УДК 681.324:007:681.3.068

О.М. ХОШАБА

Вінницький національний технічний університет, Україна

ПІДВИЩЕННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ СЕРВІС-ОРІЄНТОВАНИХ СИСТЕМ У КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ МУЛЬТИАГЕНТНОГО ПІДХОДУ

У статті розглянуті методи та засоби підвищення надійності функціонування сервіс-орієнтованих систем у комп'ютерних мережах за допомогою мультиагентного підходу. На прикладі Web-сервісу розглянуто побудова мультиагентної системи з керування потоками даних у комп'ютерних мережах. Визначено, що розпізнавання небезпечних та непотрібних потоків даних у комп'ютерних мережах дозволить суттєво підвищити надійність функціонування сервіс-орієнтованих систем.

сервіс-орієнтовані системи, мультиагентні системи, комп'ютерні мережі, підвищення надійності функціонування систем.

Вступ

Використання мультиагентних систем (МАС) для керування сервіс-орієнтованими системами (СОС) у комп'ютерних мережах (КМ) вважається ефективним вирішенням проблеми надійності функціонування інформаційних ресурсів [1 – 3]. Така особлива властивість МАС як автономність дає змогу широко впроваджувати елементи оптимізації у функціонування СОС. Тому на сьогоднішній день актуальними питаннями є побудова МАС та дослідження роботи СОС у КМ.

Постановка задачі. Нині актуальними залишаються питання підвищення ефективності функціонування СОС за рахунок збільшення швидкості та якості розпізнавання небезпечних та непотрібних потоків даних (ННПД) і зменшення часу спрацьовування підсистеми прийняття рішень СОС. Тому, для розв'язання даної проблеми необхідно [1, 3]: 1) визначити механізм функціонування проксі-сервіса для розпізнавання ННПД у СОС; 2) побудувати систему управління потоками даних (СУПД) реального часу, які основані на застосуванні МАС; 3) використати методи розпізнавання ННПД у КМ, які основані на логіко-часових характеристиках будь-яких систем, що працюють у КМ з протоколом TCP/IP [3]. Для ефективного керування інформаційними ресурсами КМ з метою вилучення ННПД передбачає розв'язання таких задач: 1) повна заборона у проходженні потоків даних (ПД) до СОС; 2) динамічне обмеження доступу у проходженні ПД до СОС з визначенням напрямку передавання даних, IP адрес, найменування протоколів, портів, встановленням часу з'єднань та тривалості періоду передачі даних.

Огляд рішень. Для вирішення цих проблем у переважній більшості випадків використовується система Firewall. До переваг цієї системи відносить гнучку і розвинену систему правил за допомогою яких можна практично повністю контролювати будь-які напрями ПД і в значній мірі підвищувати продуктивність КМ. Проте, при використанні даного класу систем існують недоліки, до головних з яких відносять: відсутність розвинених механізмів прийняття рішень в критичних ситуаціях (які полягають в пізньому часі спрацьовуванні правил); існування необхідності в повторному виконанні сервісів сервера; відсутність динамічного режиму встановлення правил фільтрування ПД; існування необхідності в аналізі кожної IP-дейтаграми.

Також в роботах, направлених на підвищення ефективності функціонування КМ, були відсутні [3]:

– методи розпізнавання ННПД що основані на логіко-часових характеристиках процесу взаємодії менеджера та агента (або клієнта-сервера);

– структури та методи побудови систем розпізнавання ННПД що основані на логіко-часових методах;

– структури та методи побудови систем реального часу що основані на механізму проксі-сервісу для прийняття рішень щодо результатів розпізнавання ННПД.

Вважається, що для вирішення першої проблеми, а саме, підвищення ефективності функціонування КМ існують потужні програмно-технічні розробки та механізми, які дозволяють досить ефективно вирішувати першу задачу. Але рішення другої задачі, яке полягає у динамічному обмеженні доступу у проходженні ПД до СОС, є не до кінця вирішена. Це відбувається завдяки труднощам у побудові потужних програмних засобів (ПЗ) та витратам системних ресурсів при роботі таких систем. Це зумовлено тим, що на сьогоднішній день проблема другої задачі вирішується шляхом аналізу змісту IP-дейтаграми у ПД.

Таке комплексне рішення ефективного керування інформаційними ресурсами СОС надасть змогу суттєво знизити ННПД на діючих серверах корпоративних та міжнародних вузлів Internet. Визначення основних характеристик взаємодії менеджера і агента МАС на основі протоколу TCP надає змогу сформувати логіко-часовий метод. Логічна частина цього методу пов'язана як з особливостями з'єднань різних сервісів КМ на основі протоколу TCP, так і з формуванням правил прийняття ефективних рішень при розпізнаванні ННПД. Часова частина пов'язана з виміром основних відрізків часу процесу з'єднання агента та менеджера СОС. Використання механізму проксі-сервісу та логіко-часового методу надає можливість на основі основних характеристик взаємодії менеджера СОС і агента визначати ННПД, ступінь завантаження каналів даних, сервера і віддаленої робочої станції. Тому, враховуючи ці чинники, визначається загальна стратегія розпізнавання ННПД та обробки ПД, які можуть мати різні рівні. Для цього також важливо проводити апостеріорний аналіз на основі інтелектуальних методів для знаходження компромісного варіанту прийняття рішення в залежності від існування таких критичних для функціонування КМ та КС ресурсів як: процесорний час, оперативна пам'ять (ОП), канали зв'язку.

Рішення задачі

Розвиток СОС та засобів керування ПД у КМ проходив в декілька етапів, головним чином яких були статичні та динамічні правила. Статичні правила відмічали певний рух ПД до СОС. Наприклад, заборона руху ззовні сервера до проксі-порту (порт 3128) та дозвіл на порти DNS (порт 53), FTP (порти 20, 21), WWW (порт 80), SMTP (порт 25), тощо. Існували випадки, коли правила, які були створені окремими організаціями були різними. Наприклад, в деяких установах була заборона звернення на порти 110 (POP3), або 80 (WWW) які виконуються ззовні. В результаті бурхливого розвитку СОС, поширенню нападів на міжнародні інформаційні ресурси, збільшення ННПД в наслідок атак або неправильного адміністрування СОС виникла необхідність у використанні динамічних правил. Використання динамічних правил полягає у блокуванні ПД з певних поодиноких або діапазонів IP-адрес. Це дозволяє суттєво зменшити ННПД, які надходять до СОС. Загальна структура з керування ПД, які надходять до СОС, зображена на рис. 1.

Узагальнена модель, яка зображена на рис. 1, може ефективно використовуватись відносно практично всіх СОС (наприклад FTP, DNS, SAMBA) та транспортних протоколів стеку TCP/IP (наприклад TCP або UDP). Модель керування ПД у КМ відображає пакети (для протоколу TCP) або дейтаграми (для протоколу UDP) в обох направленнях до СОС і аналізує запити та відповіді стосовно необхідного порту та протоколу передачі даних. В цьому випадку відокремлюється кожний ПД, визначаються вміст пакетів або дейтаграм. У разі необхідності, на етапі збору та аналізу даних існує можливість зібрати статистику функціонування дослідного СОС по основних характеристиках передачі інформації: кіль-

кість запитів, об'єм (у байтах) запитів та відповідей, відносні показники запитів та відповідей, швидкість обробки запитів серверами СОС. Після аналізу дослідної інформації формуються правила, по яким МАС повинна приймати рішення по забороні або зменшення швидкості проходження даних. Суттєвими показниками у побудові моделі (рис. 1) були швидкість та інтенсивність надходження ПД, визначення типу ПД (потрібний або непотрібний), час, при якому починають діяти правила, кількість надходжень однотипних запитів.

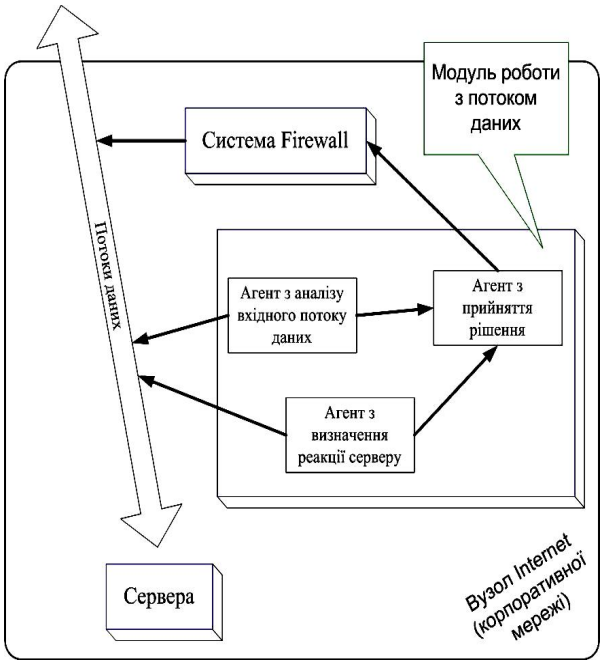

Рис. 1. Узагальнена структура з керування потоками даних які надходять до сервіс-орієнтованих систем

Для побудови концептуальної моделі МАС керування ПД у КМ вважається за необхідне вводити абстрактне визначення трьох функціональних рівнів.

Перший рівень складали клієнтські інформаційні ресурси СОС і засоби управління локальними, корпоративними або глобальної КМ. До них відносились: інформаційні ресурси СОС (в якості надання даних WWW, FTP, e-mail і т.і.); інформаційні ресурси робочих місць (в якості споживача інформації); механізми, що забезпечують безпеку інформаційних ресурсів і управління (фільтрація) ПД. Наприклад, ПЗ ipfw і ipfilter – для ОС FreeBSD, ipchains – для ОС Linux забезпечували захист інформаційних ресурсів.

При функціонуванні система керування ПД здійснювала фільтрацію інформаційних вхідних і вихідних ПД по визначених протоколах, портам, IP адресам відправника та одержувача. При цьому всі системи фільтрації і захисту даних були розташовані на серверах локальних, корпоративних або глобальних вузлах і були цілком автономними стосовно інших систем та рівнів.

Другий рівень являв собою МАС, що виконував функцію керування ПД у КМ до СОС. Основними задачами даного рівня були: динамічний розподіл функцій керування, моніторинг і контроль ПД СОС; здійснення всіх фаз взаємодії з інтелектуальними агентами (формалізація запиту на управління та одержання результату на виконання конкретних операцій). МАС виконувала передаточні і перевірочні функції на інформаційні ПД від користувача або кінцевої (клієнтської) системи (споживача інформації) до керованих ресурсів СОС. Однією з складових частин МАС були інтелектуальні агенти (ІА). МАС та ІА знаходилися на серверах операційної системи Unix.

До третього рівня відносилися сервера або системи управління базами даних/знань, орієнтовані на запити користувачів, інтеграцію і збереження результатів роботи МАС або ІА. Основною задачею даного рівня були: надання користувачам можливості на формування запитів; інтерпретація відповідей чи результатів роботи від МАС або ІА; виконання операцій по вивченню роботи інформаційних структур досліджуваних комп'ютерних мереж. У структурі третього рівня знаходилися робочі місця користувачів, на яких були встановлені операційні системи Unix, Windows і т.д. і такі, що містять графічний чи текстовий інтерфейси для роботи з МАС (ІА).

Важливою ланкою функціонування СУБД на основі МАС була ефективна робота ПЗ першого рівня, в основу якого покладені основні фактори управління ПД. В основу іншого рівня СУБД покладені функції об'єднання всіх задіяних рівнів систем. До об'єкта управління потоком і захистом даних іншого рівня відносилася таблиця правил проксі-сервісу

СОС. Виходячи з критеріїв управління потоком і захистом даних щодо протоколів, портів і IP, адрес формувався конфігураційний файл ІА.

Організація функціонування МАС складалася з роботи ІА, підсистем репозиторія та арбітра ресурсів. Для функціонування МАС використовувалися три типи ІА (рис. 2): агенти даних (D-агенти), агенти управління (С-агенти) і повідомлюючі (новинні) агенти (N-агенти).

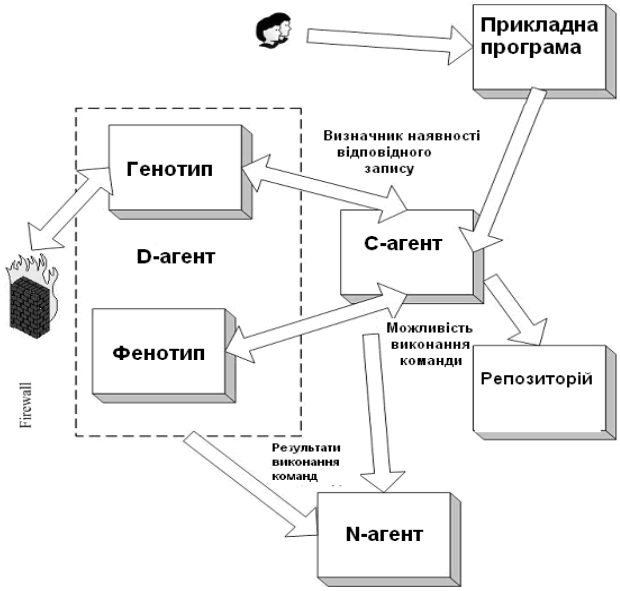

Рис. 2. Структура системи керування потоками даних у комп'ютерній мережі

Агенти даних складали важливу частину МАС і служили основною інформаційною структурою третього рівня. Кожному запиту третього рівня на управління інформаційними потоками КМ відповідав агент даних іншого рівня, який називається легітимним D-агентом. Також існували запити на керування D-агентами, про які не існували правила у таблиці системи проксі-сервісу СОС. Такі D-агенти називали нелегітимними. Легітимні D-агенти створювалися негайно після надходження запиту на управління інформаційним потоком. Знищувалися вони після виконання необхідних операцій. D-агент міг знаходитися в одному з трьох станів: активному, пасивному і режимі виконання операцій. Нелегітимні D-агенти створювалися на початку запиту користувача і знищувалися після завершення операції порівняння його ідентифікаційного поля з таблицею системи Firewall.

Легітимний D-агент характеризувався ідентифікаційним номером і двома незалежними векторами. Перший вектор (генотип D-агента) був набором номерів правил проксі-сервісу СОС і опису об'єкта третього рівня, що зберігається в базі даних/знань СУПД. Цей вектор характеризувався незмінними для кожного легітимного D-агента даними.

Другий вектор був набором команд можливих операцій для С-агента. У загальному випадку, набір іншого вектора являв собою команди проксі-сервісу СОС на керування ПД інформаційними ресурсами КМ. Набір іншого вектора називали фенотипом D-агента. Порядок опису D-агента визначала послідовність перевірки наявності відповідних правил у таблиці проксі-сервісу СОС. Протягом свого існування D-агент міг адаптуватися до умов "існування" за допомогою зміни свого фенотипу. D-агенти мали профілі розпізнавання ПД, які були такої структури: “Характер” (детермінований, ймовірносний, функціональний), “Правило”, “Оцінка роботи” (експертна, аналітична), “Час початку роботи”. В табл. 1 наведені деякі профілі розпізнавання ПД D-агентів.

Завдяки існування “Часу початку роботи” у багатьох D-агентів спостерігались перетинання змінних цього параметру. Це надавало можливість проводити оптимізацію профілів розпізнавання ПД за ознаками експертної оцінки: “ефективний”, “мало ефективний”, тощо.

Кожному D-агенту також належав список команд проксі-сервісу СОС або проксі-сервіса для С-агента, що були необхідні для керування ПД. Агенти керування (С-агенти) утворювалися за допомогою ПЗ користувачів або спеціальних команд ОС. При виконанні будь-якої команди С-агент створює повідомлення про результат виконання команди, що транспортується повідомлюючим агентом (N-агент) за адресою призначення. Знищуються С-агенти після виконання всіх необхідних операцій з будь-якими результатами операцій. У ході існування С-агентів утворюються декілька повідомлюючих агентів, що передають інформацію з деяких адрес.

Таблиця 1

Профілі розпізнавання потоків даних у D-агентів

Профілі	Характер	Правило	Оцінка	Час початку роботи
Перший	Детермінований	4-ий пакет потоку вміщує код 200, 301, 302 або 404	Експертна – малоефективний	4 пакет потоку
Другий	Детермінований	Наявність додаткового пакета який передається від менеджера до агента	Експертна – ефективний	5 пакет потоку
Третій	Ймовірносний	Час відповіді менеджера: (діапазон ...) -> прийняття рішення, ... (діапазон ...) -> прийняття рішення.	Експертна – ефективний Аналітична – помилка I та II роду	5, 7, 9 пакети потоку
Четверий	Функціональний	Наявність “нормальних” ПД від одного IP-адреса, кількість яких перевищує 10 за 1 с	Експертна – ефективний Аналітична – помилка I та II роду	10 потоків

За допомогою транспортного протоколу TCP/IP вони транспортуються на заданий вузол КМ, знаходять відповідного D-агента і виконують необхідні операції.

Основним призначенням С-агентів є: пошук відповідного D-агента з метою виконання заданої операції по управлінню інформаційними ПД у КМ; створення N-агента, що інформував про результати виконання операцій.

Повідомляючи агенти забезпечували інтерфейс між МАС (ІА) і ПЗ третього рівня, зокрема, репозиторієм. Репозиторій являв собою базу даних/знань.

Таким чином, побудована МАС ефективно виконувала функції керування ПД у КМ.

Висновки

У статті:

1) визначено розв’язання проблеми підвищення надійності функціонування СОС у КМ за допомогою мультиагентного підходу;

2) виконано огляд знайдених рішень проблеми підвищення надійності функціонування СОС у КМ за допомогою мультиагентного підходу;

3) розроблено логіко-часовий метод, що забезпечує вилучення ННПД які надходять до СОС;

4) побудована концептуальна модель МАС з керування ПД у КМ та визначені особливості функціонування кожного з трьох рівнів.

Література

1. Хошаба А.М. О проблеме определения эффективности работы мультиагентных систем при управлении потоком данных в компьютерных сетях // Оптико-електронні інформаційно-енергетичні технології. – 2004. – №1 (7). – С. 139-144.

2. Хошаба О.М. Дослідження функціонування динамічних інтелектуальних систем у комп'ютерних мережах // Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій: Збірка наукових праць у п'яти томах. Т. 2. – Євпаторія, 2005. – С. 140-144.

3. Хошаба О.М. Визначення основних характеристик завантаженості агента мультиагентної системи у комп'ютерній мережі // Інформаційні технології та комп'ютерна інженерія. – Вінниця, 2005. – №1. – С.42-48.

Надійшла до редакції 23.02.2006

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет "ХАІ" ім. М.Є. Жуковського, Харків.