УДК 681.51:519.876

У.О. Яциковська,
І.В. Васильцов,
М.П. Карпінський

ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЇ РОЗПОДІЛЕНИХ АТАК В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Статтю присвячено розгляду нових напрямів розвитку та вдосконалення мереж передачі даних.

Ключові слова: *розподілені атаки, комп'ютерна мережа, мережі передачі даних.*

Статья посвящена рассмотрению новых направлений развития и совершенствования сетей передачи данных.

Ключевые слова: *распределенная атака, компьютерная сеть, сети передачи данных.*

New areas of the development and improvement of digital data networks are considered.

Keywords: *distributed denial of service, computer network, digital data networks.*

Унаслідок відкритого принципу побудови мереж і доступу до них виникають специфічні особливості їх структури і процесів функціонування, такі як відкритість, захищеність [1], суттєва неоднорідність [2]. На сьогодні особлива увага акцентується на нових напрямах розвитку та удосконаленні мереж передачі даних. Серед них слід виділити безпровідні (мобільні) мережі. Такі мережі надають користувачеві унікальні можливості для оперативного доступу до віддалених мережевих ресурсів, у тому числі до глобальної мережі Internet, не обмежуючи його при цьому в мобільності й не прив'язуючи до дротових ліній зв'язку [3].

Із розвитком і ускладненням засобів, методів і процесів обробки інформації підвищується залежність сучасного суспільства від ступеня безпеки застосовуваних ним інформаційних технологій [4].

Комп'ютерні мережі надають всі можливості для обміну даними між клієнтом та сервером, проте на сьогодні широко розповсюджені атаки на відмову в обслуговуванні клієнтів, тому завдання визначення розподілених атак в мережі є особливо актуальною. Найпоширенішими типами таких атак є DoS/DDoS атаки, що позбавляють користувачів комп'ютерної мережі певних послуг.

Із постійним розвитком комп'ютерних мереж та збільшенням кількості користувачів зростає і кількість нових видів атак на відмову в обслуговуванні. DoS/DDoS атаки характеризуються нескладною реалізацією й складністю протидії, що ставить перед дослідниками нові завдання, які дотепер ще не вирішені. Аналіз останніх публікацій свідчить, що здійснення атак супроводжується: перехопленням конфіденційної інформації, несанкціонованим використанням пропускної здатності мережі та обчислювальних ресурсів, поширенням неправдивої інформації, порушенням адміністрування мережі.

Для вирішення поставленого завдання доцільно скористатися класифікацією інформаційних загроз, DoS/DDoS атак та формалізованими моделями [1] ступеня

впливу показників на роботу комп'ютерної мережі. Це дозволить ефективно вирішити завдання виявлення атаки на точку доступу комп'ютерної мережі. Побудуємо формалізовані математичні моделі імовірності інформаційних загроз, DoS/DDoS атак лінійного виду на основі використання методу вагових коефіцієнтів.

$$P\_IЗ(P) = \alpha_1 P_{Конф.} + \alpha_2 P_{Цл.} + \alpha_3 P_{Дост.},\ P_{Smurf}, P_{Fraggle}, P_{SYNFlood}, P_{DNS} \quad (1)$$

$$P\_DoS(P) = \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_1 P_{DNS} \quad (2)$$

$$P\_DDoS(P) = \delta_1 P_{Trinoo} + \delta_2 P_{TAN/TF2K} + \delta_3 P_{Stacheldraht} \quad (3),$$

де P_IЗ_(P) – імовірність інформаційних загроз;
P_DoS(P) – імовірність DoS атак;
P_DDoS(P) – імовірність DDoS атак;
α_i – вагові коефіцієнти, де $\alpha_i \in [0;1]$;
β_i – вагові коефіцієнти, де $\beta_i \in [0;1]$;
δ_i – вагові коефіцієнти, де $\delta_i \in [0;1]$.

Наведені математичні моделі визначають матриці активності мережі, згідно з якими робимо висновки про реалізацію атаки:

$$\alpha_{інф.загр.} = \begin{bmatrix} \alpha_1^а & \alpha_2^а & \alpha_3^а \\ \alpha_1^б & \alpha_2^б & \alpha_3^б \\ \alpha_1^в & \alpha_2^в & \alpha_3^в \\ \alpha_1^г & \alpha_2^г & \alpha_3^г \\ \alpha_1^д & \alpha_2^д & \alpha_3^д \\ \alpha_1^ж & \alpha_2^ж & \alpha_3^ж \\ \alpha_1^з & \alpha_2^з & \alpha_3^з \end{bmatrix}, \beta_{DoS} = \begin{bmatrix} \beta_1^а & \beta_2^а & \beta_3^а & \beta_4^а \\ \beta_1^а & \beta_2^а & \beta_3^а & \beta_4^а \\ \beta_1^а & \beta_2^а & \beta_3^а & \beta_4^а \\ \beta_1^а & \beta_2^а & \beta_3^а & \beta_4^а \\ \beta_1^а & \beta_2^а & \beta_3^а & \beta_4^а \\ \beta_1^а & \beta_2^а & \beta_3^а & \beta_4^а \\ \beta_1^а & \beta_2^а & \beta_3^а & \beta_4^а \end{bmatrix}, \delta_{DDoS} = \begin{bmatrix} \delta_1^а & \delta_2^а & \delta_3^а \\ \delta_1^а & \delta_2^а & \delta_3^а \\ \delta_1^а & \delta_2^а & \delta_3^а \\ \delta_1^а & \delta_2^а & \delta_3^а \\ \delta_1^а & \delta_2^а & \delta_3^а \\ \delta_1^а & \delta_2^а & \delta_3^а \\ \delta_1^а & \delta_2^а & \delta_3^а \end{bmatrix} \quad (4)$$

Дослідження показали, що всі види атак рівноймовірно впливають на роботу комп'ютерної мережі. Зі збільшенням імовірностей різновидів атак – імовірність інформаційних загроз, DoS/DdoS-атак збільшується прямопропорційно. Найбільший вплив на роботу мережі здійснюють атаки на відмову в обслуговуванні. Проте розрізнити, яка саме атака є практично реалізованою, ці моделі не дозволяють.

Для визначення виду атаки, що реалізується, сформуємо математичну модель комунікації клієнта і сервера, що включає в себе імовірність компроментації вузла та кількість усеможливих шляхів до точок доступу.

$$\text{I}\ \alpha_i^а = \frac{1}{k}\left[P_{AP}^1 + P_{AP}^2\right]$$

$$\text{II}\ \alpha_i^б = \frac{1}{k}\left[2P_{AP}^1 + P_{AP}^2\right] \quad (5)$$

$$\text{III}\ \alpha_i^в = \frac{1}{k}\left[P_{AP}^1 + 2P_{AP}^2\right]$$

$$\text{IV}\ \alpha_i^г = \frac{1}{k}\left[2P_{AP}^1 + 2P_{AP}^2\right]$$

$$\text{V}\ \alpha_i^{\partial} = \frac{1}{k}\left[2P_{AP}^1 + P_{AP}^2\right]$$

$$\text{VI}\ \alpha_i^{\text{ж}} = \frac{1}{k}\left[P_{AP}^1 + 2P_{AP}^2\right]$$

$$\text{VII}\ \alpha_i^{з} = \frac{1}{k}\left[P_{AP}^1 + P_{AP}^2\right],$$

де $\alpha_i^{\text{а,б,в,г,д,ж,з}}$ – ваговий коефіцієнт,

а, б, в, г, д, ж, з – модель комунікації,

і – види атак,

k – кількість можливих шляхів від АР до Т.

Наведемо результати чисельного експерименту із моделлю (5) у графічному вигляді (рис. 1). На рисунку позначено: α – ваговий коефіцієнт, n – кількість вузлів, $\sum_{i=1}^{n} P_{AP}^i$ – сумарна кількість імовірно скомпрометованих точок доступу.

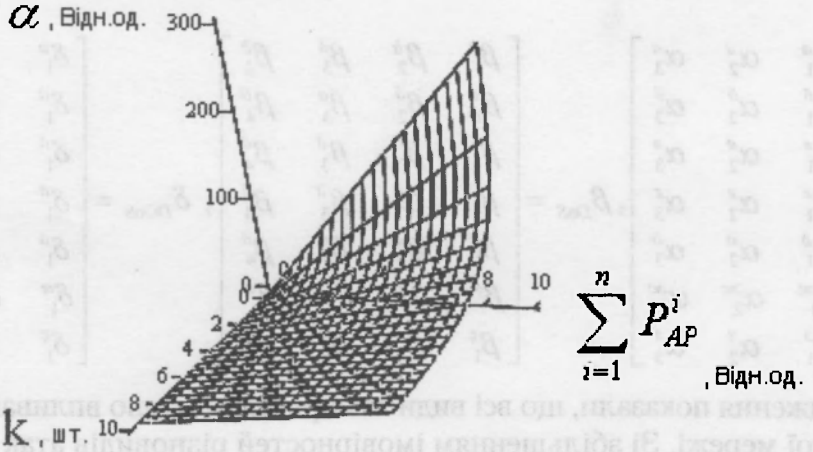

Рис. 1 Залежність вагових коефіцієнтів від імовірності скомпрометованих точок доступу і кількості всіх можливих шляхів

Дослідження показали, що при збільшенні кількості всеможливих шляхів від клієнта до сервера активність мережі є низькою, тому практичну реалізацію атаки складно визначити. При малих значеннях k активність мережі стрімко зростає, атака визначається однозначно. Рівень компрометації вузлів мало впливає на активність мережі загалом, оскільки ці вузли не визначають процесу маршрутизації.

Для того щоб розрізняти, яка атака реалізована, скористаємося таблицею 1, у якій проаналізовано її шлях та проходження через скомпрометований вузол.

Таблиця 1.

Порівняльна характеристика реалізації атак DoS/DDoS у комп'ютерній мережі

Види атак		Шлях, k			Проходження через скомпрометований вузол
		min	невизначений	визначений	
DoS	Smurf	–	+	–	–
	Fraggle	–	+	–	–
	SYN Flood	–	+	–	+
	DNS	–	–	+	–
DDoS	Trinoo	–	+	–	+
	TAN/TF2K	–	–	+	+
	Stacheldraht	–	+	–	+

Слід зазначити, що атаки DNS та TAN/TF2K реалізуються визначеним шляхом, тому в комп'ютерній мережі їх легко виявити на основі аналізу трафіку. Активність трафіку значно зростає за реалізації таких атак. В інших випадках складно визначити тип загрози.

Висновки, рекомендації та перспективи для подальшого розвитку цього напряму

Дослідження показали, що формалізовані математичні моделі імовірності інформаційних загроз та DoS/DDoS атак лінійного виду на основі використання методу вагових коефіцієнтів не дають можливості розрізнити, яка саме атака практично реалізована у комп'ютерній мережі, оскільки зі збільшенням імовірностей різновидів атак прямопропорційно збільшується імовірність інформаційних загроз та атак DoS/DDoS.

Залежності вагових коефіцієнтів від імовірності скомпрометованих точок доступу і кількості всеможливих шляхів показали, що при малих значеннях k активність мережі стрімко зростає, а атака визначається однозначно. При збільшенні кількості всеможливих шляхів від клієнта до сервера, практичну реалізацію атаки складно визначити через низьку активність мережі. Рівень компрометації вузлів мало впливає на активність мережі загалом, оскільки ці вузли не визначають процесу маршрутизації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Милокум Я.В.* Моделі та методи забезпечення обслуговування у захищених комп'ютерних мережах : автореф. дис. ... канд. техн. наук : 05.13.05 / Я.В. Милокум; Нац. авіаційний ун-т України. – К., 2009 – 19 с.

2. *Шу Чанг.* Метод адаптивного формування потоків трафіку обчислювальних мереж : автореф. дис. ... канд. техн. наук : 05.13.05 / Чанг Шу ; Нац. авіаційний ун-т України. – К., 2009. – 20 с.

3. *Колесник О.Б.* Інформаційні технології та інструментальні засоби адаптивного управління мобільними безпровідними обчислювальними мережами : автореф. дис. ... канд. техн. наук : 05.13.06 / О.Б. Колесник ; Харківський нац. ун-т радіоелектроніки України. – Х., 2008. – 25 с.

4. *Айрапетян Р.А.* Методи захисту програмного забезпечення від несанкціонованого доступу та шкідливих програм : автореф. дис. ... канд. техн. наук: 05.13.21 / Р.А. Айрапетян ; Одеський нац. політехн. ун-т України. – О., 2009. – 18 с.

Отримано 27.05.2011