ПРАВИЛА ОФОРМЛЕННЯ МАТЕРІАЛІВ
ДЛЯ УЧАСТІ В КОНФЕРЕНЦІЇ
«ПРИКЛАДНА МАТЕМАТИКА ТА КОМП'ЮТИНГ»

Для участі в конференції до Оргкомітету подаються такі матеріали:

I. ЗАЯВКА НА УЧАСТЬ В КОНФЕРЕНЦІЇ
II. ТЕЗИ ДОПОВІДІ (1 примірник)
III. ВІДОМОСТІ ПРО АВТОРІВ ТЕЗ ДОПОВІДІ
IV. КОПІЯ КВИТАНЦІЇ ПРО СПЛАТУ ОРГВНЕСКУ

I. ОФОРМЛЕННЯ ЗАЯВКИ НА УЧАСТЬ В КОНФЕРЕНЦІЇ

Учасники конференції подають до Оргкомітету заявку за таким зразком:

До Оргкомітету конференції
«Прикладна математика та
комп'ютинг»

З А Я В К А

Ми, що нижче підписалися, ПЕТРЕНКО Микола Валерійович, студент 6-го курсу ФПМ, гр. КВ-24мн,
та ВАСИЛЕНКО Володимир Сергійович, к.т.н, доцент кафедри СПСКС,
просимо допустити нас до участі в конференції з доповіддю на тему «СПОСІБ УЩІЛЬНЕННЯ МУЛЬТИМЕДІЙНИХ ДАНИХ».

З правилами оформлення матеріалів для участі в конференції ознайомлені.

Сплату оргвнеску до 27 листопада 2023 року гарантуємо.

Дата _____ Петренко М.В.
(підпис)
_____ Василенко В.С.
(підпис)

II. ОФОРМЛЕННЯ ТЕЗ ДОПОВІДІ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Обсяг тез доповіді має складати 4 – 5 сторінок формату А4 набрані 14-м кеглем з одинарним міжрядковим інтервалом (39 – 40 рядків на сторінці). Для забезпечення одинарного інтервалу в меню Формат редактора MS Word натиснути Абзац і вибрати Міжрядковий інтервал Одинарний.

Примітка. Дані Правила оформлені саме з таким міжрядковим інтервалом (39 – 40 рядків на сторінці).

Тези надсилаються на адресу dlv1973@ukr.net за узгодження з науковим керівником.

Оргкомітетом приймаються тези доповіді, які мають такі необхідні структурні елементи (розділи):

1. **Заголовок**
   а) номер УДК,
   б) науковий ступінь, вчене звання, прізвище та ініціали авторів,
   в) назва організації, яку представляють автори,
   г) назва тез доповіді (назва повинна коротко і максимально точно відображати сутність проведених досліджень).
2. **Резюме** – англійською мовою (для англомовних тез – українською)
   а) ім'я, прізвище автора (авторів), назва тез,
   б) коротка анотація, 3-4 речення, – про що йдеться в тезах доповіді; що розглянуто, запропоновано, вирішено (найголовніше).
3. **Вступ**
   а) постановка проблеми в загальному вигляді та її зв'язок з важливими науковими чи практичними задачами,
   б) короткий аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор (автори),
   в) виділення невирішених раніше питань загальної проблеми, яким присвячується доповідь.
4. **Постановка задачі**
   (формулювання мети тез доповіді).
5. Виклад основного матеріалу наукового дослідження з поділом його на частини (розділи) **з відповідними назвами**
   а) вибір методів, підходів, моделей та інструментів розв'язання поставленої задачі,
   б) власне розв'язання поставленої задачі,
   в) приклади застосування отриманих результатів.
6. **Висновки**
   а) підсумки даного дослідження,
   б) перспективи подальших розвідок у цьому напрямку.
7. **Література**

ВИМОГИ ДО ТЕКСТУ ТЕЗ ДОПОВІДІ

1. Мова: українська (або англійська); резюме – англійською (або українською).
2. Текст тез (крім назви тез та резюме) має бути набраний 14-м кеглем з одинарним інтервалом з вирівнюванням по ширині формату А4 з полями таких розмірів:
   - верхнє поле – 25 мм;
   - нижнє поле: до тексту – 35 мм, до колонтитула – 25 мм;

- ліве поле – 25 мм;
- праве поле – 25 мм.

Текст резюме – 12-м кеглем, курсивом; 3-4 речення, до 8-ми рядків.

3. Номери сторінок не проставляються.
   Ілюстрації й таблиці, розміщені на окремих сторінках, також включають до загальної нумерації сторінок.
4. Текст тез набирається в текстовому редакторі MS Word з дотриманням таких вимог: шрифт Times New Roman (розмір кегля 14), відступ першого рядка 10 мм. Клавішу «ENTER» використовувати тільки в кінці абзацу.

Одиниці фізичних величин набирають звичайним шрифтом і розміщують в один рядок з їх числовим значенням.

У математичних формулах і рівняннях цифри, літери грецького, готичного і кириличного алфавітів слід набирати звичайним шрифтом. Літери латинського алфавіту слід набирати *курсивом*, – крім математичних функцій, температури, умовних математичних скорочень.

Нумерують тільки ті формули, на які є посилання в тексті.

Індекси і показники степеня мають бути однакового розміру.

5. Формули слід набирати в редакторі формул Microsoft Equation 3.0 або Math Type. При наборі формул необхідно зробити такі установки:

Меню «Стиль»

Стиль	Шрифт	Формат символів
Текст	Times New Roman	
Функція	Times New Roman	
Змінна	Times New Roman	Курсив
Грецькі	Symbol	
ГРЕЦЬКІ	Symbol	
Символ	Symbol	
Матриця-вектор	Times New Roman	Напівжирний
Числа	Times New Roman	

Меню «Розмір»

Звичайний	14 пт
Великий індекс	10 пт
Малий індекс	12 пт
Великий символ	15 пт
Малий символ	12 пт

6. Оформлення **Заголовка** тез доповіді відрізняється від оформлення текстової частини.

Елементи заголовка розміщуються в такій послідовності:
УДК та його номер; через один рядок з абзацу – науковий ступінь, вчене звання, прізвище та ініціали автора (авторів); через один рядок – назва організації, яку представляють автори; через один рядок – назва тез доповіді, великими літерами.

Всі елементи заголовка (крім УДК) виконуються напівжирним

шрифтом, розмір шрифту – 14 пт, для назви тез – 16 пт.

Приклад оформлення заголовка (його доцільно скопіювати і підставити свої атрибути):

УДК 681.301

К.т.н, доцент Василенко В.С., магістрант Петренко М.В.

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

СПОСІБ УЩІЛЬНЕННЯ МУЛЬТИМЕДІЙНИХ ДАНИХ

7. **Резюме** подається англійською мовою (для англомовних тез – українською), розмір шрифту – 12 пт:
   - ім'я, прізвище автора (авторів) (1-й рядок) напівжирним прямим шрифтом,
   - назва тез (2-й рядок) – напівжирним шрифтом, *курсивом*;
   - основний текст резюме – з наступного рядка з абзацу, 3-4 речення, *курсивом*.

8. Елементи текстової частини тез доповіді розміщуються після назви тез доповіді в такій послідовності:

Через один рядок з абзацу – назва структурного елемента (розділу), наприклад, **Вступ** тощо; через один рядок з абзацу – текст розділу; через один рядок з абзацу – назва наступного структурного елемента (розділу) і т.д.

Назва розділу не повинна завершуватися крапкою.

Назву розділу не розміщувати в останньому рядку сторінки.

Абревіатури в назвах розділів не використовують, їх слід розшифровувати у тексті (крім загальноприйнятих, наприклад, ЕОМ, САПР, АСУ тощо). Якщо назва розділу складається з двох речень, то їх слід відокремити крапкою.

9. У тезах доповіді необхідно дотримуватись термінології та позначень відповідно до прийнятих міжнародних та державних стандартів. Використовуючи новий термін чи абревіатуру, автор повинен розшифрувати та пояснити їх.

10. При виборі одиниць фізичних величин слід дотримуватись системи СІ.

11. Формули, рисунки, таблиці мають просту арабську наскрізну нумерацію та повинні міститися після першого посилання на них у тексті. Примітки друкують під таблицею.

12. Рисунки (схеми, діаграми, графіки) мають бути виконані за

допомогою CorelDraw, MS Visio, MS Excel або засобами MS Word. Кожний рисунок повинен мати підпис. Цифрові позначення на рисунках мають бути пропорційні розміру рисунка. Товщина контурних ліній – 0,8-1,0 мм, допоміжних – 0,5 мм, масштабної сітки – 0,3 мм. Рисунки, які мають позиції *а, б*,…, повинні бути однакової висоти і скомпоновані по горизонталі.

13. Кожна таблиця повинна мати заголовок (назву). Назви таблиць та рисунків робити звичайним шрифтом, розмір кегля 12 пт.

14. Рисунки, таблиці слід подавати компактно та застосовувати обтікання тексту зліва або/та справа від них.

15. Список літератури (бажано не більше 5-ти джерел) подається в порядку посилання. Неприпустиме посилання на неопубліковані та незавершені науковій праці.

Приклад подання списку літератури:

Література

1. Говорущенко Т. О. Методологія оцінювання достатності інформації для визначення якості програмного забезпечення. – Хмельницький національний університет. – 2017. – 310 с.
2. Грицюк Ю. І. Використання пелюсткових діаграм для візуалізації результатів експертного оцінювання якості програмного забезпечення / Ю. І. Грицюк, В. С. Далявський // Науковий вісник НЛТУ України. – 2018. – Т. 28, № 9. – С.95-104.
3. Кузь М. В. Прогнозування якості програмних засобів на основі аналізу якості вимог / М. В. Кузь, Б. С. Незамай, В. А. Ровінський, Н. Д. Подубинська // Методи та прилади контролю якості. - 2023. - № 1(50). – С. 101 - 112.
4. Goyal S. Comparison of Machine Learning Techniques for Software Quality Predition // International Journal of Knowledge and Systems Science. - 2020. – Vol. 11, № 2. – P. 20 - 40.
5. Hovorushchenko T. Method for forecasting the level of software quality based on quality attributes / T. Hovorushchenko, D. Medzatyi, Y. Voichur, M. Lebiga // Journal of Intelligent and Fussy Systems. - 2023. - № 44(3). – P. 3891 - 3905.

ЕЛЕКТРОННА ВЕРСІЯ ТЕЗ ДОПОВІДІ

Електронна версія тез доповіді надсилається на адресу dlv1973@ukr.net. Разом з електронною версією тез подається заявка і відомості про авторів.

Після затвердження тез Програмним комітетом конференції автору надсилається повідомлення, що тези прийняті до друку.

Всі питання, які виникають, можна узгодити з Дрозденко Любов Володимирівною, кімната 105 – 15, тел. (044) 204-91-13, 093-9856684 (Telegram, Viber), e-mail: dlv1973@ukr.net).

Для назв файлів використовувати латинські літери (бажано прізвище магістранта (аспіранта) англійською мовою).

III. ВІДОМОСТІ ПРО АВТОРІВ ТЕЗ ДОПОВІДІ

Відомості про авторів тез доповіді подаються одночасно з першим варіантом тексту тез і мають містити такі дані: назву тез доповіді; прізвище, ім'я, по-батькові, науковий ступінь, вчене звання, адресу (домашню або службову), контактний телефон, електронну адресу кожного автора.

Приклад оформлення відомостей про авторів:

ВІДОМОСТІ
ПРО АВТОРІВ ТЕЗ ДОПОВІДІ
НА ТЕМУ
«СПОСІБ УЩІЛЬНЕННЯ МУЛЬТИМЕДІЙНИХ ДАНИХ»
на конференції «Прикладна математика та комп'ютинг»

1) ПЕТРЕНКО Микола Валерійович – магістрант ФПМ КПІ ім. Ігоря Сікорського, група КВ-22мн,

Домашня адреса: м. Київ, проспект Миколи Бажана, 14, кв. 85, тел. 573-06-28, контактний телефон: 050-3268425, електронна адреса: petrenko@gmail.com

2) аналогічно для іншого автора.

IV. КОПІЯ КВИТАНЦІЇ ПРО СПЛАТУ ОРГВНЕСКУ

Сплатити оргвнесок можна за реквізитами:

Р/Рахунок:	UA768201720313201001201013853
Банк :	ДКСУ м. Києва
МФО :	820172
ЕДРПОУ:	02070921
Отримувач:	КПІ ім. Ігоря Сікорського
Сума	**300,00** грн.
Призначення платежу:	Оплата за участь у конференції ПМК-23 (**Прізвище, ім'я, по-батькові**), в.т.ч.ПДВ-50,00 грн. Б/н 521

Після сплати оргвнеску копію квитанції. надіслати на адресу dlv1973@ukr.net

Оргвнесок сплатити до 27 листопада 2023 року, інакше Ви не будете допущені до виступу на конференції і Ваші тези доповіді надруковані **НЕ БУДУТЬ**.

V. ЗРАЗОК ОФОРМЛЕННЯ ТЕКСТУ ТЕЗ ДОПОВІДІ

УДК 004.7:004.056.5

К.т.н., асистент Погорелов В.В., магістрант Кравчук А.А.

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

МОДИФІКОВАНИЙ МЕТОД ВИЯВЛЕННЯ DDoS-АТАК ПРИКЛАДНОГО РІВНЯ НА РЕСУРСИ КОМП'ЮТЕРНИХ СИСТЕМ

Abstract

Volodymyr Pogorelov, assistant, PhD; Kravchuk Arkadii, student
Combined method of detecting application layer DDoS attacks on computer systems resources

This paper concerns the task of fast detection of application-level DDoS attacks on webservers. Existing algorithms based on statistical analysis and machine learning are studied and discussed. The modified method with calculating informational entropy of HTTP request attributes is proposed. The comparative analysis of performance of both the SVM method and the modified algorithm is fulfilled. The ways for further research are proposed as well.

Вступ

Сьогодні тренд діджиталізації, тобто цифрової трансформації суспільства, активно поширюється. Але на заваді цьому можуть стати DDoS-атаки, відсутність захисту від яких спричиняє простій атакованої системи, що призводить до матеріальних збитків, втратити репутації та довіри клієнтів. З кожним роком кількість пристроїв, підключених до мережі Інтернет, постійно збільшується, як і кількість проведених DDoS-атак, за даними огляду експертів [1]. Проблема захисту ресурсів комп'ютерних систем від таких атак полягає саме в своєчасному виявленні факту проведення атаки і встановленню її джерел. Відповідно до наявних

досліджень [2], для ідентифікації DDoS-атак прикладного рівня немає водночас ефективного та швидкодіючого методу, бо класичні методи, які добре підходять для мережевого рівня, не є дуже точними в даному випадку.

Таким чином, проблема виявлення розподілених атак на відмову в обслуговуванні ресурсів комп'ютерних систем є актуальною та потребує дослідження. Тому у даній роботі пропонується модифікований метод виявлення DDoS-атак прикладного рівня, який швидко виявлятиме джерела атак, разом з тим не втрачаючи точності ідентифікації.

Постановка задачі

Метою даного дослідження є підвищення ефективності аналізу даних Інтернет-трафіку для виявлення DDoS-атак прикладного рівня шляхом розробки та програмної реалізації методу, у якого час реагування на вторгнення буде менший, ніж в існуючих методів та алгоритмів. Відповідно до вказаної мети необхідно розв'язати такі задачі: оглянути наявні методи розпізнавання DDoS-атак прикладного рівня, запропонувати новий метод виявлення таких атак зі збільшеною швидкодією, експериментально перевірити ефективність розробленого методу.

Термінологія

LR-DDoS (скор. від англ. low-rate DDoS) – низькошвидкісні DDoS-атаки, що відзначаються низькою частотою запитів та націленістю на вичерпування ресурсів саме прикладних програм.

Middleware – шар ПЗ, який є посередником між компонентами певного фреймворку. Зазвичай підключається як додатковий програмний модуль, який має доступ до компонентів системи та може виконувати свій алгоритм.

Аналіз існуючих підходів та алгоритмів

DDoS-атаки можуть поділятися за темпом надсилання запитів на дві категорії: високошвидкісні та низькошвидкісні. Високошвидкісні атаки виснажують канали передачі даних, в свою чергу LR-DDoS – обчислювальні ресурси. Останні мають низьку швидкість і використовують ресурсоємні операції, як, наприклад, запис в базу даних великого об'єму інформації.

Високою швидкодією виявлення DDoS-атак вирізняється метод, який обчислює інформаційну ентропію [3], бо розраховується за достатньо простою формулою. Але в звичайній реалізації цей метод використовує атрибути мережевого рівня моделі OSI. Тому для виявлення LR-DDoS атак цим методом необхідно модифікувати процес збору параметрів, додавши атрибути з прикладного рівня, та вивести спосіб обчислення значень їх ентропії. Крім цього, методи машинного навчання, а саме: метод опорних векторів, штучні нейронні мережі – мають високу точність ідентифікації LR-DDoS атак, але водночас мають і велику обчислювальну складність [4].

Опис запропонованого методу

Одним із найпопулярніших прикладних протоколів в мережі Інтернет є протокол HTTP(S) для вебсторінок, оскільки зазвичай саме вебсайт є кінцевим інтерфейсом для отримання інформації чи надання послуг. Тому запропонований метод розроблявся для протоколу HTTP(S).

По-перше, було запропоновано модифікувати метод на основі інформаційної ентропії. В звичайній реалізації даного методу обчислюється ентропія кількості мережевих пакетів за наступною формулою:

$$H(x) = -p(x)\log_2 p(x) \tag{1}$$

де $p(x)$ – ймовірність появи символу x з певного алфавіту.

В формулі (1) для звичайної реалізації методу ймовірність появи пакетів $p(x)$ від джерела k обчислюється наступним чином:

$$p(x) = x_k \Big/ \sum\nolimits_i x_i \tag{2}$$

де x_i – кількість пакетів від *i*-го джерела за встановлений проміжок часу.

Згідно з дослідженням [5] було визначено атрибути HTTP запитів, аналіз яких може вказати на факт проведення LR-DDoS атаки, а саме: URI запиту та його HTTP метод, клієнт (User-Agent) запиту, розмір запиту, час обробки запиту вебсервером. Для обчислення ентропії вищезазначених характеристик, необхідно адаптувати формулу (1) та вивести спосіб розрахунку ймовірностей появи цих атрибутів, який використовується в формулі (2). Нехай, кожен запит можна представити множиною значень $\{s,u\}$, де: s – IP адреса та порт джерела, u – URI та метод запиту. З набору множин всіх запитів для кожного унікального джерела s_i можна визначити унікальні URI і методи запитів u_j^i, а також кількість повторів відповідної унікальної пари – позначимо як $c(u_j^i)$. Тоді для джерела s_i ентропія такого параметру як URI та метод запиту H_u становитиме:

$$H_u(s_i) = -\sum\nolimits_j p_u(u_j^i)\log_2 p_u(u_j^i);\ \ p_u(u_j^i) = \frac{c(u_j^i)}{\sum_i \sum_j c(u_j^i)} \tag{3}$$

де $p_u(u_j^i)$ – ймовірність появи унікальної пари URI і методу запиту u_j^i серед всіх зафіксованих пар за встановлений проміжок часу.

Відповідно для інших атрибутів, а саме: клієнт запиту, розмір запиту – ентропія обчислюється аналогічно як в формулі (3). Тільки ймовірність для характеристики часу обробки запиту вебсервером буде розраховуватись іншим чином. Час обробки запиту можна вважати неперервною випадковою величиною. Для запитів з однаковим URI та методом час надання відповіді сервером теж буде приблизно однаковим, тому можна сказати, що розподіл цієї величини є нормальним. З цього випливає, що ймовірність $p_t(t_j^i)$ для характеристики часу обробки t_j^i певного запиту від *i*-го джерела для *j*-ої

пари URI та методу запиту буде дорівнювати ймовірності попадання значення нормально розподіленої випадкової величини в заданий інтервал:

$$p_t(t_j^i) = \Phi\left(\frac{t_j^i + \delta - a}{\sigma}\right) - \Phi\left(\frac{t_j^i - \delta - a}{\sigma}\right) \quad (4)$$

де $\Phi(x)$ – значення функції Лапласа для змінної x; a – середнє значення часу обробки запиту для відповідної пари URI та методу запиту; σ – середнє квадратичне відхилення значення часу обробки запиту для відповідної пари URI та методу запиту; δ – додатне значення для допустимого часового інтервалу, яке близьке до 0, причому $\delta \square\ t_j^i$.

Формулу (4) слід використати як значення ймовірності в формулі (3) для обчислення ентропії характеристики часу обробки запиту H_t.

Загальна архітектура запропонованого методу складається з наступних етапів: збір, обробка, класифікація даних та ідентифікація джерел атак. Етап збору даних має свої особливості, адже треба отримати інформацію з декількох рівнів моделі OSI. Вхідні пакети транспортного рівня можна отримати, якщо є доступ до маршрутизатора або мережевого інтерфейсу. Але так як один HTTP запит може бути розбитий на декілька пакетів, то необхідну інформацію прикладного рівня треба отримати за допомогою розробленого middleware для вебсерверу. Тому в даному досліджені запропоновано програмний модуль для вебфреймворку (на прикладі Express.js), який вимірює час обробки кожного запиту та зберігає поля заголовків з необхідними атрибутами. Щоби зіставити потім ці дані з даними відповідних мережевих пакетів, middleware для кожного запиту визначає IP-адресу та порт відправника і отримувача. Зібрані дані з різних джерел відправляються до брокера повідомлень, наприклад, Kafka.

Обробка даних полягає у формуванні єдиного об’єкту параметрів з транспортного та мережевого рівнів: для цього серед зібраної інформації об’єднуються атрибути з однаковим часом захоплення, адресами відправника та отримувача. Для класифікації формується масив об’єктів з оброблених параметрів за певний часовий проміжок розміром Δt. Даний масив надається вищеописаному методу на основі інформаційної ентропії для отримання відповідних результатів. На заключному етапі ідентифікації джерел атак використовуються обчисленні показники ентропії визначених атрибутів кожного джерела, яке було зафіксовано в даному часовому проміжку, та порівнюються з пороговим значенням, внаслідок чого джерело може бути позначено як зловмисне. Порогове значення встановлюється емпірично та може коригуватись відповідно до зміни статистичних показників, наприклад, дисперсії величини одного з атрибутів.

Результати експериментальних досліджень

Запропонований метод було реалізовано на мові програмування Python. Для порівняння взято метод SVM з наявного дослідження [4] і також реалізовано на цій ж мові. Було використано датасет 2017 CIC DoS як вхідні дані. Для оброблення кожної тисячі значень з масиву вхідного набору даних в середньому витрачалось 2.46 секунд запропонованим методом, а методом SVM – 3.89 секунд на одному й тому самому комп'ютері. Отже, запропонований в даному дослідженні метод має дійсно більшу швидкодію.

Висновки

Отже, дана стаття була присвячена розробці модифікованого методу виявлення DDoS-атак прикладного рівня. Запропонований метод дозволяє підвищити швидкодію ідентифікації джерел DDoS-атак на вебсервери. Ідея дослідження полягала в тому, щоб використати метод на основі інформаційної ентропії, який має малу обчислювальну складність, та адаптувати його для прикладного рівня, шляхом виведення способу обчислення ентропії атрибутів HTTP запиту, серед яких є час його обробки.

Подальшого дослідження потребують наступні питання: алгоритм коригування порогового значення для ідентифікації атак; використання розподіленого обчислення для нових додаткових параметрів (наприклад, статистичних) на кластерах Hadoop екосистеми або Kubernetes.

Література

1. Cyberedge Group 2021 Cyberthreat Defense Report [Електронний ресурс] / CyberEdge. — Режим доступу: https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf.
2. *Kaur, P.* A review of detection approaches for distributed denial of service attacks [Text] / P. Kaur, M. Kumar, A. Bhandari // Systems Science & Control Engineering. — 2017. — Vol. 5, № 1. — P. 301 – 320.
3. *Bhuyan, M.H*. E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric [Text] // Security and Communication Networks. — 2016. — Vol. 9, № 16. — P. 3251 – 3270.
4. *Pérez-Díaz, J.A*. A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning [Text] // IEEE Access. — 2020. — Vol. 8. — P. 155859 – 155872.
5. *Mohammed, A*. Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks [Text] // The Scientific World Journal. — 2015. — Vol. 2015, Article ID 238230.