УДК 004.056

АЛГОРИТМ ВИЯВЛЕННЯ АТАК ТИПУ «ВІДМОВА В ОБСЛУГОВУВАННІ» В КОМП'ЮТЕРНИХ МЕРЕЖАХ

К.В. КОЛЕСНІКОВ, А.В. ЦИМБАЛ

Київський національний університет технологій та дизайну

Змодельований алгоритм виявлення атак типу «відмова в обслуговуванні» в комп'ютерних мережах, що функціонує в призначеному для користувача режимі. Отримані дані в результаті оцінки можуть бути використані для порівняння існуючих алгоритмів виявлення атак

Необхідність використання систем захисту комп'ютерної мережі обумовлена низкою таких чинників: несанкціонований доступ, використання і модифікація програмного забезпечення, незаконне розповсюдження і збут програмних продуктів у комп'ютерних мережах, незаконне втручання в інформаційне життя кожного користувача комп'ютерних мереж.

Постановка завдання

Вибір частоти дискретизації аналізу отриманих статистичних даних [1] є серйозною проблемою при побудові алгоритму, оскільки, вибираючи інтервали часу, варто варіювати між швидкодією системи та точністю отриманих даних. При цьому цей параметр потрібно коригувати, залежно від швидкодії сервера на якому використовується це програмне забезпечення. В алгоритмі розроблюваної інформаційно-аналітичної системи виявлення атак цей параметр може змінюватися в процесі роботи, отже, система може налаштовуватися, щодо необхідного використання процесорного часу.

У процесі розробки алгоритму виникали проблеми з вибором досліджуваної мережі, оскільки всі доступні для аналізу мережі було некоректно спроектовано. Неякісне фізичне виконання та відсутність належного моніторингу стану призвели до того, що є порти, які безсистемно відсилають широкомовні пакети. У зв'язку з описаними вище проблемами в програмному забезпеченні передбачена робота з модельованим трафіком.

Результати та їх обговорення

Щоб точніше змоделювати завантаженість мережного ресурсу, потрібно проаналізувати, від чого вона залежить найбільше; з'ясувати, яку подібного виду модель можна побудувати за допомогою доступних програмних засобів реалізації.

Завантаженість мережі безпосередньо залежить від людського фактора [2]. Здебільшого це доступ до мережних ресурсів з робочого місця. Отже, динаміка завантаженості каналу (рис.1) буде змінюватися протягом робочого дня. Проаналізувавши доступні дані про завантаженість *web* й *proxy* серверів, були зроблені висновки:

– піки активності припадають на 10, 16 годин;

– з 0 до 6 години ранку завантаженість мінімальна;

– інтервалом для розрахунку параметрів розподілення було взято 30 хв.

Для генерації завантаженості сервера було створено модель (Рис.2), що відповідає описаним вище вимогам.. Вона складається із суми трьох нормально розподілених величин.

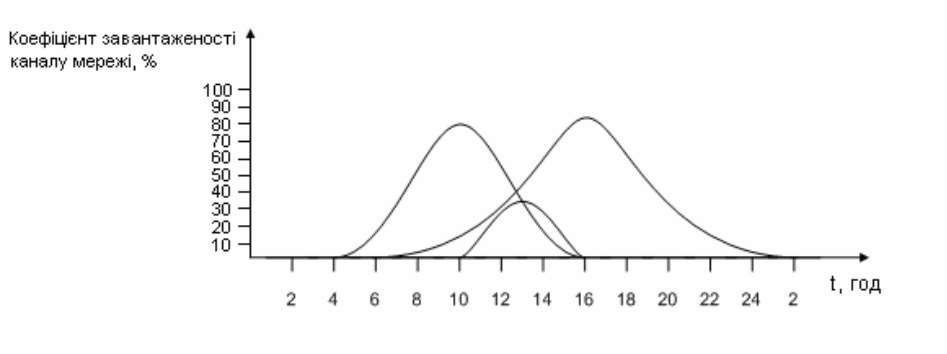

Рис.1. **Динаміка завантаженості каналу мережі**

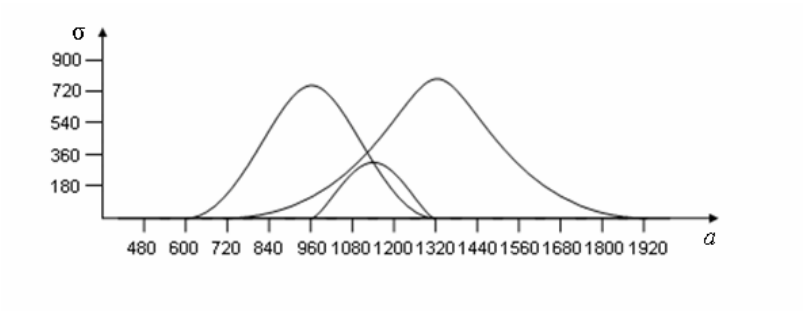

Рис. 2. **Розподілення величин за нормальним законом**

Мови програмування можуть реалізувати тільки рівномірний розподіл випадкової величини, тому, для реалізації запропонованої моделі скористаємося формулами перетворення рівномірного в нормальний розподіл.

$$y = \sqrt{\frac{3}{n}} \sum_{i=1}^{n} (2\zeta_i - n), \tag{1}$$

де y – нормально розподілена величина;

ζ_i – рівномірно розподілена величина;

n – кількість вибірок.

Отримана випадкова величина є нормально розподіленою з математичним очікуванням, що дорівнює рівним нулю, і дисперсією що дорівнює одиниці. Формула забезпечує гарні результати вже при n=8, але для зручності подальших перетворень візьмемо n=12, тоді формула набуває такого вигляду:

$$y = \sum_{i=1}^{12} \zeta_i - 6 \cdot \tag{2}$$

Для одержання нормально розподіленої величини з математичним очікуванням a і дисперсією σ, потрібно перетворити випадкову величину за формулою:

$$r = \sigma \cdot y + a, \tag{3}$$

де r – випадкова величина;

a – математичне очікування;

y – нормально розподілена величина;

σ – дисперсія;

Виразимо три необхідні нормально розподілені величини, виходячи з формули (3):

$$1)\ r = 360 * \sum_{i=1}^{12} (\zeta_i - 6) + 600\ ;$$

$$2)\ r = 780 * \sum_{i=1}^{12} (\zeta_i - 6) + 960;$$

$$3)\ r = 360 * \sum_{i=1}^{12} (\zeta_i - 6) + 720 \cdot$$

В остаточному підсумку одержали модель завантаженості сервера (рис.3.), що реалізовується алгоритмом.

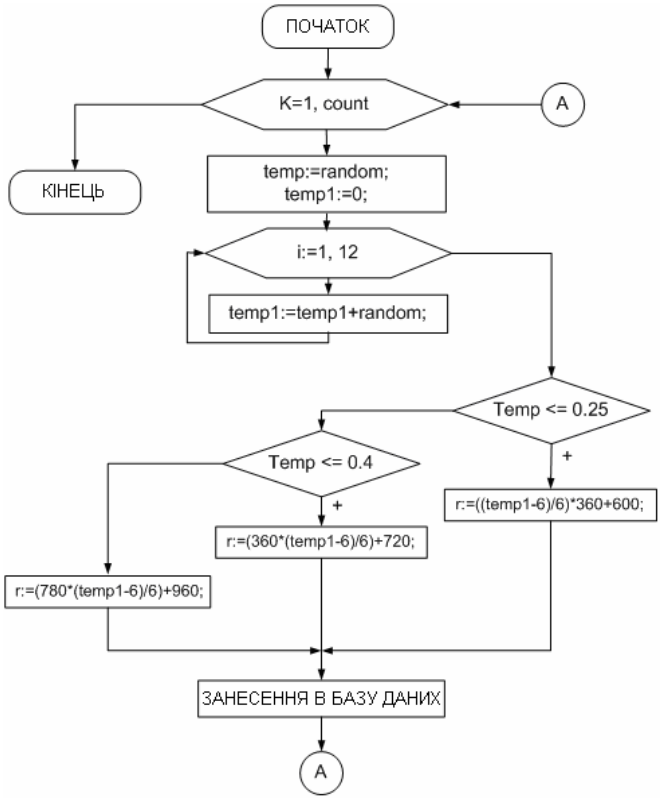

Рис.3. **Блок-схема алгоритму побудови моделі завантаженості сервера**

При аналіз можливих методів реалізації атак типу «відмова в обслуговуванні» було розроблений алгоритм виявлення шкідливих IP-адрес, на основі еталонної завантаженості сервера. Роботу алгоритму розділено на два етапи:

– збирання й аналіз статистики еталонної завантаженості сервера;

– виявлення атак і коригування еталонної моделі.

На першому етапі перехоплюються всі пакети, що прийшли на обраний мережний інтерфейс сервера, і зберігають в таблиці бази даних таку інформацію:

1. Час одержання пакета.
2. Protocol ID - протокол, пов'язаний з подією (TCP = 0, UDP = 1, ICMP = 2, ARP = 3 й Unknown = 4).
3. Вихідний порт - номер порту джерела.
4. Порт призначення - номер порту одержувача.
5. Вихідна адреса - IP-адреса джерела.
6. Адреса призначення - IP-адреса одержувача.
7. Raw Data Length – довжина даних у пакеті, байт.

Алгоритм передбачає два варіанти збереження еталонного трафіка: денний та тижневий.

Використовуючи перший варіант, ми ігноруємо залежність варіацій завантаженості трафіка від дня тижня (дослідження доступних графіків завантаженості показало, що у перші й останній робочі дні

тижня інтенсивність використання мережних ресурсів користувачами більша, ніж в інші дні) і в наступному виявленні атак застосовуємо денну завантаженість сервера. Під час використання другого варіанта знадобиться більше часу для розгортання системи, проте облік зміни інтенсивності трафіка протягом тижня дасть повнішу картину поводження цієї мережі.

На першому етапі важливу роль у процесі розгортання цієї системи відіграє системний адміністратор [4] (особа , відповідальна за безпеку й працездатність мережі), що наприкінці робочого дня при аналізі наданих йому графіків завантаженості найбільш активних IP-адрес повинен підтвердити відсутність атак типу відмова в обслуговуванні, для підтвердження безпеки зібраних статистичних даних. Після підтвердження проводиться підрахунок для кожного кванта часу (алгоритм передбачає зміну часу перерахування) пакетів від кожної IP- адреси по кожному протоколу й заносяться в тимчасову таблицю. Далі розраховується математичне очікування й середньоквадратичне відхилення по IP-адресах за півгодинний інтервал часу й заносяться в таблицю, що і буде еталонною.

На другому етапі – виявлення атак, так само як і на першому перехоплюються всі пакети, що надійшли, й інформація про пакети записується в таблицю. Після витікання кванта часу проводиться підрахунок пакетів від кожної IP-адреси й максимальний відсоток кількості однакових пакетів для кожної IP-адреси від загальної кількості надісланих їм пакетів за розглянутий період часу. Результати обчислень заносяться в тимчасову таблицю.

Наведемо кілька критеріїв виявлення атаки:

1. Нове спостереження є анормальним і розглядається як атака, якщо воно не укладається в межах довірчого інтервалу:

$$k > m + d * s, \tag{4}$$

де k – кількість пакетів від аналізованої IP-адреси;

m – математичне очікування для даного інтервалу часу й аналізованої IP-адреси;

s – середньоквадратичне відхилення для даного інтервалу часу й аналізованої IP-адреси;

d – довірчий коефіцієнт, обраний у настроюваннях інформаційно-аналітичної системи виявлення атак;

2. Якщо максимальний відсоток кількості однакових пакетів для кожної IP-адреси від загальної кількості надісланих їм пакетів за розглянутий період часу більше обраного в налаштуваннях показника;

3. Якщо загальна кількість прийнятих пакетів більша від обраної в налаштуваннях граничної величини, то небезпечними вважаються IP - адреси з максимальною інтенсивністю;

4.Якщо інформації про аналізованій IP-адресі немає в таблиці з еталонними даними й кількість прийнятих від нього пакетів більша довірчого рівня встановленого для нових IP-адрес.

При виявленні атаки передбачено кілька варіантів відповідних дій системи:

a) висновок повідомлення про виявлену атаку;

b) занесення небезпечної IP-адреси в спеціальну таблицю бази даних з подальшим фільтруванням пакетів від всіх адрес із цієї таблиці;

c) відправлення спеціальної команди по COM-порту прикордонному маршрутизатору з підтримкою ACL (Access Control List) – аркушів для занесення небезпечної IP-адреси в список заборонених. Таким чином, використовуваний сервер не буде витрачати час на обробку пакетів, відправлених цими станціями.

Незалежно від вибору варіанта відповідної дії ведеться журнал системних записів, проаналізувавши який можна повністю відновити послідовність виконаних дій системою.

Також системою передбачена адаптація до змін в завантаженості сервера. Залежно від обраного режиму збереження еталонного трафіка (денний, тижневий) наприкінці періоду система пропонує адміністратору провести коригування таблиці еталонних параметрів з урахуванням статистики за останнім часом. Коригування параметрів проходить відповідно до такої формули:

$$N = M_e + (M_i - M_e) * D, \quad (5)$$

де N – нове значення параметра;

M_e – значення, узяте з таблиці еталонних показників;

M_i – значення, отримане в результаті вимірів;

D – коефіцієнт коригування, від якого залежить, наскільки сильно будуть впливати нові значення.

Для зберігання інформації, швидкого доступу до неї й підтримки її в актуальному стані в процесі роботи інформаційно-аналітичної системи виявлення атак потрібне використання бази даних [5]. Процес створення бази даних починається з виділення основних сутностей й угруповання їх по таблицях. Правильне проектування бази даних зменшує кількість недоліків у таблицях, що приводить до прискорення виконання запитів і зменшення займаного базою місця.

Наведемо опис використаних таблиць.

Таблиця «IP», призначена для збереження інформації про отримані пакети, містить у собі такі поля:

ID – унікальний код запису, необхідний для збереження цілісності даних;

SRCIP – IP-адреса відправника пакета;

DSTIP – IP-адреса одержувача пакета;

LENGTH_ – довга даних у пакеті;

TIME_ – час прибуття пакета;

PROT – протокол;

SRCPORT – порт відправника пакета;

DESTPORT – порт одержувача пакета;

Таблиця «IP_GEN», призначена для збереження інформації про згенеровані трафіки, містить у собі такі поля:

ID – унікальний код запису, необхідний для збереження цілісних даних;

SRCIP – IP-адреса відправника пакета;

DSTIP – IP-адреса одержувача пакета;

LENGTH_ – довга даних у пакеті;

TIME_ – час прибуття пакета;

PROT –протокол;

Таблиця «MX_DX» призначена для збереження еталонної моделі поводження трафіка, містить у собі такі поля:

INTERVAL – порядковий номер інтервалу часу;

IP-IP – адреса відправника пакета;

MX – математичне очікування;

DX – середньоквадратичне відхилення.

Таблиця «TIME_IP_COUNT» призначена для зберігання тимчасових даних. Використовується для розрахунку середньоквадратичного відхилення:

TIME_ – номер інтервалу часу;

IP - IP – адреса відправника пакета;

COUNTT – кількість відправлених пакетів за інтервал часу.

Таблиця «CHART_TABLE» призначена для зберігання тимчасових даних. Використається при висновку на екран графіків:

TIME_ – номер інтервалу часу;

COUNTT – кількість відправлених пакетів за інтервал часу.

Таблиця «ZAPRET_IP» призначена для зберігання IP-адрес, пакети від яких не пропускаються далі в систему:

ID – унікальний код запису, необхідний для збереження цілісності даних;

IP – заборонений IP-адреса;

TIME – час занесення адреси в таблицю.

Висновки

Отриманий алгоритм виявлення атак дозволяє визначати вірогідність DOS-атак комп'ютерної мережі в довільні моменти часу.

Це рішення дає можливість отримувати кількісні оцінки для даних алгоритмів виявлення атак, що функціонують в призначеному для користувача режимі. Одержані оцінки можуть бути використані для порівняння існуючих алгоритмів виявлення атак. Кількісну оцінку можна розглядати як вірогідність того, що комп'ютерна мережа не буде атакована за певний проміжок часу. Алгоритм може застосовуватися для будь-яких програмних систем захисту інформації, призначених для роботи в режимі користувача.

ЛІТЕРАТУРА

1. Бурдаев О.В., Иванов М.А., Тетерин И.И. Компьютерная вирусология., КУДИЦ. – 2002 г.
2. Лукацкий А.В., Цаплев Ю.Ю. Системы обнаружения атак. Стратегия выбора // Internet Security System, Inc., –1999 г.
3. С. Норткат, Д. Новак Обнаружение нарушений безопасности в сетях.3-е издание. – М.: Вильямс, – 2003г.
4. Алиев А.Т. Технологии защиты сетей //Искусственный интеллект – №4, – 2005 г.
5. Колесников К.В., Шадхин В.Е. Системный анализ критериев и параметров проектирования системы защиты. //Радіоелектронні і комп'ютерні системи — 2006 г. – №6(18),

Надійшла 21.04.2009