УДК 004.272

Петровська Н.О., магістр; **Трапезон К.О.**, к.т.н.

ВПЛИВ DDoS-АТАК НА «МЕРЕЖЕВИЙ ОРГАНІЗМ». ЗАГАЛЬНИЙ ПІДХІД ДО СИМУЛЯЦІЇ В СЕРЕДОВИЩІ OMNeT++

Petrovska N.O., Trapezon K.O. Influence DDoS-attack on the «Network body». General approach to environment simulation in OMNeT++. For the modern world the word "cybercrime" has long ceased to be a new and after some time acquired great popularity in business plane. Large and small corporate computer networks are exposed to the greatest risk because the purpose of any cyber attacks is often economic benefit. Ignoring the basic principles of network security policies, corporations endanger primarily their information sources. Moreover, the repeated loss of business from security breaches greatly exceed the cost of its implementation and support. One of the most common types of attacks is to attack denial of service due to which users lose access to computer resources and related services that prevents the normal exchange of data.

The danger of DDoS-attacks is also in that they threaten not only the servers of the companies themselves, but also the infrastructure provider side. Since the simulation is an effective means of developing methods for identifying and easing the impact of DDoS-attacks on computer networks basic principle and characteristics, that are necessary for understanding and correct formulation of the problem during simulation of this type of attack. Particular attention is paid to the parameters of DDoS-attacks that can change in the course of the experiments and the values of which affect the flow of the dynamic process of spreading attacks on the network.

Keywords: DDoS, OMNeT++, attack, imitational modeling, model

Петровська Н.О., Трапезон К.О. Вплив DDoS-атак на «мережевий організм». Загальний підхід до моделювання в середовищі OMNeT++. Атака на відмову в обслуговуванні є одним із найпопулярніших видів атак, спрямованих на перешкоджання комерційній діяльності підприємств, шляхом завдання шкоди їх інформаційним ресурсам. В статті представлений аналіз впливу DDoS-атак на працездатність комп'ютерних мереж, перераховані основні характеристики даного типу та сформовано загальний підхід до моделювання атаки на відмову в обслуговуванні в комп'ютерних мережах. Результати роботи можуть бути корисними на етапі проектування мережі та розробки політики безпеки.

Ключові слова: DDoS, OMNeT++, атака, імітаційне моделювання, модель

Петровская Н.А., Трапезон К.А. Влияние DDoS-атак на «сетевой организм». Общий подход к моделированию в среде OMNeT++. Атака на отказ в обслуживании является одним из самых популярных видов атак, направленных на препятствование коммерческой деятельности предприятий путем причинения вреда ее информационным ресурсам. В статье представлен анализ влияния DDoS-атак на работоспособность компьютерных сетей, перечислены основные характеристики данного типа атак и сформирован общий подход к моделированию атаки на отказ в обслуживании в компьютерных сетях. Результаты работы могут быть полезными на этапе проектирования сети и разработки политики безопасности.

***Ключевые слова*:** DDoS, OMNeT++, атака, имитационное моделирование, модель

Вступ

Атака розподіленої відмови в обслуговуванні (DDoS) продовжує стрімко розвиватися протягом останніх двох десятиліть. Відносна простота реалізації, складність відслідковування і катастрофічні ефекти для «жертви» роблять DDoS-атаки популярним вибором у світі кіберзлочинності. До теперішнього часу дослідники запропонували безліч рішень для виявлення і пом'якшення дії DDoS-атак, але дуже мало уваги приділяється дослідженню методів їх запобігання. Використання середовища імітаційного моделювання OMNeT++ за допомогою додаткових фреймворків (INET Framework) та інструментів (ReaSE і ReaSEGUI tools) дає можливість зімітувати механізм поширення DDoS-атаки в «мережевому організмі», виявити його слабкі місця та зпрогнозувати можливі наслідки для інформаційних ресурсів системи. Таким чином, попереднє створення та тестування моделі комп'ютерної мережі є першочерговою задачею для комерційних підприємств, які піклуються про безпеку своїх інформаційних ресурсів та продуктивність роботи самої мережі.

Оскільки імітаційне моделювання є ефективним засобом розробки методів виявлення та ослаблення впливу DDoS-атак на комп'ютерні мережі, в роботі наведено їх принцип дії та основні характеристики, розуміння яких необхідне для правильної постановки задачі на етапі моделювання мережі та проведення симуляції даного типу атак. Особлива увага приділяється параметрам DDoS-атак, які можна змінювати в процесі проведення експериментів і значення яких впливають на перебіг динамічного процесу поширення атаки в мережі.

1. DDoS-атака – мережевий ГРВІ

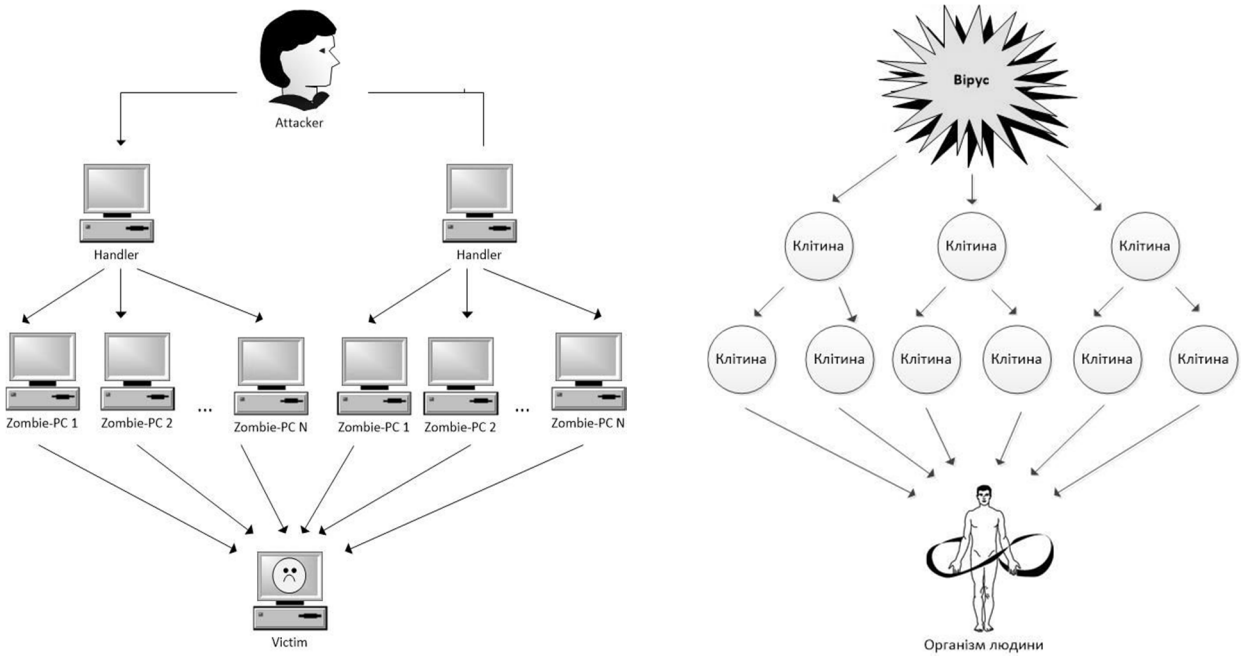
DDoS-атака (Distributed Denial-of-service attack) – є розподіленою атакою на відмову в обслуговуванні комп'ютерної системи під час якої серверу або іншому ресурсу мережі надсилається велика кількість запитів з різних точок доступу. Кінцевою метою атаки є обмеження пропускної здатності мережі, що робить комп'ютерні ресурси недоступними для її користувачів і порушує процес нормального обміну даними [1].

Принцип дії звичайної DDoS-атаки можна порівняти із впливом ГРВІ на організм людини, який здійснюється в три етапи (рис. 1).

1 етап: *Attacker (Атакуючий)/вірус* подає команду на *Handler (Керуюча консоль)*, від якої потім надходитимуть сигнали про атаку на інші комп'ютери. Цей самий алгоритм відбувається при *зараженні епітеліальних клітин вірусом.*

2 етап: *PCs-Zombie (Комп'ютери-зомбі)*, отримуючи сигнал від Handlers, починають атаку на «жертву», так само, як і *клітини-зомбі,* які з'явилися внаслідок ділення *зараженої вірусом епітеліальної клітини.*

3 етап: перевантаження пропускної здатності мережі або обмеження доступу до інформаційних ресурсів *Victim (жертви)* – ерозія слизистої носа та горла, зараження *організму людини.*



а) б)

Рис. 1. Порівняння принципів дії: а) DDoS-атаки та б) вірусної атаки

2. Основні характеристики DDoS-атак

DDoS-атаки можливі на всіх семи рівнях моделі OSI, але найчастіше зловмисники вдаються до атак на мережевому та транспортному рівнях, використовуючи ICMP-повідомлення або ICMP-запити для перевантаження пропускної здатності цільової мережі.

Серед основних характеристик, які відрізняють даний тип атак від інших, можна виділити: централізованість; синхронізація у часі; велика кількість використовуваних пристроїв (комп'ютерів-зомбі); складна локалізація зловмисника; «жертвою» може стати система або ПК будь-якої потужності; простота реалізації [2].

3. Середовище моделювання

В якості інструмента для моделювання мереж та процесів передачі інформації було обрано пакет моделювання OMNeT++, який відповідає усім вимогам:

- зручний та зрозумілий для користувача інтерфейс;
- реалістичність процесів моделювання;
- прозоре розгортання процесів виявлення атак в реальній системі;
- наявність усіх необхідних узгоджених інструментів.

Програма представляє собою інтегроване середовище, призначене для створення, налаштування і запуску імітаційних дискретних моделей. Це середовище, розроблене на основі мови C++, є масштабованим, модульним рішенням. OMNeT++ надає інфраструктуру для конструювання модулів, визначення структури повідомлень та визначення правил їх обробки. Його назва утворена від – Objective Modu ar Network Testbed in C++ (об'єктний модульний полігон для моделювання мереж на C++). В системі OMNeT ++ закладена детальна реалізація протоколів, починаючи від мережевого рівня, можливість написання і підключення власних надмодулів, розвинений графічний інтерфейс.

Програма OMNeT++ підходить для моделювання будь-якої мережі, основою якої є дискретне подія. Процес зручно відображається у вигляді об'єктів, що обмінюються повідомленнями.

Процес моделювання можна запускати в різних призначених для користувача інтерфейсах. Графічно анімований інтерфейс користувача зручний для демонстрації та налагодження мережі, а інтерфейс командного рядка зручний для внесення змін.

Основними компонентами OMNeT ++ є:

1) коренева бібліотека моделювання; 2) OMNeT ++ IDE на базі платформи Eclipse; 3) графічний інтерфейс виконуваного моделювання, посилання на виконуваний файл (Tkenv); 4) призначений для користувача інтерфейс командного рядка для виконання моделювання (Cmdenv); 5) документація, приклади.

OMNeT ++ працює на базі найпоширеніших операційних систем: (Linux, Mac OS / X, Windows) [3].

4. Симуляція засобами OMNeT++

Для симуляції дії DDoS-атак в середовищі OMNeT++ необхідне використання наступних компонентів: - INET Framework з відкритим початковим кодом, який містить молелі для Інтернет-стеку (TCP, UDP, IPv4, IPv6, OSPF, BGP и т.д.), протоколи провідного та безпровідного канального рівня (Ethernet, PPP, IEEE 802.11, и т.д.), падтримку мобільності, протоколів MANET, DiffServ, MPLS з LDP та RSVP-TE, декілька моделей додатків, а також багато інших протоколів і компонентів; - інструмент ReaSE, розроблений для створення реалістичних умов симуляції дискретних подій в середовищі OMNeT++, та розглядає можливість формування топології на AS-рівні та на рівні маршрутизатора, моделі атаки та трафіка атаки; - ReaSEGUI – зовнішній графічний користувацький інтерфейс, який дозволяє створювати топології файлів NED [4].

На етапі створення власної моделі для дослідження DDoS-атак користувач має зробити ряд необхідних налаштувань та задати усі необхідні парметри через графічний інтерфейс ReaSEGUI на вкладках Topology, Traffic Profiles, Server Settings та Replace Node Types (рис. 2).

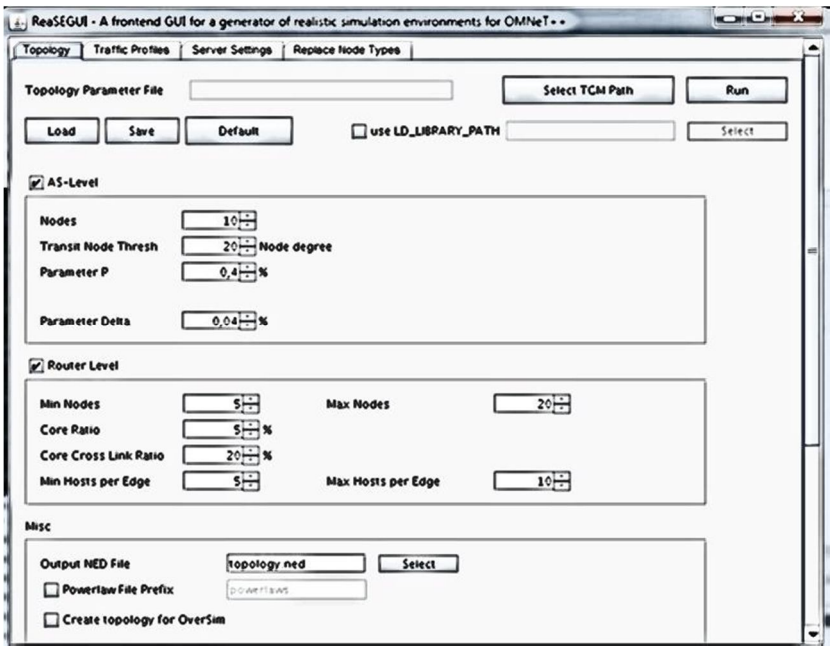


Рис. 2. Генератор реалістичного середовища між послідовним запитами моделювання ReaSEGUI

Інтерфейс дозволяє користувачу самостійно згенерувати топологію на AS-рівні, на рівні маршрутизатора або застосувати комбінацію двох способів (вкладка Topology). Налаштування профілю трафіка є одним з найважливіших етапів при симуляції DDoS атак. Вхідні дані, такі як мінімальний розмір запитуваного пакету, пакету-відповіді, мінімальна пакетів-відповідей, які надсилаються на кожен запит, мінімальний час очікування тощо, є необхідними для коректного розподілу ймовірностей (розподіл Парето з параметром 3) та підсумувань випадкових значень на основі нормального розподілу N (0; 1) по відповідному параметру (вкладка Traffic Profiles). Налаштування серверів та каналів між різними типами вузлів відбувається у вкладці Server Settings. Безпосередня генерація DDoS-атак задається у вкладці Replace Node Types за допомогою використання спеціальних додаткових об'єктів *DDoSZombie.* Це відбувається шляхом задання співвідношення у відсотках, яка показує скільки клієнтських вузлів моделі буде замінено на *DDoSZombie*, що здійснюють DDoS-атаки у мережі [5].

Приклад згенерованої за допомогою інтерфейса ReaSEGUI моделі зображено на рис. 3.

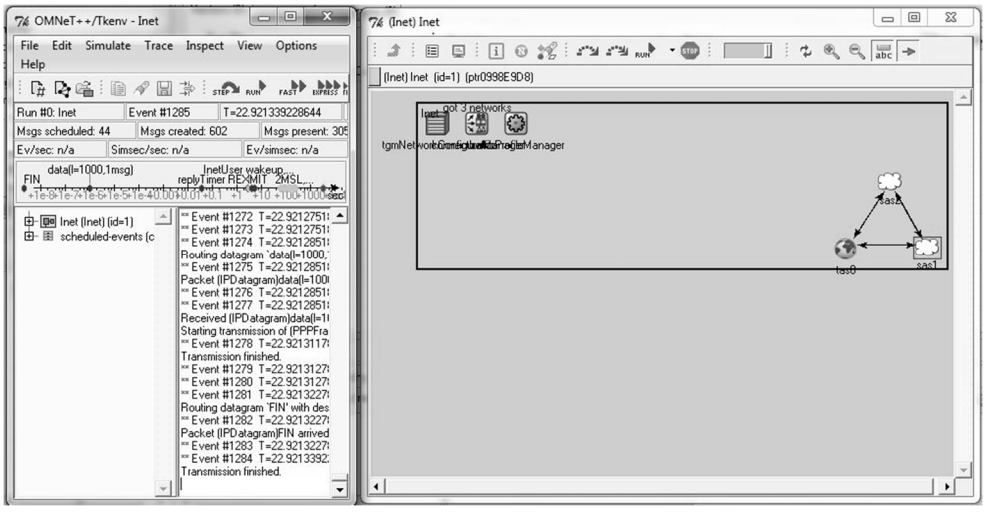


Рис. 3. Приклад симуляції згенерованої за допомогою ReaSEGUI моделі з *DDoSZombie*

Висновки

В роботі розглянуто сучасний стан проблеми впливу DDoS-атак на комп'ютерні мережі, серед яких було визначено та описано три етапи за які здійснюється кінцева мета проведення атаки. Не зважаючи на те, що даний тип атак здійснюється з багатьох різних пристроїв, він є централізованим (джерелом команд про атаку на «жертву» є лише один відповідний вузол зловмисника).

Імітаційне моделювання в середовищі OMNeT++ визначено ефективним методом попередження впливу DDoS-атак на комп'ютерну мережу за умови його застосування на етапі розробки та тестування системи.

Описано необхідний набір додаткових інструментів, необхідних для симуляції дії DDoS-атак та перелік параметрів, значення яких впливають на результати моделювання. Генерація атаки відбувається шляхом заміни клієнтських вузлів мережі на *DDoSZombie*, здійснюють DDoS-атаки.

Література

1. Уэнстром М. Организация защиты сетей Cisco / М. Уэнстром; пер. с англ. А.Г. Сивка - Москва: Издательский дом «Вильямс», 2005. – 768 с.

2. Котенко И.В. Исследование бот-сетей и механизмов защиты от них на основе методов имитационного моделирования / И.В. Котенко, А.М. Коновалов, А.В. Шоров // Изв. Вузов. Приборостроение. - 2010. - Т.53, №11. - С. 42-45.

3. OMNeT++ User Manual [Електронний ресурс] // – Режим доступу: https://omnetpp.org/doc/omnetpp/manual/usman.html (23.12.2015 р.).

4. Gamer T. Realistic Simulation Environments for IP-based Networks [Електронний ресурс] / T. Gamer, M. Scharf // – Режим доступу: http://doc.tm.kit.edu/2008/omnet2008.pdf (23.12.2015 р.).

5. Kotenko I. Simulation of Internet DDoS Attacks and Defense [Електронний ресурс] / I. Kotenko, A. Ulanov // – Режим доступу: https://pdfs.semanticscholar.org/a964/2c05418b726298a22f0eacd7190f8725e136.pdf (23.12.2015 р.).

Автори статті

Петровська Наталія Олександрівна – магістр кафедри звукотехніки та реєстрації інформації, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна. Тел. +38 063 336 69 04. E-mail: funybunny@ukr.net

Трапезон Кирило Олександрович – кандидат технічних наук, доцент кафедри звукотехніки та реєстрації інформації, Національний технічний університет України «Київський політехнічний інститут», Київ, Україна. Тел. +38 068 851 51 84. E-mail: trapezon@ukr.net

Authors of the article

Petrovska Nataliya Oleksandrivna – master of Department of Audio Engineering and Information Registration, National Technical University of Ukraine «Kyiv Polytechnic Institute», Kyiv, Ukraine. Tel. +38 063 336 669 04. E-mail: funybunny@ukr.net

Trapezon Kyrylo Oleksandrovych – candidate of science (technic), associate professor, associate professor of Department of Audio Engineering and Information Registration, National Technical University of Ukraine «Kyiv Polytechnic Institute», Kyiv, Ukraine. Tel. +38 068 851 51 84. E-mail: trapezon@ukr.net

Дата надходження в редакцію: 08.12.2015 р. Рецензент: д.т.н., проф. О.В. Барабаш