УДК 004.942

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 91-97

ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕМЕДИЧНИХ СИСТЕМАХ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Л.О. Дубчак

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: dlo@tneu.edu.ua

У даній статті розглянуто метод захисту інформації, що передається в телемедичних мережах, шляхом вибору алгоритму шифрування даних на основі нечіткої логіки. Побудована нечітка система дозволяє здійснювати адекватний захист даних в реальному часі, враховуючи поточний стан самої комп'ютерної системи.

Ключові слова: нечітка система, телемедицина, захист інформації, DES, RSA, криптоалгоритм на основі еліптичних кривих

Вступ

Телемедицина – це галузь медицини, яка використовує телекомунікаційні та електронні інформаційні (комп'ютерні) технології для надання медичної допомоги і послуг в сфері охорони здоров'я в точці необхідності (в тих випадках, коли географічна відстань є критичним фактором) [1]. Глобальна мережа Інтернет в даному випадку є засобом зв'язку між клієнтом та комп'ютерною системою медичного закладу. Звідси випливають усі проблеми захисту інформації, що використовується в телемедицині, з точки зору інформаційної системи та мережі.

Як правило, інформаційна система включає [2]: прикладне програмне забезпечення (ППЗ), яке відповідає за зв'язок системи з клієнтом; системи управління базами даних (СУБД); операційну систему для обслуговування ППЗ та СУБД; мережу, яка забезпечує взаємодію всіх вузлів інформаційної системи. Найнебезпечнішими для таких інформаційних систем є несанкціонований доступ до паролів чи конфіденційної інформації, порушення прав доступу, атаки типу «відмова в обслуговуванні», «пряма» атака, віруси, сучасні атаки по побічних каналах витоку інформації. Несанкціонований доступ полягає у підборі чи викраденні пароля або підміні IP-адреси законного користувача системи. До цього виду атак вразливі усі компоненти інформаційної системи.

Існує чотири стандартні підходи, за допомогою яких можна обмежити доступ до інформації [3]:

- контроль доступу;
- розширення парольного захисту;
- шифрування;
- використання брандмауерів.

Атака типу «відмова в обслуговуванні» полягає у створенні неправильного пакету даних чи передачі великої кількості пакетів даних по мережі з метою блокування роботи контролера домена, що зупиняє роботу комп'ютерної системи. Для захисту компонентів інформаційної системи застосовуються спеціальні програми виявлення такого типу атак чи міжмережеві екрани [4].

Комп'ютерний вірус – комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати

шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Для захисту від вірусів на даний час існує багато антивірусних програм, що захищає інформаційну систему від пошкодження.

Побічними каналами витоку інформації під час передачі пакетів даних по мережі є електромагнітне випромінювання, час виконання алгоритмів шифрування та реакція системи на спеціально внесені помилки. Для протидії таким атакам використовуються, як правило, архітектурна та операційна надлишковість, тобто додаткові апаратні та програмні засоби [3, 5].

Постановка завдання дослідження

Загалом можна визначити наступні методи захисту інформаційної системи від втрати чи викриття конфіденційної інформації [2].

Установка перешкоди – метод фізичного перешкоджання шляху зловмиснику до інформації, що захищається, у тому числі спроб з використанням технічних засобів знімання інформації і дії на неї.

Маскування – метод захисту інформації з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації.

Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

- ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);
- автентифікацію (встановлення автентичності) об'єкту або суб'єкта після пред'явленого їм ідентифікатору;
- перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);
- дозвіл і створення умов роботи в межах встановленого регламенту;
- реєстрацію (протоколювання) звернень до ресурсів, що захищаються;
- реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Проте, застосування всіх відомих методів захисту даних інформаційної системи не гарантує збереження цілісності даних, тому розробка нових підходів залишається актуальною задачею.

Одним із шляхів розв'язку цього завдання є застосування нечіткої логіки до побудови системи захисту інформації.

Нечітка система вибору алгоритму захисту інформації

Для здійснення захисту інформації в телемедицині необхідно визначити рівень доступу поточного клієнта до інформаційної системи. Крім того, варто враховувати ризик виникнення атаки через поточний канал передачі інформації, який може визначатися співвідношенням кількості звернень даного клієнта до кількості збоїв під час передачі даних через його канал.

На даний час відомі симетричні та асиметричні криптоалгоритми. Найпоширеніші серед них – симетричний DES, асиметричний RSA на основі еліптичних кривих [5].

Загальна схема вибору алгоритму захисту інформації зображена на рисунку 1. В даному випадку в якості критеріїв вибору виступають рівень доступу клієнта до інформації (*access*) та ризик виникнення атаки при передачі інформації поточному клієнту (*risk*), а підсистемою вибору є система обробки нечіткої інформації на основі механізму Мамдані. Виходом такої системи є один з криптоалгоритмів, відповідний вхідним критеріям вибору, застосовуючи який, комп'ютерна система забезпечить свою оптимальну роботу.

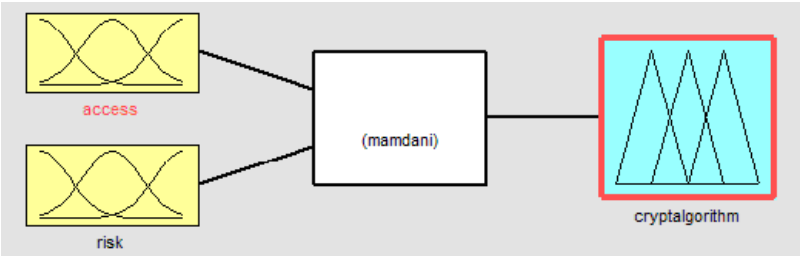

Рис. 1. Загальна схема оптимального вибору методу модулярного експоненціювання для розподілу доступу клієнтів комп'ютерної системи

В інженерних задачах застосовується, як правило, механізм нечіткого висновку Мамдані [6, 7]. В ньому використовується мінімаксна композиція нечітких множин. Даний механізм включає наступну послідовність дій [8]:

1) процедура фазифікації: визначаються степені істинності, тобто значення функцій належності $MF_i(x)$ для лівих частин кожного *i*-го правила (передумов);

2) нечіткий висновок. Спочатку визначаються мінімальний рівень «відсічення» для лівої частини кожного з правил $A_i = \min(MF_i(x))$, а потім знаходяться «усічені» функції належності висновку $B_i = \min(A_i, B_i)$;

3) композиція або об'єднання отриманих «усічених» функцій, для чого використовується максимальна композиція нечітких множин $MF(y) = \max(B_i(y))$;

4) дефазифікація або приведення до чіткості. Існує декілька методів дефазифікації. Наприклад, метод середнього центру або центроїдний метод. Геометричний зміст такого значення – центр ваги для кривої функції належності отриманого виходу.

Застосовуючи засіб *Fuzzy Logic Toolbox* середовища *MathWorks* MATLAB 7.7.0 (R2008b) [9], можна побудувати запропоновану нечітку систему вибору криптоалгоритму.

Значення функцій належності вхідних змінних *access* та *risk* задається трапецевидною функцією, що визначається четвіркою чисел (a,b,c,d), які позначають абсциси вершин трапеції:

$$MF(x) = \begin{cases} \dfrac{b-x}{b-a}, a \le x \le b \\ 1, b \le x \le c \\ \dfrac{x-c}{d-c}, c \le x \le d \\ 0, \text{в інших випадках} \end{cases}.$$

Функція належності виходу *cryptoalgorithm* задається трикутною формою, яка залежить від трьох змінних (a,b,c) (абсциси вершин трикутника) [9]

$$MF(x)=\begin{cases}\dfrac{b-x}{b-a}, a\le x\le b\\ \dfrac{x-c}{c-b}, b\le x\le c\\ 0, \text{в інших випадках}\end{cases},$$

при чому в даному випадку має місце випадок симетричної трикутної функції належності, тобто $(b-a)=(c-b)$.

Функції належності для змінних *access* та *risk*, подані на рисунках 2 та 3, відповідно. Вони поділені на три інтервали кожна для точного опису змінних, зокрема, для опису рівня доступу до інформації застосовується змінна *low*, що позначає низький рівень доступу (може надаватися, наприклад, новим клієнтам), *middle* - середній рівень та *high* - високий рівень доступу (може надаватися адміністратору інформаційної системи).

Для задання рівня ризику виникнення атаки пропонуються змінні *low*, *middle* та *high*, що відповідають низькому, середньому та високому рівню.

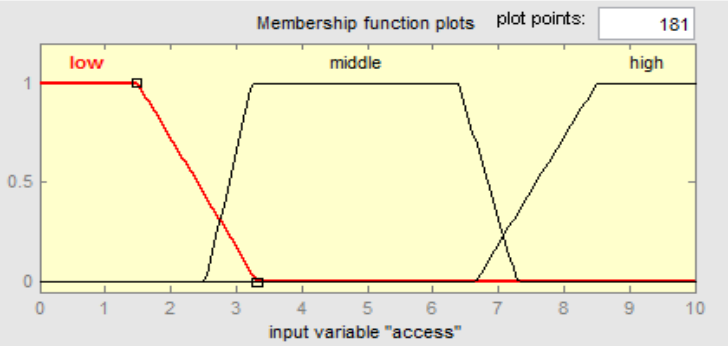

Рис. 2. Функції належності змінної *access*

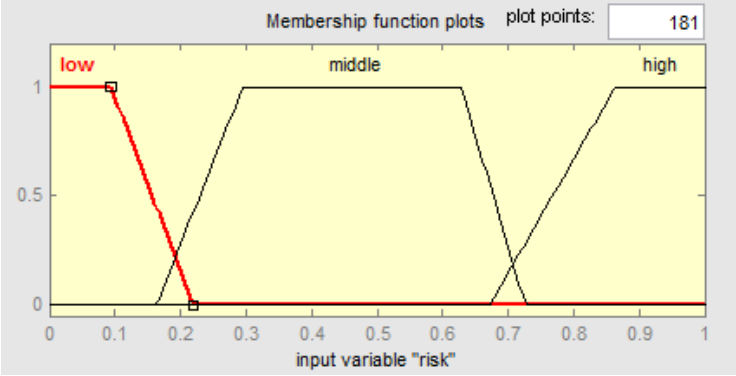

Рис. 3. Функції належності змінної *risk*

Функції належності для вихідної змінної *cryptoalgorithm* зображено на рисунку 4. Вони позначаються однаковими інтервалами на осі ординат для точного визначення центру ваги, що позначає нечіткий висновок системи. *None* позначає відсутність необхідності застосування алгоритму захисту інформації (наприклад, у випадку, коли до інформаційної системи звертається адміністратор), *DES*, *RSA* та *EC* – криптоалгоритм DES, RSA та на основі еліптичних кривих, відповідно. Кожен з цих алгоритмів має свої переваги і недоліки, свій рівень стійкості та продуктивності, які описані в [5].

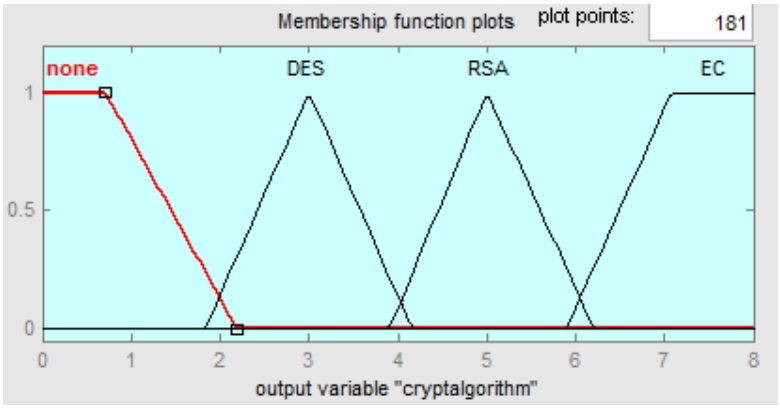

Рис. 4. Функції належності змінної *method*

База знань для побудови даної нечіткої моделі складається з правил типу «якщо — то» [9], усі вхідні змінні мають по три нечітких стани і ще один стан, коли значення вхідної змінної не задане системою. Випадок, коли значення усіх вхідних змінних не задані, на практиці неможливий, тому кількість правил нечіткого висновку досліджуваної системи $N = 4 \times 4 - 1 = 15$. База правил розробленої нечіткої системи має вигляд, зображений на рисунку 5 і задається наступним чином:

1) **IF** (access is low) **AND** (risk is low) **THEN** (cryptalgorithm is RSA)
2) **IF** (access is low) **AND** (risk is middle) **THEN** (cryptalgorithm is RSA)
3) **IF** (access is low) **AND** (risk is high) **THEN** (cryptalgorithm is EC)
4) **IF** (access is low) **THEN** (cryptalgorithm is EC)
5) **IF** (access is middle) **AND** (risk is low) **THEN** (cryptalgorithm is DES)
6) **IF** (access is middle) **AND** (risk is middle) **THEN** (cryptalgorithm is DES)
7) **IF** (access is middle) **AND** (risk is high) **THEN** (cryptalgorithm is EC)
8) **IF** (access is middle) **THEN** (cryptalgorithm is RSA)
9) **IF** (access is high) **AND** (risk is low) **THEN** (cryptalgorithm is none)
10) **IF** (access is high) **AND** (risk is middle) **THEN** (cryptalgorithm is DES)
11) **IF** (access is high) **AND** (risk is high) **THEN** (cryptalgorithm is EC)
12) **IF** (access is high) **THEN** (cryptalgorithm is none)
13) **IF** (risk is low) **THEN** (cryptalgorithm is DES)
14) **IF** (risk is middle) **THEN** (cryptalgorithm is RSA)
15) **IF** (risk is high) **THEN** (cryptalgorithm is EC)

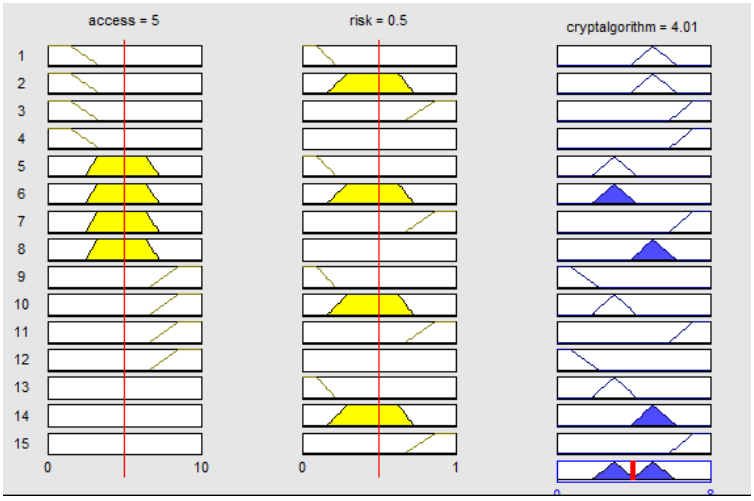

Рис. 5. База правил нечіткої системи вибору криптоалгоритму

Поверхня значень розробленої нечіткої системи вибору алгоритму захисту інформації в телемедицині зображена на рисунку 6.

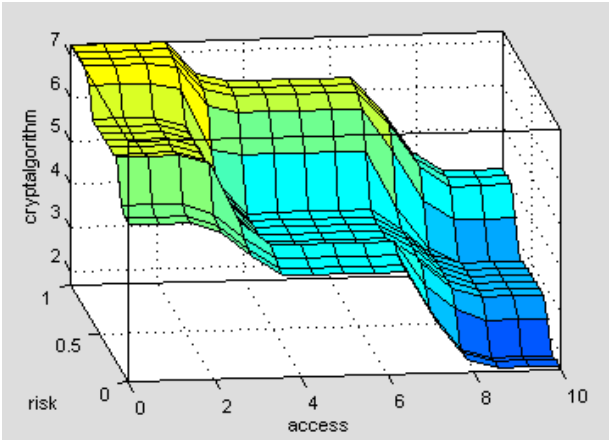

Рис. 6. Поверхня значень нечіткої системи вибору криптоалгоритму

Дослідження бази правил (див. рис. 5) та поверхні значень (див. рис. 6) запропонованої нечіткої системи показали правильність її роботи.

Висновок

В даній статті запропоновано систему захисту інформації в телемедичній системі, яка базується на нечіткому висновку Мамдані. Розроблена нечітка система дозволяє застосувати оптимальний для кожного клієнта криптоалгоритм в реальному часі, що забезпечить найкращу роботу всієї інформаційної системи в цілому.

Список літератури

1. Владзимирский, А.В. Телемедицина [Текст] : [монография] / А.В. Владзимирский. — Донецк : НОУЛИДЖ, 2011. — 436 с.
2. Лукацкий, А. Атаки на информационные системы. Типы и объекты воздействия / А.Лукацкий // Электроника: Наука, Технология, Бизнес. — 2000. — № 1. — С. 16–21.

3. Васильцов, І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними [Текст]: монографія / І.В. Васильцов. — Кременець : Вид. центр КОГРІ, 2009. — 264 с.
4. Дубчак, Л.О. Атаки на сучасні інформаційні системи та методи захисту проти них / Л.О. Дубчак // Materiály IX mezinárodní vědecko-praktická konference «Vědecký pokrok na přelomu tysyachalety – 2013». — Praha Publishing House «Education and Science» s.r.o, 2013. — PP. 3–5.
5. Романец, Ю.В. Защита информации в компьютерных системах и сетях : 2 изд., перераб. и доп. / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин ; ред. В.Ф. Шаньгин. — Москва : Радио и связь, 2001. — 376 с.
6. Ross, T.J. Fuzzy Logic with Engineering Applications / T.J. Ross. — New York : McGraw-Hill, 1995. — 600 p.
7. Штовба, С.Д. Введение в теорию нечетких множеств и нечеткую логику / С.Д. Штовба. — Винница : Изд-во ВГТУ, 2001. — 198 с.
8. Бережная, М.А. Методы проектирования нечетких устройств принятия решений на основе программируемых логических интегральных микросхемах. / М.А. Бережная // Технология приборостроения. — 2009. — № 2. — С. 16–23.
9. Лазарєв, Ю.Ф. Моделювання динамічних систем у Matlab. Електронний навчальний посібник / Ю.Ф. Лазарєв — К.: НТУУ «КПІ», 2011. — 421 с.

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕМЕДИЦИНСКИХ СИСТЕМАХ НА ОСНОВЕ НЕЧЁТКОЙ ЛОГИКИ

Л.О. Дубчак

Тернопольский национальный экономический университет,
ул. Львовская, 11, 46020, Тернополь, e-mail: dlo@tneu.edu.ua

В статье рассмотрен метод защиты информации, передаваемой в телемедицинских сетях, путем выбора алгоритма шифрования данных на основе нечёткой логики. Построенная нечёткая система позволяет осуществлять адекватную защиту данных в реальном времени, учитывая текущее состояние самой компьютерной системы.
Ключевые слова: нечёткая система, телемедицина, защита информации, DES, RSA, криптоалгоритм на основе эллиптических кривых

INFORMATION SECURITY IN TELEMEDICINE SYSTEMS BASED ON FUZZY LOGIC

Lesya O. Dubchak

Ternopil National Economical University,
11 Lvivska str., 46020, Ternopil, e-mail: dlo@tneu.edu.ua

In this article the method of protecting information, transmitted in telemedicine networks, by selecting encryption algorithm based on fuzzy logic had been proposed. Proposed fuzzy system allows for adequate protection of data in real time, considering the current state of the computer system.
Keywords: fuzzy systems, telemedicine, information security, DES, RSA, crypto algorithm based on elliptic curves