УДК 004.7

ПРОТИДІЯ АТАКАМ НА ВІДМОВУ В МЕРЕЖІ ІНТЕРНЕТ: КОНЦЕПЦІЯ ПІДХОДУ

П.І. Андон, О.П. Ігнатенко

Інститут програмних систем НАН України,
03187, Київ 187, проспект Академіка Глушкова, 40.
Тел.: 526 60 25, e-mail: o.ignatenko@isofts.kiev.ua

Робота присвячена дослідженню одного з типів вторгнень через мережу Інтернет – атакам на відмову. Описана історія виникнення проблеми та причини, що зумовили її появу. Проведено огляд існуючих видів атак. Розглянута загальна архітектура системи захисту від атак на відмову. Запропонована модель протидії атакам на основі технології інтелектуальних агентів та теорії ігор.

This work deals with denial of service attacks. The papers propose historic overview of the existing attacks and methods of attack detection. Intrusion detection system (IDS) architecture is investigated. We propose a novel agent-based distributed system, which integrates the desirable features provided by the distributed agent-based design methodology with the game theory.

Вступ

Протягом останніх 15 років ми спостерігаємо надзвичайний розвиток мережі Інтернет та його переосмислення в новій якості. Розроблений як дослідницький інструментарій для вчених Інтернет поступово трансформувався на головну інфраструктуру світової інформаційної спільноти. Уряди використовують всесвітню мережу для надання громадянам інформації та послуг по всьому світу. Компанії цілодобово обмінюються інформацією зі своїми підрозділами, постачальниками, партнерами та клієнтами для підвищення ефективності своєї роботи. Дослідницькі та навчальні інститути використовують Інтернет в першу чергу як платформу співпраці та засіб дистанційного навчання і лише потім як інструмент швидкого обміну результатами досліджень.

Однак з поширенням мереж почали з'являтись факти здійснення злочинів з використанням Інтернет. Одним з небезпечних видів зловмисної діяльності у всесвітній мережі є так звані «атаки на відмову». Вони полягають у заблокуванні доступу користувачів до сервісу, що надається цільовим об'єктом. Взагалі кажучи, така атака може бути здійснена двома способами. Перший спосіб використовує слабкості програмного забезпечення, встановленого на клієнті об'єкта атаки, що дозволяє обвалити систему шляхом пересилки шкідливих пакетів. Другий спосіб полягає в використанні великих об'ємів беззмістовного трафіку для завантаження ресурсів системи, необхідних для обробки запитів легітимних користувачів. І якщо від першого способу атаки можна захиститися знешкоджуючи слабкості шляхом оновлення програм, то попередити атаку другого типу вже не так просто. Якщо трафік атаки на відмову надсилається з багатьох джерел, то такі атаки називаються розподіленими атаками на відмову. Шляхом використання багатьох джерел потужність атаки посилюється і проблема захисту від неї ускладнюється ще більше. Ще один негативний фактор полягає в використанні ефекту віддзеркалення трафіку, що також ускладнює ідентифікацію джерел атаки.

Крім того, останні тенденції показують на появу нових типів атак – прихованих атак. В цьому випадку підконтрольні атакуючому комп'ютери отримують доступ до цільового сервісу на цілком законних підставах (наприклад відвідують веб сайт компанії) і завантажують канал ресурсоємними операціями (атака погіршення якості) або в певний момент «вибухають» беззмістовним трафіком, що ставить перед системами захисту нові нетривіальні задачі виявлення і протидії.

Останнім часом все частіше вживається термін «кібернетичний тероризм», що означає організовану діяльність, спрямовану проти Інтернет інфраструктури певної держави. На сьогоднішній день доводиться констатувати, що надійного комплексного засобу протидії цим атакам немає. Отже, нині надійність і захищеність мережі Інтернет це навіть не стільки питання втрати доходів бізнесу (хоча й це дуже важливо), скільки питання національної безпеки.

Атаки на відмову: опис, характеристики, класифікація

На сьогоднішній день існує досить багато різних видів атак на відмову, кожна з яких використовує певну особливість побудови мережі або вразливості програмного забезпечення. Наприклад, атаки можуть здійснюватися шляхом безпосередньої пересилки великої кількості пакетів (SYN, UDP, ICMP flood), використання проміжних вузлів (Smurf, Fraggle), передачі занадто довгих пакетів (Ping of Death), некоректних пакетів (Land) або великої кількості трудоємних запитів. Зауважимо, що протягом останнього часу відбувається

бурхливий розвиток цього напряму діяльності та поява нових видів і способів атак. З останніх тенденцій можна відзначити появу атак погіршення якості (Quality Reduction Attack) та низькочастотних атак (Low Rated Attack) і, безумовно, цей процес буде продовжуватися, потребуючи нових досліджень та розробки нових методів протидії.

Основні існуючі класи атак досить добре вивчені. Представляють інтерес, однак, різні підходи до їх класифікації. У роботі [1] атаки класифіковані згідно з протоколами, за якими вони здійснюються. Виділені такі атаки: SYN flood, TCP reset, ICMP flood, UDP flood, DNS request, CGI request, Mail bomb, ARP storm і атаки на алгоритмічну складність.

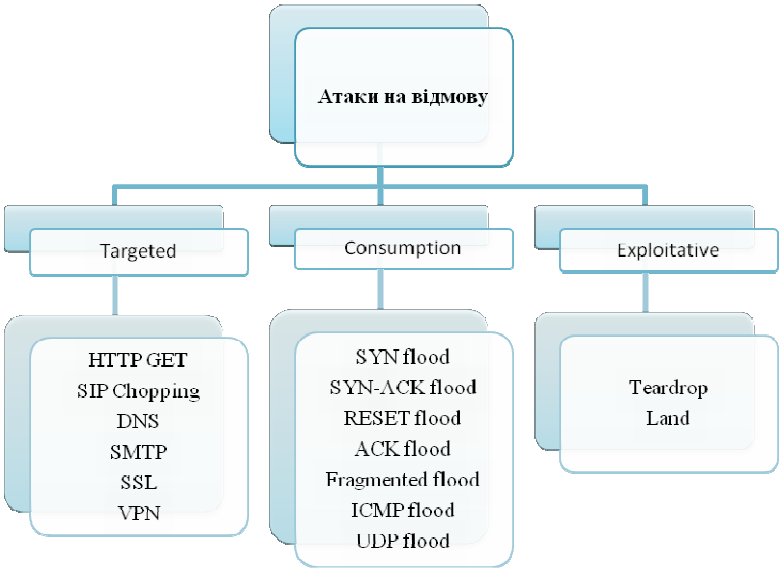

Рис. 1. Класифікація атак на відмову. Prolexic Technologies

У звіті Prolexic Technologies [2] приводиться класифікація атак за технікою здійснення (рис. 1). Виділяють три типи атак:

- targeted attacks (використовують недоліки в протоколах, прикладних програмах);
- consumption attacks (поглинання ресурсів системи);
- exploitative attacks (використовують вразливості, помилки кода).

У звіті також описуються відомі атаки для кожного типу.

Дослідженнню класифікації розподілених атак на відмову присвячена робота [3], в якій наведений досить розгорнутий опис атак, який коротко покажемо у вигляді схеми (рис. 2).

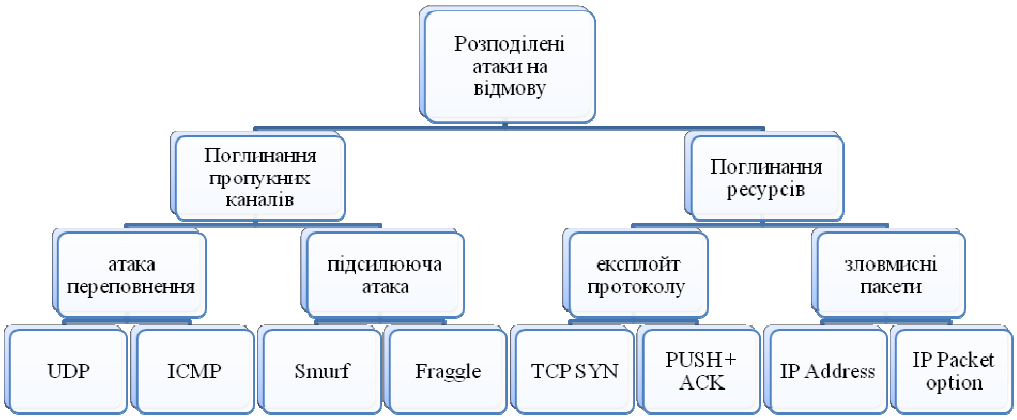

Рис. 2. Класифікація атак на відмову

Широкий огляд досягнень у даній області приведено в роботі А.В. Уланова і І.В. Котенко [4]. Зокрема автори пропонують підрозділяти розподілені атаки на відмову (за способом реалізації і об'єкту дії) на два класи:

- поглинання ресурсів мережі;
- поглинання ресурсів вузла.

Поглинання ресурсів мережі полягає в пересилці великої кількості пакетів в мережу жертви. Вони зменшують її пропускну здатність для законних користувачів. Існує декілька видів таких атак:

- UDP/ICMP flood полягає в пересилці значної кількості великих (фрагментованих) пакетів по протоколам UDP/ICMP;
- Smurf/Fraggle полягає у пересилці пакетів UDP/ICMP ECHO на широкий діапазон адрес з сфальшованою IP адресою. При цьому на адресу жертви приходить велика кількість пакетів-відповідей.

Поглинання ресурсів вузла полягає в пересилці трудоємних або некоректних запитів жертві. До цього вида відносяться наступні атаки:

- TCP SYN – свідоме переривання процесу встановлення з'єднання і створення великої кількості напіввідкритих TCP/IP з'єднань (оскільки це число обмежене, то вузол перестає приймати запити на з'єднання).
- Land – пересилка пакету TCP SYN з однаковими адресами одержувача і джерела та портами (при посилці таких пакетів вузол з Windows NT зависає).
- Ping of Death – посилка пакету «ping» дуже великої довжини, який ОС не може обробити.
- Пересилка некоректних пакетів при обробці яких на вузлі можуть виникнути помилки.
- Пересилка трудоємних запитів для завантаження вузла.

У роботі [5] наводиться найбільш розгорнута схема класифікації розподілених атак. Критерії, що використовуються в цій класифікації охоплюють наступні аспекти:

- стадію реалізації атак;
- ступінь їх автоматизації;
- стратегію сканування і розповсюдження;
- механізми взаємодії агентів;
- склад і організацію агентів;
- вразливості, що використовуються;
- способи виконання атак;
- склад пакетів атаки;
- індивідуальну поведінку агентів;
- інформацію про агентів атаки.

Спираючись на опрацьовані роботи та провівши додаткові дослідження ми виділили множину з декількох аспектів, важливих з точки зору побудови системи захисту, які достатньо повно характеризують атаку на відмову. Опишемо ці аспекти.

Тип атаки. Будемо розглядати атаки двох типів: *просту* (коли атака йде з однієї машини) та *розподілену* (коли використовуються машини-агенти).

Напрям атаки – визначає конкретну частину інфраструктури мережі, яка зазнає атаки. Виділимо дві частини: *ресурси мережі* (тобто пропускних каналів) та *ресурси цілі* (тобто ресурси конкретного комп'ютера) [4].

Схема атаки – визначає план здійснення атаки, тобто доставки атакуючим зловмисного трафіка жертві. Може бути *прямою* (персилка трафіка з одного або багатьох машин), *віддзеркаленою* (пересилка трафіка через третіх осіб) або *прихованою* (зловмисний трафік ховається в «законному») [6].

Спосіб атаки – визначає які вразливості використовуються при здійсненні атаки. Виділимо такі способи атаки: *спрямована*, яка використовує недоліки конкретних прикладних програмних систем, служб, протоколів, *поглинаюча*, яка намагається завантажити всі ресурси системи або мережі, *експлойтна*, яка використовує вразливості програмних систем [7].

У роботі [8] авторами описана класифікація існуючих типів атак у розрізі цих аспектів.

Системи, що підлягають захисту

Для успішного функціонування системи захисту від атак на відмову надзвичайно важливо виділити множину припущень про систему, яка підлягає захисту. Очевидно, що захист систем різного типу має бути побудований на основі різних принципів, що ґрунтуються на типових характеристиках, класах атак, що спрямовані проти систем даного типу, вимог до функціонування системи захисту. Як правило, ці припущення стосуються нормальної роботи системи, що підлягає захисту. Виділення таких емпіричних характеристик суттєво полегшує виявлення атаки при умові збереження їх відповідності реальному стану системи.

Існує також декілька базових припущень, які використовуються в усіх системах захисту. Перше з них полягає в тому, що атаки взаємопов'язані з незвичним використанням системи і тому їх дія суттєво відрізняється від типової роботи. Тобто вважається, що атаки супроводжуються аномальною поведінкою системи, яку легко можна відрізнити від звичайної. У роботі [9] здійснена спроба узагальнити і описати існуючі припущення, на основі яких функціонує більшість систем виявлення. Можна виділити декілька ключових припущень, які лягли в основу багатьох систем виявлення, це:

користувачі створюють приблизно однакову кількість трафіку [10];

кількість пакетів в одиницю часу (загально або тільки по окремим протоколам) при звичайній роботі представляє собою статистично однорідну послідовність (тобто його характеристики залишаються сталими протягом часу) [11, 12];

кількість постійних, легітимних користувачів протягом достатньо довгого періоду часу залишається сталою або поступово змінюється [10, 13];

при атаці на відмову відбувається суттєва зміна статистичних характеристик роботи системи [14];

Також неявно припускається, що:

- атаки на відмову є аномальним використанням системи;
- атаки на відмову є рідкісною, надзвичайною ситуацією;
- аномалії шкодять функціонуванню системи;
- визначення аномальної поведінки не залежить від мережі. (аномалії є універсальними, або залежать тільки від протоколу взаємодії);
- адміністратори можуть адекватно інтерпретувати аномальні явища, що виникають при функціонуванні мережі.

Виділяють наступні типи систем, що можуть бути ціллю атаки:

- окремий сервіс;
- окремий вузол (поштовий або файловий сервер);
- мережа;
- ad-hoc мережа (динамічна мережа);
- інфраструктура мережі Інтернет.

Для кожної з них система захисту має враховувати окремі припущення і бути налаштована на різні типи атак. Зупинимось коротко на кожному з цих типів.

Окремий сервіс. Кожен вузол мережі забезпечує роботу декількох сервісів, кожний з яких, як правило, пов'язаний з окремою прикладною програмою. Атака може бути спрямована на особливості або вразливості реалізації такого сервісу. Це може заблокувати доступ користувачів до сервісу, хоча робота всього комп'ютера не буде зупинена. Атаки такого типу складно виявляти оскільки зміни в роботі всієї системи можуть бути незначними.

Окремий вузол. Атаки на вузол спрямовані на механізми, що забезпечують його зв'язок з мережею. Це можуть бути атаки, пов'язані з TCP/IP, UDP або іншими протоколами мережі. При такій атаці часто змінюються статистичні характеристики трафіка. Також часто виконується припущення про приблизно однакову кількість трафіка кожного користувача.

Мережа. Атаки, що спрямовані на мережу намагаються заповнити її пропускну здатність фальшивими пакетами. В разі успіху весь зв'язок користувачів з системою, яку атакують буде перерваний. При нормальній роботі мережі статистичні характеристики трафіка змінюються повільно, кількість користувачів часто залишається сталою (це залежить від природи послуг, що надаються). Тому для виявлення атак існують досить розвинені методи. Більш складною задачею є відділення атакуючих пакетів від пакетів користувачів. Для повного її розв'язання потрібне широке запровадження системи маркування пакетів, що дозволить протидіяти спуфінгу IP адрес.

Ad hoc мережа. Ці мережі набули поширення порівняно недавно. Як правило, це безпровідні мережі, що дозволяють підключитись користувачам з будь-якого місця. Вони характеризуються високою динамічністю трафіка і кількості користувачів. Одним з прикладів можуть слугувати пірингові мережі, що набули широкої популярності і використовуються для розповсюдження музики, фільмів або програм мережами. Атаки на такі мережі (або з використанням таких мереж) мають ряд особливостей і досить складні для виявлення.

Інфраструктура мережі Інтернет. Атаки на інфраструктуру намагаються вивести з ладу сервіси і компоненти, функціонування яких критичне для роботи мережі Інтернет. У разі успішності такої атаки наслідки можуть бути катастрофічні для всієї мережі. На сьогоднішній момент DNS сервери добре забезпечені додатковими ресурсами і можуть протистояти практично будь-якій атаці, однак спроби нападу регулярно відбуваються з року в рік.

Існуючі механізми захисту від атак на відмову

Взагалі кажучи, можна виділити чотири задачі, які стоять перед системою захисту від атак на відмову: попередження атаки, виявлення атаки, ідентифікація джерел атаки, протидія атаці. Задача попередження атаки полягає в протидії атаці на підступах до жертви. Задача виявлення атаки полягає в детектуванні атаки на відмову в разі її появи. Виявлення атаки – це важливий етап, від якого залежать всі подальші дії. Ідентифікація джерела атаки призначена для виявлення істинного місця здійснення атаки, оскільки трафік атаки може бути фальшований або віддзеркалений. Ідентифікація має велике значення для зменшення потужності атаки, крім

того ризик виявлення стримує потенційних нападників. Протидія атаці призначена для знешкодження атаки. Це заключна частина захисту і тому визначає загальну характеристику всього механізму. Основна проблема протидії атаці полягає в наступному: як відфільтрувати трафік атаки і не вплинути на трафік звичайних користувачів.

Попередження атаки. Попередження атаки полягає в зупинці атаки ще до того як вона почала ураження жертви. При розв'язанні цієї задачі вважається, що атакуючий трафік сфальшовано, тобто адресу джерела замінено на іншу, що дійсно має місце в багатьох реальних ситуаціях. Такий підхід застосовується в схемах фільтрації пакетів, які впроваджуються в маршрутизаторах. Фільтрація пакетів використовується для того, щоб пропускати тільки дійсний (несфальшований) трафік. Це значно зменшує ймовірність появи атаки на відмову. Однак розробити правило фільтрації, яке б точно відрізняло сфальшований трафік від дійсного зовсім не просто. Більше того, більшість схем фільтрації вимагають для своєї ефективної роботи широкого впровадження алгоритмів спеціальної обробки пакетів. На жаль, мережа Інтернет являється відкритою спільнотою без центральних адміністративних органів, що робить таке впровадження нелегкою справою.

Виявлення атаки. Наступним кроком після попередження атаки є виявлення атаки. Для будь-якої схеми виявлення атаки показником ефективності є відсоток виявлення атак. Виявлення атаки на відмову відрізняється від виявлення несанкціонованого вторгнення. Оскільки наслідком атаки є відмова в обслуговуванні, то факт здійснення атаки досить легко визначити. Однак тут є проблема помилкового виявлення. Річ у тому, що хоча деякі типи атак використовують експлойти, вразливості програмного забезпечення, фальшування і специфічну форму пакетів, взагалі кажучи, це не є обов'язковою умовою атаки на відмову. Певні типи атак імітують звичайний трафік і завантажують ним канали зв'язку. Тому будь-яка схема ризикує помилково прийняти інтенсивний звичайний трафік за атакуючий. Виникає питання – навіщо тоді потрібна система виявлення атаки? Для цього є декілька причин. По-перше, при вчасному виявленні атаки жертва може виграти час для виконання заходів з протидії та захисту своїх ресурсів. По-друге, виявлення атаки може допомогти ідентифікувати нападників. По-третє, якщо буде швидко виявлені джерела атаки, трафік можна відсікти до того, як він завантажить пропускні ресурси системи.

При дослідженні питань функціонування механізму виявлення увага буде, в основному, зосереджена на тому, в яких випадках алгоритм допускає *фальшиві виявлення* (звичайний трафік пріймається за атаку) та *не виявлення* (трафік атаки приймається за звичайний). У роботі [15] описані характеристики, що визначають появу фальшивих виявлень і не виявлень:

- рівень виявлення. Це основний рівень трафіка мережі, за яким здійснюється моніторинг. Рівнем виявлення може бути пакетний рівень, рівень потоків пакетів, рівень з'єднань мережі та рівень з'єднань програм;
- інформація, необхідна для виявлення атак. Це, як правило, статистичні дані, що отримані при моніторингу трафіка мережі або його вмісту. Інформація може включати заголовки пакетів, частоти пакетів для потоків/з'єднань або інформацію про відкинуті пакети;
- особливості трафіка атаки. Це особливі параметри, значення яких використовуються для виявлення атаки. Фальшиве виявлення відбувається, якщо в звичайному трафіку присутні ці особливості. Не виявлення відбувається, якщо трафік атаки не містить цих особливостей;
- причини фальшивого виявлення/не виявлення. Це обставини, що можуть спричинити появу в звичайному трафіка особливостей атаки або в їх відсутність в атакуючому трафіка.

У широкому розумінні механізми виявлення можна розділити на три категорії: виявлення перевантажень, виявлення особливостей та виявлення аномалій. Виявлення перевантажень полягає в оцінці завантаження ланок мережі, ресурсів системи або системи в цілому. Досягнення певного рівня означає наявність атаки. Виявлення особливостей полягає в пошуку певних особливих характеристик, притаманним атакам на відмову і нехарактерних для звичайного трафіка. Можна виділити одновимірне (коли оцінюється одна характеристика) та багатовимірне (коли таких характеристик декілька) виявлення особливостей. Виявлення аномалій включає в себе побудову профілю нормального функціонування системи. При цьому можуть застосовуватись різноманітні математичні техніки, наприклад, обчислення статистичних характеристик трафіка, нейронні мережі, методи *Data mining* тощо.

Ідентифікація джерела атаки. Після виявлення атаки найкращою протидією було б блокування трафіка джерел атаки. Однак не завжди можна однозначно відстежити джерело атакуючих пакетів. По-перше, адреса джерела пакетів може бути сфальшована. По-друге, динамічна маршрутизація, при якій роутери володіють інформацією лише про наступний крок пересилки пакета не дозволяє прослідити його шлях. Хоча існують різні способи маркування, які б дозволили значно полегшити боротьбу зі спуфінгом, їх широке запровадження проблематичне.

Протидія атаці. Четвертим і останнім етапом захисту є протидія атаці. В залежності від типу атакуючого трафіка система захисту може застосувати одну з трьох дій:

- керування пропускною здатністю;
- відкидання окремих пакетів;
- фільтрація пакетів на роутерах.

Алгоритми протидії атакам на відмову

На сьогодні лише методи виявлення атак розвинуті в достатній мірі для ефективного застосування.

Механізм виявлення атаки на відмову є важливою складовою системи захисту. Результатом його роботи є одна, рідко декілька змінних, що характеризують якусь особливість вторгнення або наявність аномалій в системі. Наступним і дуже важливим кроком є визначення алгоритму прийняття рішення про наявність атаки. Можна відмітити, що якщо задача побудови механізму захисту є інформаційно-математичною, то визначення алгоритму виявлення атаки – цілком математична задача. В більшості робіт при побудові системи захисту дане питання опускається, вважається, що користувачі можуть налаштувати параметри алгоритмів виявлення атаки на свій розсуд. Однак це зовсім не проста задача.

Відомі наступні алгоритми виявлення:

простий поріг;

адаптивний поріг;

сковзне середнє (moving average або MA) та його модифікації;

метод накопиченої суми (CUSUM) та його модифікації.

Узагальнену модель алгоритму виявлення можна описати наступним чином. Розглянемо стохастичний n - компонентний процес $x_t = \left(x_t^1, x_t^2, ..., x_t^n\right)$, де кожна компонента x_t^i відповідає одному з каналів вимірів, визначених механізмом виявлення. Як випливає з попереднього розділу це може бути об'єм усього трафіка протягом фіксованих інтервалів часу, об'єм трафіка за кожним з'єднанням протягом фіксованих інтервалів часу, кількість байт, пакетів або з'єднань, час очікування на з'єднання та інші.

Оскільки виміри проводяться через певні інтервали, то x_t – послідовність при $t = 1,2,...m$.

Найпростішим способом визначення атаки, що застосовується в багатьох системах захисту, є перевищення порога $\alpha > 0$, якщо $x_t^i > \alpha$, то по каналу i в момент часу t відбувається атака. Виявлення при простому перевищенні порогового значення, як правило, неявно припускає статичність розподілу трафіка системи. Системи з простим порогом призначені для боротьби з конкретними типами атак [16].

Модифікацією простого порогового значення є інтегральне порогове значення. Визначимо функцію $\delta(x_t^i, \alpha) = \begin{cases} 0, & x_t^i \le \alpha \\ 1, & x_t^i > \alpha \end{cases}$, тоді якщо $\sum_{j=t-k}^{t} \delta(x_j^i, \alpha) > k$, то по каналу i в момент часу t відбувається атака.

Більш складним способом виявлення є адаптивне порогове значення. В цьому алгоритмі для коригування порогового значення використовується оцінене середнє значення. В деяких роботах для оцінки використовується експоненційно зважене сковзне середнє значення (exponentially weighted moving average – EWMA) [17]:

Оцінка трафіка $\overline{\mu}_t^i$ визначається за формулою $\overline{\mu}_t^i = \beta_i \overline{\mu}_{t-1}^i + (1-\beta_i) x_t^i$, де $\beta_i \in [0,1]$ – EWMA фактор. Тоді умова виявлення атаки для порога $\alpha > 0$, Якщо $x_t^i > (\alpha+1)\overline{\mu}_{t-1}^i$, то по каналу i в момент часу t відбувається атака.

Для оцінки трафіка, окрім EWMA, також можуть використовуватися звичайне сковзне середнє (moving average – MA), S-подібне сковзне середнє (S-shaped moving average – SMA) або авторегресійне інтегроване сковзне середнє (AutoRegressive Integrated Moving Average (ARIMA)) [18]. Інтегральне адаптивне порогове значення визначається аналогічно:

$$\overline{\mu}_t^i = \beta_i \overline{\mu}_{t-1}^i + (1-\beta_i) x_t^i,$$

якщо $\sum_{j=t-k}^{t} \delta(x_j^i, (\alpha+1)\overline{\mu}_{t-1}^i)) > k$, то по каналу i в момент часу t відбувається атака.

Сковзне середнє використовується також для виявлення атак [19].

Припустимо, що послідовність x_t розподілена з густиною $p_{\theta_0}(x)$. У момент часу $t = T$ відбувається зміна розподілу, і при $t > T$ послідовність x_t розподілена з густиною $p_{\theta_1}(x)$. Визначимо логарифмічну функцію правдоподібності:

$$s(x) = \ln \frac{p_{\theta_1}(x)}{p_{\theta_0}(x)}.$$

Визначимо розрахункову функцію g_t так

$$g_t = \sum_{i=0}^{N-1} \gamma_i \ln s(y_{t-i}),$$

де γ_i – вагові коефіцієнти, N – параметр, що регулює гладкість алгоритму. Розглянемо дискретну зміну $\Delta g_t = g_t - g_{t-1}$. Умова часу виявлення атаки:

$$t_a = \{t : \sum_{i=0}^{N-1} \delta(\Delta g_{t-i}, h) \geq \eta\}.$$

Наступна група алгоритмів пов'язана з методом CUSUM [20]. Це класичний метод, що застосовується для виявлення точки зміни розподілу випадкової послідовності. Параметричний варіант методу полягає в наступному [19]:

$$S_t^k = \sum_{j=t}^{k} s_j(x),$$

$$s_j(x) = \ln \frac{p_{\theta_1}(x_j)}{p_{\theta_0}(x_j)}.$$

Тоді оптимальне правило прийняття рішення полягає тому, що:

$$d = \begin{cases} 0, & S_1^N < h, \\ 1, & S_1^N \geq h. \end{cases}$$

Момент часу T_d, для якого $d = 1$ і є часом виявлення атаки. Метод CUSUM базується на припущенні, що якщо відбуваються аномалії, або вторгнення в роботу системи, змінюється розподіл послідовності, яка вимірюється. Параметричний варіант методу вимагає знання щільності розподілу послідовності до і після зміни. Однак, мережа Інтернет надзвичайно складна динамічна система, і побудова теоретичної конструкції Інтернет-трафіка залишається складною проблемою. Отже, ключовою проблемою є моделювання x_t. Одним з можливих способів зняття цієї проблеми стала розробка непараметричного CUSUM [21]. Головна ідея непараметричного методу полягає в накопиченні значень x_t, які суттєво більші за середнє значення при нормальному функціонуванні. При цьому зберігається основний плюс методу CUSUM – послідовний розрахунок, що забезпечує виявлення в реальному часі.

Одним з початкових припущень непараметричного алгоритму є те, що математичне сподівання при нормальних умовах від'ємне. Тому потрібно сформувати допоміжну послідовність Z_t, наприклад, так:

$$Z_t = x_t - \overline{\mu}_{t-1} - \beta,$$

де $\overline{\mu}_t$ – середня оцінка трафіка, обчислена за одним з вищезазначених методів, β – параметр, що підбирається для конкретної мережі. Вважаємо, що при початку атаки значення x_t суттєво підвищиться, а значення Z_t стане додатнім (припущення роботи методу). Підвищення в одній точці може бути спричинено збігом обставин або помилками вимірів, будемо вважати зміну суттєвою, якщо математичне сподівання підвищилося не менше ніж на параметр $h > 0$. Тому вводиться третя змінна y_t, яка акумулює додатні значення Z_t. Якщо y_t досягає певного порогового значення N, вважається, що відбувається атака.

Формальне визначення непараметричного методу CUSUM таке:

$$y_t = Q_t - \min_{1 \leq j \leq t} Q_j,$$

$$Q_j = \sum_{i=1}^{j} Z_i,$$

$$Q_0 = 0.$$

З метою зменшення обчислень (які потрібно проводити в реальному часі), використовується рекурсивна версія непараметричного алгоритму CUSUM [20, 21]:

$$y_t = (y_{t-1} + Z_t)^+,$$

$$y_0 = 0,$$

де x^+ дорівнює x, якщо $x > 0$, і 0 в іншому випадку. Функція прийняття рішення має вигляд:

$$d_N(y_t) = \begin{cases} 0, & y_t < N, \\ 1, & y_t \geq N. \end{cases}$$

При описі попередніх методів вважалось, що атака проявляється по одному з каналів – це була ідеалізація, яка підходить для простих систем виявлення, створених проти одного типу атак. На практиці, система вимірює дані по різним каналам, однак атака проявляється лише по деяким з них. Задача полягає в тому, як урахувати збурення за кількома каналами, та обчислити загальну ймовірність атаки. В роботі [22] використовуються «шаблони поведінки» – множини порогів для вхідних сигналів. При досягненні цих значень формується сигнал

про наявність атаки. Інший підхід описано в роботі [13], де в рамках алгоритму накопиченої суми пропонується узагальнення «Cumulative-CUSUM» тест, яке враховує багатоканальні дані:

$$\tau(h) = \min\left\{ t \geq 1 : \max_{1 \leq k \leq t} \sum_{j=k}^{t} \sum_{i=1}^{N} \Delta Q_i^j \geq h \right\}.$$

В роботі [8] авторами був запропонований підхід до побудови багатоканального алгоритму. Нехай виділена множина параметрів $c_k(t_i)$, що характеризують трафік і вимірюються періодично в моменти часу t_i. При цьому постулюється, що при атаці певна частина цих параметрів змінює свої статистичні характеристики. Таким чином, задача виявлення атаки може бути переформульована як задача визначення точки зміни за гарантований час і з мінімальним ризиком помилки. Задачі такого типу виникли в класичній теорії керування для забезпечення якості керування більше 40 років назад. Огляд методів розв'язання, які було розроблено приведено в роботах [20, 21]. В області виявлення атак важливе узагальнення класичної постановки на багатовимірний випадок. Зауважимо, що оскільки розподіл трафіка невідомий, то застосовні лише непараметричні методи виявлення.

Позначимо μ_k математичне сподівання послідовності $c_k(t_i)$ до початку атаки, θ_i – після початку атаки. Як правило в прикладних задачах μ_k може бути обчислене, а θ_k може бути приблизно оцінено.

Розглянемо наступну рекурентну послідовність

$$y_k(t_i) = \max(0, y_k(t_{i-1}) + c_k(t_i) - \mu_k - \beta_k), \; y_k(t_0) = 0,$$

де β_k – параметр, який вибирається з умови від'ємності математичного сподівання послідовності $c_k(t_i) - \mu_k$.

Нехай вибрані порогові значення h_k, перевищення яких означає виявлення атаки. Введемо функції

$$p_k(y_k(t_i)) = \min(1, \frac{y_k(t_i)}{h_k}).$$

Область значень p_k – число від нуля до одиниці. Функція p_k означає рівень загрози атаки для кожного параметра. Загальна загроза обчислюється по формулі:

$$p(t_i) = 1 - \prod_{k=1}^{n} (1 - p_k(t_i)).$$

Отже, навіть при низькочастотній атаці, яка маскується під звичайну роботу системи, виявлення відбувається за рахунок сумісного обчислення змін всіх параметрів.

Вищеописані алгоритми застосовуються, як правило, для виявлення досить простих типів атак, таких як SYN flood. При деяких умовах та правильному виборі параметрів можливе виявлення і більш складних атак, але в загальному випадку необхідні інтелектуальні алгоритми, які б могли комбінувати та використовувати сильні сторони всіх існуючих алгоритмів.

Отже, актуальним напрямком розвитку протидії атакам на відмову є дослідження методів, які б давали змогу виявляти атаки по різним каналам, використовуючи всю наявну інформацію. Також важливо застосовувати сучасні математичні моделі на всіх етапах протидії атакам на відмову, що дозволить значно підвищити надійність та ефективність системи захисту від них.

Концепція підходу ефективної протидії атакам на відмову

Розвиток систем захисту від атак на відмову відбувався у відповідь на існуючі загрози. Спочатку це були прості індикатори, що фіксували, наприклад, кількість байт в секунду або кількість відкритих з'єднань. З появою більш складних типів атак відповідно ускладнювались механізми захисту. При цьому відбувалось залучення математичних моделей з області статистики, нейронних мереж, імітаційного моделювання та інших. Сучасні системи виявлення атак – це системи прийняття рішення в умовах невизначеності інформації, динамічних змін середовища та можливих загроз. Для визначення аномальних явищ у таких системах використовуються складні математичні алгоритми та спеціально побудовані бази знань. Однак існуючі системи захисту через вищезазначені причини не можуть забезпечити достатній рівень виявлення і протидії атакам на відмову.

Для ефективної протидії атакам на відмову в сучасних мережах система захисту має задовольняти таким вимогам.

Адаптивність. Вимоги до безпеки в організаціях можуть бути різними або змінюватися з часом. Тому при зміні параметрів та настройок системи її функціональність має змінюватись відповідно.

Гнучкість. Мережа, за якою ведеться спостереження, може змінюватися протягом часу. Це може бути спричинене появою додаткових можливостей або ресурсів. Отже, система захисту повинна мати можливість змінювати свою функціональність без перезапуску – в режимі он-лайн. Агентні системи можуть забезпечити необхідну гнучкість шляхом встановлення цілей для кожного агента. При змінах відбувається зміна цілей, що не призводить до перезапуску.

Навчання. Фундаментальна характеристика, що дозволяє виявляти нові атаки. З огляду атак видно, що сценарії атак постійно змінюються, знаходять нові вразливості або схеми здійснення. Пропонується здійснювати навчання двома способами. Перший полягає в заданні адміністратором нових цілей для інтелектуальних агентів. Іншим способом є самонавчання агентів, та використання методів інтелектуальної обробки інформації (видобування знань, статистичних моделей, нейронних мереж тощо).

Розподіленість. Одною з властивостей мережі є взаємозв'язанність її компонент. Для успішної роботи потрібна чітка взаємодія всіх складових елементів (роутерів, маршрутизаторів, файлових серверів, окремих комп'ютерів). Нападнику достатньо здійснити атаку проти однієї з цих ланок, щоб вся мережа або її частина стала враженою. Наприклад, він може затопити мережу фальшивими ICMP запитами від імені третіх осіб. Або спрямувати атаку проти провайдера, що надає Інтернет послуги. Тому система виявлення атаки, побудована на базі кінцевого комп'ютера може виявитись неефективною. Більш результативним уявляється проведення розподіленного моніторингу з різних точок мережі.

Автономність. Для спрощення задачі виявлення атак необхідно виконати розподілення обчислювальних задач за різними вузлами. При цьому значно скоротиться час реагування, але слід також створити систему обміну інформацією, яка б дозволила доповнювати виміри вузла даними з інших місць. Інший аспект, пов'язаний з автономністю – це функція делегування. Динаміка процесів в комп'ютерних мережах часто вимагає у відповідь на початок атаки негайне застосування змін у настройках безпеки. Наприклад, чим раніше будуть увімкнені фільтри виявлених фальшованих адрес, тим менша буде потужність атаки. Тому делегування елементам системи виявлення певних функцій адміністрування системи дозволить значно скоротити час реакції та загальну ефективність системи захисту.

Базою для створення такої системи пропонується технологія інтелектуальних агентів, що використовують методи статистичного аналізу та теорії ігор. Підхід інтелектуальних систем для розв'язання складних проблем, зокрема, в області керування комп'ютерними мережами описаний і обґрунтований в багатьох роботах, наприклад, [23, 24]. Багатоагентні системи являються більш мобільними, крім того вони мають додаткові особливості, такі як, наприклад, розподіленість, можливість працювати в умовах непередбачуваних змін як мережі так і зловмисної діяльності, виявлення і документування значимих подій, навчання, аналіз зібраної інформації, планування дій, автономність, адаптивність.

Архітектура системи захисту від атак на відмову

Як уже зазначалось, існуючі системи виявлення принципово можна розділити на системи виявлення аномалій і системи виявлення особливостей. Основний недолік систем виявлення особливостей полягає у тому, що вони розроблені для виявлення конкретних типів атак (як правило найбільш небезпечних на час створення системи). При появі нових атак або зміні характеристик трафіка задачу виявлення необхідно фактично розв'язувати заново. Системи виявлення аномалій (в силу складності моделювання нормального Інтернет трафіка) використовують різні припущення про функціонування системи, таких як, наприклад, статистична однорідність трафіка. При цьому групи комп'ютерних систем, для яких ці припущення мають місце або умови їх виконання не обговорюються. В результаті незначні зміни в структурі трафіка або послуг, що надаються можуть призвести до необхідності нової навчання алгоритму виявлення.

Одним з можливих розв'язків такої ситуації є використання до побудови системи захисту від атак на відмову комплексного підходу, що включає в себе моніторинг функціонування системи, збереження історії трансакцій, ведення спеціального сховища для інтелектуального аналізу активності нападників та їх дій, прийняття рішення щодо вибору стратегії протидії. Пропонується будувати систему захисту на основі наступних елементів:

- агенти стеження;
- агенти попередньої обробки і зберігання;
- сховище для зберігання інформації про трансакції, що описують функціонування системи;
- сховище з аналітичними компонентами для виявлення загроз та ознак здійснення зловмисної активності;
- агенти протидії атакам.

Важливим елементом побудови такої системи є визначення відповідного математичного забезпечення для кожного етапу роботи.

1. **Стеження за трафіком**. Перехват пакетів з метою оцінки завантаження, складу трафіка, активності користувачів. Для здійснення цієї задачі необхідно розробити алгоритми визначення кількості і частоти перехоплення пакетів в залежності від завантаження каналу й інших параметрів. Якщо пакети будуть перехоплюватися занадто часто це може призвести до вповільнення трафіку. Якщо ж пакети будуть перехоплюватися через певні постійні проміжки часу це може створити «сліпі зони», про які не буде відомостей.

2. **Попередня обробка захоплених пакетів, оцінка найбільш небезпечних загроз, збереження інформації у сховищі**. Оскільки на цьому етапі необхідна швидка оцінка з мінімальними затратами ресурсів, доцільно використовувати прості й адаптивні порогові значення або (за необхідності) послідовний CUSUM.

3. **Аналіз даних при завантаженні у сховище, виявлення атак, оцінка загроз**. Після запису інформації в сховище можна провести комплексну оцінку й обчислити можливі загрози. Для цього доцільно використовувати вищеописані багатоканальні алгоритми CUSUM та сковзне середнє.

4. **Фоновий аналіз даних для встановлення спроб сканування, атак погіршення якості, пульсуючих атак**. Здійснюється постійно або за розкладом. Оскільки ці атаки представляють меншу загрозу, то є час для більш детального їх аналізу. Використовуються методи Data Mining, системи інтелектуальних правил, нейронні мережі тощо.

5. **Прийняття рішення про виявлення атаки**. При перевищенні певних порогових значень на одному з попередніх етапів формується признак про можливу загрозу атаки. В цьому випадку має бути створена експертна система, яка б могла оцінити рівень загрози та прийняти рішення про здійснення атаки.

6. **Оцінка загрози, вибір моделі, її верифікація, пошук стратегії**. Виявлення атаки відразу ставить питання про визначення протидії. У залежності від типу і навіть особливостей конкретної атаки така протидія може значно змінюватися. Тобто можна говорити про «стратегію» протидії. У залежності від умов якості протидії, наприклад, якість обслуговування зареєстрованих користувачів, буде змінюватися стратегія. База можливих стратегій має утворюватися за результатами аналітичного моделювання взаємодії між нападниками та агентами захисту. Дослідження аналітичних моделей дозволяє вивчити ефективність протидії та можливі наслідки. Ігрова постановка тут випливає з самої природи конфліктної взаємодії нападника та системи захисту, а основна величина, на яку впливають гравці – завантаженість системи. Це може бути загальна завантаженість або завантаженість окремих, критичних для роботи системи, вузлів (процесора, оперативної памяті, каналів мережі). Позначимо p_i – завантаженість i-го вузла системи, $p = (p_1,..., p_n)$. При цьому будемо вважати, що $p_i \in [0,1]$, де 1 – позначає повну завантаженість, або відмову вузла. Мета команди нападника полягає у максимальному збільшенні хоча б одного з p_i, система захисту намагається, в свою чергу, утримати всі p_i у прийнятних межах і не допустити їх зростання. Оскільки функціонування системи протягом часу також впливає на $p(t)$, то в результаті маємо динамічну керовану систему:

$$p(t_{k+1}) = f(t_k, p(t_k), u(t_k), v(t_k)).$$

Складість описаної системи приводить до необхідності введення певних припущень і ідеалізацій динаміки руху та керувань конфліктуючих груп. Аналіз динаміки та визначення прийнятних стратегій захисту являються складною проблемою, дослідження якої необхідне для успішного функціонування всієї системи.

Для формування стратегії протидії необхідно спочатку оцінити параметри динамічної моделі, в рамках якої відбувається протиборство. В цей процес входить:

1. Визначення типу динаміки.
2. Оцінка кількості і потужності нападників.
3. Оцінка рівня загрози.
4. Визначення можливої протидії та прогнозування наслідків.
5. Застосування протидії та порівняння наслідників з передбаченням.

Після застосування стратегії захисту система має оцінювати ефективність стратегії, вимірюючи загрозу. Якщо атака продовжується, необхідно переглянути стратегію.

Висновки

У роботі розглядалися питання захисту від одного з найбільш небезпечних видів зловмисної діяльності в мережі Інтернет – атак на відмову. Описана історія виникнення проблеми та причини, що зумовили її появу. Проведено огляд основних типів атак та їх класифікація. Окремо розглянуті системи, що підлягають захисту – кожна з них має свої характеристики, важливі при побудові системи виявлення атак.

Система протидії або захисту від атак на відмову має вирішувати наступні задачі: попередження атаки, виявлення атаки, ідентифікація джерел атаки, протидія атаці. Задача виявлення атаки полягає в детектуванні атаки на відмову в разі її появи, це важливий етап, від якого залежать всі подальші дії. Тому алгоритмам виявлення надається велике значення. Вони мають задовольняти вимогам за швидкістю, надійністю, ефективністю. У роботі розглядуються відомі на сьогодні алгоритми виявлення атак, що дозволяють швидко аналізувати дані як з одного, так і з багатьох каналів спостереження.

Основним результатом даної роботи є концепція підходу до побудови системи захисту з використання інтелектуальних агентів та елементів теорії ігор. Багатоагентні системи являються найбільш мобільними, крім того вони мають додаткові особливості, такі як, наприклад, розподіленість, можливість працювати в умовах непередбачуваних змін як мережі так і зловмисної діяльності, виявлення і документування значимих подій, навчання, аналіз зібраної інформації, планування дій, автономність, адаптивність. Описується загальна архітектура такої системи, склад і основні задачі її елементів.

1. *Xiang Y., Zhou W., Chowdhury M.* A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia, March 2004.
2. http://www.prolexic.com/downloads/whitepapers/Prolexic_WhitePaper-DDoS.pdf
3. *Specht S. and Lee R.* Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures // Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, 2004 September. – P. 543 – 550.
4. *Уланов А. В., Котенко И. В.* Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. – 2007, INSIDE, № 1-3.
5. *Mircovic J., Dietrich S., Dietrich D., Reiher P.* Internet Denial of Service: Attack and Defense // Mechanisms. Prentice Hall, Engle Wood Cliffs, NJ. 2005.
6. *Peng T., Leckie C., and Ramamohanarao K.* Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems // ACM Computing Surveys. – 2007. – Vol. 39, N 1. – P. 31 – 42.
7. *Rocky K., Chang C.* Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial // IEEE Communications Magazine, 2002 October, – P. 42 – 51.
8. *Ігнатенко О.П.* Виявлення низькочастотних атак на відмову на основі історичних даних // Комп'ютерні науки та інформаційні технології, – Львів: 2008, – № 1.
9. *Gates C., Taylor C.* Challenging the Anomaly Detection Paradigm. A provocative discussion // NSPW 2006, – Germany: September 19-22, 2006, Schloss Dagstuhl.
10. *Peng T., Leckie C., Kotagiri R.* Proactively detecting distributed denial of service attacks using source ip address monitoring // Proceedings of the Third International IFIP-TC6 Networking Conference. – Networking: 2004. – P. 771–782.
11. *Gil T., Poletto M.* MULTOPS: A data-structure for bandwidth attack detection // In Proceedings of the 10th USENIX Security Symposium, 2001.
12. *Abdelsayed S., Glimsholt D., Leckie C., Ryan S., Shami S.* An efficient filter for denial-ofservice bandwidth attacks // In Proceedings of the 46th IEEE Global Telecommunications Conference (GLOBECOM'03). – P. 1353–1357.
13. *Peng T., Leckie C., Kotagiri R.* Information sharing for distributed intrusion detection systems // J. of Network and Computer Applications. – 2007. – 30. – P. 877–899.
14. *Borgnat P. and al.* Extracting Hidden Anomalies using Sketch and Non-Gaussian Multiresolution Statistical Detection Procedures // LSAD'07, Kyoto, Japan: August 27–31 2007.
15. *Chen L., Longstaff T. A., Carley K. M.* Characterization of defense mechanisms against distributed denial of service attacks // Computer & Security. – 2004. – N 23. – P. 665 – 678.
16. *Siris V., Papagalou F.* Application of anomaly detection algorithms for detecting SYN flooding attacks // Computer Communications. – 2006. – N 29. P. 1433–1442.
17. *Ren W., Jin H., Liu T.* Congestion Targeted Reduction of Quality of Service DDoS Attacking and Defense Scheme in Mobile Ad Hoc Networks // Proceedings of the Seventh IEEE International Symposium on Multimedia (ISM'05).
18. *Krishnamurthy B., Sen S., Zhang Y., Chen Y.* Sketchbased Change Detection: Methods, Evaluation, and Applications // IMC'03, October 27–29, 2003, Miami Beach, Florida, USA.
19. *Zheng C., Ji L., Pei D., Wang J., and Francis P.* A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-Time // SIGCOMM'07, Kyoto, Japan: August 27–31 2007. – P. 277 – 288.
20. *Brodsky B., Darkhovsky B.* Nonparametric Methods in Change-point Problems. Kluwer Academic Publishers, Dordrecht, The Netherlands.
21. *Basseville M., Nikiforov I. V.* Detection of Abrupt Changes: Theory and Application (Prentice Hall, 1993).
22. *Chen Y., Hwang K.* Collaborative Change Detection of DDoS Attacks on Community and ISP Networks // IEEE International Symposium on Collaborative Technologies and Systems (CTS 2006), Special Session on Collaboration Grids and Community Networks, Las Vegas, NV. – 2006 May 15-17. – P. 401 – 410.
23. *Jansen W. A.* Intrusion detection with mobile agents // Computer communications. – 2002. – 25. – P. 1392 – 1401.
24. *Krmíček V., Celeda P., Rehák M., Pěchouček M.* Agent-Based Network Intrusion Detection System // In Intelligent Agent Technology. IEEE Computer Society. Los Alamitos, California. – 2007. – P. 528 – 531.