УДК 004.056

П.О. Кравець, О.М. Сегеда

Національний університет «Львівська політехніка», Львів

БЕЗПЕКА МУЛЬТИАГЕНТНИХ ПРОГРАМНИХ СИСТЕМ

Вступ

Розвиток технологій програмування йшов від структурного до об'єктно-орієнтованого, а далі – до компонентного та аспектного програмування. Поряд з цим еволюціонували і обчислювальні середовища – від однозадачного до багатозадачного, від однопотокового до багатопотокового, паралельного, від локалізованого до розподіленого.

Враховуючи сучасний розвиток інформаційних систем, їх розподілену природу та функціонування в умовах невизначеності, зароджується нова технологія для їх програмної підтримки на основі інтелектуальних агентів [1, 2]. Для цього в обчислювальній мережі формуються команди програм-агентів, призначені для розв'язування поставлених користувачами задач.

На сьогодні не існує ефективних математичних моделей, які могли б гарантовано передбачити поведінку таких систем. В умовах невизначеності, конкуренції за обмежені ресурси, при здатності агентів до автономного прийняття рішень можливі переходи популяцій агентів в некеровані, хаотичні стани, що призводить до необхідно розробляти додаткові заходи безпеки функціонування мультиагентних систем.

Програмні агенти

Програмний агент – це об'єкт, який інкапсулює код та дані для вирішення сформульованої розробником проблеми у визначеному інформаційному середовищі. На відміну від звичайних об'єктів, агент є активною програмною одиницею, здатною сприймати та аналізувати дані інформаційної мережі, вести переговори з іншими агентами, приймати автономні рішення, інформувати систему та користувача про результати своїх дій.

Мультиагентна система – група агентів інформаційної мережі, які взаємодіють між собою для досягнення визначеної розробником мети.

Базовими властивостями програмних агентів є:

1) автономність – виконуючи поставлену ціль, агент може самостійно приймати рішення на основі власних знань, не потребуючи зовнішнього керування;

2) реактивність – агент може сприймати зовнішню інформацію, виробляти та реалізовувати адекватні дії;

3) інтелектуальність – здатність агента навчатися, адаптуватися до змін середовища, опрацьовувати отримані дані методами штучного інтелекту, приймати оптимальні рішення;

4) мобільність – для досягнення мети агент може переміщуватися по інформаційній мережі;

5) координація – розподіл ролей та узгодження дій агентів при розв'язування спільної задачі;

6) інтерактивність – агент взаємодіє з іншими агентами, з інформаційними ресурсами мережі та з користувачем;

7) комунікативність – здатність агентів спілкуватися та розуміти один одного на заданій мові;

8) персональність – унікальні якості агента, що моделюють його психологічні риси характеру, поточні емоції та ін.

Перераховані властивості у значній мірі визначатимуть вимоги до безпеки мультиагентних програмних систем.

Аспекти безпеки програмних агентів

Виділимо два аспекти безпеки агентних систем:

1) технічний, пов'язаний з перевищеннями пропускної здатності та потреб у наявних обчислювальних ресурсах;

2) інформаційний, пов'язаний з нераціональною, несанкціонованою або деструктивною поведінкою агентів.

Технічний аспект безпеки обумовлений масштабуванням мультиагентної системи. Для оперативного розв'язування задач здійснюється їх розпаралелювання за рахунок координованого розподілу робіт у групі автономних програмних агентів. Корегування роботи колективу агентів забезпечується запуском у мережу агентів з новими функціями. Крім того, підвищення надійності роботи інформаційної системи досягається клонуванням програмних агентів. Враховуючи додаткову можливість міграції мобільних програмних агентів, при неконтрольованому зростанні їх чисельності в інформаційній мережі можуть виникнути вузькі місця, що може призвести до краху всієї системи.

Інформаційний аспект безпеки обумовлений логікою функціонування та взаємодії інтелектуальних агентів. Агенти є функціональними одиницями розподіленого штучного інтелекту і їх поведінка визначається знаннями та правилами, закладеними при їх створенні розробником. Як правило, така інформація є неповною. Тому агент проектується як активна, здатна до навчання програмна одиниця. Навчання здійснюється на основі аналізу поточних станів інформаційної мережі. В умовах дефіциту ресурсів можливе спотворення інформації про стани мережі зі сторони конкуруючих колективів агентів. Загрозу безпеці функціонування агентів спричиняє розвідувальний, несанкціонований збір інформації про конкурентів. Можна допустити також прямі акти агресії агентів, які полягають у несанкціонованому вилученні з мережі або інвазивним перепрограмуванням функцій. Крім того, певні спотворення

функцій можливі при продукуванні агентів фабриками класів на основі застарілих даних. В результаті усіх цих та інших чинників дії агентів повинні бути безпечними для людини.

Технічний аспект вирішується розробленням спеціалізованого технічного і програмного мережного забезпечення, орієнтованого на ефективне та безпечне виконання програм-агентів, яке автоматично керує трафіком та обчислювальними ресурсами колективів агентів.

Інформаційний аспект вирішується підвищенням рівня інтелектуальності агентів, здатних адаптуватися до поточних станів системи, навчатися діяти раціонально, забезпечуючи оптимальне вирішення поставлених задач та протидію цілеспрямованим атакам зі сторони інших агентів.

Сервіси безпеки програмних агентів

За аналогією стандартних засобів безпеки COM+, базові протоколи безпеки мультиагентних систем можуть бути реалізовані у вигляді бібліотек провайдерів сервісів безпеки. До таких сервісів належать:

1) аутентифікація агентів – при взаємодії з іншими агентами необхідно підтвердити власну автентичність за допомогою пред'явлення спеціальних ідентифікаційних квитків;

2) перевірка цілісності даних за допомогою контрольної суми пакетів даних;

3) шифрування трафіка, яке захищає дані від несанкціонованого перегляду.

Для мультиагентних систем будуть необхідними ряд додаткових сервісів для контролю над діями автономних інтелектуальних агентів:

1) розроблення та ведення бази нормативних правил поведінки агентів у мережі;

2) розроблення сервісних агентів, призначених для здійснення операцій розподіленого контролю за дотриманням нормативних правил поведінки;

3) виявлення сигнатур агентів з несанкціонованими діями, їх лікування або вилучення з мережі;

4) виявлення та усунення протиріч в інформаційних базах агентів;

5) вирішення конфліктів агентів на основі нормативних правил;

6) забезпечення комунікаційних послуг та інтерфейсів для спілкування агентів з агентами і з користувачами;

7) планування задач, синхронізація та координація дій, забезпечення пластичності агентів однієї популяції для досягнення сформульованої мети при зміні інфраструктури взаємодії агентів;

8) навчання, консультування та допомога агентам у прийнятті раціональних рішень.

Крім перерахованих, мультиагентна система може мати ряд додаткових сервісів, характерних для соціуму інтелектуальних елементів.

При дотриманні основних правил співіснування у соціумі, безпека інтелектуальних агентів в основному визначається їх інформаційним базисом.

Висновки

Безпека програмних мультиагентних систем досягається за рахунок децентралізованого розв'язування задачі, введенням надлишкових агентів, протоколами аутентифікації, перевірки цілісності та шифруванням даних. Мультиагентні системи, крім традиційних вимог до безпеки функціонування розподілених інформаційних систем, висувають ряд нових, пов'язаних з інтелектуальною організацією програмних агентів.

Раціональна поведінка агентів в основному залежить від достовірності даних та ефективності і функціональної надійності методів штучного інтелекту, якими володіють агенти.

Забезпечення надійності та стійкості функціонування мультиагентних систем може бути досягнуто побудовою нових сервісів для збору та опрацювання інформації, координації взаємодії, навчання та прийняття рішень колективом агентів.

Список літератури

1. Weiss. G. Adaptation and Learning in Multiagent Systems / Gerhard Weiss, Sandip Sen, editors. – Berlin: Springer Verlag, 1996. – 585 p.

2. Stone. P. Layered Learning in Multiagent Systems / P. Stone. – MIT Press, 2000. – 300 p.