Q-Learning-Based Detection of IPv6 Intrusions: A Behavioral and Performance Study

Proceedings - 2025 International Seminar on Application for Technology of Information and Communication: Advancing Electrical Engineering and Informatics Through Quantum Computing and Intelligence Technologies, iSemantic 2025 • Conference Paper • 2025 •
DOI: 10.1109/ISemantic67418.2025.11291642

Daru, April Firman [a] ; Hirzan, Alauddin Maulana [a] ;
Bashi, Zainab Senan Mahmod Attar [b] ; Fanani, Fajriannoor [a]

[a] Universitas Semarang, Faculty of Information Technology and Communication, Semarang, Indonesia

Abstract

Intrusion attacks remain a persistent threat in computer networks, occurring unpredictably across various geographic locations. Among these, IPv6-based flood attacks are particularly concerning due to the expanded address space, which enables the transmission of large packets. This problem can significantly affect local network performance or completely deny service to targeted servers. While numerous studies have proposed intrusion detection systems based on supervised learning models, a critical limitation persists. These models require retraining to recognise new attacks. This time-consuming retraining process may increase vulnerability during adaptation periods, as the networks will be exposed to zero-day attacks until updated training data is available. To address this

limitation, the present study proposes a self-learning model using reinforcement learning techniques, specifically the Q-Learning algorithm, to classify network intrusions based on learned behavioural patterns autonomously. The system improves classification accuracy with each training epoch, enhancing its reliability. Three agents were designed, each employing different exploration-exploitation strategies characterised by epsilon E-0.1, E-0.5, and E-0.9. This study launched different ICMPv6 attacks individually and gathered five million samples for each intrusion attack. The agent with E-0.1 demonstrated superior performance, achieving 198,235 correct classifications with a cumulative reward of 883,835. The agent followed this with E-0.5, which recorded 100,984 correct classifications and a total reward of 87,075. The agent with E-0.9 performed the poorest, with only 20,850 correct classifications and a negative cumulative reward of -714,035. The findings indicate that the proposed self-learning model based on Q-Learning can effectively identify network intrusions without requiring manual retraining, thereby offering a scalable and adaptive solution for real-time intrusion detection.

Author keywords

Classification; Intrusion; Patterns; Q Learning; Reinforcement Learning

Indexed keywords

Engineering controlled terms

Computer crime; Intrusion detection; Learning algorithms; Learning systems; Network intrusion; Reinforcement learning; Self-supervised learning; Supervised learning; Zero-day attack

Engineering uncontrolled terms

Behavioural studies; Geographic location; Intrusion; Network intrusions; Pattern; Performance; Performance study; Q-learning; Reinforcement learnings; Self-learning models

Engineering main heading

Classification (of information)

Funding details

Details about financial support for research, including funding sources and grant numbers as provided in academic publications.

Funding sponsor	Funding number	Acronym
Kulliyyah of Information and Communication Technology		
International Islamic University Malaysia See opportunities by IIUM		IIUM
Faculty of Information and Communication Technology, Universitas Semarang		

Funding text

The authors gratefully acknowledge the sponsorship and support provided through the international collaboration between the Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, and the Faculty of Information and Communication Technology, Universitas Semarang.

Corresponding authors

Corresponding author	A.F. Daru
Affiliation	Universitas Semarang, Faculty of Information Technology and Communication, Semarang, Indonesia
Email address	firman@usm.ac.id

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us

ELSEVIER