УДК 621.382

МЕТОД ВИЯВЛЕННЯ DOS АТАК В SDN МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ ЕНТРОПІЇ ШЕННОНА

Валуйський С.В., Єфименко О.С.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: o.yefymenko@gmail.com

Method of DoS attacks detecting in SDN networks using Shannon entropy

The article describes the technology of DoS attacks detecting using the method of calculating the entropy for traffic to destination IP addresses. Entropy is calculated by the Shannon formula, based on the analysis of the entropy value SDN controller redistributes the traffic between the scanners and changes the monitoring time intervals. This is how the DoS attacks are detected and further counteracted.

У статті описана технологія виявлення DoS-атак за допомогою методу обчислення ентропії трафіку до IP-адрес призначення. Ентропія обчислюється за формулою Шеннона, на основі аналізу значення ентропії контролер SDN перерозподіляє трафік між сканерами та змінює інтервали моніторингу часу. Таким чином здійснюється виявлення та протидія атакам DoS.

Централізоване управління є головною перевагою SDN, але у той же час і єдиною точкою відмови у разі виходу його із ладу. Однією з найпоширініших причин, яка може вивести з ладу контроллер SDN – це атаки DDoS, які можуть використовувати потенційні вразливості в контролері SDN [1], [2]. В даній статті пропонується метод побудови система виявлення вторгнень, що дозволить ефективно виявляти та протидіяти DdoS атакам в SDN мережі.

Запропонована система виявлення вторгнень складається з двох мережевих комутаторів (switches), основного SDN контролера та деякої кількості процесорів для обробки пакетів (сканерів), як показано на рисунку 1. Мережеві комутатори (S_1 та S_2) представляють собою вхідну та вихідну точки системи виявлення вторгнень. Мережевий комутатор S_1 відповідає за розподілення трафіку, який надходить до системи виявлення вторгнень із зовнішньої мережі, а S_2 збирає трафік від сканерів та направляє трафік до внутрішньої мережі. Коли трафік надходить до системи виявлення вторгнень, він пропускається через процесори для обробки пакетів (P_1, P_2...P_n).

Даний метод використовує тільки інформацію, що зберігається в адресному полі мережевого рівня PDU (protocol data unit моделі OSI), тож

система не повинна бути пакетно-орієнтованою, також не потрібно проводити глибоке дослідження пакетів. Кожний сканер обробляє вхідний трафік та визначає атаку, використовуючи алгоритм, який базується на теоремі Шеннона. Якщо один з процесорів виявляє вище ніж нормальне навантаження по трафіку, правила розподілення трафіку на комутаторі S_1 налаштовуються для балансування кількості трафіку, спрямованого на кожен зі сканерів.

Механізм виявлення базується на значенні ентропії обчисленої для кінцевих адрес трафіку, який проходить через кожен сканер від комутатора S1. Ентропія розраховується за методом Шеннона, де p позначає ймовірність появи IP-адреси, як місця призначення пакету:

$$H = -\sum p * \log_2 p \tag{1}$$

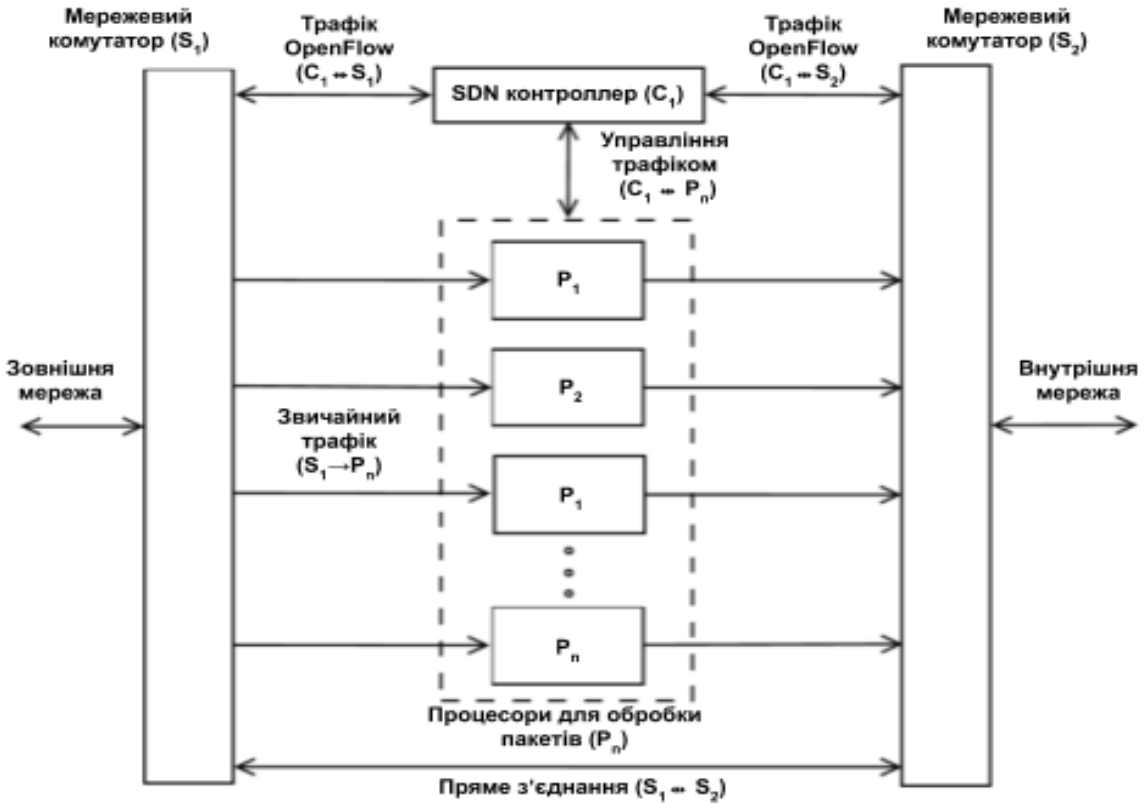

Рис.1. Архітектура системи виявлення вторгнень на базі SDN пристроїв (TIDS).

Основна ідея алгоритму полягає в тому, що зменшення значення ентропії для адрес призначення показує, що кількість трафіку, спрямованого на

невелику кількість хостів, збільшилася і що зараз вона займає значну частину загального трафіку. Якщо зниження ентропії різке (воно відбувається за короткий проміжок часу), це може сигналізувати про те, що DoS атака розпочалась. Різниця в ентропії більш очевидна, коли трафік атаки займає більшу частку від загальної кількості трафіку (або коли інтенсивність фонового трафіку менша порівняно з трактом атаки). Розподіляючи загальну кількість трафіку на декілька вузлів обробки, TIDS (Transparent Intrusion Detection System) зменшує кількість фонового трафіку, який обробляється кожним процесором, тим самим підкреслюючи аномальний трафік та спрощує його виявлення. Крім того, процедура врівноваження тимчасово припиняється під час підозрілих мережевих дій (тобто коли один з процесорів сигналізує про те, що в даний час можлива атака), щоб запобігти перерозподілу трафіку атаки між процесорами. Перерозподіл зменшив би інтенсивність трафіку атаки на процесор, який виявив підозрілу активність, тим самим збільшивши значення ентропії, що зменшило б шанси на успішне виявлення атаки. TIDS розділяє інтервал моніторингу на часові вікна (фрагменти), які містять статистику пакетів за цей часовий інтервал. Тривалість окремих фрагментів впливає на надійність та чутливість системи. Більш тривалі відрізки часу забезпечують стійкість до помилкових позитивних виявлень, які можуть з’являтися через короткі сплески мережевого трафіку, тоді як більш короткі часові відрізки збільшують чутливість системи.

Література

1. P. Zanna, B. O'Neill, P. Radcliffe, S. Hosseini and S. Ul Hoque, 'Adaptive threat management through the integration of IDS into Software Defined Networks', 2014.
2. MM and K. Okamura, “Securing Distributed Control of Software Defined Networks,” in International Journal of Computer Science & Network Security, vol. 13, no. 9, 2013.