УДК 004.942:004.772

І. М. Дронюк, О. Ю. Федевич
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління.

АНАЛІЗ ТРАФІКУ КОМП’ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ ЕКСПЕРИМЕНТАЛЬНИХ ДАНИХ СЕРЕДОВИЩА WIRESHARK

Проаналізовано трафік комп’ютерних мереж, отриманий за допомогою аналізатора мережевих протоколів Wireshark. Спостереження проводилось за такими показниками: сумарна кількість пакетів, середня кількість пакетів, середній розмір пакета та середня швидкість передавання пакетів. Отримані дані використовуються для перевірки теоретичних моделей.

Ключові слова: трафік, комп’ютерна мережа, аналізатор мережевих протоколів, швидкість передачі даних.

This article analyzes the changes in traffic networks, obtained via Wireshark network protocol analyzer. Observations have been conducted by the following parameters: the total number of packets, the average number of packets, average packet size and average bit rate packages. The received data is used to test theoretical models.

Key words: traffic, computer network, network protocol analyzer, bit rate.

Вступ. Загальна постановка проблеми

Проблема дослідження трафіку є актуальною, оскільки комп’ютерні мережі дедалі ширше використовуються у діяльності людини. Швидкий розвиток комп’ютерних мереж та широке застосування систем зв’язку спричинило зростання уваги до питань оцінювання якості та надійності роботи таких систем. Задачі аналізу трафіку комп’ютерних мереж набули значного поширення в вирішенні проблем забезпечення якості провідного та безпровідного зв’язку, безвідмовної роботи інформаційних ресурсів, інформаційного пошуку. Прогнозування завантаження мережі дозволяє забезпечити надійність роботи, раціональне використання ресурсів мережі, ефективне використання обладнання. Інформаційні системи аналізу та прогнозування трафіку показують на практиці свою ефективність, але модернізація комп’ютерних мереж вимагає нових підходів до моделювання, аналізу та прогнозування трафіку комп’ютерних мереж.

Аналіз останніх досліджень і публікацій

Оптимізація роботи комп’ютерних мереж з погляду пошукової оптимізації розглянуто в роботі [1]. Огляд наукових статей про моделювання комп’ютерних мереж на основі моделювання соціальних мереж представлено у [2]. Прогнозування завантаження мережі [3] дозволяє забезпечити надійність роботи, раціональне використання ресурсів мережі, збереження електроенергії. Використовуються для моделювання трафіку такі підходи: метод самоподібності [4], дифузійні рівняння [5], теорія масового обслуговування [6]. Авторами запропоновано моделювання трафіку на основі диференціальних рівнянь коливних процесів [7], що розв’язуються за допомогою асимптотичного методу Боголюбова-Митропольського [8]. Кожен з них має свої переваги та недоліки. Проте для кожного з методів моделювання та прогнозування важливим є апробація моделі на реальних даних. У цій статті проаналізовано експериментальні дані. За допомогою аналізатора мережевих протоколів Wireshark проведено спостереження за трафіком комп’ютерної мережі кафедри АСУ Національного університету “Львівська політехніка” протягом одного місяця.

Формулювання мети

Метою роботи є експериментальне дослідження та аналіз трафіку комп’ютерної мережі на основі спостережень над комп’ютерною мережею кафедри автоматизованих систем управління (АСУ) НУ ЛП. Інструментом для дослідження вибрано аналізатор мережевих протоколів Wireshark,

який є доступним для безкоштовного користування. Здійснений аналіз трафіку планується використати для оптимізації завантаження мережевого обладнання та перевірки достовірності розроблених математичних моделей трафіку у мережі.

Аналіз отриманих наукових результатів

Дослідження трафіку у мережі. Для апробації теоретичних розрахунків, запропонованих у роботі [7], необхідно було провести експериментальні дослідження трафіку у комп'ютерних мережах. Для збору експериментальних даних завантаження мережі використана мережа кафедри АСУ Національного університету "Львівська політехніка" (лютий 2015 р.). Збір даних проводився за допомогою середовища Wireshark. Також було розглянуто дані місячного трафіку (травень 2014 р.) комп'ютерної мережі Інституту теоретичної та прикладної інформатики Польської академії наук (ПАН), надані у межах співпраці з Національним університетом «Львівська політехніка» [9]. Дані, отримані протягом травня 2014 року через Інтернет-шлюз Інституту теоретичної та прикладної інформатики ПАН у Глівіце, Польща.

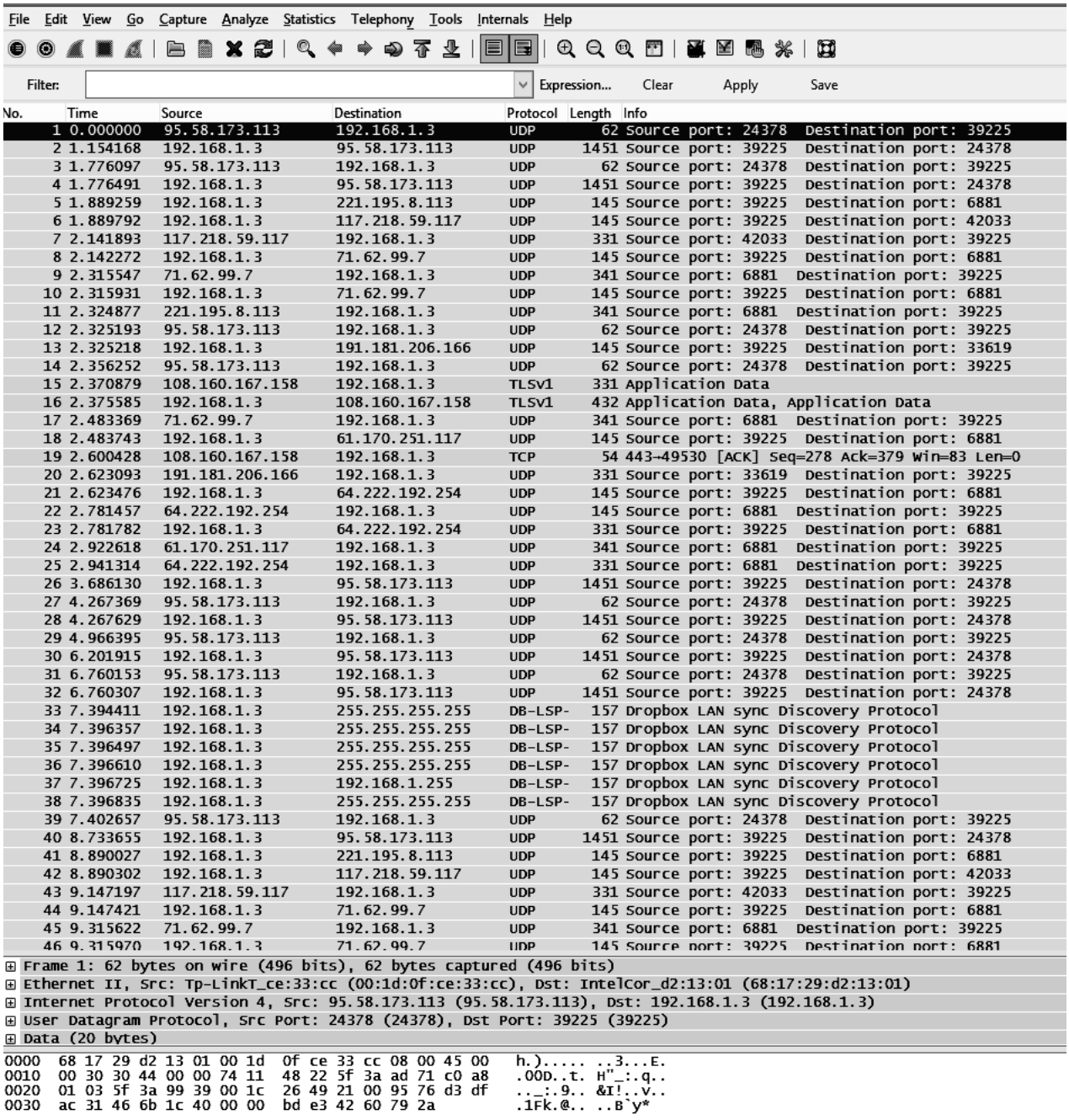

Рис. 1. Відображення частини даних мережевого трафіку кафедри АСУ в середовищі Wireshark

Трафік приблизно містить дані кількох десятків офісних користувачів (дослідників), які в основному працюють з понеділка по п'ятницю з 8 ранку до 4 вечора. 1–3 травня в Польщі – державні вихідні, таким чином трафіку могло бути менше. Деяку перерву в даних трафіку зафіксовано 22 травня о 14:53:32 2014 CET. IP-пакети були обмежені 64 байтами – здебільшого вони містять всі заголовки, плюс кілька байтів корисного навантаження транспортного протоколу. Місцевий трафік DNS є невидимим, через здійснені попередньо конкретні налаштування мережі. IP-адреси не є анонімними. Мережа кафедри АСУ містить близько 20 робочих комп'ютерів співробітників, що завантажені в середньому з 8:30 до 17:30, близько 4 комп'ютерів завантажені до 21:00, та 3 комп'ютерні класи з 32 робочими станціями, які завантажені в середньому з 8:30 до 16:00.

Wireshark є найвідомішим світовим аналізатором мережевих протоколів [9]. Це середовище дозволяє користувачеві бачити те, що саме відбувається у його мережі на «мікроскопічному» рівні. Розроблений компанією The Wireshark Team, стабільно оновлюється з 21 червня 2012 року і до сьогодні. Це середовище було створене за допомогою мови програмування C++. Розповсюджується згідно з умовами GNU GPL. Програма використовує кросплатформну бібліотеку GTK+ для формування та відображення графічного інтерфейсу.

На рис. 1–3 показано деякі результати спостережень у такому вигляді, який фіксує середовище Wireshark. На рис.1 доступна інформація: номер пакета, відносний час отримання пакета (відлік проводиться від першого пакета; параметри відображення часу можна змінити в налаштуваннях), IP адреса відправника, IP адреса одержувача, протокол, за яким пересилається пакет, а також додаткова інформація про нього. Можна побачити, що різні протоколи передавання даних підсвічені різними кольорами, що додає наочності і спрощує аналіз. Далі можна побачити вікно, в якому представлена детальна інформація про пакет згідно з мережевою моделлю OSI. Найнижче вікно показує нам пакет в шістнадцятковому вигляді, тобто побайтово. Конфігурація інтерфейсу може бути легко змінена в меню View. Наприклад, можна закрити вікно побайтового подання пакета (Packet Bytes в меню View), оскільки здебільшого (крім аналізу даних у пакеті) воно не потрібне та лише дублює інформацію з вікна детального опису.

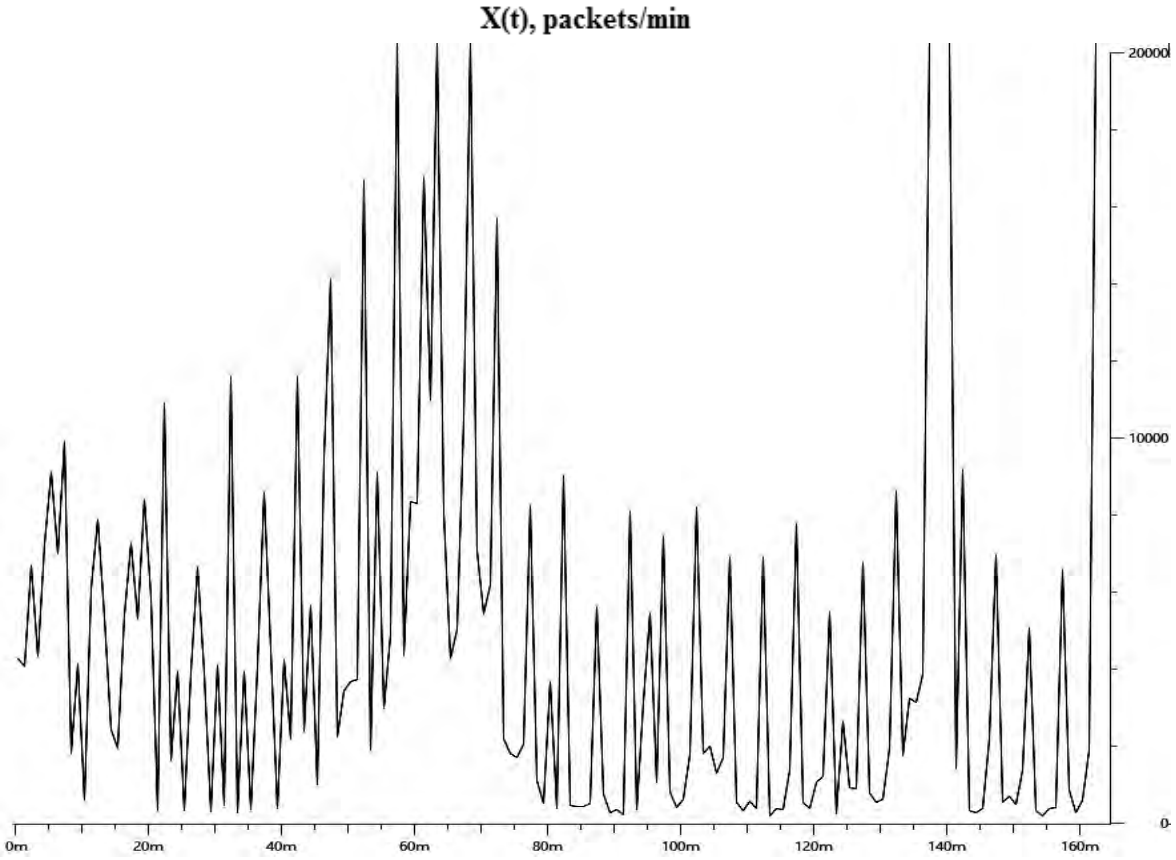

Рис. 2. Частина даних трафіку (2год. 40 хв) за 01.05.14
в Інституті теоретичної та прикладної інформатики ПАН

На рис. 3 зображено частину добового трафіку кафедри АСУ НУ «ЛП», візуалізована засобами Wireshark. Частина узагальнених даних подана в табл. 1.

Wireshark належить до програмного забезпечення, що називається сніфером. Термін «сніфер» бере свій початок від англійського дієслова «to sniff» (нюхати) та є програмним забезпеченням або програмно-апаратним пристроєм, який призначений для перехоплення, подальшого аналізу, або винятково аналізу мережевого трафіку.

Захоплення трафіку можна здійснювати за допомогою таких методів [10]:

- за допомогою аналізу побічних електромагнітних випромінювань та відновленням у такий спосіб того трафіку, який власне «прослуховується»;
- через відгалуження (апаратне або програмне) трафіку, а також із відсиланням копії його на сніфер;
- «прослуховуванням» мережевого інтерфейсу (цей метод є ефективним за умови використання в сегменті концентраторів («hubs») замість комутаторів («switches»), в іншому випадку метод є дуже малоефективним, оскільки на аналізатор мережевих протоколів потрапляють всього лише окремі фрейми);
- під'єднанням аналізатора мережевих протоколів у розрив каналу;
- через здійснення атаки на мережевому (IP- spoofing), чи канальному (MAC- spoofing) рівні, що призводить до перескерування даних трафіку «жертви» або загалом всього трафіку обраного сегменту на аналізатор з подальшим поверненням інформації на належну адресу.

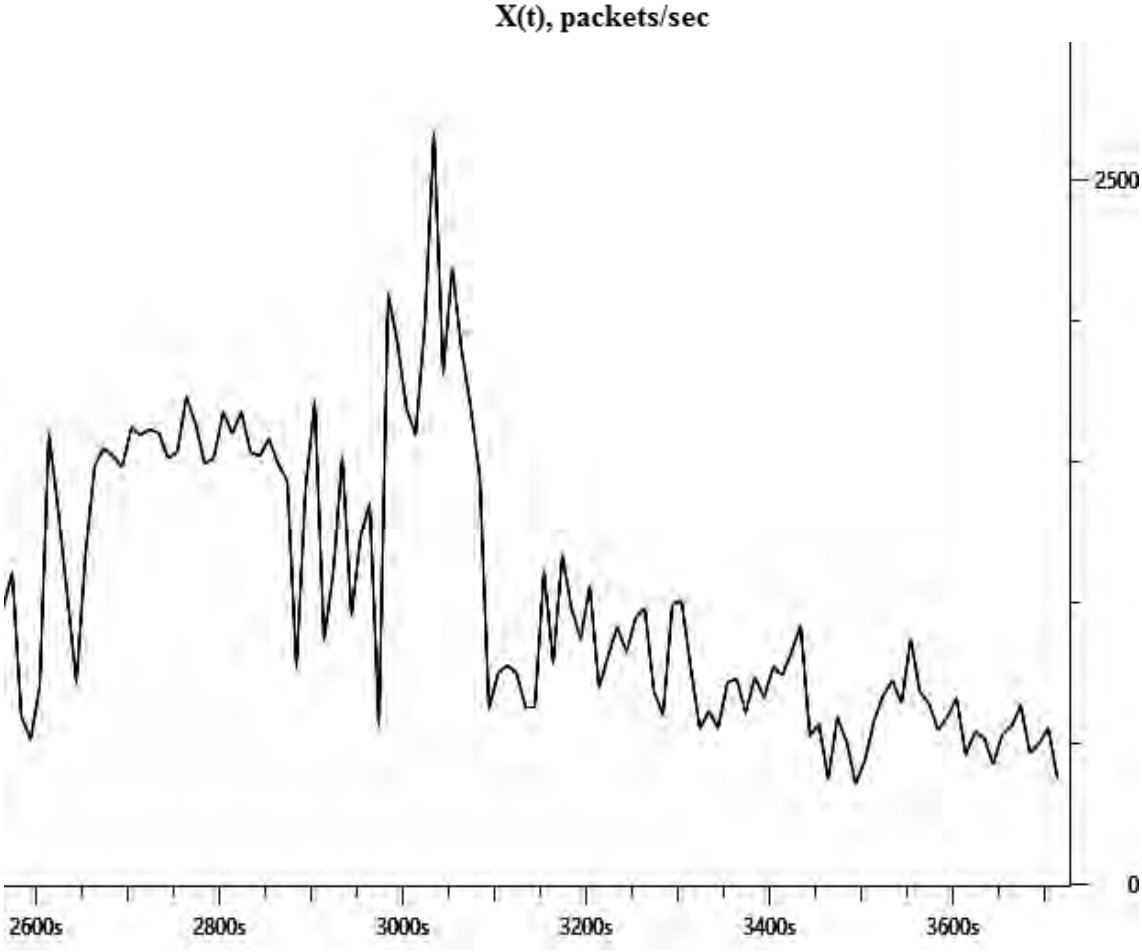

Рис. 3. Частина добового трафіку (16,6 хв.) комп'ютерної мережі кафедри АСУ в середовищі Wireshark

Оскільки Wireshark розпізнає структуру різноманітних мережевих протоколів, то він дозволяє розібрати пакет мережевого трафіку, показуючи значення всіх полів протоколу будь-якого рівня ієрархії. Для захоплення та зберігання пакетів використовуються функції бібліотеки pcap, також існує можливість захоплення інформації з тих мереж, які підтримуються даною бібліотекою. Проте аналізатор мережевих протоколів Wireshark вміє працювати із безліччю форматів початкових даних, тому можна переглядати файли даних, які були захоплені за допомогою інших програм та середовищ, що розширяє самі можливості захоплення даних.

Таблиця 1

Дані трафіку кафедри АСУ Національного університету "Львівська політехніка" за період 17.02–23.02.2015

17.02.2015		
Назва показника	НУ «ЛП» (день)	НУ «ЛП» (ніч)
Кількість пакетів	1635345	2340903
Тривалість захвату (сек)	21803, 687	21555,93
Середня к-ть пакетів/сек	108,597	75,003
Середній розмір пакета (байт)	792	692
Середня к-ть байт/сек	66052,059	31909,328
18.02.2015		
Назва показника	НУ «ЛП» (день)	НУ «ЛП» (ніч)
Кількість пакетів	1364822	575179
Тривалість захвату (сек)	21619,284	21595,292
Середня к-ть пакетів/сек	63,130	26,634
Середній розмір пакета (байт)	698	614
Середня к-ть байт/сек	44066,690	16340,517
19.02.2015		
Назва показника	НУ «ЛП» (день)	НУ «ЛП» (ніч)
Кількість пакетів	1781818	137184
Тривалість захвату (сек)	21345,855	21599,663
Середня к-ть пакетів/сек	79,738	6,351
Середній розмір пакета (байт)	755	471
Середня к-ть байт/сек	60185,722	2989,050
20.02.2015		
Назва показника	НУ «ЛП» (день)	НУ «ЛП» (ніч)
Кількість пакетів	1605884	274321
Тривалість захвату (сек)	21607,273	21574,014
Середня к-ть пакетів/сек	74,321	12,715
Середній розмір пакета (байт)	809	578
Середня к-ть байт/сек	60104,673	7357,042
21.02.2015		
Назва показника	НУ «ЛП» (день)	НУ «ЛП» (ніч)
Кількість пакетів	1537954	331872
Тривалість захвату (сек)	21651,566	21600,403
Середня к-ть пакетів/сек	71,032	15,364
Середній розмір пакета (байт)	704	344
Середня к-ть байт/сек	50029,882	5292,749
22.02.2015		
Назва показника	НУ «ЛП» (день)	НУ «ЛП» (ніч)
Кількість пакетів	422899	228289
Тривалість захвату (сек)	21655,512	21563,267
Середня к-ть пакетів/сек	19,528	10,587
Середній розмір пакета (байт)	689	273
Середня к-ть байт/сек	13451,908	2891,262
23.02.2015		
Назва показника	НУ «ЛП» (день)	НУ «ЛП» (ніч)
Кількість пакетів	869697	159097
Тривалість захвату (сек)	21597,469	21592,413
Середня к-ть пакетів/сек	40,268	7,368
Середній розмір пакета (байт)	621	617
Середня к-ть байт/сек	25021,540	4545,977

У цьому дослідженні було використано експериментальні дані трафіку комп'ютерної мережі (КМ) АСУ Національного університету "Львівська політехніка", отримані за допомогою середовища Wireshark. Проведено аналіз трафіку та обробку отриманих даних. Результати показані на рис. 4–8. На рис. 4 наведено дані сумарного трафіку КМ. На рис. 5 показана середня кількість пакетів трафіку. На рис. 6 та 7 відображено середній розмір пакета та середня швидкість передавання пакетів відповідно. Як видно з рис. 4 сумарний трафік істотно зменшується в кінці тижня (21.02. –22.02 – вихідні дні). На рис. 5 показано, що графік зміни середньої кількості пакетів має такий самий характер як графік сумарного трафіку. Рис. 6 демонструє малу залежність середнього розміру пакетів від завантаження мережі. Характер зміни швидкості переданання пакетів навпаки залежить від завантаження мережі (див. рис. 7). Швидкість передавання пакетів тим більша, чим менша завантаженість мережі, що видно на рис. 8. Для побудови графіку на рис.8 обчислювався коефіцієнт завантаження мережі як відношення швидкості передавання пакетів до сумарної кількості пакетів.

Сніфери загалом застосовуються і у позитивних, і в негативних цілях. Аналіз трафіку, який пройшов через таке програмне забезпечення, дозволяє побачити таке:

- зауважити паразитний або зациклений трафік, наявність котрого збільшує завантаження мережевого приладдя та каналів зв'язку (аналізатори тут малоефективні, проте у таких випадках, як правило, використовують дані різноманітної статистики, зібраними зі серверів та активного мережевого устаткування, та подальший аналіз);
- зауважити у комп'ютерній мережі шкідливе та несанкціоноване програмне забезпечення, (мережеві сканери, клієнти пірінгових мереж, троянські програми тощо. Як правило, це здійснюється за допомогою спеціалізованих аналізаторів мережевого трафіку – моніторів мережевої активності);
- захопити будь-який незашифрований (але інколи й зашифрований) користувацький трафік з метою отримати інформацію;
- локалізувати несправність комп'ютерної мережі або помилку в конфігурації мережевих агентів (для такої мети такі аналізатори мережевих протоколів доволі часто використовуються, зокрема системними адміністраторами).

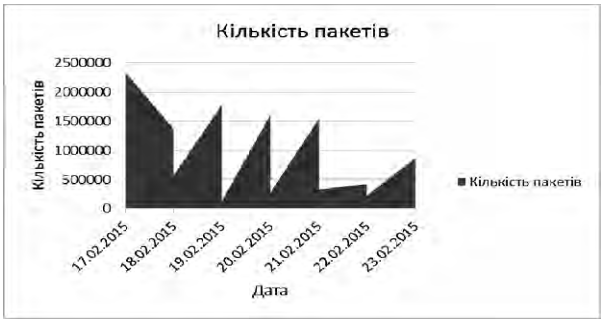

Рис. 4. Сумарна кількість пакетів трафіку комп'ютерної мережі

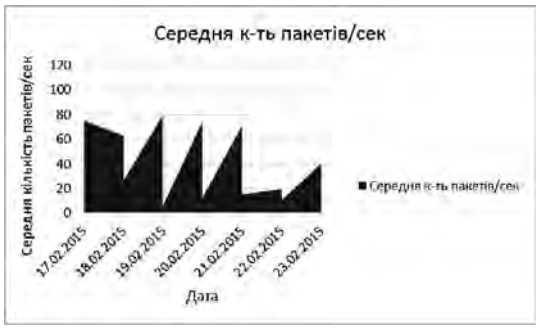

Рис. 5. Середня кількість пакетів трафіку комп'ютерної мережі

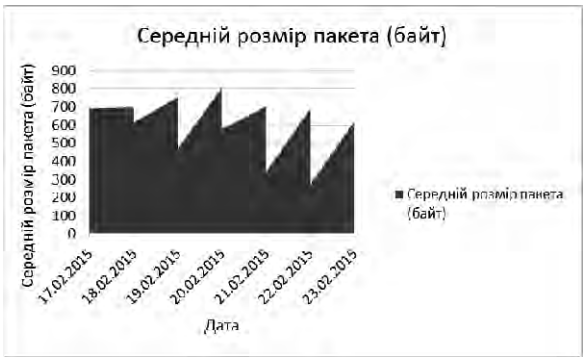

Рис. 6. Середній розмір пакета комп'ютерної мережі

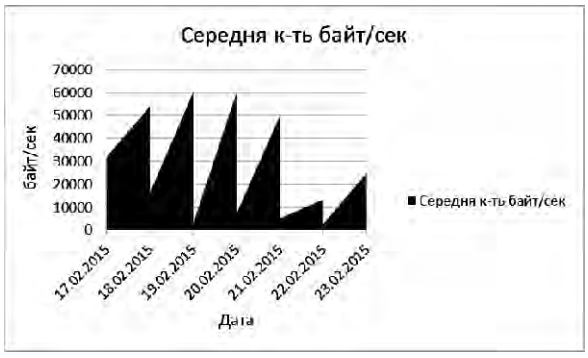

Рис. 7. Середня швидкість передавання пакетів комп'ютерної мережі

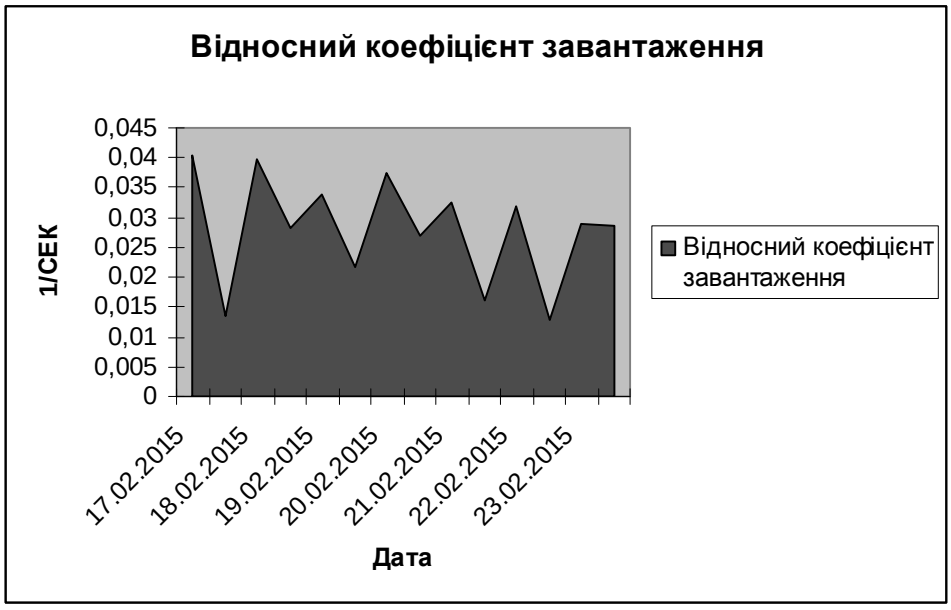

Рис. 8. Відносний коефіцієнт завантаження мережі

Wireshark має величезний набір функцій та різноманітних особливостей, які мають такі можливості [10]:

- Глибока перевірка протоколів, з більшою кількістю тих, котрі постійно додаються.
- Онлайн захоплення та оффлайн аналіз даних.
- Стандартний трипанельний пакет браузера.
- Мультиплатформа: Працює на Windows, OS X, FreeBSD, Linux, Solaris, NetBSD, та на багатьох інших операційних системах.
- Захоплений мережевий трафік може бути переглянутий за допомогою графічного інтерфейсу або завдяки TTY - режиму утиліти TShark.
- Містить найпотужніший дисплей фільтрів.
- Має потужний аналіз VoIP.
- Забезпечує зчитування / запис багатьох форматів файлів захоплення: TCPdump (Libpcap), Catapult DCT2000, Network General Sniffer (стислий і нестислий), Tektronix K12xx, Sniffer Pro, і NetXray, Network Instruments Novell LANalyzer, RADCOM WAN / LAN Analyzer, Observer, Shomiti / Finisar Surveyor, Visual Networks Visual UpTime, Pcap NG, WildPackets EtherPeek/ TokenPeek, Cisco Secure IDS IPLog, NetScreen Snoop, Microsoft Network Monitor, та багато інших.
- Захоплення файлів, які були стиснуті через Gzip, та можуть бути розпаковані миттєво.
- Оперативні дані можуть бути зчитані з Ethernet, PPP/HDLC, ATM, Bluetooth, Token Ring, IEEE 802.11, Frame Relay, FDDI, USB, та ін. (в залежності від платформи).
- Підтримка дешифрації для багатьох протоколів, зокрема IPsec, Kerberos, SNMPv3, WEP, WPA/WPA2, SSL / TLS, ISAKMP.
- Правила розфарбовування можуть бути застосовані в списках пакетів для швидкого та інтуїтивного аналізу.
- Вихідна інформація може бути виведена в файли типів CSV, XML, PostScript, або як звичайний текст.
- Wireshark не є системою для виявлення вторгнень. Він не попередить користувача про те, що хтось здійснює несанкціоновані речі в мережі. Однак, якщо це справді відбувається, середовище Wireshark допоможе зрозуміти, що ж насправді сталося в користувацькій комп'ютерній мережі.
- Wireshark не був створений з метою генерувати мережевий трафік, він здатен лише аналізувати існуючий. Загалом, Wireshark ніяк не показує себе в комп'ютерній мережі, окрім лише під час резолвінгу доменних імен, але й ця функція може бути вимкненою.

Висновки і перспективи подальших наукових розвідок

У цій статті проведено аналіз добового трафіку комп'ютерної мережі протягом одного місяця на основі безкоштовного програмного забезпечення для аналізу роботи мережі Wireshark. Проаналізовані основні можливості аналізатора, показані його переваги та недоліки. З метою дослідження мережі апробовано головні функції програмного забезпечення.

Результати досліджень візуалізовано та систематизовано у таблицях. Для таких показників, як сумарна кількість пакетів, середня кількість пакетів, середній розмір пакета та середня швидкість передавання пакетів, побудовано графіки. Обчислено також коефіцієнт завантаження мережі. Отримані результати планується використати у подальших дослідженнях, зокрема, для порівняння з теоретичними розробками для прогнозування добових коливань трафіку.

1. Басюк Т. М., Василюк А. С.Ранжування веб-сайтів в мережі Інтернет / Т. М. Басюк, А.С. Василюк // Вісник Нац. ун-ту "Львівська політехніка". – 2013. – № 770 : Інформаційні системи та мережі. – С. 3–12. 2. Федонюк А. А. Деякі аспекти моделювання соціальних мереж / А.А. Федонюк // Вісник Нац. ун-ту "Львівська політехніка". – 2014. – № 783 : Інформаційні системи та мережі. – С. 487–496. 3. Matychyn I. I., Onyshchenko V. V. "Modeling and analysis of traffic in telecommunication systems and networks," DUICT Announcer 2013 № 4, pp. 20–27. 4. Tsybakov B., Georganas N. Self-similar processes in communications IEEE Trans. Inform. Theory. vol. 44. – P. 1713–1725, Sep. 1998. 5. Tadeusz Czachórski, Ferhan Pekergin, "Diffusion Approximation as a Modelling Tool" Network Performance Engineering 2011: 447–476, 2010. 6. V. Klimenok, A. Dudin, V. Vishnevsky Tandem Queueing System with correlated Input and Cross-Traffic Proceeding of the 20th International Science Conference: Computer Networks CN 2013, 17–21 June 2013, Lwówek Śląski, Poland. – P. 416–425 .7. Ivanna Droniuk, Maria Nazarkevych, Olga Fedevych. "Asymptotic method of traffic simulation" Communications in Computer and Information Science. Springler 2014, Vol. 279. – P. 1–9. 8. Bogolyubov, N. N., Mitropolsky, Y. A. "Asymptotic methods in the theory of nonlinear oscillations." M. Izd. Fiz-Mat. Lit., 407 (1963). 9. P. Foremski "Mutrics: Multilevel traffic classification" [Електронний ресурс]. – Режим доступу: http://mutrics.iitis.pl/ 10. Wireshark.org [Електронний ресурс]. – Режим доступу: http://www.wireshark.org/docs/dfref.