# SAIRF: A similarity approach for attack intention recognition using fuzzy min-max neural network

*Abdulghani Ali Ahmed, Mohammed Falah Mohammed*

Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, 26300, Kuantan, Pahang, Malaysia

## Abstract

Sensitive information can be exposed to critical risks when communicated through computer networks. The ability of cybercriminals to hide their intention to attack obstructs existing protection systems causing the system to be unable to prevent any possible sabotage in network systems. In this paper, we propose a **S**imilarity approach for **A**ttack **I**ntention **R**ecognition using **F**uzzy Min-Max Neural Network (*SAIRF*). In particular, the proposed *SAIRF* approach aims to recognize attack intention in real time. This approach classifies attacks according to their characteristics and uses similar metric method to identify motives of attacks and predict their intentions. In this study, network attack intentions are categorized into specific and general intentions. General intentions are recognized by investigating violations against the security metrics of confidentiality, integrity, availability, and authenticity. Specific intentions are recognized by investigating the network attacks used to achieve a violation. The obtained results demonstrate the capability of the proposed approach to investigate similarity of network attack evidence and recognize the intentions of the attack being investigated.

**Keywords:** Network forensics**;** Attack intention**;** Similarity of evidence**;** FMM neural network