УДК 519.711.3

Рустам Камілович Мурасов *(канд. техн. наук)*
Ярослав В'ячеславович Мельник

Національний університет оборони України імені Івана Черняховського, Київ, Україна

ЗАВЧАСНЕ ПОПЕРЕДЖЕННЯ ПРО DDoS АТАКУ НА БАЗІ МЕТОДІВ ПРОГНОЗУВАННЯ

У статті на основі системного аналізу розглядаються сучасні способи DDoS-атак, наведена статистика щодо зростання кібернетичних атак по роках та збитки від них. Для своєчасної та ефективної протидії DDoS-атак, запропоновано здійснювати прогнозування DDoS-атак, розглядаючи їх як випадковий, нестаціонарний, скалярний процес. Дана методика не накладає обмежень на випадковий процес, забезпечує оптимальну точність прогнозу. Також дана методика застосовує кореляційні зв'язки проміж складовими, що відображається на достовірності прогнозу. Особливо ефективно прогнозування буде здійснюватись при різкій зміні стану випадкового процесу. Також не накладається обмеження на дисперсію випадкового процесу, що значно розширює можливості прогнозування.

Ключові слова: *DDoS-атаки; прогнозування; випадковий процес.*

Вступ

Роль Інтернету в сучасному суспільстві набігає вагомого значення. Спілкування, інформування, банківські послуги, медиаінформування, управління, сайти державних установ, Інтернет-магазини – все це напряму залежить від здатності функціонування системи Інтернету. Для організації роботи вказаних об'єктів вкладаються великі кошти та зусилля.

Зрозуміло що всі вищевказані об'єкти є ціллю для атаки зловмисників чи противника. Одним з видів Інтернет атак є DDoS-атака (Distributed Denial Of Service Attack).

Постановка проблеми. Особливістю даної атаки є те що зловмисники не ставлять за мету проникнення до захищеної комп'ютерної мережі чи викрадення/знищення даних. Метою даної атаки є паралізувати роботу веб-вузлу що атакується (Рис.1).

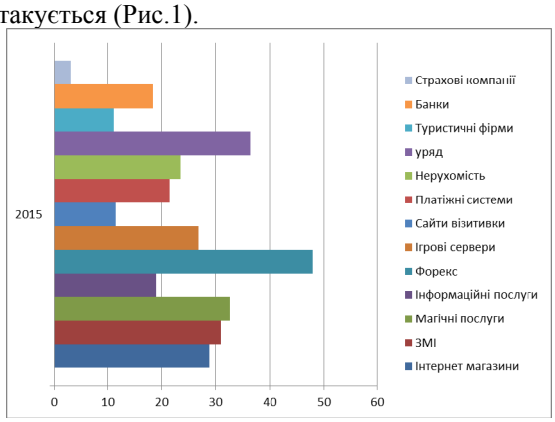

Рис. 1. Кількість DDoS атак по сферам.

Аналіз останніх досліджень і публікацій.

Перші згадки про DDoS-атаки відносяться до 1996 року. Але вперше, як про серйозну проблему було піднято питання у 1999 році коли було атаковано сайти таких великих корпорацій як: Amazon, Yahoo, CNN, eBay, E-Trade і інші менш відомі корпорації. Через рік атака повторилася, сайти були атаковані по DDoS технології при повному безсиллі мережевих адміністраторів. З того часу подібні атаки вже не рідкість (Рис.2).

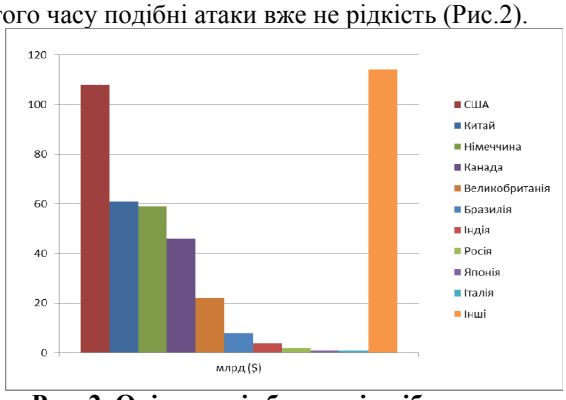

Рис. 2. Орієнтовні збитки від кібератак за 2015рік.

Метою статті є розгляд DDOS атаки, методи та способи її здійснення та шляхи вирішення протидії DDOS атаки.

Виклад основного матеріалу дослідження

Схема DDoS-атаки виглядає наступним чином (Рис.3). На обраний в якості жертви сервер здійснюється велика кількість хибних запитів з великої кількості комп'ютерів розташованих в різни місцях світу. Сервер витрачає час та ресурси на обробку цих запитів і стає практично недоступним для звичайних користувачів. Складність ситуації полягає ще в тому, що користувачі комп'ютерів з яких посилаються запити, можуть і не підозрювати про те що, їх машина використовується хакерами, так-як на неї встановлено спеціальні програми.

Класично схема будується як трьохрівнева структура. Ієрархічно така структура виглядає так.

Управляюча консоль – комп'ютер з якого зловмисник подає сигнал про початок атаки.

Головні комп'ютери – комп'ютери, котрі отримують сигнал з управляючої консолі та передають його комп'ютерам-зомбі. На одну

управляючу консоль може приходитись до кількох сотень головних комп'ютерів.

Агенти – безпосередньо заражені комп'ютери – зомбі, які атакують своїми запитами вузол-мішень.

Головною проблемою є проста організація даної атаки, Її розподіленість і те що ресурси зловмисників майже не обмежені.

Іншою проблемою є те, що зловмисникам не потрібно володіти спеціальними знаннями та програмами, все це знаходиться у вільному доступу мережі Інтернет. Це пов'язано з тим що, спеціальне програмне забезпечення DDoS створювалось для тестування роботи мереж і їх здатності до роботи в період навантажень та стійкості до зовнішніх навантажень. Найбільш ефективним є використання ICMP-пакетів (Internet control messaging protocol), пакетів які мають помилкову структуру. На обробку даного пакета необхідно більше ресурсів - після визначення про помилку пакет відправляється назад до відправника, таким чином навантаження мережі досягає максимального рівня.

З моменту появи перших програмних засобів було розроблено більш сучасне програмне забезпечення і на даний час існує такі DDoS атаки:

1. UDP flood – здійснюється відправка на адрес системи-цілі множені пакетів UDP (User Datagram Protocol). Даний метод використовувався в перших атаках і на даний час вважається найменш небезпечним. Програми які використовують цій тип атаки легко виявляються, так як при обміні головного контролера і агентів використовуються незашифровані протоколи TCP і UDP.

2. TCP flood - відправлення на адрес мішені множені TCP-пакетов, що також призводить до "зв'язування" мережевих ресурсів.

3. TCP SYN flood – відправлення великої кількості запитів на ініціалізацію TCP- з'єднань з вузлом – мішенню, що в результаті вимагає витрачати усі власні ресурсі на відстеження частково відкритих з'єднань.

4. Smurf-атака – пінг - запити ICMP (Internet Control Message Protocol) на адресу направленої широкомовної по адресу розсилки з використанням в пакетах запиту фальшивої адреси, адрес джерела в результаті є мішенню що атакована.

5. ICPM flood - атака, така сама, як Smurf але без використання розсилки.

Найбільш небезпечними є програми, що використовують одночасно декілька видів атак що було описано. Вони отримали назву TFN и TFN2K і вимагають високого рівня підготовки.

Однією з останніх і досконалих програм для DDoS-атак є Stacheldracht (колючий дріт), яка дозволяє організовувати різноманітні типи атак і лавини широковещательних пінг – запитів з шифруванням обміну даними проміж контролерами і агентами.

На даний час для протидії DDoS-атакам пропонується вирішити два типи задач:

1. Діагностувати DDoS-атаку на ранніх стадіях. Чім раніше буде діагностовано DDoS-атаку, тим раніше може втрутитися в процес мережевий адміністратор і тім раніше будуть проводитися анті DDoS заходи. Крім того, при виявленні DDoS-атакі можливо, не чекаючи дій адміністратора, автоматично запустити захолоди по протидії: задіяти резервні канали, увімкнути мережеві фільтри і.т.д.

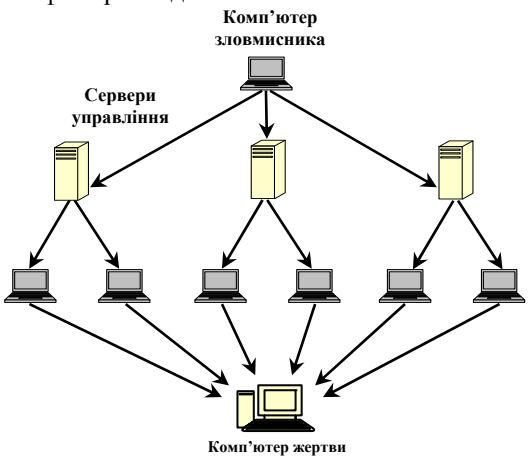

Рис. 3. Схема DDOS атаки.

2. Друга задача пов'язана з розподіленням мережевого трафіку на шкідливий та звичайний. Проаналізував трафік та виділивши шкідливий трафік створюються правіла для між мережевого екрану та ACL, або передати ці данні на вищестоящий мережевий маршрутизатор.

Перша задача є достатньо новою. Основним методом боротьби на даний час є виконання другої задачі. Але зловмисники удосконалюють способи і методи атак даного типу. Сучасні атаки відрізняються складністю і наявністю підготовчого етапу. Під час підготовчого етапу, зловмисник намагається виявити слабкі місця для атаки. Це можуть бути деякі скріпти, котрі здійснюють запити до бази даних, тим чином використовують ресурси системи, відслідковуючи час на відповідь запиту. Для виявлення подібних місць для атаки здійснюється серія міні DDoS-атак. Знайшовши слабке місце зловмисник може паралізувати сервер використовуючи бот-мережу меншого розміру. Якщо завчасно виявити DDoS-атаку мережевий адміністратор буде мати час на оптимізацію скриптів, побудови системи фільтрів та інше.

Для виявлення DDoS-атак за першим типом атаки визначимо такі методи що базуються на статистичному аналізі. Це кількісний аналіз, аналіз середньоквадратичних відхилень, кластерний аналіз, методи прогнозування випадкових процесів.

Основними параметрами за якими здійснюється аналіз атаки можуть бути:

- кількість запитів за визначений період;
- швидкість надходження запитів;
- кількість запитів з визначеного джерела чи мережі;

- кількість запитів до визначеного джерела (для web - серверу це визначений скріпт);
- час проміж запитами;
- інші параметри мережевої активності.

Крім того можемо розглядати DDoS-атаку як векторний випадковий процес з корельованами або некорельованими складовими. Де за складові можемо обрати джерело атаки, час запиту, частоту запитів, кількість запитів і т.д. – в залежності від наявності даних для аналізу.

Розглянемо математичну формалізацію DDoS-атаки.

Окрему DDoS-атаку розглянемо як скалярний випадковий процес без післядії. Даними випадкового процесу будуть кількість запитів за проміжок часу.

$$\overline{X} = \{x(1), x(2), ..., x(I)\}.$$

Найбільш універсальним з точки зору відсутності обмежень на клас випадкових процесів і зручним для обчислення є метод екстраполяції, що базується на канонічному розкладенні Пугачова. Дане розкладення в дискретному ряді точок t_i, $i = \overline{1,I}$ випадкового процесу що досліджується $\overline{X}(t)$ має вигляд

$$X_h = m_h(i) + \sum_{\lambda=1}^{h} \sum_{\upsilon=1}^{i} V_\upsilon^{(\lambda)} \phi_{h\nu}^{(\lambda)}(i), h = \overline{1,H}, \quad (1)$$

де $\phi_{h\nu}^{(\lambda)}(i)$ - невипадкові координатні функції, що визначаються як

$$\phi_{h\nu}^{(\lambda)}(i) = \frac{1}{D_\nu^{(\lambda)}} \overset{0}{M}[X_h(i) V_\nu^{(\lambda)}], \ \phi_{h\nu}^{(\lambda)}(i) = 0 \text{ при } i > \nu \text{ або } \lambda > h; \quad (2)$$

$\phi_{h\nu}^{(\lambda)}(i) = 1$ при $h = \lambda$ і $\nu = i$;

$V_\nu^{(\lambda)}$ - випадкові коефіцієнти , що мають наступні властивості :

$M[V_\nu^{(\lambda)}]=0$, $M[V_\nu^{(\lambda)} V_\mu^{(\varsigma)}]=0$ при невиконанні жодної умови $\nu = \mu$ і $\lambda = \varsigma$; $M[|V_\nu^{(\lambda)}|^2] = D_\nu^{(\lambda)}$.

Як слідує з (2), єдиним обмеженням що накладається на процес апаратом канонічних розкладень є конечність дисперсій відповідних коефіцієнтів, що звичайно задовольняється для реальних фізичних процесів і не є суттєвим.

Показано, що канонічне розкладення (1) точно описує функцію що розкладеться в точках дискретизації t_i, $i = \overline{1,I}$ і забезпечує мінімум середнього квадрату помилки наближення в проміжках проміж ними.

Таким чином, враховуючи переваги метода екстраполяції, що базується на канонічному розкладі випадкового процесу (відсутність на клас процесів що прогнозується, простота обчислення), даний підхід може бути прийнятим за основу в подальших дослідженнях.

Висновки й перспективи подальших досліджень

Вирішення даної задачі дозволить завчасно спрогнозувати та виявити DDoS-атаки та вжити необхідні заходи по протидії та захисту інформаційної та комп'ютерної мережі.

Література

1. Кудрицкий В. Д. Прогнозирующий контроль радиоэлектронных устройств / В.Д. Кудрицкий – К.:Техника, 1982. – 166 с. **2. CyberArk**, Security for the Heart of Enterprise http://www.cyberark.com/ (26.06.2015). **3. Butler B.** Interop network squares off against controlled 70G bit/sec DDoS attack. http://www.networkworld.com/article/2166091/data-center/interop-network-squares-off-against-controlled-70g-bit-sec-ddosattack.html (26.06.2015). **4. Wang J.**, Phan R. C.-W., Whitley J. N., Parish D. J. Advanced DDoS Attacks Traffic Simulation with a Test Center Platform // International Journal for Information Security Research (IJISR). 2011. Vol. 1(4).

ЗАБЛАГОВРЕМЕННОЕ ПРЕДУПРЕЖДЕНИЯ ОБ DDoS АТАКЕ НА БАЗЕ МЕТОДОВ ПРОГНОЗИРОВАНИЯ

***Рустам Камилович Мурасов** (канд. техн. наук)*
Ярослав Вячеславович Мельник

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье на основе системного анализа рассматриваются современные способы DDoS-атак, представлена статистика про увеличение количества кибернетических атак по годам и убытки нанесённые данными атаками. Рассмотрены варианты DDoS-атак и показаны современные программные комплексы, которые применяются. В статье для наглядности приведена классическая схема DDoS-атаки. Для своевременного и эффективного противодействия DDoS-атакам, предложено осуществлять прогнозирование DDoS-атак, рассматривая их как случайный, нестационарный, скалярный процесс. Данная методика не накладывает ограничений на случайный процесс, обеспечивает оптимальную точность прогноза. Так же данная методика применяет корреляционные связи между составными элементами, которые отображаются на достоверном прогнозе. Особенно эффективно прогнозирование будет осуществляться при резком изменении состояния случайного процесса. Также не накладывается ограничений на дисперсию случайного процесса, что значительно расширяет возможности прогнозирования.

Ключевые слова: *DDoS-атаки; прогнозирование; случайный процесс.*

EARLY WARNING INFORMATION ON DDOS ATTACKS BASED ON THE PREDICTION METHODS

Rustam K. Murasov ***(Candidate of Technical Sciences)***
Yaroslav V. Melnyk

National Defense University of Ukraine named after Ivan Chernyakhovsky, Kyiv, Ukraine

The article is based on the analysis considering modern methods of DDoS-attacks, presented statistics on the increase of cyber-attacks and losses them. To counteraction DDoS-attacks is proposed to forecast DDoS-attacks, considering them as random, transient, scalar process. This technique does not impose restrictions on the random process ensures optimum accuracy of the forecast. Also, this method uses the correlation between the components displayed on the reliability prediction. Especially prediction will effectively be carried out with a sharp change in the state of a random process. Also, there are no constraints on the variance of a random process, which significantly expands the possibilities of forecasting.

Keywords: *DDoS-attacks; forecasting; random process.*

References

1. Kudritskiy V.D. (1982), Predictive control of electronic devices. [*Prognozirujushhij kontrol' radiojelektronnyh ustrojstv*], Kyiv: Technic, 166 p. **2. CyberArk**, Security for the Heart of Enterprise.http://www.cyberark.com/ (26.06.2015). **3. Butler B.** Interop network squares off against controlled 70G bit/sec DDoS attack. http://www.networkworld.com/article/2166091/data-center/interop-network-squares-off-against-controlled-70g-bit-sec-ddosattack.html (26.06.2015). **4. Wang J.**, Phan R. C.-W., Whitley J. N., Parish D. J. (2011), Advanced DDoS Attacks Traffic Simulation with a Test Center Platform, International Journal for Information Security Research (IJISR), Vol. 1(4).

Отримано: 06.08.2016 року.