. – С. 120-141.

6. Aho Efficient string matching: an aid to bibliographic search / A. Aho, M. Corasick //Communications of the ACM. – 2005. – №18(6):340. – С. 113-137.

7. Дєєв К. С. Вивчення характеру взаємодії типу точка-точка для класифікації мережевого трафіку / К. С. Дєєв // Автоматизовані системи управління і прилади автоматики. – 2013. – №163. – С. 94-101.

8. M. Roughan Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification / M. Roughan, S. Sen, O. Spatscheck, N. Duffield // Proc. of the 4th ACM SIGCOMM conference on Internet measurement., - 2014. - С. 135–148

9. Vivek Gite .Огляд архітектури Linux NAPI [Електронний ресурс]. – Режим доступу: http://www.cyberciti.biz/faq/rhel-centos-fedora-debian-configure-rx-polling-mode/

10. J. Fan Identifying hidden voice and video streams / J. Fan, D. Wu, A. Nucci, R. Keralapura //Society of Photo-Optical Instrumentation Engineers (SPIE), conf. series. – 2009. – Вип. 7344. – С. 14-21..

11. Luca Deri //Опис бібліотеки OpenDPI. – 2009. – С. 1-12. – Режим доступу: http://www.opendpi.org/nettools/opendpi/OpenDPI-Manual.pdf.

References

1. F. Constantinou, P. Mavrommatis “Identifying Known and Unknown Peer-to-Peer Traffic” in Proc. of Fifth IEEE International Symposium on Network Computing and Applications (NCAA ‘06), 2006 pp. 93–102

2. T. Bujlow, V. Carela-Espacol, P. Barlet-Ros “Comparison of Deep Packet Inspection (DPI) Tools for Traffic Classification” in Conference Proceeding Technical Report, Version 3., 2013 pp. 78-92.

3. K. S. Deev, “Analiz metodiv ta zasobiv realizaciji paketnoji filjtraciji dlja ghlybokogho analizu merezhevykh paketiv” Visnyk Vinnycjkogho politekhnichnogho instytutu, Vol. 6, 2014 pp. 84-90

4. P. Haffner, S. Sen, O. Spatscheck, D. Wang “Automate construction of application signatures” in proc. ACM SIGCOMM workshop on Mining network data (ACM 2005), 2005 pp. 202

5. D. Zuev, A. Moore “Traffic Classification Using a Statistical Approach. Passive And Active Network Measurement” in proc. of 6th International Workshop (6WS), 2005 pp. 120-141

6. Aho, M. Corasick “Efficient string matching: an aid to bibliographic search” in proc. Communications of the ACM, Vol. 18(6):340, 2005 pp. 113-137

7. K. S. Deev “Vyvchennja kharakteru vzajemodiji typu tochka-tochka dlja klasyfikaciji merezhevogho trafiku” Avtomatyzovani systemy upravlinnja i prylady avtomatyky, Vol. 163, 2013 pp. 94-101

8. M. Roughan, S. Sen, O. Spatscheck, N. Duffield “Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification” in proc. of the 4th ACM SIGCOMM conference on Internet measurement (ACM IM `14), 2014 pp. 135–148

9. Vivek Gite ”Linux NAPI architecture” (03/10/2015) – open access http://www.cyberciti.biz/faq/rhel-centos-fedora-debian-configure-rx-polling-mode/

10. J. Fan, D. Wu, A. Nucci, R. Keralapura “Identifying hidden voice and video streams” in proc. Society of Photo-Optical Instrumentation Engineers (SPIE), Vol. 7344, 2009 pp. 14-21

11. Luca Deri ”OpenDPI library reference” (03/10/2015) – open access http://www.opendpi.org/nettools/opendpi/OpenDPI-Manual.pdf.

Рецензія/Peer review : 9.4.2015 р. Надрукована/Printed : 14.5.2015 р.
Рецензент: д. т. н., проф., Погорілий С. Д.