УДК 004.632

[1]О.В. Присада, [1]Л.В. Мелещук, [2]В.А. Волошин
[1]Ковельський промислово-економічний коледж Луцького НТУ, Україна
[2]Тернопільський національний економічний університет, Україна

УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО РЕСУРСІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ

O.V. Prysada, L.V. Meleshchuk, V.A. Voloshyn

USERS ACCESS MANAGEMENT TO INFORMATION SYSTEM RESOURCES

Адміністрування ресурсів загального доступу інформаційної системи є актуальною задачею. Тенденції розвитку мереж та інформаційних систем є такими, що, скільки б додаткових ресурсів не мала розподілена інформаційна система, настає момент, коли їх стає недостатньо. Із збільшенням мереж, зростає і кількість ресурсів, що ускладнює їх адміністрування. Необхідна наявність спеціальних аналітичних та інформаційних засобів, що дають можливість здійснювати прийняття рішень в складних умовах невизначеності. У цих умовах виникає необхідність контролю доступу до ресурсів на основі якихось правил або вимог. Одним з напрямів контролю доступу є використання набору правил на основі апарату нечіткої логіки [1, 2].

Математична теорія нечіткої логіки є узагальненнями класичної теорії формальної логіки. Основною причиною появи цієї теорії стала наявність нечітких і наближених міркувань при описі людиною процесів, систем, об'єктів.

Основними перевагами нечітких систем у порівнянні з іншими є [1, 2]:

– можливість оперувати вхідними даними, заданими нечітко, наприклад, значеннями, що невпинно змінюються в часі (динамічні задачі);

– можливість нечіткої формалізації критеріїв оцінки і порівняння;

– можливість проведення якісних оцінок як вхідних даних, так і виведених результатів, оскільки система оперує не тільки власне значеннями даних, а й їх ступенем вірогідності та її розподілом;

– можливість проведення швидкого моделювання складних динамічних систем та їх порівняльний аналіз із заданим ступенем точності.

В інженерних задачах застосовується, як правило, механізм нечіткого висновку Мамдані [3–6], в якому використовується мінімаксна композиція нечітких множин.

Застосування апарату нечіткої логіки при створенні системи управління доступом шляхом вибору відповідного класу детекторів комп'ютерних атак для кожного окремого клієнта з врахуванням поточних параметрів самої комп'ютерної мережі дозволить забезпечити високу продуктивність та стійкість системи в режимі реального часу.

Комп'ютерна система при передачі інформації використовує мережу для здійснення доступу клієнтів. Деякі клієнти мережі можуть бути випадковими чи новими, тому вони не є надійними для сервера з точки зору безпеки, тобто є велика ймовірність проведення всіх видів сучасних атак. Інші клієнти можуть вважатися надійними, тобто ймовірність виникнення атаки під час з'єднання з ними прямує до нуля. Клієнти мережі, відомі серверу по IP-адресі і, враховуючи «стаж» користування мережею, мають свій рівень довіри, що можна задати ймовірністю збоїв при передачі пакетів інформації.

Отже, якщо клієнт є новим для даної системи або має рівень довіри дуже низький, то ймовірність виникнення атаки рівна 1, тобто в даному випадку необхідно

підключати усі детектори нейронної мережі. І навпаки, для клієнта з дуже високим рівнем довіри значення ймовірності виникнення атаки може бути рівня 0, тобто можна не застосовувати систему ідентифікації атак, що забезпечить підвищення швидкодії системи. Ймовірність виникнення атак може бути отримана із значення атрибутів аналізатора мережевого з'єднання. Для визначення ймовірності виникнення будь-якого типу атак P_i може бути використане наступне співвідношення: $P_i=k/n$, де k – кількість випадків виникнення атаки даного типу, n – кількість з'єднань з даним джерелом інформації.

Необхідний рівень продуктивності та доступний об'єм пам'яті також є важливими параметрами нечіткої системи, оскільки залежно від їхнього поточного значення необхідно оптимізувати нечіткий висновок, тобто визначити клас детекторів найнебезпечніших в кожному конкретному випадку. Значення цих вхідних змінних можуть отримуватися з самої комп'ютерної системи в режимі реального часу.

За механізмом Мамдані нечітка система працює на основі правил типу «if-then»:

1. Якщо ймовірність виникнення атаки з джерела рівна 0, то клас детекторів рівний 0;

2. Якщо ймовірність виникнення атаки з джерела рівна 0.5, ймовірність DoS-атаки рівна 0.8, ймовірність Probe-атаки рівна 0.4, ймовірність R2L-атаки рівна 0.5, ймовірність U2R-атаки рівна 0.6, продуктивність – середня, об'єм пам'яті – малий, то клас детекторів рівний DoS;

3. Якщо ймовірність виникнення атаки з джерела рівна 0.7, ймовірність DoS-атаки рівна 0.2, ймовірність Probe-атаки рівна 0.2, ймовірність R2L-атаки рівна 0.8, ймовірність U2R-атаки рівна 0.7, продуктивність – висока, об'єм пам'яті – середній, то клас детекторів рівний R2L та U2R;

4. Якщо ймовірність виникнення атаки з джерела рівна 1, то клас детекторів рівний DoS, Probe, R2L, U2R.

Запропоновану нечітку систему можна побудувати застосовуючи засіб Fuzzy Logic Toolbox середовища MATLAB.

Література

1. Ross T.J. Fuzzy Logic with Engineering Applications / T.J. Ross. – McGraw-Hill Inc.(USA), 1995. – 600 p.

2. Shtovba S.D. Ensuring Accuracy and Transparency of Mamdani Fuzzy Model in Learning by Experimental Data / S.D. Shtovba // Journal of Automation and Information Sciences. – 2007. – № 39 – P. 39-52.

3. Dubchak L. Speedy procesing method of fuzzy data for intelligent systems of intrusion detection / L. Dubchak, M. Komar, A. Sachenko, V. Kochan // Projekt interdyscyplinarny projektem XXI wieku. – Bielsko-Biala, 2017. – Tom 2: Processing, transmission and security of information. – S. 65-74.

5. Dubchak L. Fuzzy Data Processing Method / L. Dubchak, N. Vasylkiv, V. Kochan, A. Lyapandra. // Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications : Proceedings of the 7th IEEE International Conference, Berlin (Germany), September 12-14, 2013. – V1. - P. 373-375.

5. Васильків Н.М. Нечітка система розподілу завдань для тестування студентів / Васильків Н.М., Л.О.Дубчак, Т.В.Лендюк, І.В.Турченко // Науковий вісник Чернівецького національного університету: Комп'ютерні системи та компоненти. – Чернівці. – 2016. – Т. 7, вип. 2. – С. 20-24.

6. Дубчак Л.О. Средство ускоренной обработки нечетких данных на основе механизма Мамдани / Л.О. Дубчак, В.В. Кочан, Н.М. Василькив // Вестник Брестского государственного технического университета. Серия физика, математика, информатика. – 2016. – №5. – С. 23-26.