УДК 681.3 DOI: 10.18372/2073-4751.74.17881

Кулаков Ю.О., д.т.н.,
orcid.org/0000-0002-8981-5649,
Обозний Д.М.,
orcid.org/0000-0003-0108-4587

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ТРАФІКУ DPI В МЕРЕЖАХ SDN

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

ya.kulakov@gmail.com

Вступ

Основними, найбільш поширеними технологіями, що дозволяють здійснювати обмін інформацією по всьому світу, є розподілені мережеві протоколи керування та транспортування. Незважаючи на їх поширення, традиційні IP- мережі є складними в конфігурації та управлінні. Вони потребують налаштування кожного мережевого пристрою окремо, з використанням команд низького рівня, часто специфічними для окремого постачальника. Окрім цього, механізми автоматичної зміни конфігурації практично відсутні, тому таке мережеве середовище не стійке до збоїв та змін навантаження.

Ще одним чинником, що ускладнює роботу розподілених мереж є їх вертикальна інтегрованість. Тобто, функціонал обробки та передачі трафіку об'єднані всередині мережевих пристроїв. Це у свою чергу зменшує гнучкість підходу, а також ускладнює розвиток такої мережевої інфраструктури.

Варто згадати, що у 2008 році розпочався перехід від IPv4 до IPv6, який свідчить про цю проблему, хоча насправді IPv6 являв собою лише оновлення протоколу. Планувалось, що період цієї трансформації буде тривати декілька років, але він і досі в основному не завершений.

Виходячи з цього прикладу, процес переналаштування архітектури Інтернету (наприклад, заміна IP) вважається важким завданням – просто нездійсненним на практиці [1]. Зрештою, ця ситуація призвела до збільшення капітальних та експлуатаційних витрат на роботу IP-мережі.

Існуючі мережі, архітектура яких має деревоподібну структуру, тобто кілька видів статичних комутаторів Ethernet, мають недостатню потужність для того, щоб задовольнити великі обсяги моделей трафіку, наприклад, віртуалізація серверів, обробка великих обсягів даних, хмарні обчислення чи мобільні додатки з великою кількістю користувачів [4]. У свою чергу, новітні інфраструктури повинні забезпечити високу продуктивність, енергоефективність, надійність та масштабованість мережі з наданням універсальних цифрових послуг, які забезпечують суворі гарантії якості обслуговування (QoS). Для реалізації загально-мережевих політик і підтримки будь-яких нових послуг, сьогодні доводиться налаштовувати тисячі мережевих пристроїв і протоколів, що ускладнює застосування узгодженого набору QoS, безпеки та інших політик. [2] Проведений аналіз літературних джерел показав, що існуючі протоколи, як правило, побудовані ізольовано під вирішення конкретних задач без фундаментальних абстракцій.

Підтримка та обслуговування мережі ускладнюється додаванням тисяч пристроїв, що мають власні технології керування, пересилання даних. Лише невелика кількість інтерфейсів стандартизована, більшість потребує унікального підходу [3].

Сукупність цих факторів спонукало до пошуку нового рішення для побудови мережевого обладнання, що дозволяє динамічно зв'язувати елементи пересилання та керування технологій.

Мета

Метою даної роботи є огляд технології побудови мереж SDN та розпізнавання видів трафіку на базі технології SDN.

Для досягнення мети будуть розглянуті такі теми:

- Передумови виникнення технології SDN
- Архітектурні особливості в порівнянні з класичними мережами
- Методи розпізнавання трафіку та порівняння різних застосунків
- Вразливості мереж SDN

Необхідно проаналізувати існуючі рішення в сфері розпізнавання шифрованого трафіку, який є найбільш популярний в сучасних мережах. Порівняти алгоритми розпізнавання, швидкість їх роботи та точність розпізнавань. Дослідити вразливості та потенційні рішення в сфері безпеки мереж SDN.

Основна частина

Програмно-конфігуровані мережі – це передова парадигма в сфері комп'ютерних мереж, яка дозволяє вирішувати проблеми наявні в сучасних мережах. З плином часу розвиток віртуалізації операційних систем та абстракцій операційних систем дав можливість перейти від апаратних мережевих пристроїв до їх віртуальних аналогів, які можуть бути розгорнуті на будь-якому пристрої, який має достатню кількість ресурсів. Тобто площина мережі ділиться на 2 структури: рівень передачі мережевого трафіку та рівень управління мережею. [5] Такий підхід спрощує масштабування мережі проте виникають нові проблеми. Рівень управління мережею (data plane) повинен мати гарантії доступності, бути відмовостійким.

Взаємодія між рівнем управління мережею та рівнем передачі відбувається за допомогою чітко визначених програмних інтерфейсів (API). Найбільш популярним протоколом взаємодії є OpenFlow. Кожен з комутаторів в мережі має одну чи декілька таблиць потоків. Такі таблиці визначають дії які повинні відбуватись з підмножиною пакетів, які відносяться до потоку: пересилання, зміна, відкидання тощо. За допомогою абстракції реалізованій в протоколі SDN Openflow, пристрої на рівні передачі даних можуть виконувати різні ролі: комутатор, маршрутизатор, брандмауер, балансувач навантаження тощо.

Тож за рахунок абстракції, визначення певних ролей та розвитку віртуалізації кожен з умовних рівнів вирішує поставлені задачі: рівень передачі даних вирішує безумовну передачу потоків пакетів згідно з таблицями обробки, рівень управління вирішує задачу управління та спостереження за мережею, та її реконфігурацію. Це дозволяє більш ефективно здійснювати передачу даних та мати більш вищий рівень доступності мережі аніж з класичними підходами.

Методи розпізнавання трафіку

Однією з причин виникнення комп'ютерних мереж була необхідність передачі інформації. Спочатку інформація була строго класифікована та для кожного з таких типів були введені окремі протоколи прикладного рівня, що використовують певний протокол транспортного рівня та порт. Наприклад для синхронізації часу за допомогою протоколу NTP використовується транспортний протокол UDP та 123 порт. Кожна ОС побудована на базі UNIX має цей список у файлі /etc/protocols. Проте з розвитком мережі інтернет та RPC деякі з протоколів стали "універсальними". Одним з таких є протокол HTTP та його шифрована версія HTTPS.

Сьогодні задачі протоколу HTTP та HTTPS є більш розширеними аніж передача гіпертекстових документів. За рахунок гнучкості заголовків та MIME специфікації протокол використовується в цілях, для яких були створені інші протоколи. Прикладом може слугувати протокол FTP для передачі файлів, який зараз при певних умовах може бути замінений протоколом HTTP. Це дає розуміння, що класичне співставлення пари "транспортний протокол - порт" не може більше слугувати критерієм для розпізнавання мережевого трафіку. Натомість почався розвиток нової технології докладного аналізу пакетів (Deep Packet Inspection, DPI), яка

піддає аналізу не лише заголовки пакетів, а й їх вміст. Першими компаніями, які почали дослідження в цій сфері стали Cisco з їх пропрієтарним протоколом NBAR та Palo Alto Networks фаєрволи з розпізнаванням додатків.[6] Проте технологія DPI потребує великої кількості ресурсів, тому що зачасту базується на технологіях машинного навчання. Деякі з авторів заявляють, що такого роду алгоритми забезпечують високу точність в розпізнаванні, проте реальні тести показують, що часту такі протоколи мають низку проблем [7]:

- Здатні класифікувати лише частину видів трафіку
- Деякі з тестів показують низьку точність розпізнавання
- Ціна комерційних бібліотек є дуже великою, як і підтримка. Також комерційна пропозиція може засновуватись на розмірі прибутку компанії.

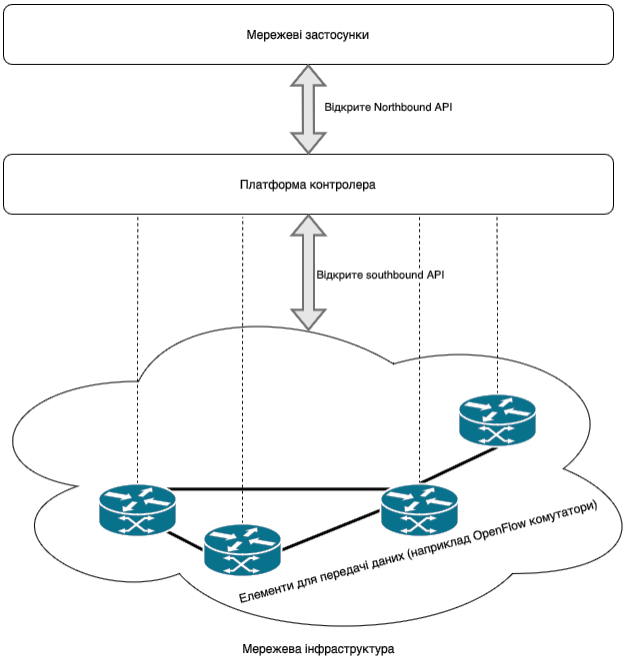

Рис. 1. Архітектура SDN

Порівняння застосунків для розпізнавання трафіку

Дослідники відзначають, що при порівнянні різних інструментів (PACE, OpenDPI, L7-filter, nDPI, Libprotoident і NBAR) з класифікації мережевого трафіку найкращі результати має PACE, проте він має закритий код. Серед застосунків з відкритим кодом гарні результати дає nDPI та Libprotoident. Для об'єктивності порівняння був сформований набір даних, який містить більше 750 тис. потоків трафіку 22 програм загальним об'ємом 51.93 Гб. [6] На відміну від PACE, nDPI, Libprotoidebt такі технології, як NBAR та L7-filter показують дещо нижчий рівень розпізнавання трафіку, що робить їх не рекомендованими до роботи. Не зважаючи на це постійний розвиток застосунків, виникнення нових видів трафіку зумовлює й потребу в розвитку систем розпізнавання трафіку.

Вразливість SDN

З розвитком SDN технологій, з'являються нові способи атак, які дозволяють викрасти дані користувачів. Більшість атак можна поділити за рівнями мережевих моделей [8]. Найбільш цікавим з точки зору SDN є атаки на рівень контролю [9]. На рис. 2 зібрані потенційні атаки на мережу SDN, що показані на її різних архітектурних рівнях. В табл. надано порівняльний аналіз основних атак, спрямованих на мережу SDN та їх аналоги в класичних мережах. Як бачимо основні атаки мереж SDN мають свої аналоги в класичних мережах [15]. Більшість атак мають спільний характер, проте вектор та ціль таких атак все ж відрізняється. Це зумовлено розділенням структури SDN мережі на рівні.

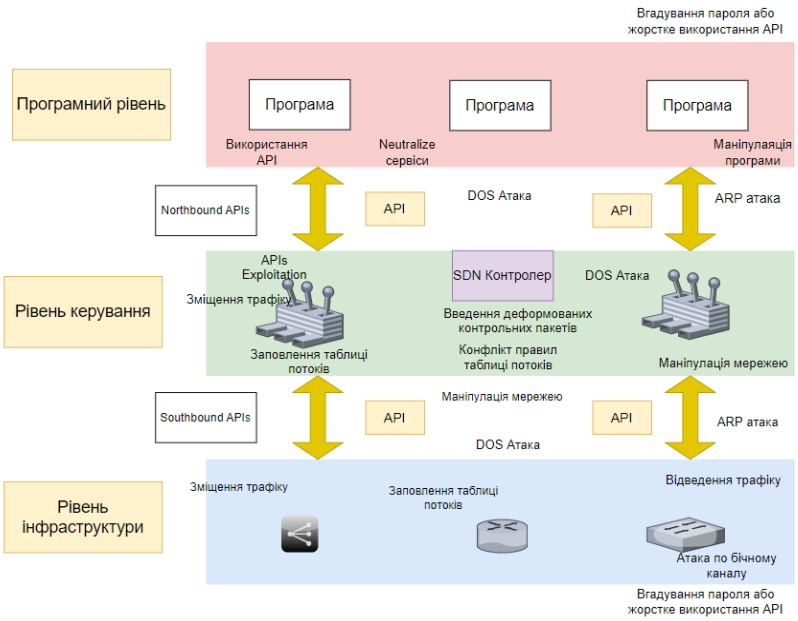

Рис. 2. Атаки на мережу SDN

Таблиця. Порівняльний аналіз атак

Вид атаки	Потенційна загроза	Аналог атаки в звичайній мережі
DOS/DDoS	DoS/DDoS-атаки можуть вплинути на рівень керування, рівень даних або канал зв'язку. Атака на пристрій в площині управління може призвести до збою всієї мережі, тоді як атака на пристрій у площині даних або канал зв'язку призводить до скидання пакетів і недоступності мережі. [10]	Механізм атаки схожий та відбувається за рахунок відсилання великої кількості пакетів даних, обробка яких забирає на себе усі ресурси пристроя, що призводить до того, що пристрій перестає передавати пакети клієнтів
API	Зловмисник може отримати доступ до даних мережі через вразливі програмні компоненти API. Ціллю такої атаки можуть бути викриття обміну інформацією між рівнем керування та прикладним рівнем, а також припинення роботи конкретної програми.[11,12]	Пристрої в класичній мережі зазвичай мають менше API компонентів, тому вектор атаки дуже рідко спрямований в цьому напрямку.
Конфлікт правил таблиці потоків	Зловмисники можуть атакувати компоненту задання правил, та створювати нові правила до таблиці потоків, що викликатимуть конфлікти з існуючими.Це може призвести до скидання або блокування деяких пакетів даних у мережі та конфлікту в мережевих політик.	Однією з відповідних атак є BGP hijacking [13], що полягає в підміні маршрутів в таблиці маршрутизації на рівні провайдерів. Це призводить до перенаправлення трафіку та конфліктів в таблицях маршрутизації
Переповнення таблиці потоків	Атака виконується випадковим надсиланням великої кількості пакетів. Оскільки розмір таблиці потоків обмежений, то такі дії переповнюють її, що впливає на продуктивність контролера через велику кількість пакетів, які потрібно адресувати	Одним з аналогів є CAM Table Overflow [14] Принцип цієї атаки у тому, щоб викликати переповнення комутаційної матриці. У разі чого комутатор, г перетворюється на хаб і починає розсилати кадри, що надходять, у всі порти, що викликає ідеальні умови для перехоплення трафіку. При заповненні таблиці MAC-адрес зловмисник зможе бачити всі кадри, що розсилаються, з усіх портів.

Висновки

На основі відомих джерел інформації можна зробити висновок, що технології SDN є актуальними та дозволяють побудувати мобільні мережі великої розмірності, задовольняючи високий рівень відмовостійкості.

В роботі було проаналізовано різні вектори атак та потенційних вразливостей в мережах SDN, а також порівняння з вразливостями класичних мереж.

Отримані дані показують, що для побудови відмовостійкої мережі SDN, як і в класичній мережі, потрібно мати альтернативні канали зв'язку. З поширенням різних видів медіа трафіку, шифрування та використання VPN, класичний QoS підхід працює не завжди ефективно. Збільшення кількості способів використання протоколу HTTP та HTTPS ускладнює задачу розпізнавання. Цю проблему вирішує підхід DPI, в основі якого лежить логіка різних алгоритмів співпадіння (наприклад алгоритм Бойера Мура). Інтеграція цієї технології в SDN дозволяє на програмному рівні аналізувати аномалії, змінювати traffic flow таблиці, що в свою чергу призведе до змін показників обладнання на інфраструктурному рівні.

Література

1. Kreutz D., Ramos F., Veríssimo P., Esteve Rothenberg C., Azodolmolky S., Uhlig S. Software-Defined Networking: A Comprehensive Survey. 2014. 61 p.

2. Hakiri A., Gokhale A., Berthou P., Schmidt D., Gayraud T. Software-Defined Networking: Challenges and research opportunities for Future Internet. *Computer Networks*. 2014. V. 74. P. 453–471.

3. Thomas D. Nadeau, Ken Gray. Software defined networks. O'Reilly Media, 2013. 384 p.

4. SDN: A Definition. URL: https://sdn.systemsapproach.org/intro.html#sdn-a-definition

5. Mendiola Alaitz, Astorga Jasone, Jacob Eduardo, Higuero Marivi. A Survey on the Contributions of Software-Defined Networking to Traffic Engineering. *IEEE Communications Surveys & Tutorials*. 2017. V. 19, Iss. 2. P. 918–953.

6. Deri Luca, Martinelli Maurizio, Bujlow Tomasz, Cardigliano Alfredo. NDPI: Open-source high-speed deep packet inspection. *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)* / Nicosia, Cyprus, 2014. P. 617–622.

7. Bujlow Tomasz, Carela-Español Valentín, Barlet-Ros Pere. Independent comparison of popular DPI tools for traffic classification. *Computer Networks*. 2015. V. 76. P. 75-89.

8. Alhaj Ali, Dutta Nitul. Analysis of Security Attacks in SDN Network: A Comprehensive Survey. C*ontemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems*. 2022. V. 281. P. 27–37.

9. Lubna Fayez Eliyan, Roberto Di Pietro. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*. 2021. V. 122. P. 149–171.

10. Agrawal N., Tapaswi S. An SDN-Assisted Defense Mechanism for the Shrew DDoS Attack in a Cloud Computing Environment. *Journal of Network and Systems Management*. 2021. V. 29, Iss.2. 12.

11. Dover Jeremy M. A denial of service attack against the Open Floodlight SDN controller. Research report. 2013. 8 p.

12. Feghali A., Kilany R., Chamoun M. SDN security problems and solutions analysis. *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)* / Paris, France, 2015. P. 1–5.

13. Cho Shinyoung, et al. BGP hijacking classification. *2019 Network Traffic Measurement and Analysis Conference (TMA)* / Paris, France, 2019. P. 25-32.

14. Trabelsi Zouheir. Switch's CAM table poisoning attack: hands-on lab exercises for network security education. *Proceedings of the Fourteenth Australasian Computing*

Education Conference. 2012. V. 123. P. 113–120.

15. Elsayed Mahmoud Said, et al. Ddos-net: A deep-learning model for detecting network attacks. *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* / Cork, Ireland, 2020. P. 391–396.

Кулаков Ю.О., Обозний Д.М.

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ТРАФІКУ DPI В МЕРЕЖАХ SDN

В роботі розглянуто передумови виникнення програмно-визначених мереж SDN, що сьогодні користуються неабияким попитом.

Метою роботи є огляд технології побудови мереж SDN та розпізнавання видів трафіку на базі технології SDN. Проаналізувати існуючі рішення в сфері розпізнавання шифрованого трафіку, який є найбільш популярний в сучасних мережах. Порівняти алгоритми розпізнавання, швидкість їх роботи та точність розпізнавань. Дослідити вразливості та потенційні рішення в сфері безпеки мереж SDN.

Авторами запропоновано подальше дослідження способів використання технології DPI в програмно-конфігурованих мережах з метою підвищення ефективності використання наявних каналів зв'язку.

Наведено результати порівняння систем розпізнавання трафіку та їх вразливостей в порівнянні з класичними мережами.

***Ключові слова**: програмно-конфігуровані мережі (SDN), розпізнавання трафіку, вразливість SDN, кіберзлочинність, технологія DPI, QoS.*

Kulakov Y.O., Oboznyi D.M.

DPI TRAFFIC CLASSIFICATION TECHNOLOGIES IN SDN NETWORKS: A SURVEY

The work considers the prerequisites for the emergence of software-defined SDN networks, which are in great demand today.

The purpose of the work is to review the technology of building SDN networks and recognizing types of traffic based on SDN technology. Analyze existing solutions in the field of recognition of encrypted traffic, which is the most popular in modern networks. Compare recognition algorithms, their speed of operation and recognition accuracy. Explore vulnerabilities and potential solutions in SDN security.

The authors suggested further research into ways of using DPI technology in software-configured networks in order to improve the efficiency of using existing communication channels.

The results of a comparison of traffic recognition systems and their vulnerabilities in comparison with classic networks are presented.

***Keywords**: software-defined networks (SDN), traffic classification, SDN vulnerability, cybercrime, DPI technology, QoS.*