МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИХ НАЦШОНАЛЬНИЙ УНИВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

АНДЕРС КАРЛССОН

УДК 621.391

МОДЕЛЬ ТА МЕТОД ВИЯВЛЕННЯ НИЗЬКОІНТЕНСИВНИХ МЕРЕЖЕВИХ АТАК НА ПРИКЛАДНОМУ РІВНІ

Спеціальність 05.12.02 – телекомунікаційні системи та мережі

АВТОРЕФЕРАТ

дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2017

Дисертацією є рукопис

Робота виконана в Харківському національному університеті радіоелектроніки, Міністерство освіти і науки України

Науковий керівник: доктор технічних наук, професор
Дуравкін Євген Володимирович,
Харківський національний університет радіоелектроніки,
професор кафедри інфокомунікаційних систем.

Офіційні опоненти: доктор технічних наук, професор
Толюпа Сергій Васильович,
Київський національний університет імені Тараса Шевченка,
професор кафедри кібербезпеки та захисту інформації;

доктор технічних наук, доцент
Семко Віктор Володимирович,
Державний університет телекомунікацій,
Навчально-науковий Інститут захисту інформації,
професор кафедри інформаційної та кібернетичної безпеки.

Захист відбудеться «1» листопада 2017 р. о 13 годині на засіданні спеціалізованої вченої ради Д 64.052.09 при Харківському національному університеті радіоелектроніки адресою: 61166, м. Харків, пр. Науки, 14.

З дисертацією можна ознайомитись у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, пр. Науки, 14.

Автореферат розісланий «30» __вересня___ 2017.

Вчений секретар
спеціалізованої вченої ради Д 64.052.09 О. Б.Ткачова

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми.

Концепція безпеки мережевої інфраструктури є однією з основних вимог, які повинні бути реалізовані в усіх сучасних інфокомунікаційних системах. Важливість цієї концепції зростає зі збільшенням проникнення інфокомунікаційних систем в різні аспекти життя суспільства. Широке і зростаюче проникнення технології хмарних обчислень, як складової інфокомунікаційних систем привертає увагу не тільки кінцевих користувачів та розробників клієнтських послуг, але і зловмисників. Відсутність універсальних стандартів інформаційної безпеки в хмарних системах є перешкодою для розвитку і освоєння цієї області. Однією з ключових проблем сучасних інфокомунікаційних систем є захист послуг, що надаються від атак типу відмова в обслуговуванні (DOS-атак).

Аналіз статистики компаній, що забезпечують захист інформаційних ресурсів мережі, показав значне збільшення обсягу і складності DOS-атак за останні кілька років.

Зусилля провайдерів в усьому світі спочатку були зосереджені на очищенні каналів від трафіку, що лише забирає пропускну здатність каналу зв’язку. Наприклад, багато інтернет-провайдерів використовували спеціалізовані рішення: встановлення та налаштування брандмауера, маршрутизація в «чорні діри», використання систем виявлення вторгнень (IDS), списки контролю доступу та інш. Спеціалізовані засоби захисту від DOS-атак мережевого рівня основані на аналізі трафіку і виявленні аномалій в його структурі. Відповідно до цього підходу будуються профілі трафіку в різних умовах роботи і виконується пошук аномалій в спостережуваному діапазоні. В цьому випадку аномалія трафіку є відхилення характеристик від статистичних значень. Цей підхід заснований на використанні статистичних методів, вівлет аналізі, методах підпису, кластерному аналізі та інш. Вказані методи дозволяють ефективно розпізнавати та обробляти лавинні DoS-атаки мережевих і транспортних рівнів, спрямовані на заповнення пропускної здатності каналу (Smurf, UDP-повінь і т. д.) і перевищення нормального навантаження окремих вузлів (SYN-flood, Teardrop, Ping смерті і т. д.).

У той же час дані рішення не дозволяють ефективно виявляти DoS-атаки прикладного рівня, що викликає значне зростання їх кількості. На відміну від атак третього і четвертого рівнів атаки прикладного рівня не вимагають великої атакуючої бот-мережі і надійно «відкидають» атакуємий ресурс, залишаючись практично невидимими для спеціалізованого обладнання, встановленого

провайдером. Основною особливістю даного типу атак є порівняно низька інтенсивність трафіку з атаками на мережевому рівні. Аналіз профілю інтенсивності такого трафіку не містить аномалій. Відрізнити трафік, що генерується під час таких атак від законного трафіку, досить складно.

Основні зусилля по впровадженню таких атак – це відкриття з'єднання з сервером без відправки навіть одного байту. Відкриття з'єднання і очікування відповіді не вимагає майже ніяких ресурсів від зловмисника, але він завжди пов'язує один серверний процес, який чекає виконання запиту. Сервер буде чекати закінчення витоку часу очікування, а потім буде закрито.

Відкриття тільки одного з'єднання не призведе до значних пошкоджень, але одночасне відкриття сотень підключень займе всі доступні серверні процеси. При досягненні максимальної кількості процесів (а їх набагато менш ніж пропускна здатність мережі на мережевому рівні) сервер реєструє цю подію в журналі помилок («сервер досяг максимальної кількості запитів (Max Clients), розгляне можливість збільшення кількості Max Clients») і почне зберігати нові підключення в черзі. Якщо відкриття нових з'єднань триватиме з високою швидкістю, звичайні запити не будуть обслуговані. Якщо відкриття цих з'єднань триватиме з ще більшою швидкістю, черга буде переповнюватися, що призведе до відмови від нових з'єднань.

Завданнями розробки та впровадження засобів захисту телекомунікаційних мереж від DOS-атак займаються крупні IT-компанії, такі як Cisco, HP, IBM, Juniper та академічні інститути - ONF, IRTF, IETF, ETSI, SDNRG. Методам дослідження та розробки системи управляння, зокрема, моделям та методам аналізу коректності поведінки та розподілу мережевих ресурсів присвячено ряд робіт дослідників у всьому світі.

Виходячи з цього, науково-прикладна задача, що полягає у підвищенні доступності послуг, що надаються мультисервісною мережею за рахунок вдосконалення існуючих та розробки нових методів виявлення мережевих атак, а отже й тема дисертаційної роботи «Модель та метод виявлення низькоінтенсивних атак прикладного рівня», що спрямована на вирішення зазначеної задачі, є актуальною.

Метою дисертаційної роботи є підвищення доступності послуг, що надаються мультисервісною мережею за рахунок вдосконалення існуючих та розробки нових методів виявлення мережевих атак прикладного рівня.

Для досягнення поставленої мети у дисертаційній роботі розв’язано наступні наукові задачі:

1. Аналіз особливостей реалізації низькоінтенсивних атак на відмову в обслуговуванні;

2. Відбір набору конкретних характеристик для кожного типу низькоінтенсивних атак на відмову в обслуговуванні;

3. Розробка математичної моделі web-сервера при реалізації низькоінтенсивних атак на відмову в обслуговуванні;

4. Розробка математичної моделі для прогнозування стану сервісу, що надається на рівні додатків, з урахуванням одночасного обслуговування декількох запитів;

5. Розробка методу виявлення та класифікації низькоінтенсивних атак на відмову в обслуговуванні на web-сервіси (Slow-http атак).

Об'єкт дослідження – процес виявлення мережевих атак на відмову в обслуговуванні на прикладному рівні.

Предмет дослідження – моделі та методи виявлення низькоінтенсивних атак на відмову в обслуговуванні на web-сервіси.

Методи дослідження. Підчас розв'язання поставлених задач, зокрема, при оцінці взаємодії мережевих елементів у процесі надання комплексних сервісів було використано положення теорії управління багаторівневими системами; положення теорії множин використано під час аналізу та розробки моделі web-серверу; теорія масового обслуговування та теорія графів – під час вирішення задачи з розробки моделі низькоінтенсивної мережевої атаки, та методи аналізу розподілу ресурсів - під час оцінки коректності та ефективності розподілу мережевих ресурсів; методи імітаційного моделювання та математичної статистики - під час проведення та оцінки результатів експериментального дослідження.

Наукова новизна отриманих результатів. В ході розв'язання наукової задачі було отримано наступні нові наукові результати:

1. Вперше розроблено модель виявлення низькоінтенсивних мережевих атак, на відмову в обслуговуванні прикладного рівня. Використання ланцюгів Маркова для подібного виявлення мережевих атак є новизною запропонованого підходу. Розроблена модель дає змогу аналізувати поведінку сервера, що атакується та обчислити ймовірність переходу web-серверу у стан «відмова в обслуговуванні». Застосування розробленої моделі дає можливість запровадити попереджувальні кроки та запобігти стані «відмови в обслуговуванні».

2. Вперше розроблено модель аналізу навантаження серверів додатків на основі графів вірогідності та часу. Застосування розробленої моделі дає можливість обчислювати час переходу сервера до стану «відмови в

обслуговуванні» та оцінити динаміку впливу мережевих атак і вибрати контрзаходи для зниження його ефективності.

3. Вперше, розроблено метод виявлення та класифікації низькоінтенсивних атак типу «відмова в обслуговуванні» на web-сервіси. Розроблений метод дає можливість генерувати механізми зниження ефективності впливу подібних атак і, як наслідок, збільшити доступність послуг в мультисервісних мережах.

Обґрунтованість і достовірність отриманих в роботі нових наукових результатів забезпечена та підтверджена коректним використанням ключових положень добре відомого та апробованого математичного апарату – ланцюгів Маркова, теорії управління багаторівневими системами, теорії множин, теорії графів та поширеними підходами до процесу реплікації та методів балансування навантаження.

Наукове значення. Запропоновані у дисертаційному дослідженні методи та моделі дозволяють підвищити якість надання сервісів у мультисервісній мережі, а саме підвищити доступність та захищеність від мережевих атак типу «відмова в обслуговуванні» що реалізуються на прикладному рівні.

Результати дисертаційної роботи також можуть бути рекомендовані до використання при проектуванні та вдосконаленні конвергентних телекомунікаційних систем, зокрема мультисервісних хмарних систем. Запропоновані методи та моделі можуть бути використані як науково-методична база для подальших досліджень функціонування та надання сервісів у різних типах мультисервісних систем, зокрема тих, що реалізуються у хмарному середовищі.

Практична значимість результатів досліджень полягає в тому, що запропоновані математичні моделі і методи можуть бути використані підчас розробки, підтримки, проектування та впровадження різноманітних мультисервісних хмарних систем. Запропонований метод був використаний для захисту хмарної лабораторії ReSeLa, та застосовується для підготовки фахівців в області інформаційної безпеки. Матеріали дисертаційної роботи використано в навчальному процесі кафедри інфокомунікаційних систем ХНУРЕ в курсі «Методи колективного захисту інформації».

Особистий внесок здобувача. Усі основні наукові результати, що висвітлено в дисертаційній роботі, здобувач отримав самостійно. Крім того, в роботі [1] автором особисто розроблено імітаційну модель низькоінтенсивної атаки прикладного рівня на хмарне середовище. В роботі [2] автором особисто розроблена модель поведінки web-серверу на базі ланцюгів Маркова. В роботі [3] автором розроблена модель, що дозволяє розрахувати час переходу web-сервера у

стан «відмова в обслуговуванні». В роботі [4] автором розроблено метод виявлення та класифікації Slow-http атак на хмарні системи. В роботі [5] автором розроблено модель Slow-http атаки на соціальні мережі.

Апробація основних положень дисертаційної роботи була проведена у ході п’яти конференцій та п’яти форумів, а саме EastWest Design & Test Symposium (EWDTS) 2013, First International Scientific-Practical Conference Problems of Infocommunications Science and Technology 2014, IEEE East-West Design & Test Symposium (EWDTS’2014), First International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC_S&T 2014), East-West Design &Test Test Symposium (EWDTS’2015), First IEEE International Workshop on Orchestration for Software Defined Infrastructures (co-located with IEEE ICC 2016), East-West Design & Test Symposium (EWDTS’2016), East-West Design & Test Symposium (EWDTS’2017)

Публікації. Основні результати дисертаційної роботи опубліковані в п’ятнадцяти наукових працях: одна стаття у закордонному фаховому журналі [14], п’ять статей у фахових науково-технічних журналах та збірках наукових праць [1-4, 14]. Апробація результатів дисертації проходила в ході десяти доповідей на міжнародних науково-технічних конференціях [9-13, 15-17] які проходили під егідою IEEE та індексуються в міжнародних наукометричних базах Scopus та IEEE Xplore Digital Library.

Структура та обсяг дисертації. Дисертація складається зі вступу та чотирьох розділів. Загальний обсяг роботи становить 150 сторінок, в тому числі 130 сторінок основного тексту, 40 рисунків та 8 таблиць на 13 сторінках. Список використаних джерел містить 110 найменувань, викладених на 10 сторінках.

ЗМІСТ РОБОТИ

У **вступі** розкрито стан проблем, що досліджуються, обґрунтовано актуальність теми дисертаційної роботи, визначено мету досліджень та ряд науково-практичних задач, що потребують вирішення задля досягнення поставленої мети. Наведено наукову новизну та практичну значимість отриманих результатів. Надано дані щодо апробації отриманих результатів та публікації автора за темою дисертації.

У **першому розділі** проведено аналіз низькоінтенсивних атак типу «відмова в обслуговуванні» на прикладному рівні, виділено їх основні характеристики та сценарії реалізації. Проведено дослідження вразливості різних протоколів прикладного рівня до такого класу атак.

У результаті аналізу було встановлено, що найбільш сучасні мультисервісні мережі широко використовують хмарне середовище для організації та надання послуг. Даний вибір в першу чергу обумовлений тим, що при розробці мультисервісних систем в області інфраструктури основна взаємодія між компонентами виконується або на базі SOA технологій, або REST. В основі обох технологій лежить механізм взаємодії по протоколу HTTP, тобто через web-сервер. Тому саме низькоінтенсивні атаки типу «відмова в обслуговуванні» на web-сервер (Slow-http атаки) є найбільш ефективними переривання доступності всього хмарного середовища. Цьому типу атак і було приділено найбільшу увагу з метою з'ясування основних сценаріїв їх реалізації та особливостей впровадження. На рис. 1 наведені сценарії розвитку двох найбільш розповсюджених низькоінтенсивних атак – SlowHeader та SlowBody.

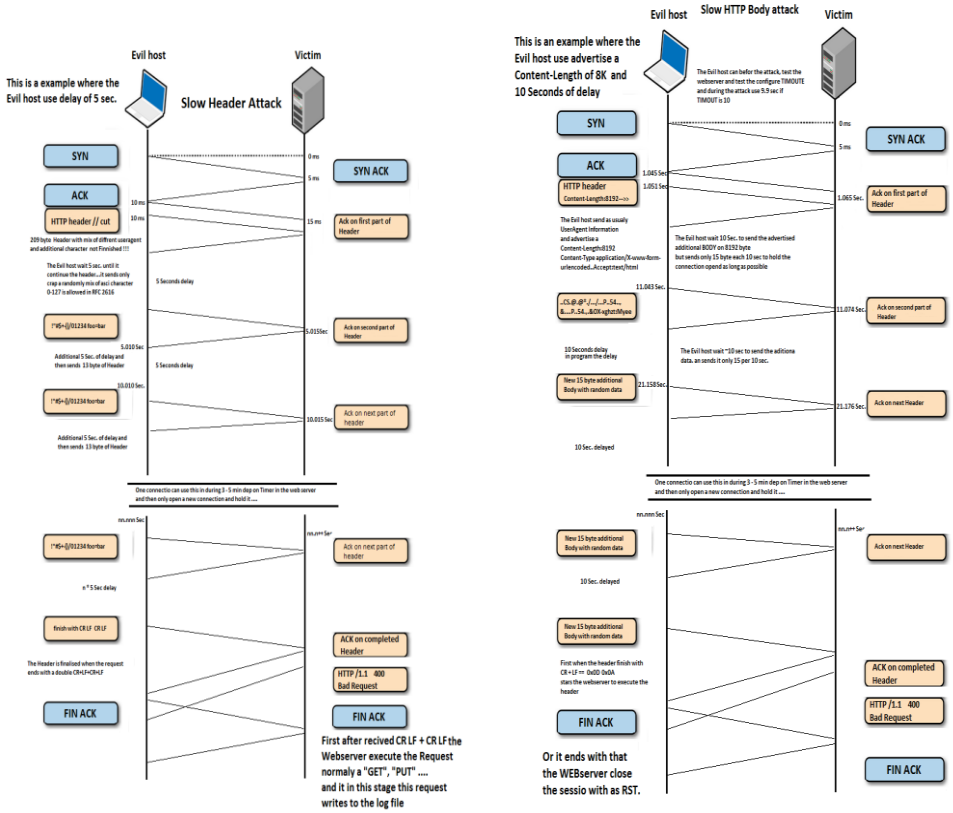

Рис. 1. Схеми основних сценаріїв низькоінтенсивних атак на базі протоколу HTTP

Як випливає з наведених діаграм принцип таких атак полягає в утриманні як можна довше з'єднання у відкритому стані. Кожен з web-серверів має досить обмежену кількість з'єднаннь, що одночасно обслуговуються. Таким чином з одного боку зловмиснику немає потреби використовувати потужні ресурси для

генерування трафіку атаки, а з іншого - атакуючий трафік незначною мірою відрізняється від звичайного. Атаки даного типу є великою загрозою для web-серверів, діагностика і виявлення даного типу атак становить складність для адміністраторів – трафік не перевищує нормальних значень. Схожість такого трафіку з легальним, ускладнює фільтрацію атакуючих пакетів, що дозволяє зловмисникові досить швидко і легко домогтися відмови в обслуговуванні web-сервера.

Більшість існуючих систем виявлення вторгнень спрямовані на виявлення і запобігання атак мережевого і транспортного рівня, суть яких полягає в генерації значного трафіку, що дозволяє заповнити всю пропускну здатність вузла, що атакується. Особливістю Slow-http атак є відсутність великих обсягів трафіку.

Аналіз реалізації низькоінтенсивних атак дозволив виявити їх особливості, які можуть буди використані для виявлення та класифікацій. Такі особливості наведені у таблиці 1.

Таблиця 1

Аналіз особливостей низькоінтенсивних атак

Slowloris	Slow POST	Slow READ
Одночасна кількість запитів з однієї IP-адреси (варіює від декількох сотень до декількох десятків тисяч запитів, в залежності від масштабності сервера;		Включені постійні з'єднання (Keep-Alive) і HTTP конвеєр;
Значення затримки між передачами частин запиту прагне до величини тайм-ауту з'єднання сервера, але не досягає його;		Значення затримки отримання даних відповіді сервера прагне до величини тайм-ауту з'єднання сервера, але не досягає його;
Відправка заголовка запиту маленькими частинами(10-20байтів);	Відправлення тіла запиту маленькими порціями (10-20байтів);	Початковий розмір вікна прийому досить великий;
Очікування подвійного CRLF практично до досягнення значення тайм-ауту.	Досить велике поле «content length», з порівняно маленькими блоками переданих даних.	На web-сервер приходять SYN-пакети з аномально малим розміром TCP вікна.

Аналіз наведених особливостей дозволяє формалізувати набір параметрів, що характеризують стан web-сервера, необхідний для здійснення Slow-http атак:

Для Slowloris і Slow POST характерними параметрами є:

1) Кількість запитів.

2) Кількість ip-адрес.

3) Швидкість з'єднання.

4) Інтервал активності клієнта близький до тайм-ауту.

5) Співвідношення заявленого розміру вікна і переданих даних.

Для Slow READ характерними параметрами є:

1) Кількість запитів.

2) Кількість ip-адрес.

3) Швидкість з'єднання.

4) Інтервал активності клієнта близький до тайм-ауту.

5) Різниця між початковим і подальшим розмірами TCP вікна (прагне до 0).

6) Наявність або відсутність постійних з'єднань (Keep-Alive) і HTTP конвеєр.

Наведена формалізація необхідна для порівняльного аналізу існуючих підходів до виявлення атак. Виділені параметри виступають в якості критеріїв атаки, і в залежності від одержуваного ними значення, можуть свідчити про наявність того або іншого типу атаки. Залежно від алгоритму виявлення та математичного апарату, що використовується в системі виявлення атак, дані критерії можуть виступати в якості вхідних даних в сценаріях виявлення, або мати ознаки наявності або відсутності атаки.

Відповідно до ознак, характерних Slow-http атакам та специфічному характері їх реалізації завдання виявлення можна сформулювати як виявлення моменту початку атаки і запобігання атаки, до моменту відмови в обслуговуванні web-сервера. Задано:

Послідовність спостережуваних станів web-сервера: $S = S1, S2, S3, , \dots \dots Sn.$

Час переходу web-серверу у кожний стану: $T = T1, T2, T3, , \dots \dots Tn.$

Множина значень параметрів серверу, що відображають наявність атаки та є пороговими значеннями: $X = \{X_1^i, X_2^i, \dots \dots X_n^i\},$ де $i -$ тип Slow-http атаки.

Вимагається оцінити імовірність та час переходу web-серверу у стан «відмова в обслуговуванні».

Сучасні системи захисту ресурсів мультисервісніх мереж від DOS-атак базуються на використанні декількох математичних апаратів: підхід на основі кінцевих автоматів, детермінований підхід на основі правил, підхід на основі нечіткої логіки, підхід, на основі нейронних мереж, підхід на заснований на генної інженерії та інш.

Зазначені підходи малоефективні для виявлення низькоінтенсивних DOS-атак прикладного рівня, особливістю яких є відсутність аномалій в характеристиках

трафіку. Відрізнити трафік, що генерується в ході таких атак від легального трафіку досить складно. Отже, застосування сигнатурних методів так само є не ефективним.

Ґрунтуючись на аналізі недоліків вищевикладених підходів, очевидним фактом є неможливість виділення методу, який дозволить ефективно вирішити задачу виявлення Slow-http атак.

Таким чином виникає задача модифікації вищевикладених підходів і використання їх в доповненні з іншими існуючими математичними апаратами що дозволить виявляти і прогнозувати виникнення Slow-http атак, на підставі визначених параметрів web-серверу.

У **другому розділі** проведено аналіз особливостей реалізації Slow-http атак. Встановлені основні математичні закономірності між параметрами атаки та станом web-сервера, що атакується. Це дозволило розробити відповідну математичну модель поведінки сервера під час атаки. Отримано розподіл ймовірностей стану web-серверу під час реалізації Slow-http атак різного типу. Адекватність математичної моделі підтверджено практичним експериментом.

Дослідження природи Slow-http атак показали, що в процесі реалізації потік заявок з джерела атаки можна вважати найпростішим. Про це свідчить те, що досліджуваний потік заявок володіє трьома властивостями, характерними найпростішого потоку подій: стаціонарність, ординарність і відсутність наслідків.

Параметри http-запитів (довжина, швидкість прийому даних, розмір даних, що приймаються, затримки між підтвердженнями, методи запитів) так само є однаковими і незмінними.

Даний факт дозволяє описати web-сервер, що атакується, як систему масового обслуговування типу M/M/N, де N - максимальна кількість одночасно оброблюваних http-запитів (максимальна кількість процесів (потоків), які може запустити web-сервер). Наприклад, для сервера Apache2 це параметр «MaxClients» в файлі конфігурації «http.conf».

Наявністю буфера очікування в web-сервері в даному випадку можна знехтувати, так як він не впливає на факт початку атаки, а впливає лише на її тривалість.

Відповідно граф станів такого web-серверу наведено на рис. 2.

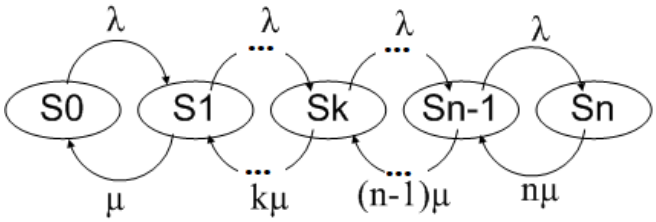

Рис. 2. Загальний граф станів та переходів web-серверу

Станами web-серверу є:

S0 – запити на обслуговування відсутні;

S1 –обслуговується 1 запит;

Sk – обслуговується k запитів;

Sn-1 - обслуговується$n-1$ запит;

Sn - обслуговується n запитів, сервер перевантажено.

Параметрами моделі є:

n - максимальна кількість запитів, що обслуговуються;

k- поточна кількість запитів;

λ- інтенсивність надходження запитів;

μ - інтенсивність обслуговування запитів.

Відповідно до теорії масового обслуговування в один і той же момент часу може статися одне з двох подій, які призводять до зміни стану web-сервера:

- надходження http-запиту, що приводить до переходу у наступний стан з більшим номером, причому якщо сервер знаходиться в стані *Sn*, то його стан не зміниться, що відповідає відмові в обслуговуванні;

- завершення обслуговування http-запиту і перехід в стан з меншим номером.

Наведені міркування дозволяють використовувати формули Ерланга для обчислення ймовірності будь-якого (k-го) стану $p_k$web-сервера:

$$p_k = \frac{\frac{\alpha^k}{k!}}{\sum_{k=0}^{n}\frac{\alpha^k}{k!}} \quad , \tag{1}$$

де:

$$\alpha = \frac{\lambda}{\mu}.$$

Наведені вирази дозволяють отримати розподіл імовірностей станів web-серверу при різних умовах реалізації slow-http атак.

Перевірка адекватності математичної моделі виконувалась шляхом практичного експерименту. Параметри якого наведені у табл. 2.

Таблиця 2

Параметри експерименту

Тип атаки	Slowloris	Slow POST	Slow READ
Кількість з’єднань	100-1000	50-450	100-1000
Тип запиту	GET	POST	-
Параметри окна відповіді (байт)	-	-	20-572
Швидкість читання з буферу	-	-	32байта/5 сек
Значення поля заголовку Content-Length	209	8192	-
Додаткове поле даних	52	66	-
Інтервал між пакетами (сек)	5	10	-
З’єднань у секунду	50-300	20-200	10-100
Тривалість тестування (сек)	600	600	600

На рис. 3 наведено розподіл імовірностей станів web-серверу для різних варіантів slow-http атак.

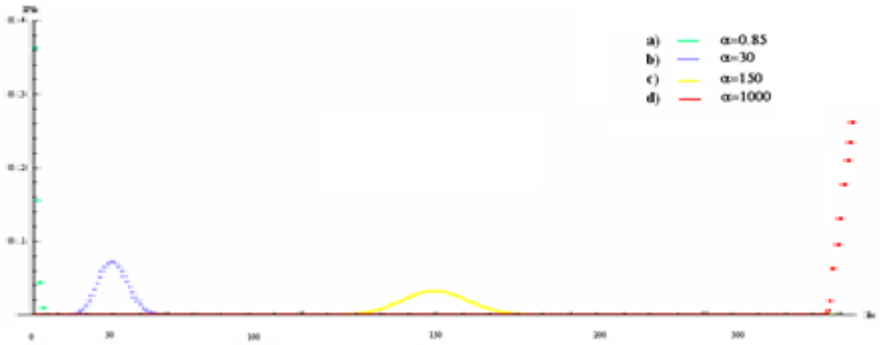

Рис. 3. Розподіл імовірностей станів web-серверу для різних варіантів slow-http атак

З наведеного графіку видно, що результати експеременту підтверджують результати математичної моделі. Таким чином, запропоновану математичну модель станів web-серверу під час різноманітних slow-http атак можна використовувати при розробці системи виявлення атак.

У **третьому розділі** розроблено математичну модель прогнозування стану «відмова в обслуговуванні» для web-серверу. Модель базується на аналізі динаміки переходів між станами серверу.

Аналіз засобів моделювання динаміки станів інфокомунікаційних систем показав, що найбільш прийнятним засобом є ймовірносно-часові графи. Даний

математичний апарат дозволяє зв’язати модель станів системи, що отримана у попередньому розділі з динамікою функціонування системи.

У відповідності до методу web-сервер визначається як набір станів та ймовірнісно-часові характеристики переходів між ними (рис. 4).

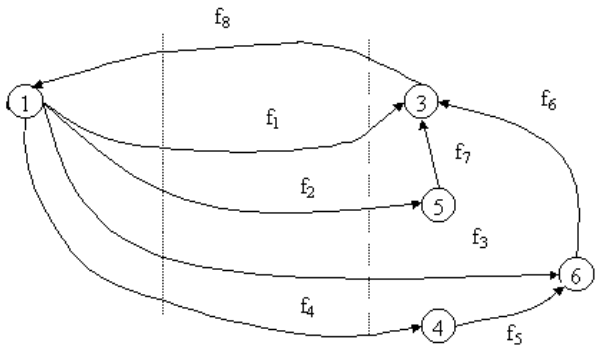

Рис. 4. Ймовірнісно-часовий граф станів web-серверу

Характеристики мають вигляд функції: $f(p_i, t_i) = p_i z^{t_i}$, де p_i– ймовірність переходу в стан i; t_i – час переходу між станами. Початковий розподіл ймовірностей між станами визначається виразом:

$$p_i = \frac{\lambda_i \frac{p_i^{d-1}}{\mu_i^{d-1}}(1-\frac{p_i}{\mu_i})}{\sum_{j=1}^{J} \lambda_{j*}(1-\frac{p_i^{m_i}}{\mu_i^{m_i}})}. \quad (2)$$

Матриця ймовірностей переходу між станами визначається за виразом:

$$p(i,j) = p_{i.j} \frac{\frac{p_j^{d_j-1}}{\mu_j^{d_j-1}}(1-\frac{p_j}{\mu_j})}{1-\frac{p_j^{m_i-1}}{\mu_j^{m_i-1}}}. \quad (3)$$

Результуючою функцією такого графа буде функція:

$$F_n'(z) = (\sum_{i=1}^{n} P_i z^{t_i}) * (1 - P_0 z^{t_0})^{-1}. \quad (4)$$

Використовуючи вираз (5), можливо визначити час переходу сервера, що атакується у стан «відмова в обслуговуванні»:

$$T_{\text{ср}n} = \frac{dF_n'(z)}{dz}\Big|_{z=1} = \frac{(\sum_{i=1}^{n} P_i t_i)*-(1-P_0)+\sum_{i=1}^{n} P_i * P_0 t_0}{(1-P_0)^2}, \quad (5)$$

де:

$$t_i = \frac{1}{\lambda} * k_i \ .$$

На рис. 5 наведена залежність часу переходу web-сервера у стан перевантаження або «відмова в обслуговуванні» в залежності від параметрів атаки (співвідношенні вхідного на вихідного потоків).

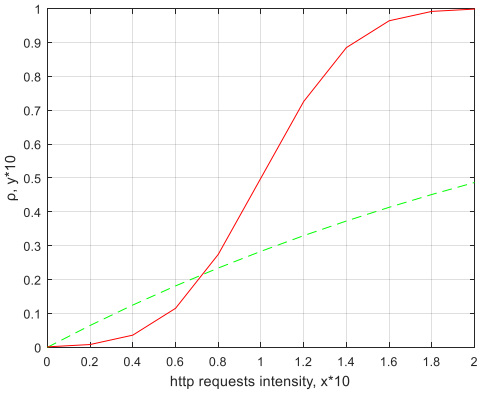

Рис. 5. Часові характеристики зміни станів web-серверу в залежності від параметрів атаки

Аналіз характеру залежності показав, що вона є нелінійною. Характер нелінійності слід враховувати при визначенні порогових показників спрацьовування системи попередження про атаку.

У **четвертому розділі** розроблено загальний метод виявлення та класифікації slow-http атак на web-сервер. Метод ґрунтується на моделях стану та динаміки функціонування web-сервера. Виконана практична імплементація методу у якості системи виявлення та попередження про мережеву атаку на web-сервер. Ефективність практичної реалізації методу перевірялась при захисті хмарного середовища мультисервісної мережі. Проведений експеримент показав спроможність виявляти slow-http атаки в різних варіантах їх реалізацій та запобігати стану «відмова в обслуговуванні».

Розроблені математичні моделі, що дозволяють розраховувати розподіл ймовірностей станів web-серверу в залежності від параметрів вхідного та вихідного потоків можуть буди використані як ядро системи виявлення та протидії мережевим атакам на web-сервери. Загальна структурна схема такої системи наведена на рис. 6.

Процесна система складається з декількох етапів:

1. На першому етапі трафік надходить на вхід системи.

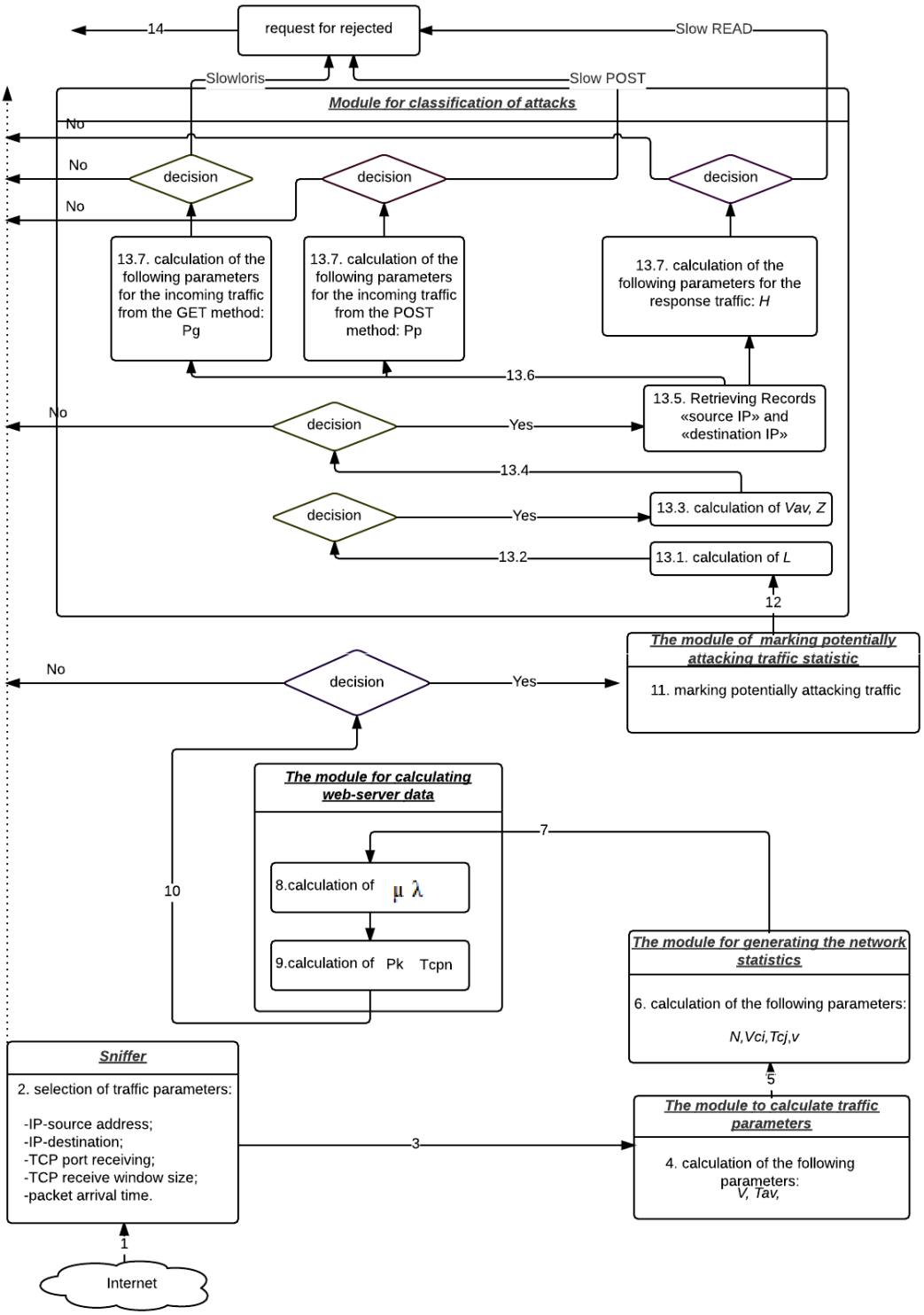

Рис. 6. Загальна схема методу виявлення та класифікації slow-http атаки

2. Протягом певного періоду часу модуль для збирання трафіку розподіляє параметри трафіку, необхідні для подальших розрахунків: джерело IP-адреси, IP-адреса джерела, TCP-порт прийому, розмір вікна TCP та час прибуття пакету.

3. Вибрані параметри передаються модулю для обчислення параметрів трафіку.

4. На наступному етапі для кожної IP-адреси розраховуються такі характеристики трафіку:

Загальна кількість даних, що передаються протягом аналізованого періоду часу:

$$V = \sum_{i=1}^{k} V_{i|} \mid_{\Delta t} \quad , \tag{6}$$

де:

V - загальний обсяг даних;

V_i - обсяг і-го пакету даних;

k - кількість пакетів;

Δt - проаналізований період часу.

Середній інтервал часу між переданими пакетами:

$$T_{av} = \frac{\sum_{i=1}^{k} (t_{i+1} - t_i)}{i-1} \mid \Delta t \quad . \tag{7}$$

5. Розраховані параметри передаються модулю формування мережевої статистики.

6. Модуль генерації зберігає набір записів статистики про трафік та обчислює наступні параметри:

- кількість сесій за певний проміжок часу $(N \mid \Delta t)$;

- кількість даних для кожної сесії:

$$Vci = \sum_{i=1}^{k} V_i \quad , \tag{8}$$

де:

Vci - обсяг даних на *i*-й сесії;

k - кількість пакетів за сесію;

i - номер сесії.

- затримка між пакетами з сеансом:

$$Tcj = t_{j+1} - t_j \lim_{\delta x \to 0} , \tag{9}$$

де:

Tcj - затримка між пакетами протягом сеансу;

t_j - час прибуття j -го пакету;

t_{j+1} - час прийому $(j+1)-$го пакета;

j - номер пакета в сесії;

v - швидкість підключення.

Вбудований таймер дозволяє нам записувати початок і кінець сеансу, що дозволяє контролювати тривалість відкритих з'єднань.

7. Розрахункові параметри передаються модулю для обчислення параметрів сервера.

8. На наступному етапі модуль для обчислення параметрів сервера розраховується інтенсивність надходження та обробки запитів, що супроводжується кожним проміжним інтервалом: співвідношення отриманих пакетів з певними IP-адресами за заданий проміжок часу.

Інтенсивність надходження запитів:

$$\lambda = \frac{k_i}{t}, \tag{10}$$

де: k_i - кількість запитів на надходження, що аналізуються на заданому інтервалі;

t - інтервал спостереження.

Інтенсивність обслуговування запитів:

$$\mu = \frac{k_j}{t}, \tag{11}$$

9. Виходячи з розрахованої інтенсивності визначається навантаження сервера та час, коли він досягне умов перевантаження.

10. На наступному етапі визначається імовірність атаки на основі розрахованих параметрів. Статистика трафіку відповідно до IP-адресів, де параметри перевищують певні статичні пороги, передаються модулю маркування трафіку атаки.

11. Детальна статистика трафіку, розраховані параметри якої перевищують статичні пороги, позначаються як "потенційно атакуючий трафік".

12. Статистика передається модулю класифікації атаки.

Завдання модуля класифікації атак полягає в тому, щоб віднести атакуючий трафік до класу Slow-http атак або видалити маркер атаки.

13. Процес цього модуля складається з декількох етапів:

13.1 На першому етапі обчислюється співвідношення IP-адрес, позначених трафіком до кількості запитів за заданим інтервалом часу:

$$L = \frac{N}{k}\Big|_{\Delta t}, \tag{12}$$

де:

L - співвідношення IP-адрес маркованого трафіку до кількості запитів за певний проміжок часу;

N - кількість IP-адрес маркованого трафіку;

k - кількість запитів за певний проміжок часу;

Δt - заданий період часу.

13.2 На другій стадії розраховані параметри порівнюються з пороговими:

- якщо значення L не перевищує статичних порогових значень, приймається рішення про те, що трафік належить до легального трафіку потенційного користувача і статистика маркерів атаки, видаляється;

- якщо значення L перевищує заданий поріг, статистика сумується для наступного етапу класифікації атаки.

13.3 На третьому етапі для кожної IP-адреси враховується середня швидкість підключення та затримка між пакетами:

$$V_{av} = \frac{\sum_{i=1}^{n} V_i}{i}, \tag{13}$$

де:

Vi -трансферна швидкість i-ї частини запиту;

n - кількість переданих частин за запитом.

13.4 На четвертій стадії розраховані параметри порівнюються з заданими пороговими значеннями:

- Якщо Vav та Z значення не перевищують заздалегідь визначеного порогу, то вирішено, що трафік належить дійсному користувачеві, а маркер "Статистика трафіку потенційних атак " видаляється.

- Якщо Vav та Z значення перевищують заданий поріг, статистика сумується для віднесення до наступного етапу класифікації атаки.

13.5 На п'ятому етапі класифікації атак відкидаються помилкові зв’зки «джерело IP» і «IP-адреса призначення» із статистики потенційно атакуючого трафіку.

13.6 На шостому етапі потенційно атакуючий трафік класифікується відповідно до запиту, отриманого методом вилучення.

13.7 На сьомому етапі здійснюється статистичний аналіз вхідного та вихідного трафіку:

- співвідношення загального розміру заголовку запиту до середнього значення переданих даних за заданий період часу та відношення загального розміру тіла запиту до середнього значення переданих даних для попередньо визначеного:

$$Pg = \frac{Vg}{\sum_{i=1}^{n} Vg(i)/i} \quad , \tag{14}$$

де:

Pg - співвідношення загального розміру заголовку запиту до середнього значення переданих даних у вказаний час для GET запиту;

Vg - загальний розмір заголовка запиту;

$Vg(i)$ - частина переданого заголовка запиту;

n - кількість заготовок переданого запиту.

$$Pp = \frac{Vp}{\sum_{i=1}^{n} Vp(i)/i}, \tag{15}$$

де:

Pp - відношення загального розміру тіла запиту до середнього значення переданих даних у вказаний час для POST запитів;

Vp - загальний розмір заголовка;

$Vp(i)$ - i- від закладеного заголовка запиту;

n - кількість переданих частин заголовка запиту.

Якщо значення Pg голови або тіла Pp не перевищують визначеного порогу, то вирішується, що трафік належить законному користувачеві і маркер "потенційного трафіку атаки" буде видалено.

Якщо значення Pg перевищує заданий поріг, вирішено класифікувати вхідний трафік у клас низькоактивних атак типу Slow Head, а система виявлення вторгнення надсилає запит на сервер, щоб закрити з'єднання з вказаних IP-адрес.

Якщо значення Pp перевищує заданий поріг, вирішено класифікувати вхідний трафік у клас низькоактивних атак типу Slow Body, а система виявлення вторгнення надсилає запит на сервер, щоб закрити з'єднання з вказаних IP-адрес.

Для потоку трафіку відповідей на запити до web-сервету розраховується співвідношення вихідного розміру вікна прийому TCP до розміру частин потоку, що повертає трафік:

$$H = \frac{Vtcp}{\sum_{i=1}^{n} V(i)/i}\ , \tag{16}$$

де:

H - співвідношення вихідного розміру вікна прийому TCP до розміру частин, що повертають потоки трафіку;

$V(tcp)$ -початковий розмір вікна прийому TCP;

$Vp(i)$ - відповідь запиту;

n - кількість запитаних сервісних частин за вказаний проміжок часу.

Якщо значення H не перевищує попередньо визначеного порогу, приймається рішення, що трафік належить законному користувачеві, і маркер статистики потенційного трафіку атаки видаляється.

Якщо значення H перевищує поріг, вирішено класифікувати трафік до класу slow-http атаки (Slow-Read) та система виявлення вторгнення надсилає запит сервера на закриття з'єднання з вказаної IP-адреси.

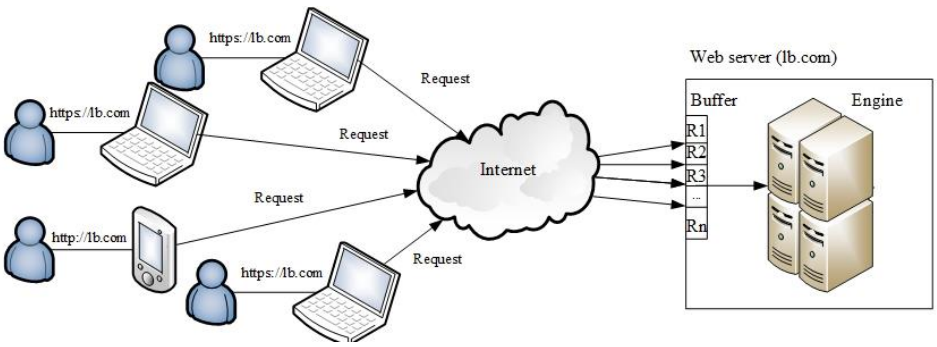

Рис. 7. Схема експерименту розподіленої slow-http атаки

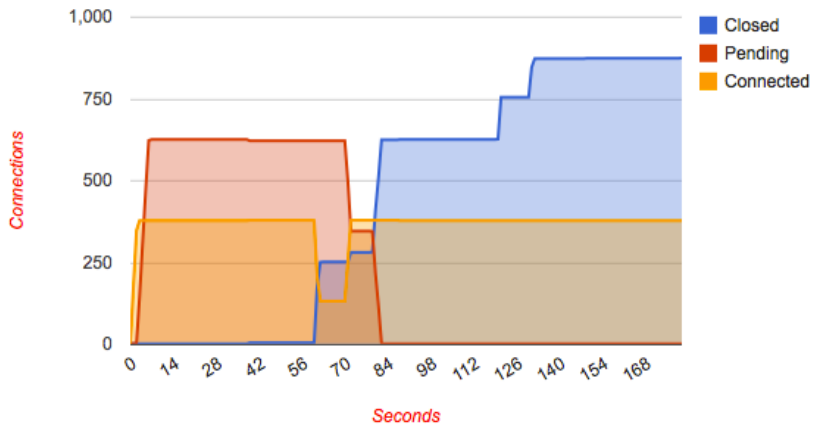

Рис. 8. Результати дослідження ефективності розробленого методу

ВИСНОВКИ ПО РОБОТІ

В роботі розв'язана ***актуальна науково-прикладна задача,*** що полягає у підвищенні доступності послуг, що надаються мультисервісною мережею за рахунок вдосконалення існуючих та розробки нового методу виявлення мережевих атак.

За підсумками вирішення науково-прикладної задачі зроблено наступні висновки:

1. Аналіз поточного стану та перспектив розвитку інфокомунікаційних систем та мереж показав, що все частіше причиною відсутності доступу до певних сервісів є мережеві атаки. В останній час все більшої популярності набувають так звані атаки на відмову в обслуговуванні, що реалізуються на прикладному рівні.

2. Проведений аналіз методів та засобів виявлення та протидії мережевим атакам на відмову в обслуговуванні показав, що вони досить ефективні від атак, що реалізуються на мережевому та канальному рівнях. У той же час у випадку атак на відмову в обслуговуванні на прикладному рівні їх ефективність досить невисока.

3. Загально відомі засоби та методи виявлення атак на відмову в обслуговуванні базуються на детектуванні аномалій трафіку, характерних для атак. В той же час атаки на відмову в обслуговуванні прикладного рівня не вимагають генерації великого обсягу трафіку тому атаки цього типу досить важно ідентифікуються звичайними системами.

4. Проведено експеримент з реалізації низькоінтенсивних атак прикладного рівня на web-сервер (slow-http). В ході виконання експерименту досліджено різні

сценарії даного типу атак, виявлено відмінні риси та параметри трафіку, що можуть ідентифікувати кожний тип атаки.

5. Розроблено модель поведінки web-серверу, що дозволяє визначити імовірність реалізації slow-http атаки. Модель базується на використанні ланцюгів Маркова та дозволяє розрахувати розподіл імовірностей між можливими станами web-серверу.

6. Розроблено модель визначення часу переходу web-серверу у стан «відмова в обслуговуванні». Модель базується на використанні ймовірносно-часових функцій та базується на інформації, що попередньо отримана за допомогою моделі станів web-серверу.

7. Проведено експеримент з моделювання атак на web-сервер, що дозволив перевірити адекватність розроблених моделей.

8. Розроблено загальний метод виявлення та класифікації атак на відмову в обслуговуванні прикладного рівня на web-сервер. Розроблений метод дозволяє виявити факт виконання атаки, визначити джерело нападу та блокувати зловмисний трафік.

9. В основі запропонованої системи захисту лежить аналіз поведінки сервера в нормальному режимі та при реалізації різновидів типу Slow-http атак. Аналіз дозволив ідентифікувати найбільш чутливі параметри для атак повільного нападу, а також встановити їх пороги в залежності від потужності каналу, продуктивності обладнання та параметрів конфігурації сервера.

10. Процес виявлення атаки реалізується на основі моделі Маркова за поведінкою сервера, параметрами моделі є статистичні характеристики вхідного, вихідного трафіку, а також динаміки серверу ресурсного використання. Перевага запропонованої системи полягає в тому, що вона дозволяє виявляти атаку на відмову в обслуговуванні сервера, що дає можливість своєчасно активувати відповідні механізми захисту.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Carlsson A. Analysis of realization and method of detecting low-intensity HTTP-attacks [Электроний ресурс] / A. Carlsson, E.V. Duravkin, A.S. Loktionova // Проблеми телекомунікацій. – 2013. – № 3 (12). – С. 61-70. – Режим доступу до журналу: http://pt.journal.kh.ua/2013/3/1/133_carlsson_ attack.pdf

2. Carlsson A. A. Analysis of realization and method of detecting low-intensity HTTP-attacks. Part 2. Method of detecting Slow HTTP attacks [Электроний ресурс] / A.A. Carlsson, I.V. Duravkin, A.S. Loktionova // Проблеми

телекомунікацій. – 2014. – № 1 (13). – С. 96-100. – Режим доступу до журналу: http://pt.journal.kh.ua/2014/1/1/ 141_carlsson_attack.pdf.

3. Carlsson A. A. Method of slow-attack detection / Carlsson Anders, I. V. Duravkin, A. S. Loktionova // Системи обробки інформації. — 2014. — № 8. — С. 102-106.

4. Carlsson Anders. Detecting cyber threats through social network analysis/ Carlsson Anders, Kirichenko Lyudmyla, Radivilova Tamara // SocioEconomic Challenges, – Vol 1, issue 1, – 2017. –p. 20-34.

5. Anders Carlsson. Model of network attack on the cloud platform OpenStack/ Anders Carlsson // In proc. of Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, Ukraine. – 2015. – p. 30-33

6. Anders Carlsson Infrastructure of pentesting and vulnerability management // Vladimir Hahanov, Anders Carlsson, Svetlana Chumachenko/“In Proc. of conference, Kharkov, Ukraine,ISBN 0135-17, – 10Sep. 2012, – P. 10-24.

7. Wajeb Gharibi, Hahanov V. I., Anders Carlsson, Hahanova I. V., Filippenko I.V. Quantum technology for analysis and testing computing systems // In Proc. of IEEE EastWest Design & Test Symposium (EWDTS), Rostov-on-Don, Russia, Sep. 27-30 , 2013.

8. Anders Carlsson; Rune Gustavsson: “Resilient Smart Grids.”// In Proc. of First International Scientific-Practical Conference Problems of Infocommunications Science and Technology, Kharkov, Ukraine, Oct. 14-17, 2014

9. Alexander Adamov, Vladimir Hahanov, Anders Carlsson. Discovering New Indicators for Botnet Traffic Detection / Alexander Adamov, Vladimir Hahanov, Anders Carlsson // Proc. of IEEE East-West Design & Test Symposium (EWDTS’2014), September 26–29, 2014, Kiev, Ukraine. – Kiev, 2014. – P. 281–285.

10. Anders Carlsson, Rune Gustavsson. Resilient Smart Grids //In Proc. of First International Scientific-Practical Conference Problems of Infocommunications Science and Technology, Kharkov, Ukraine, Oct. 14-17, 2014 PIC_S&T– pp. 79-82

11. Adamov A, Carlsson A. A Sandboxing Method to Protect Cloud Cyberspace / Adamov A, Carlsson A // Proceedings of IEEE East-West Design & Test Test Symposium (EWDTS’2015), September 27-30, 2015, Batumi, Georgia – P. 180–183.

12. Anders Carlsson. Model of network attack on the cloud platform OpenStack / Anders Carlsson // In proc. of Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, Ukraine, Oct. 13 -15, – 2015

13. Kurt Tutschku, Vida Ahmadi Mehri, Anders Carlsson, Krishna Varaynya Chiukula, Johan Christenson. On Resource Description Capabilities of On-Board Tools for Resource Management in Cloud Networking and NFV Infrastructures / Kurt Tutschku, Vida Ahmadi Mehri, Anders Carlsson, Krishna Varaynya Chiukula, Johan Christenson // In Proc. of First IEEE International Workshop on Orchestration for Software Defined Infrastructures (co-located with IEEE ICC 2016), Kuala Lumpur, Malaysia, May 23 - 27, 2016.

14. Kurt Tutschku, Vida Ahmadi Mehri, Anders Carlsson. Towards Multi-layer Resource Management in Cloud Networking and NFV Infrastructures / Kurt Tutschku, Vida Ahmadi Mehri, Anders Carlsson // In Proc. of 12th Swedish National Computer Networking Workshop (SNCNW), Sundsvall, Sweden, Jun. 1-2, 2016.

15. Alexander Adamov, Anders Carlsson. Cloud incident response model / Alexander Adamov, Anders Carlsson // Proc. of IEEE East-West Design & Test Symposium (EWDTS'2016), October 14–17, 2016, Yerevan, Armenia. – P. 250–253.

16. Ievgeniia Kuzminykh, Arkadii Snihurov, Anders Carlsson. Testing of communication range in ZigBee technology / Ievgeniia Kuzminykh, Arkadii Snihurov, Anders Carlsson // In Proc. of 14th International Conference on The Experience of Designing and Application Systems in Microelectronics (CADSM'2017), Polyana, Svalyava (Zakarpattya), Ukraine, Feb. 21 – 25, 2017.

17. Alexander Adamov, Anders Carlsson. The State of Ransomware. Trends and Mitigation Techniques / Alexander Adamov, Anders Carlsson // Proc. of IEEE East-West Design & Test Symposium (EWDTS'2017), Sep 29 – Oct 2, 2017, Belgrad, Serbia. – P. 121–128.

АННОТАЦИЯ

Андерс Карслссон. Модель и метод обнаружения низкоинтенсивных атак прикладного уровня. – Рукопись. Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.02 – телекоммуникационные системы и сети, – Харьковский национальный университет радиоэлектроники, – 2017.

Диссертационная работа посвящена решению актуальной задачи, заключающейся в повышении доступности услуг в мультисервисных телекоммуникационных сетях за счет разработки нового метода обнаружения низкоинтенсивных атак типа «отказ в обслуживании» на прикладном уровне.

Рост популярности мультисервисных сетей использующих облачную инфраструктуру показал значительную уязвимость для различного рода атак на отказ в обслуживании (DOS-атак).

DoS атаки могут быть осуществлены как снаружи, так и внутри облака. Важным аспектом безопасности облачной инфраструктуры является то, что архитектура облака, в частности OpenStack, состоит из множества взаимосвязанных компонент. Следовательно, создание ситуации, когда одна из core-компонент будет недоступна приводит к отказу доступности всего облачного сервиса.

Обеспечение основных критериев безопасности (идентификация и аутентификация пользователей, файерволов, доменов безопасности, формирование VPN туннелей) и хранение пользовательских данных в зашифрованном виде не позволяет обеспечить полноценную защиту облачной инфраструктуры от DoS атак.

Одним из наиболее эффективных методов DOS-атак на облачные инфраструктуры являются низкоинтенсивные DOS-атаки. Основная их особенность заключается в том, что они расходуют ресурс прикладного уровня, который в несколько раз меньше ресурса транспортного уровня, на который направлены обычные DOS-атаки.

Обнаружение низкоинтенсивных DOS-атак проблематично, так как профиль трафика такой атаки совпадает с профилем обычного трафика в случае подключения плохого качества.

Анализ традиционных методов обнаружения и классификации DOS-атак показал, что они основаны на анализе профилей траффика на сетевом и канальном уровнях. Работа таких систем сводится к обнаружению аномалий траффика. Особенность реализации низкоинтенсивных DOS-атак прикладного уровня не предполагает генерации больших объемов траффика, следовательно, и традиционные методы поиска аномалий показывают низкую интенсивность в случае данного типа атак.

С целью устранения данного недостатка в работе разработаны модели и метод обнаружения и классификации низкоинтенсивных DOS-атак на web-сервер (slow-http).

Проведен эксперимент по реализации slow-http атаки, который позволит выявить характерные особенности каждого типа атаки и выдвинуть предположения по возможности их обнаружения.

Разработана модель поведения web-сервера, позволяющая оценить распределение вероятностей его состояний в зависимости от состояния сети и входного/выходного траффика.

Разработана модель определения времени перехода web-сервера в состояние «отказ в обслуживании».

Разработан метод обнаружения и классификации атак на отказ в обслуживании прикладного уровня на web-сервер. Разработанный метод позволяет выявить факт выполнения атаки, определить источник нападения и блокировать злонамеренный трафик.

Метод базируется на анализе поведения сервера в нормальном режиме и при реализации разновидностей slow-http атак.

Процесс обнаружения атаки реализуется на основе модели Маркова, а также вероятностно-временных графов.

Преимущество предлагаемой системы заключается в том, что она позволяет выявлять атаку на отказ в обслуживании сервера, что позволяет своевременно активировать соответствующие механизмы защиты.

Ключевые слова: облачная инфраструктура, мультисервисные сети, цепь Маркова, вероятностно-временной граф, доступность сервиса, DOS-атака, slow-http атака.

АНОТАЦІЯ

Андерс Карлссон. Модель та метод виявлення низькоінтенсивних атак на прикладному рівні. – Рукопис. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.02 - телекомунікаційні системи та мережі, – Харківський національний університет радіоелектроніки, – 2017.

Дисертаційна робота присвячена вирішенню актуального завдання, що полягає в підвищенні доступності послуг в мультисервісних телекомунікаційних мережах за рахунок розробки нового методу виявлення низькоінтенсивних атак типу «відмова в обслуговуванні» на прикладному рівні.

Одним з найбільш ефективних методів DOS-атак на хмарні інфраструктури є низькоінтенсивні DOS-атаки. Основна їх особливість полягає в тому, що вони витрачають ресурс прикладного рівня, який в кілька разів менше ресурсу транспортного рівня, на який спрямовані звичайні DOS-атаки.

Виявлення низькоінтенсивних DOS-атак проблематично, так як профіль трафіку такої атаки збігається з профілем звичайного трафіку в разі підключення поганої якості.

Аналіз традиційних методів виявлення і класифікації DOS-атак показав їх низьку ефективність у випадку низкоінтенсивніх атак на прикладному рівні.

З метою усунення даного недоліку в роботі розроблені моделі і метод виявлення низькоінтенсивних DOS-атак на web-сервер (slow-http).

Розроблено модель поведінки web-сервера, що дозволяє оцінити розподіл ймовірностей його станів в залежності від стану мережі та вхідного \ вихідного трафіку.

Розроблено модель визначення часу переходу web-сервера в стан «відмова в обслуговуванні».

Розроблено метод виявлення і класифікації атак на відмову в обслуговуванні прикладного рівня на web-сервер. Розроблений метод дозволяє виявити факт виконання атаки, визначити джерело нападу і блокувати зловмисний трафік.

Метод базується на аналізі поведінки сервера в нормальному режимі і при реалізації різновидів slow-http атак. Процес виявлення атаки реалізується на основі моделі Маркова, а також ймовірносно-часових графів.

Перевага пропонованої системи полягає в тому, що вона дозволяє виявляти атаку на відмову в обслуговуванні сервера, що дозволяє своєчасно активувати відповідні механізми захисту.

Ключові слова: хмарна інфраструктура, мультисервісні мережі, ланцюг Маркова, ймовірносно-часової граф, доступність сервісу, DOS-атака, slow-http атака.

ABSTRACT

Anders Carlsson. Model and method of detecting low-intensity attacks of application level. - The manuscript. Dissertation for the degree of a candidate of technical sciences in specialty 05.12.02 – telecommunication systems and networks, – Kharkov National University of Radio Electronics, – 2017.

The dissertation is devoted to solving the actual problem, which is to increase the availability of services in multiservice telecommunication networks by developing a new method of detection low-intensity "denial of service" attacks at the applied level.

One of the most effective methods of DOS attacks on cloud infrastructure is low-intensity DOS attacks. Their main feature is that they spend an application-level resource that is several times smaller than the transport-level resource to which ordinary DOS attacks are directed.

Detection of low-intensity DOS attacks is problematic, since the traffic profile of such an attack coincides with the profile of normal traffic in case of connection poor quality.

The web server behavior model is developed, which allows to estimate the distribution of probabilities of its states depending on the network status and incoming / outgoing traffic.

A model for determining the transition time of a web-server to a state of "denial of service" was developed.

The method of detection and classification of attacks on the refusal to maintain the application level on a web-server is developed. The developed method can detect the fact of an attack, determine the source of the attack and block malicious traffic.

The method is based on the analysis of server behavior in the normal mode and in the implementation of varieties of slow-http attacks. The process of detecting an attack is realized on the basis of the Markov model, as well as probabilistic-time graphs.

The advantage of the proposed system is that it allows you to detect an attack on denial of service of the server, which allows timely activation of the corresponding security mechanisms.

Key words: cloud infrastructure, multiservice networks, Markov chain, probabilistic-time graph, service availability, DOS attack, slow-http attack.