https://doi.org/10.31891/2219-9365-2024-77-23
УДК: 004.7:519.87

РОМАНЕЦЬ Ігор
Західноукраїнський національний університет
https://orcid.org/0000-0002-7061-6527
e-mail: i.romanets@wunu.edu.ua

ЗАХИСТ ВІД ТЕРМІНАЦІЇ ТРАФІКУ В IP-МЕРЕЖІ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Технологія голосового Інтернет-протоколу (VoIP) широко впроваджується, оскільки інтеграція голосу та даних у мережі зменшує зусилля та витрати на управління. Оскільки VoIP використовує ту ж саму інфраструктуру, що й традиційні мережі даних, він успадковує всі проблеми з безпекою від них. Більше того, VoIP має свої власні проблеми з безпекою, пов'язані з новими протоколами та компонентами мережі. Ця стаття акцентує увагу на конкретних загрозах безпеці VoIP та заходах захисту для їх мінімізації.

Ключові слова: VoIP, Asterisk, DDoS, TCP/IP, нечітка база знань, нечітка система, нечітка логіка.

ROMANETS Ihor
West Ukrainian National University

PROTECTION FROM TRAFFIC TERMINATION IN IP NETWORK BASED ON FUZZY LOGIC

Voice over Internet Protocol (VoIP) has been widely deployed since the integration of the voice and data networks reduces management effort and cost. Since VoIP share the same infrastructure with traditional data network, it inherits all security problems from data network. Furthermore, VoIP also has its own security problems coming from new protocols and network component. This article focuses on these VoIP specific security threats and the countermeasures to mitigate the problem.

Keywords: VoIP, Asterisk, DDoS, TCP/IP, fuzzy knowledge base, fuzzy system, fuzzy logic.

Постановка проблеми у загальному вигляді та її зв’язок із важливими науковими чи практичними завданнями

Враховуючи бурхливий розвиток інформаційних технологій, одним із ключових питань є кібербезпека [18-21]. Одним із вразливих сегментів із точки зору безпеки є телефонія, а саме VoIP – технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP [1].

На сьогодні IP-телефонія дає змогу використовувати будь-яку IP-мережу, у режимі реального часу, забезпечує зручність, надійність та невисоку вартість порівняно з аналоговим зв’язком.

Однак із швидкими темпами розвитку IP-телефонії паралельно й розвивалися різні сервісу для її використання. Одним із таких сервісів є заробляння грошей, тобто дзвінки на платні номери. Такі сервіси створюють шахраї переважно у країнах «третього світу» де практично закони не діють.

Завдяки цьому поширився вид шахрайства, що має назву трафік за чужий рахунок або термінація трафіка. Термінація трафіка – це встановлення, підтримка фізичного та/або логічного з'єднання, пропуск трафіка між телекомунікаційною мережею, з якої надходить виклик або ініціюється з'єднання, та кінцевим обладнанням, до якого спрямовується виклик або ініціюється з'єднання [2].

В більшості випадків адміністратори системи стараються захисти систему від фізичного проникнення на сервер, тому всі зусилля та програмні засоби направляють для захисту таких сервісів як Open SSH server, поштовий сервіс, від DDoS-атак і т.д. Тому мало хто уваги звертає на інші сервіси які можуть знаходитись на серверах [3].

На відміну від інших сервісів для взлому сервісу SIP не потрібно фізичного проникнення на сервер [9].

Оскільки при розподілі доступу клієнтів необхідно врахувати поточні параметри системи, такі як рівень доступу клієнта, тобто перелік прав клієнта залежно від його IP-адреси, якість зв’язку мережі клієнта, час здійснення дзвінка клієнтом та відповідний часовий пояс адресата, то для вирішення цієї задачі варто застосувати апарат нечіткої логіки [12-17].

Математична теорія нечітких множин (fuzzy sets) і нечітка логіка (fuzzy logic) є узагальненнями класичної теорії множин і класичної формальної логіки. Дані поняття були вперше запропоновані американським ученим Лотфі Заде (Lotfi Zadeh) у 1965 р. [12]. 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: [12, 14]

- 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.

Аналізуючи літературу щодо термінації трафіку слід сказати, що даною проблематикою мало хто із науковців займався. У статті Г.В. Куцо та С.В. Юлова містяться базові відомості щодо організації системи рефайлінгу (термінації VoIP трафіку), розглянуто необхідне для цього апаратне та програмне забезпечення. Стисло розглянуто загальновживане програмне забезпечення, яке використовується для організації рефайлінгу. Вказане програмне забезпечення та наведена інструкція до його використання для уникнення блокування обладнання з боку операторів стільникового зв'язку.[22]

Але в статті не описано методів як запобігти термінації VoIP трафіку

Пропонований метод захисту системи ip-телефонії від термінації трафіку

Автором розроблено метод захисту системи IP-телефонії від не санкціонованого доступу та дзвінків на платні сервіси.

Найчастіше зловмисники при спробі проникнення на сервер IP-телефонії використовують стандартні логіни, що прописані у Dialplan та пробують метод підбору паролів Brute force [4]. Для того щоб виявити зловмисника спостерігаємо за log.file на сервері Asterisk [5]. Так як записів у файлі може бути досить багато тому доцільно автоматизувати цей процес за допомогою програми Fail2ban [7].

Запропонований метод можна описати сукупністю наступних кроків:

Встановлюємо Fail2ban на сервер шляхом програми Fail2ban виконуємо наступні команди:

sudo apt-get update

sudo apt-get install fail2ban

Для того, щоб встановлена програма працювала належним чином необхідно внести деякі правки у файл конфігурації. По замовчуванні це є /etc/fail2ban/jail.conf.

Але розробники не рекомендують редагувати його напряму для того щоб запобігти збою сервера, тому необхідно створити локальну копію даного файлу командою:

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Тепер потрібно виконувати редагування тільки /etc/fail2ban/jail.local. Він буде підключений системою автоматично та має вищий пріоритет при виконанні.

Відкриваємо файл jail.local для редагування:

sudo vi /etc/fail2ban/jail.local

При цьому потрібно звернути увагу на секцію [DEFAULT].

В ній знаходяться основні правила, що задані по замовчуванні для Fail2ban.

ignoreip – значення цього параметру говорять, які IP-адреси блокуватися не будуть. Якщо ми хочемо щоб Fail2ban ігнорував при перевірці декілька IP-адрес, то їх необхідно вказати в параметрі ignoreip через пробіл.

bantime – даний параметр означає час в секундах, протягом якого підозрілий IP-адрес буде заблокований. По замовчуванні це 10 хв.

findtime – визначає проміжок часу в секундах, протягом якого програма буде визначати наявність підозрілої активності.

maxretry – допустиме число не вдалих спроб отримання доступу до сервера. При перевищені вказаного значення IP-адреса блокується.

На Рис. 1. показано зміни у файлі, а саме змінені параметри *ignoreip=127.0.0.1/8*, це означає пропускати всі IP адреси із локальної мережі; *bantime=600*, тобто блокування користувача буде тільки 10 хв.; *findtime=600*, система буде визначати підозрілу активність 10 хв.; *maxretry=5*, кількість невдалих спроб доступу до сервера.

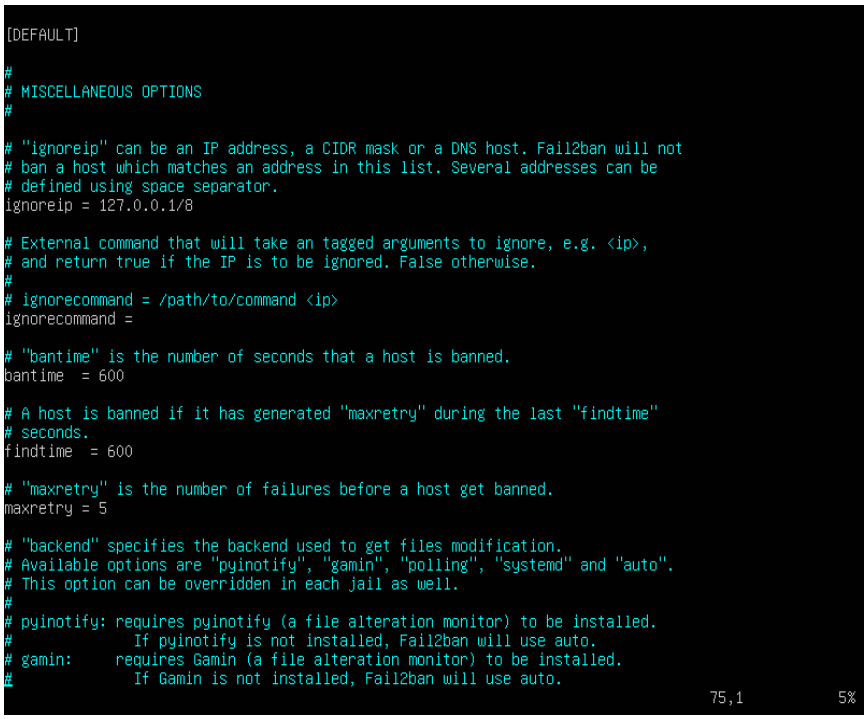

Рис.1. Вигляд файлу jail.local після редагування

Після редагування jail.local обов'язково потрібно перезапустити Fail2ban командами
sudo service fail2ban restart
tail /var/log/fail2ban.log
Тепер перейдемо до налаштування Fail2ban в Asterisk.
Відкриваємо конфігураційний файл Asterisk, який відповідає за логування подій в /var/log/asterisk/messages:
sudo vi /etc/asterisk/logger.conf
Додаємо security в messages:
messages =>notice,warning,error,security
Перезапустим систему логування asterisk:
sudo asterisk –rvv
logger reload
quit

Рис. 2. Вигляд консолі після перезапуску logger

На Рис. 2 показано виконання команд перезапуску Asterisk.
Додаємо файл налаштувань Asterisk в директорію с конфігурацією Fail2Ban тим самим активувавши спостереження його логів:
sudo vi /etc/fail2ban/jail.d/asterisk.conf ,
де 86400 в секундах = 24 години, тобто зловмисник буде заблокований на добу.
На Рис. 3 показано виконання команди bantime, де вона блокує зловмисника на 24 год.

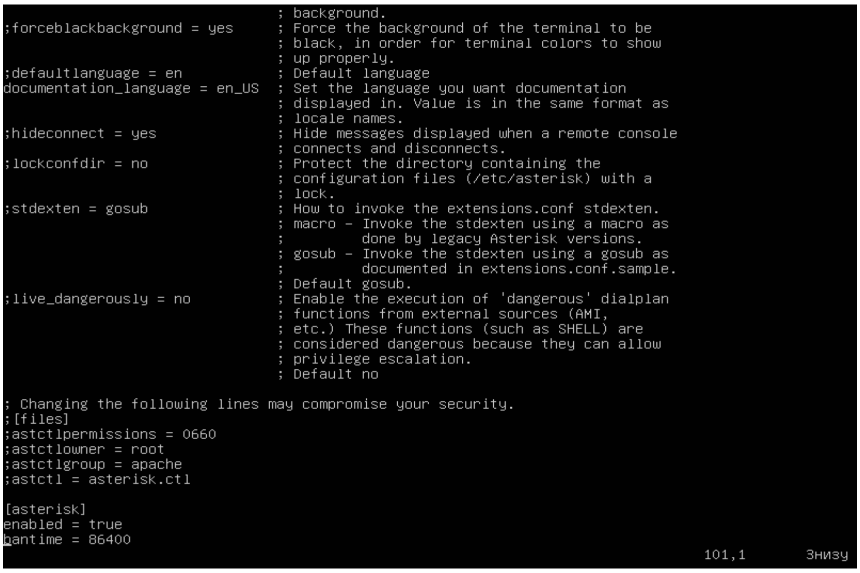

Рис. 3. Вигляд зміненого файлу asterisk.conf

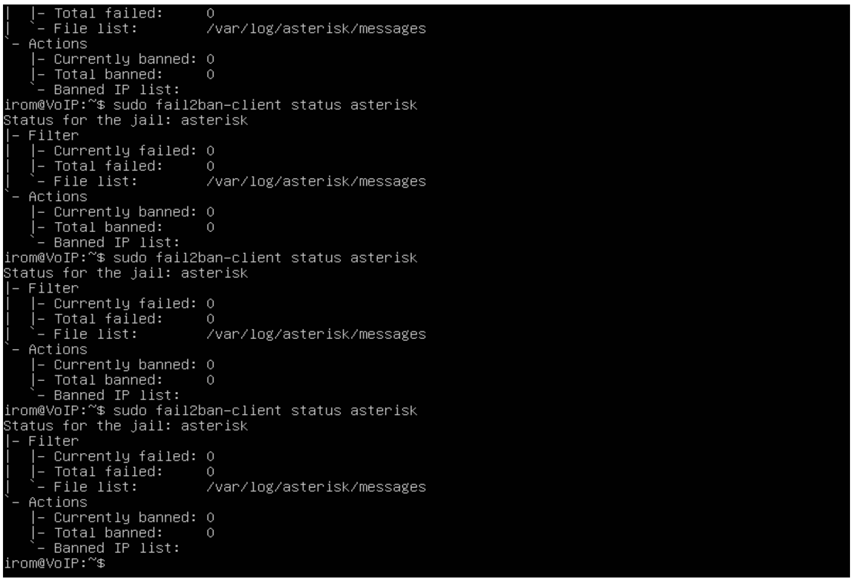

Рис. 4. Вигляд консолі після перевірки статусу

[asterisk]
enabled = true
bantime = 86400
Перезапустим fail2ban для завантаження нового файлу налаштувань:
sudo fail2ban-client reload
Перевірим:
sudo fail2ban-client status asterisk

На Рис. 4 показано виконання команди яка виводить на консоль, де вказано, що Currently banned=0, Total banned=0 та Banned IP list – пустий.

В результаті Fail2Ban буде блокувати IP-адреса з яких не вірно вводяться паролі до екаунтів Asterisk.

Запропонований метод демонструє як можна убезпечити свою систему від зловмисників. Однак коли спроб атак на певну систему буде багато, то також буде назбируватись велике накопичення IP-адрес які будуть записуватись у лог файлі. Тому застосування розробленого методу захисту є актуальним але при великій кількості атак мало ефективним, так як адміністратору буде дуже багато рутинної роботи із визначення IP адрес зловмисників.

НЕЧІТКА СИСТЕМА РОЗПОДІЛУ ДОСТУПУ В СИСТЕМІ IP-ТЕЛЕФОНІЇ

Концепція побудови нечіткої системи розподілу доступу в IP-телефонії

Розподіл доступу на основі нечіткої логіки є основою системи захисту IP-телефонії. На його вхід поступають критерії здійсненого дзвінка, які опрацьовуються підсистемою розподілу доступу на основі механізму нечіткого висновку Мамдані [11-13].

Застосовуючи засіб Fuzzy Logic Toolbox середовища MATLAB, можна побудувати нечітку систему розподілу доступу (*access*) залежно від значень рівня довіри клієнта, по його IP-адресі (*IP-identification*), часу здійснення дзвінка клієнтом (*client-call-time*), часового пояс адресата дзвінка (*addr-call-time*) та якості зв'язку мережі клієнта (*connection-quality*). Загальний вигляд запропонованої нечіткої системи подано на рисунку 5.

Значення функцій належності вхідних змінних задається дзвоноподібною, а вихідної змінної – трапецевидною функцією [11].

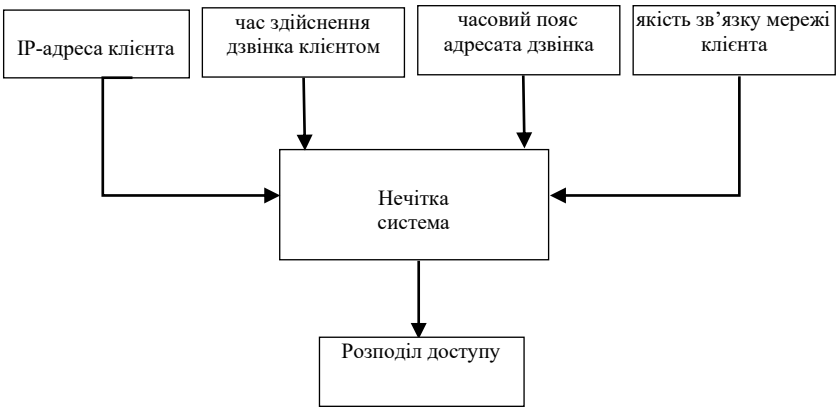

Рис. 5. Загальна схема нечіткої системи розподілу доступу в IP-телефонії

Функції належності вхідної змінної IP-identification відображаються трьома множинами: low, middle, high, що відображають відповідно низький, середній та високий рівень довіри клієнта IP-телефонії. Цей показник легко можна сформувати зі статистичних даних IP-адреси клієнта, його присутності в IP-телефонії, здійснених атак чи наявності збоїв при здійсненні дзвінків та правах доступу, надані йому адміністратором мережі.

Функції належності змінної connection-quality, що відображає якість зв'язку мережі, з якої здійснює запит до IP-телефонії на дзвінок клієнт, аналогічно поділені на три інтервали low, middle, high. Низька якість зв'язку може бути у мобільних мережах через різницю у покритті та якості надання послуг мобільними операторами. Середня якість зв'язку, як правило, можлива при застосуванні користувачем регіональної мережі Інтернет, а висока якість забезпечується використанням клієнтом локальної мережі.

Для задання функцій належності змінної client-call-time, що показує час здійснення дзвінка клієнтом. Логічно, що дана змінна задається в інтервалі [0, 24], який поділений на три відрізки morning, work time, night.

Змінна addr-call-time відображає часові пояси світу, які поділені на три зони (I-timezone, II-timezone, III-timezone), які подані на інтервалі [-12, 12] та враховуються при побудові бази правил відносно часу здійснення дзвінка клієнта.[23]

Функції належності для вихідної змінної access позначаються двома трапецевидними інтервалами deny, allow для точного визначення центру ваги, що позначає нечіткий висновок системи.

База знань для побудови даної нечіткої моделі складається з правил типу «якщо - то» [12], усі вхідні змінні мають по три нечітких стани і ще один стан none, 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 4•4•4•4-1=255.

Реалізація системи

Нечіткий висновок моделі розподілу доступу, побудованого на основі заданих 255 правил з поточними значеннями вхідних та вихідної змінних, має вигляд, фрагмент якого представлений на рисунку 6

ISSN 2219-9365

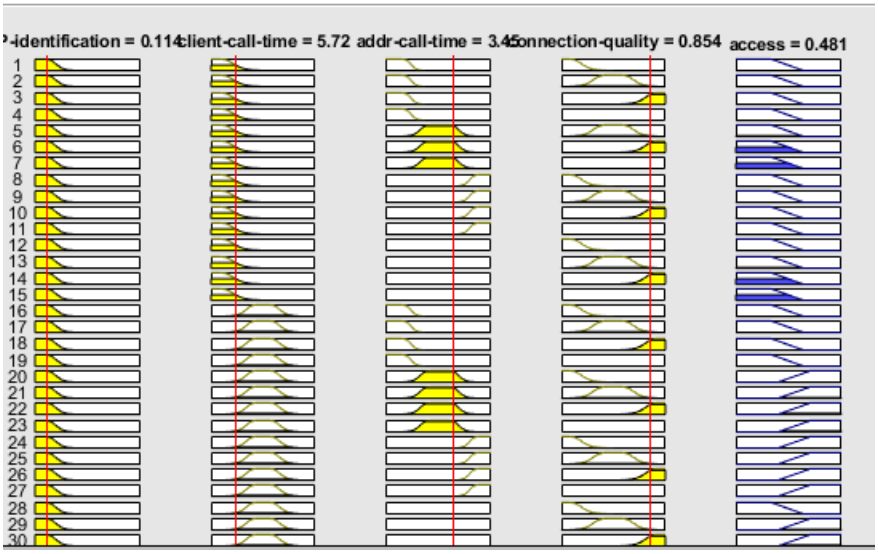

Рис. 6. Нечіткий висновок моделі розподілу доступу в IP-телефонії

На рисунку 6 зображено випадок, коли клієнт, рівень довіри якого низький, здійснює дзвінок у ранковий час в країну, яка має той самий часовий пояс, що і Україна і якість зв'язку свідчить, що дзвінок здійснюється з локальної мережі. Висновок запропонованої нечіткої системи в даному випадку становить 0.48, що відповідає дозволу на здійснення даного дзвінка. Перевірка інших комбінацій значень вхідних змінних підтверджує правильність роботи такої нечіткої системи.

Запропонована нечітка система може реалізовуватися як програмно, так і апаратно у вигляді нечіткого контролера для успішного захисту від термі нації трафіку.

Нечіткий контролер змодельований у середовищі Simulink має загальний вигляд, поданий на рисунку 7.

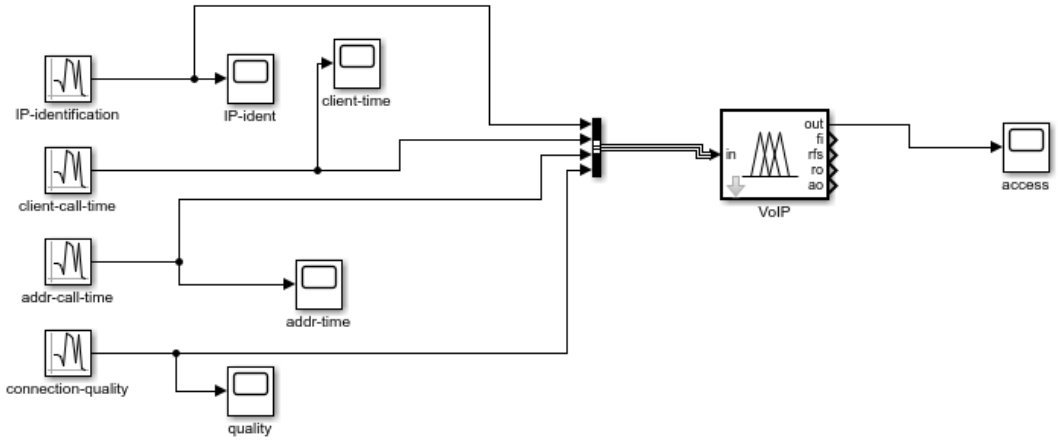

Рис. 7. Нечіткий контролер розподілу доступу в IP-телефонії

Значення вхідних змінних, описаних вище, задаються випадковим чином, що зображено на рисунку 8.

ISSN 2219-9365

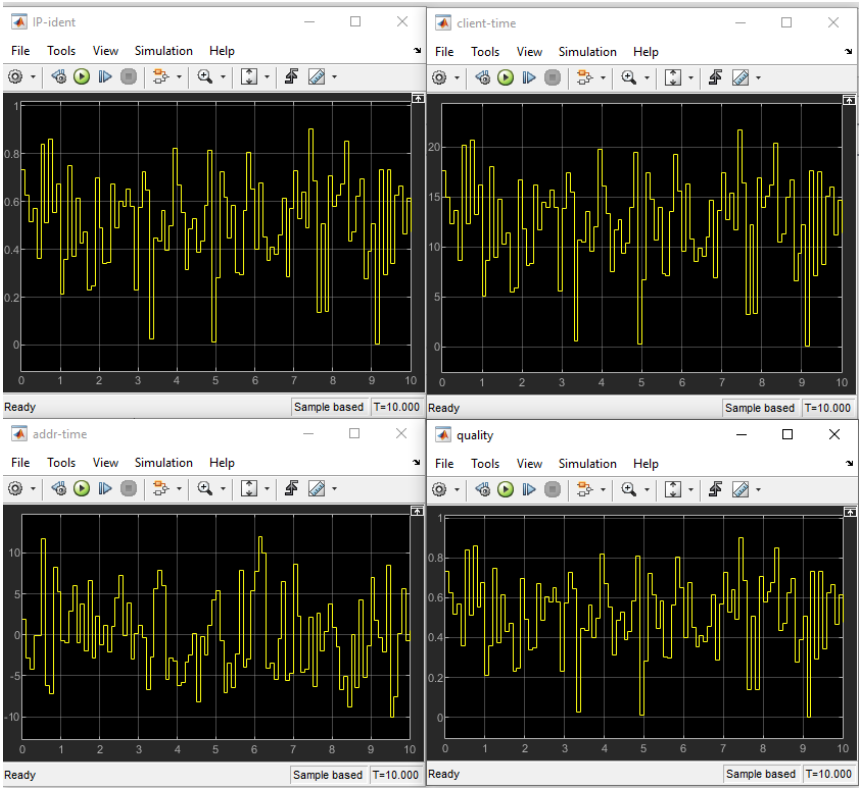

Рис. 8. Значення вхідних змінних нечіткого контролера

Значення вихідної змінної змодельованого нечіткого контролера, що інтерпретує рівень доступу клієнта, подано на рисунку 9.

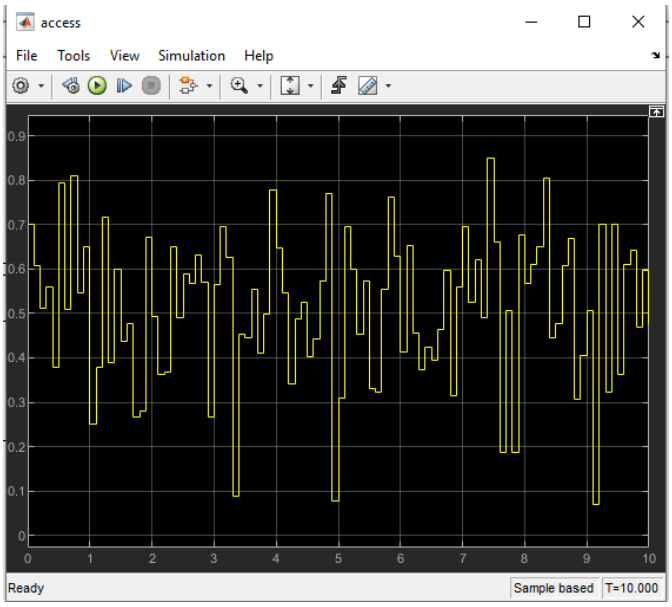

Рис. 9.Значення вихідної змінної нечіткого контролера

Симуляція роботи запропонованого нечіткого контролера підтверджує правильність його роботи, тому можна стверджувати про можливість подальшої реалізації такого апаратного засобу на основі нечіткої логіки для здійснення розподілу доступу в IP-телефонії.

Висновки та перспективи подальшого розвитку у даному напрямі

Незважаючи на сучасний прогрес у більшості сфер використання комп'ютерних мереж та відповідного програмного забезпечення, розробка нових підходів до захисту трафіку в IP-мережі є дуже перспективним напрямом науково-практичних досліджень.

В рамках даної роботи запропоновано метод, який базується розподілі доступу з використанням нечіткої логіки. Описано особливості функціонування системи захисту IP-телефонії із використанням запропонованого методу, зокрема, врахування параметрів здійсненого дзвінка, які опрацьовуються підсистемою розподілу доступу на основі механізму нечіткого висновку Мамдані.

Проведено ряд експериментальних досліджень, здійснено оцінку ефективності запропонованих підходів з використанням змодельованого нечіткого контролера у середовищі Simulink.

У подальших дослідженнях планується розробка та реалізація нових алгоритмів захисту трафіку в IP-мережі, які здатні адаптуватися до змінних умов і змінювати параметри захисту на основі навчання та досвіду.

References

1. Voice over IP. [Online]. Available: https://en.wikipedia.org/wiki/Voice_over_IP
2. OECD (2014), "International Traffic Termination", OECD Digital Economy Papers, No. 238, OECD Publishing. DOI:10.1787/5jz2m5mnlvkc-en
3. “What is a DDoS attack?” https://www.digitalattackmap.com/understanding-ddos/
4. K. Apostol, Brute-force Attack, SaluPress, 2012.
5. Asterisk [Online]. Available: https://uk.wikipedia.org/wiki/Asterisk.
6. J. Van Meggelen, L. Madsen, and J. Smith, Asterisk: The Future of Telephony, Second Edition, O’Reilly Media Inc., 2007.
7. Fail2ban, [Online]. Available: https://www.fail2ban.org
8. Dialplan, [Online]. Available: https://wiki.asterisk.org/wiki/display/AST/Dialplan
9. D. Sisalem at al., SIP Security, John Wiley & Sons, Ltd., 2009.
10. Installation of Debian, [Online]. Available: http://www.asteriskguru.com/tutorials/asterisk_installation_compilation_debian.html
11. M.S. Abadeh, J. Habibi, C. Lucas, “Intrusion detection using a fuzzy genetics-based learning algorithm,” Journal of Network and Computer Applications, no. 30, pp. 414-428, 2007.
12. T.J. Ross, Fuzzy Logic with Engineering Applications, McGraw-Hill Inc., USA, 1995.
13. L. Dubchak, N. Vasylkiv, V. Kochan, A. Lyapandra, “Fuzzy data processing method,” Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS’2013), September 12-14, 2013, Berlin, Germany, Vol. 1, pp. 373-375.
14. S. Shtovba, Introduction to the Theory of Fuzzy Sets and Fuzzy Logic, [Online]. Available: http://matlab.exponenta.ru/fuzzylogic/book1/
15. V.S. Mikhaylenko, V.V. Nikolsky, “Use of Fuzzy Adaptive Control System for Computer Monitoring of Boiler Network Network,” Automation, Electrotechnical Complexes and Systems, [Online]. Available: http://aaecs.org/mihailenko-vs-nikolskii-vv-ispolzovanie-nechetkoi-adaptivnoi-sistemi-upravleniya-dlya-kompyuternogo-monitoringa-setyu-kotelnih-ustanovok.html
16. L.A.Zadeh, “Fuzzy logic – a personal perspective,” Fuzzy Sets and Systems, vol. 281, pp. 4-20, 2015
17. M.Komar, V.Kochan, L.Dubchak, A.Sachenko, V.Golovko, S.Bezobrazov, I.Romanets, “High performance adaptive system for cyberattacks detection,” Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS’2017), September 21-23, 2017, Bucharest, Romania, Vol. 2, pp. 853-858.
18. Balyk, M. Karpinski, A. Naglik, G. Shangytbayeva, and I. Romanets, “Using graphic network simulator 3 for DDoS attacks simulation,” International Journal of Computing, vol. 16, issue 4, pp. 219-225, 2017.
19. M. Komar, V. Golovko, A. Sachenko, and S. Bezobrazov, “Development of neural network immune detectors for computer attacks recognition and classification,” Proceedings of the IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS’2013), September 12-14, 2013, Berlin, Germany, Vol. 2, pp. 665-668.
20. V. Golovko, M. Komar, & A. Sachenko, “Principles of neural network artificial immune system design to detect attacks on computers,” Proceeding of the 2010 IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET’2010), February 2010, pp. 237-237.
21. Sergii Lysenko,Oleg Savenko, Kira Bobrovnikova, Andrii Kryshchuk. Self-adaptive System for the Corporate Area Network Resilience in the Presence of Botnet Cyberattacks, International Conference on Computer Networks, Springer CN 2018: Computer Networks pp 385-401.
22. Криміналістика і судова експертиза: міжвідом. наук. -метод. зб. / Київський НДІ судових експертиз; Куцо Г. В., Юлов С. О. Дослідження телекомунікаційного обладнання термінації VoIP трафіку (рефайлінгу), побудованого на базі модемів HUAWEI. Київ, 2017- С. 344-352. Вип. 62. – 1072 с
23. I. Romanets, A. Sachenko and L. Dubchak, "Method of Protection Against Traffic Termination in VoIP," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2018, pp. 1-5, doi: 10.1109/ECAI.2018.8678992.