УДК 004.075

В.В. ЖЕЛЄЗНЯК, О.А. МЯСІЩЕВ
Хмельницький національний університет

МЕТОД МОНІТОРИНГУ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ НА ОСНОВІ СПІЛЬНОГО АНАЛІЗУ ТИМЧАСОВИХ ТА ФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК СТЕКА ПРОТОКОЛІВ TCP / IP

У зв'язку з наявністю на даний момент часу недосконалих систем мережевого моніторингу (СММ), актуальною задачею є розробка нових засобів спостереження мережі, які будуть базуватися на тимчасових закономірностях в роботі стека протоколів TCP / IP. Відповідно, виникає потреба побудови досконалого методу моніторингу мережі, в якому будуть враховуватися недоліки теперішніх методів. Базуючись на застосованих подібних методах в задачах моніторингу мережі та забезпечення мережевої інформаційної безпеки, результатом є запропонований метод ідентифікації операційної системи (ІОС), заснований на спільному аналізі функціональних і часових характеристик стеку TCP/IP з використанням методів класифікації.

Ключові слова: моніторинг мережі, стек протоколів, ідентифікація операційної системи.

V.V. ZHELIEZNIAK, O.A. MYASISCHEV
Khmelnytsky National University

METHOD OF MONITORING COMPUTER NETWORKS BASED ON THE GENERAL ANALYSIS OF TEMPORARILY AND FUNCTIONAL CHARACTERISTICS OF THE TCP / IP PROTOCOL STACK

Wide dissemination of network monitoring systems in corporate and public information systems leads to the need to pay close attention to solving their inherent problems of uninterrupted and long-term functioning. As a result of the analysis carried out in the article the relevance of the development of methods and algorithms for monitoring computer networks (CN) based on the analysis of time patterns in the work of the TCP / IP protocol stack and the construction of a network monitoring system on their basis. As a result of the research carried out by the authors, it was concluded that the perspective direction of improving the technology of monitoring the computing network is the development of methods for analyzing the information environment, which are implemented through the mechanism of retransmissions. A comparative analysis is performed on the criteria listed for extracting TCP / IP functional values that are used by the corresponding methods of identification of the operating system (IOS). An analysis of the main characteristics of the TCP / IP protocol stack was performed, which resulted in the main values for the development of the method. Due to the presence of imperfect systems of network monitoring (SNM) at present, the actual task is the development of new network monitoring tools that will be based on the timing patterns in the TCP / IP protocol stack. Accordingly, there is a need to build a perfect network monitoring method that takes into account the shortcomings of the current methods. Based on similar methods used in network monitoring and network information security tasks, the proposed method for identifying an operating system based on a joint analysis of the functional and time characteristics of the TCP / IP stack using classification methods is the result.

Key words: network monitoring, protocol stack, identification of operating system.

Вступ. В останні роки важливе значення набувають питання діагностики інформаційних систем та розробки ефективних засобів моніторингу. Класичні системи моніторингу забезпечують безперервний моніторинг тільки поточного стану вузлів, що входять до складу обчислювальних мереж (ОМ). На даному етапі розвитку мережевих технологій пред'являються вимоги щодо забезпечення можливостей прогнозування і діагностики стану обслуговуваних інформаційних систем в короткостроковій і довгостроковій перспективах, а також реалізації комплексного моніторингу, що включає аналіз не тільки поточного стану вузлів ОМ, але і комплексний аналіз системи.

Актуальними проблемами розробки систем моніторингу мережі є збільшення точності аналізу стану входять до складу ОМ вузлів, тобто забезпечення максимальної відповідності показань системи моніторингу реального стану інформаційної системи, а також мінімізація впливу підсистеми моніторингу (підсистем забезпечення мережевої інформаційної безпеки) на функціонування інших підсистем та зменшення інтенсивності обміну службовим трафіком.

Оскільки необхідність підтримки систем в працездатному стані відіграє важливу роль, розподілені інформаційні системи набувають важливу роль, завданням яких є постійний контроль за роботою обчислювальної мережі, що становить основу будь-якого сучасного цифрового обчислювального комплексу або інший розподіленої системи.

Постановка задачі. Розробка методу моніторингу обчислювальної мережі на основі спільно аналізу тимчасових та функціональних характеристик стеку протоколів TCP/IP. Визначення факторів, що впливають на його роботу та проаналізувати його ефективність відносно різних операційних систем. Порівняти функціональні особливості вилучення значень функціональних характеристик TCP / IP.

Основна частина.

Автором пропонується метод ІОС, заснований на спільному аналізі тимчасових і функціональних характеристик стека протоколів TCP / IP (transmission control protocol/internet protocol) цільового вузла (далі – метод ATFK) і зберігає переваги – необхідність наявності тільки одного відкритого TCP-порту на цільовому вузлі , низький рівень споживання трафіку і низький ступінь виявлення системами IDS (Intrusion Detection System) [1–3].

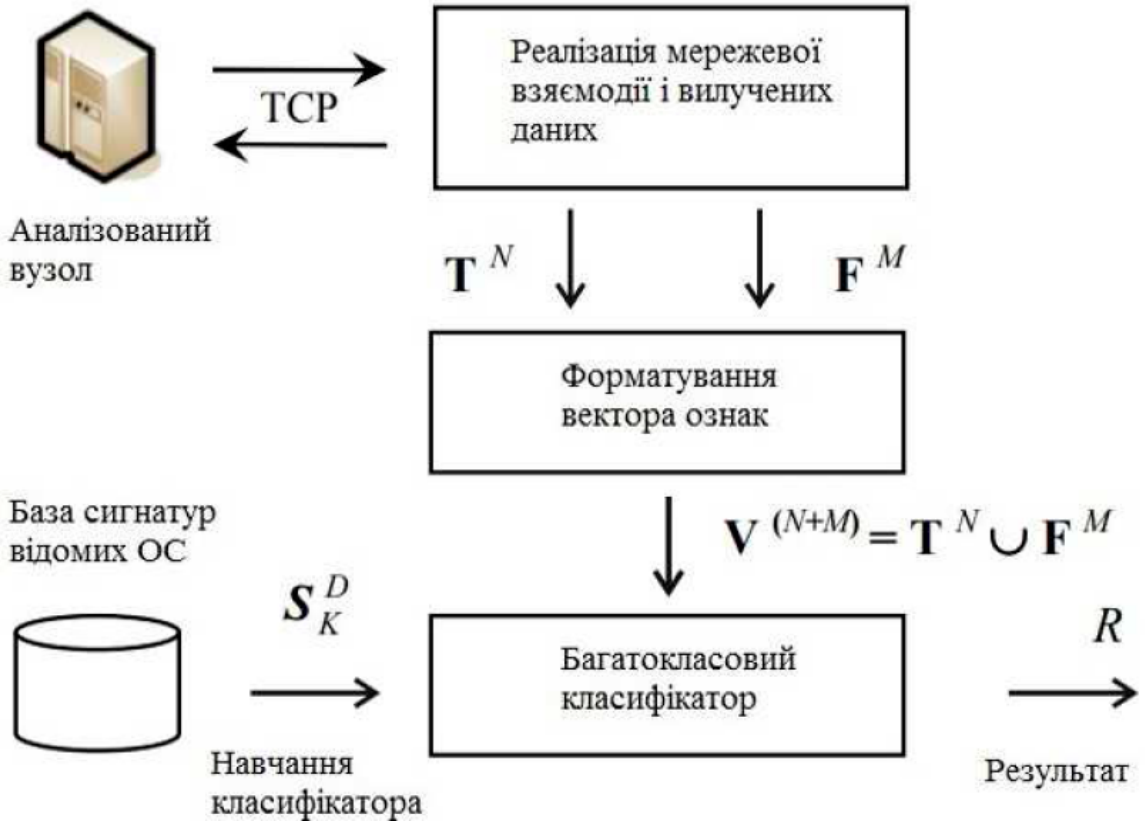

Рис. 1. Схема роботи методу ATFK

Для реалізації функцій ІОС ініціюється TCP-з'єднання з аналізованих вузлом і здійснюється збір значень тимчасових характеристик. Далі здійснюється збір функціональних характеристик TCP / IP. Вектори значень тимчасових характеристик T^N і розмірністю N і функціональних характеристик F^M розмірністю M об'єднуються в єдиний вектор ознак V^D розмірністю D, $D = N + M$, $V^D = T^D \cup F^M$, після чого вектор V^D передається для аналізу багатокласовому класифікатором, попередньо навченому на даних з еталонної бази сигнатур S_K^D. Результатом класифікації є номер R сигнатури з бази сигнатур, найбільш близькою до сигнатурі V^D. Версія ОС, відповідна результуючої сигнатурі R, є найбільш вірогідною версією ОС, що виконується на уже згадуваному вузлі.

Вибір набору використовуваних функціональних характеристик визначається функціональними вимогами, поставленими при розробці методу ATFK, а саме мінімізацією рівня споживання трафіку, прозорістю для систем IDS, система виявлення вторгнень і мінімізацією вимог по кількості відкритих і / або закритих портів TCP / UDP на цільовому вузлі. Для формування набору функціональних характеристик TCP / IP, що використовуються методом ATFK, проведено порівняльний аналіз за переліченими критеріями алгоритмів вилучення значень функціональних характеристик TCP / IP, що використовуються відповідними методами. Результати порівняльного аналізу представлені в таблиці 1.

Поставленим критеріям задовольняють алгоритми вилучення таких функціональних характеристик TCP / IP: розмір вікна TCP, опції TCP, значення тимчасової мітки, підтримка функцій ECN (Explicit Congestion Notification, повідомлення про перевантаженість в протоколі IP), значення біта дефрагментації, час життя пакета. Важливою особливістю перерахованих характеристик є можливість їх вилучення за допомогою аналізу пакету SYN-ACK, переданого цільовим вузлом в рамках процедури встановлення TCP-з'єднання. Таким чином, процедури вилучення значень функціональних і часових характеристик стека протоколів TCP / IP в рамках методу ATFK можуть бути об'єднані.

Відомо [4], що найважливішими показниками, що характеризують версію ОС і стека протоколів TCP / IP мережного вузла є розмір вікна і опції TCP, а також час життя пакета. Оскільки алгоритми вилучення значень перерахованих характеристик задовольняють вимогам, поставленим при розробці методу ATFK, аналіз даних характеристик в рамках методу ATFK за доцільне.

З метою визначення доцільності обробки в рамках методу ATFK значень тимчасової мітки і біта дефрагментації був проведений аналіз значень зазначених характеристик у складі пакету SYN-ACK більш ніж 40 різних версій ОС різних сімейств, включаючи Linux, Windows, FreeBSD, OpenBSD, NetBSD, Mac OS, Novell Netware, QNX, OS / 2, Solaris. В результаті дослідження встановлено такі факти:

Таблиця 1

Порівняльний аналіз функціональних особливостей ви лучення значень функціональних характеристик TCP / IP

Функціональна характеристика TCP / IP	Вимоги до наявності відкритих і закритих портів TCP / UDP	Кількість переданих пакетів; орієнтовний обсяг трафіку (байт)	Типи переданих пакетів	Прозорість для систем IDS
Розмір вікна TCP	Один відкритий порт TCP	2; 120	SYN SYN-ACK	Висока
Опції TCP		2; 120	SYN SYN-ACK	Висока
Алгоритм формування ISN		Не менше 6; не менше 360	SYN SYN-ACK	Низька
Значення тимчасової мітки		2; 120	SYN SYN-ACK	Висока
Підтримка TCP Overlap		Не менше 6; не менше 400	SYN SYN-ACK ACK Дані	Висока
Накопичувальне вікно TCP		Не менше 5; не менше 300	SYN SYN-ACK ACK Дані	Висока
Підтримка ECN		2; 120	SYN SYN-ACK	Висока
Значення біта дефрагментації	Не потрібно або один відкритий порт TCP	Не менше 2; не менше 120	SYN-ACK або ICMP echo-запит / echo-відповідь	Середня
Час життя пакету				Висока
Спосіб формування ідентифікатора заголовка IP	Один відкритий порт TCP	Не менше 6; не менше 300	SYN SYN-ACK	Низька

1. Біт дефрагментації не встановлюють такі ОС: деякі версії OpenBSD (зокрема версії 5.5, 6.0, 6.2), OS / 2 Warp 4, QNX 6.3, а також Windows Server 2012.

2. У разі підтримки тимчасових міток нульове значення тимчасової мітки встановлюють такі ОС: QNX 6.3, Windows 7, Windows Server 2012, Windows 10. Інші ОС встановлюють значення тимчасової мітки, відмінне від нуля [7].

Оскільки перелічені ОС в порівнянні з іншими проаналізованими ОС характеризуються розрізняються значеннями основних функціональних характеристик (набору опцій, розміру вікна і часу життя пакета), їх ідентифікація з використанням методу ATFK може бути виконана з високою ступенем достовірності, що не залежить від обліку значень біта дефрагментації і тимчасової мітки. Таким чином, включення значень тимчасової мітки і біта дефрагментації до складу аналізованих функціональних характеристик стека протоколів TCP / IP в рамках методу ATFK не є необхідним [10].

Аналіз підтримки функцій ECN не проводився. Сучасні реалізації стека протоколів TCP / IP забезпечують підтримку ECN, але дана функція є/відключається, що дозволяє користувачам вручну управляти її використанням [4]. Таким чином, факт наявності або відсутності підтримки ECN не є відмінною характеристикою конкретної реалізації стека протоколів TCP / IP і версії ОС, в зв'язку з чим використання даної характеристики в рамках методу ATFK не є доцільним.

На основі вищесказаного сформовано перелік функціональних характеристик стека протоколів TCP / IP, що використовуються для аналізу в рамках методу ATFK, до складу якого такі характеристики TCP / IP: набір опцій і порядок їх оголошення, розмір вікна TCP, час життя пакета (TTL). Додатково до складу аналізованих функціональних характеристик включено також значення опції масштабування вікна (Window Scale, WS). Встановлено, що в разі підтримки відповідної опції значення WS може бути нульовим, або відмінним від нуля і динамічно встановлюються ОС. При цьому в ряді випадків різні версії ОС можуть відрізнятися методом ATFK, які оперують перерахованими вище функціональними характеристиками, тільки за умови врахування значення WS (зокрема, це справедливо для ОС Linux 14.04 і Linux 16.04), що свідчить про доцільність окремого обліку значення даного параметра [5].

Виходячи з вищесказаного вектор функціональних характеристик TCP / IP, аналізованих в рамках методу ATFK, виглядає наступним чином:

$$F = \{T, K, S, 0\}$$

де T – значення часу життя пакета (TTL);

K – характеристика використання аналізованих стеком протоколів TCP / IP функції масштабування вікна;

S – значення розміру вікна TCP;

O – код набору опцій (кожної унікальної послідовності опцій TCP ставиться у відповідність цілочисельний порядковий номер) [9].

Діапазони допустимих значень і типи даних, що відповідають параметрам вектора функціональних характеристик, представлені в таблиці 2.

Таблиця 2

Типи даних і діапазони допустимих значень параметрів вектора функціональних характеристик TCP/IP [8]

Параметр	Тип даних	Діапазон значень
T – час життя пакету	Беззнаковий символьний (unsigned char)	0..255
K – характер використання опції масштабування вікна	Символьний (char)	-1..1 (-1 - опція WS не використовується; 0 – значення WS дорівнює нулю; 1 – значення WS відмінно від нуля)
S – розмір вікна TCP	Беззнакове коротке ціле (unsigned short)	0..65535
O – код набору опцій (порядковий номер у базі сигнатур)	Те ж	1..65535

Висновки

Найважливішими характеристиками методу є мінімізація рівня споживання трафіку, прозорістю для систем IDS, система виявлення вторгнень і мінімізацією вимог по кількості відкритих і / або закритих портів TCP / UDP на цільовому вузлі [6].

Запропоновано метод ІОС, заснований на спільному аналізі функціональних і часових характеристик TCP / IP з використанням методів класифікації, що відрізняється низьким споживанням трафіку і використанням тільки стандартних мережевих пакетів. Результати дослідження свідчить про перевагу алгоритму ATFK в порівнянні з існуючими активними методами ІОС, які отримали практичне застосування, за критеріями достовірності результатів і обсягом споживаного мережевого трафіку.

Сьогодні, мережевий моніторинг являю собою невід'ємну частину функціонування обчислювальних мереж. Розробка нових методів та алгоритмів є перспективною, оскільки технічний прогрес є досить швидкім. Удосконалення методів у цій сфері є досить актуальним.

Література

1. Лавров А. А. Метод идентификации версии системного программного обеспечения удаленного сетевого узла, основанный на комплексном анализе характеристик TCP/IP / А. А. Лавров, А. К. Большее // Известия СПбГЭ-ТУ «ЛЭТИ». – 2012. – № 1. – С. 45–51.

2. Лавров А. А. Идентификация ОС удаленного сетевого узла на основе комплексного анализа характеристик стека TCP/IP / А. А.Лавров, А. К. Большее, В. В. Яновский // Материалы VII международной научно-практической конференции «Перспективные разработки науки и техники». Przemysl, 07–15 ноября 2011. – Sp. z o.o. «Nauka I studia», 2011. – Т. 53. – С. 13–15.

3. Лавров А. А. Метод идентификации ОС удаленного узла на основе анализа функциональных и временных характеристик стека TCP/IP / А. А. Лавров // Сборник трудов XVII Международной открытой научной конференции «Современные проблемы информатизации в анализе и синтезе технологических и программно-телекоммуникационных систем» Воронеж, ноябрь 2011 – январь 2012. – Воронеж : Изд-во «Научная книга», 2012. – Вып. 17. – С. 271–273.

4. Lyon G. F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning / G. F. Lyon. – Nmap Project, 2009.

5. Кореньков В. В. История развития технологий мониторинга информационных систем / В. В. Кореньков, А. В. Ужинский // Системный анализ в науке и образовании. – 2007. – № 1. – С. 36–49.

6. Олифер Н. А. Средства анализа и оптимизации локальных сетей / Н. А. Олифер, Н. Г. Олифер. – М. : Центр Информационных Технологий, 1998.

7. Лавров А. А. Мониторинг и администрирование в корпоративных вычислительных сетях : монография / С. А. Ивановский, А. А. Лавров, В. В. Яновский. – СПб : Изд-во «СПбГЭТУ «ЛЭТИ», 2013. – 160 с.

8. Шыхалиев Р. Г. О применении интеллектуальных технологий в мониторинге компьютерных сетей

/ Р. Г. Шыхалиев // Informasiya Texnologiyalan Problembri. – 2011. – № 2. – С. 82–90.

9. Лавров А. А. Алгоритмы классификации в задаче идентификации версии ОС удаленного сетевого узла / А. А. Лавров // Сб. тр. 65-й науч.-техн. конф. проф.-преп. состава СПбГЭТУ «ЛЭТИ». – СПб, 2012. – С. 102–106.

10. Ермаков А. В. Использование сетевого сканера для повышения защищенности корпоративной информационно-вычислительной сети / А. В. Ермаков. – М., 2001. – 16 с. – (Препринт / Институт прикладной математики им. М. В. Келдыша РАН; № 61).

References

1. Lavrov A. A. Metod identifikacii versii sistemnogo programmnogo obespechenija udalennogo setevogo uzla, osnovannyj na kompleksnom analize harakteristik TCP/IP / A. A. Lavrov, A. K. Bol'shee // Izvestija SPbGJe-TU «LJeTI». - 2012. - № 1. - S. 45-51.

2. Lavrov A. A. Identifikacija OS udalennogo setevogo uzla na osnove kompleksnogo analiza harakteristik steka TCP/IP / A. A.Lavrov, A. K. Bol'shee, V. V. Janovskij // Materialy VII mezhdunarodnoj nauchno-prakticheskoj konferencii «Perspektivnye razrabotki nauki i tehniki». - Przemysl, 07-15 nojabrja 2011 g. - Sp. z o.o. «Nauka I studia», 2011. - 53 t. - S. 13-15.

3. Lavrov A. A. Metod identifikacii OS udalennogo uzla na osnove analiza funkcional'nyh i vremennyh harakteristik steka TCP/IP / A. A. Lavrov // Sbornik trudov XVII Mezhdunarodnoj otkrytoj nauchnoj konferencii «Sovremennye problemy informatizacii v analize i sinteze tehnologicheskih i programmno-telekommunikacionnyh sistem». - Voronezh, nojabr' 2011 g. - janvar' 2012 g. - Voronezh: Izd-vo «Nauchnaja kniga», 2012. - Vyp. 17. - S. 271-273.

4. Lyon G. F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning / G. F. Lyon. - Nmap Project, 2009.

5. Koren'kov V. V. Istorija razvitija tehnologij monitoringa informacionnyh sistem / V. V. Koren'kov, A. V. Uzhinskij // Sistemnyj analiz v nauke i obrazovanii. - 2007. - № 1. - S. 36-49.

6. Olifer H. A. Sredstva analiza i optimizacii lokal'nyh setej / N. A. Olifer, N. G. Olifer. - M.: Centr Informacionnyh Tehnologij, 1998.

7. Lavrov A. A. Monitoring i administrirovanie v korporativnyh vychislitel'nyh setjah: monografija / S. A. Ivanovskij, A. A. Lavrov, V. V. Janovskij. - SPb.: Izd-vo «SPbGJeTU «LJeTI», 2013 - 160 s.

8. Shyhaliev R. G. O primenenii intellektual'nyh tehnologij v monitoringe komp'juternyh setej / R. G. Shyhaliev // Informasiya Texnologiyalan Problembri. - 2011. - № 2. - S. 82-90.

9. Lavrov A. A. Algoritmy klassifikacii v zadache identifikacii versii OS udalennogo setevogo uzla / A. A. Lavrov // Sb. tr. 65-j nauch.-tehn. konf. prof.-prep. sostava SPbGJeTU «LJeTI». - SPb., 2012. - S. 102-106.

10. Ermakov A. V. Ispol'zovanie setevogo skanera dlja povyshenija zashhishhennosti korporativnoj informacionno-vychislitel'noj seti / A. V. Ermakov. - M., 2001. - 16 s. (Preprint / Institut prikladnoj matematiki im. M. V. Keldysha RAN; № 61).

Рецензія/Peer review : 13.10.2017 р. Надрукована/Printed :26.01.2018 р.
Рецензент: д.т.н. проф. Сорокатий Р.В.