

ЗАСТОСУВАННЯ НЕЧІТКОЇ ЛОГІКИ У СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

Анотація

Робота присвячена дослідженню застосування нечіткої логіки у системах виявлення вторгнень в Інтернеті речей. Розглядаються основні проблеми безпеки IoT-систем, а також переваги використання нечіткої логіки для забезпечення безпеки таких мереж.

Ключові слова: Інтернет речей, безпека, нечіткий контролер.

Abstract

The paper is dedicated to the study of the application of fuzzy logic in intrusion detection systems for the Internet of Things. It discusses the main security issues of IoT systems, as well as the advantages of using fuzzy logic to ensure the security of such networks.

Keywords: Internet of things, security, fuzzy controller.

Вступ

З розвитком Інтернету речей (IoT) зростає кількість пристроїв, які з'єднуються між собою і обмінюються даними через Інтернет. Це забезпечує нові можливості для автоматизації процесів, зручності користування та ефективності, проте водночас створює суттєві ризики для безпеки. У зв'язку з цим виявлення вторгнень у такі системи стає однією з найбільш актуальних проблем, адже традиційні методи захисту, які використовуються для комп'ютерних мереж, не завжди ефективні в умовах IoT.

Одним з перспективних підходів для вирішення цієї проблеми є застосування нечіткої логіки. Нечітка логіка дозволяє обробляти дані, що містять невизначеність та неповноту, а також адаптувати системи до змінних умов. Вона є корисним інструментом для виявлення аномальних поведінкових патернів і потенційних атак в реальному часі, навіть у тих випадках, коли повна точність інформації недоступна.

Результати дослідження

Нечітка логіка (fuzzy logic) — це розширення класичної бінарної логіки, яка дозволяє опрацьовувати дані, що не є строго визначеними або чіткими. Вона використовується для моделювання процесів прийняття рішень, коли є невизначеність або нечіткість у вхідних даних. Нечітка логіка дає змогу працювати з інтуїтивними поняттями, такими як "підвищений ризик", "помірний потік даних" або "нормальна активність", що часто зустрічаються в реальних системах.

У зв'язку з величезною кількістю пристроїв IoT, їх різноманітністю та обмеженими ресурсами, IoT мережі піддаються численним загрозам та атакам. Тому безпека в IoT є однією з найбільших проблем, адже масштаб і різноманітність пристроїв створюють численні вразливості, які можуть бути використані зловмисниками [1]. До основних проблем безпеки належать: обмежені ресурси пристроїв, необхідність у безперервному з'єднанні з мережею, гомогенність і незахищеність програмного забезпечення, проблеми аутентифікації та управління доступом, масштабованість атак, недостатність стандартів безпеки, вразливість через сторонні сервіси.

Нечіткий контролер для системи виявлення вторгнень в IoT може бути розроблений для покращення точності та адаптивності виявлення аномалій в умовах швидко змінюваних даних, що надходять від сенсорних пристроїв. Він може працювати з нечіткими наборами правил, які дозволяють більш гнучко реагувати на різні типи атак, знижуючи ймовірність помилкових спрацьовувань і забезпечуючи більшу точність виявлення [2].

Розглянемо конкретний приклад застосування нечіткої логіки для виявлення вторгнень у мережі IoT. Уявімо систему смарт-будинку, де є кілька типів пристроїв: камери спостереження, термостати,

датчики руху і дверні замки. Кожен з цих пристроїв генерує дані про активність. Якщо система спостерігає за змінами у цих параметрах, вона може використовувати нечітку логіку для виявлення вторгнення. Система виявлення вторгнень отримуватиме дані з різних сенсорів IoT, що можуть бути пов'язані з мережею, пристроями, або фізичними характеристиками (температура, вологість, використання ресурсів тощо). Вхідні дані можуть включати: трафік мережі (наприклад, кількість запитів, частота підключень), поведінку пристроїв (споживання енергії, зміни в поведінці пристроїв), системні події або повідомлення з датчиків (підключення/відключення пристроїв), аномалії в трафіку або системах обміну даними.

Результат роботи нечіткого контролера може бути виражений у вигляді нечіткої міри ймовірності, що певне вторгнення відбулося. Визначення ймовірності вторгнення проводиться на основі отриманих значень вхідних даних:

- Висока ймовірність атаки: Якщо значення виходять за межі визначених порогів, контролер може активувати механізми захисту, такі як блокування пристроїв або мережевих портів.

- Низька ймовірність атаки: Якщо всі вхідні дані в межах нормального діапазону, контролер не буде вживати ніяких дій, але може зафіксувати події для подальшого аналізу.

Система може бути інтегрована з іншими елементами інфраструктури IoT для виконання автоматичних дій, таких як інтеграція з брандмауерами для блокування атак; сповіщення адміністратора для мануального втручання; використання інших методів виявлення аномалій, таких як методи машинного навчання чи статистичний аналіз для покращення точності [3].

Перевагами використання нечіткого контролера в системах виявлення вторгнень IoT є:

- Адаптивність: нечітка логіка дозволяє моделювати та адаптувати правила до нових умов без необхідності повного перепроєктування системи.

- Гнучкість: здатність працювати з нечіткими, неточними даними дозволяє ефективно виявляти атаки, які можуть бути складними для детектування в традиційних системах.

- Зниження числа помилкових спрацьовувань: оскільки нечітка логіка дозволяє гнучко інтерпретувати вхідні сигнали, можна зменшити ймовірність помилкових спрацьовувань і точніше виявляти реальні загрози.

Висновки

Нечіткий контролер є потужним інструментом для виявлення вторгнень у системах IoT, оскільки здатний ефективно обробляти неясні або неповні дані, які часто зустрічаються в реальних умовах IoT. Він дозволяє створювати гнучкі, адаптивні системи захисту, що здатні вчасно реагувати на нові загрози, знижуючи ймовірність помилок і підвищуючи точність виявлення аномалій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. M. Almseidin, J. Al-Sawwa, and M. Alkasassbeh, "Anomaly-based Intrusion Detection System Using Fuzzy Logic," *2021 International Conference on Information Technology (ICIT)*. IEEE, pp. 290–295, Jul. 14, 2021. doi: 10.1109/icit52682.2021.9491742.
2. M. Alalhareth and S. C. Hong, "An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning," *Sensors*, vol. 23, no. 22, Jan. 2023, Art. no. 9247, <https://doi.org/10.3390/s23229247>.
3. F. S. Alrayes et al., "Optimal Fuzzy Logic Enabled Intrusion Detection for Secure IoT-Cloud Environment," *Computers, Materials & Continua*, vol. 74, no. 3, pp. 6737–6753, 2023, <https://doi.org/10.32604/cmc.2023.032591>

Семенова Олена Олександрівна – канд. техн. наук, доцент кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: semenova.o.o@vntu.edu.ua

Джус Андрій Васильович — аспірант групи 172-23а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: dzhus1988@gmail.com

Мартинюк Володимир В'ячеславович — аспірант групи 172-22а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: vm4ukr@gmail.com

Semenova Olena O. – Cand. Sc. (Eng), Associate professor at the Department of Infocommunication systems and technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: semenova.o.o@vntu.edu.ua

Dzhus Andrii V. – post-graduate student of 172-23a group, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: dzhus1988@gmail.com

Martyniuk Volodymyr V. – post-graduate student of 172-23a group, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: vm4ukr@gmail.com