Int J Syst Assur Eng Manag (December 2024) 15(12):5454–5468
https://doi.org/10.1007/s13198-024-02438-0

ORIGINAL ARTICLE

# Mutation mayfly algorithm (MMA) based feature selection and probabilistic anomaly detection model for cyber-physical systems

C. Babu Vignesh[1] · E. Arul[2] · V. C. Mahavishnu[3] · A. Punidha[4]

Received: 10 February 2024 / Revised: 24 April 2024 / Accepted: 16 July 2024 / Published online: 14 November 2024

**Abstract** With advances in Cyber-Physical Systems (CPS), privacy-preserving and security issues have attracted substantial attention. A crucial function provided by CPS is anomaly detection on large-scale, complicated, and dynamic data. Physical and network information about the systems for safeguarding original data and identifying cyberattacks is needed in order to develop a reliable privacy-preserving anomaly detection approach. Conventional anomaly detection techniques cannot be directly used to solve these problems because they must deal with the expanding amount of data and need domain-specific expertise. By filtering and choosing key aspects from the original data for improved safety, this research presents a privacy preservation approach for secure anomaly detection. For selecting features, the Mutation Mayfly Algorithm (MMA) has been developed. The proposed program combines key benefits of swarm intelligence and evolutionary algorithms. The usage of MMA in feature selection results from its better accuracy and straightforward structure. Then, a strategy for identifying anomalies based on a Kalman Filter (KF) model and a Gaussian Mixture Model (GMM) has been created to find cyberattacks in CPS. Furthermore, the efficacy of privacy-preserving anomaly detection is being improved through the utilization of a Gaussian Mixture Model (GMM) to convert the noteworthy features into representative characteristics. The present study provides a description of the KF approach, which involves the analysis of the dynamics pertaining to both normal and attack events. The system employs a dynamic thresholding technique to detect anomalous behavior by calculating the lower and upper boundaries of normal activity. The architecture is assessed using two open datasets, UNSW-NB15 for network data and Power System for data on cyber power.

**Keywords** Privacy preservation · Anomaly detection · Cyber-physical system (CPS) · Supervisory control and data acquisition (SCADA) · Power systems · Cyber-attacks · Gaussian mixture model (GMM) · Mutation Mayfly algorithm (MMA) · Kalman Filter (KF)

## 1 Introduction

An important industrial infrastructure, an infrastructure, such as a power, gas, railroad, or water system, is managed and controlled by a Supervisory Control and Data Acquisition (SCADA) system (Erez and Wool 2015; Fahad et al. 2014). Users may interact with and control physical processes using a Cyber-Physical System (CPS) interface that uses communication technology (Song et al. 2017). As a result of the many sensors, actuators, and connected network

✉ C. Babu Vignesh
babuvignesh.c@gmail.com

E. Arul
arulcitit@gmail.com

V. C. Mahavishnu
mahavishnu.vc@gmail.com

A. Punidha
punitulip@gmail.com

[1] Analytics and Software Tools, Western Digital (SanDisk), Bangalore, Karnataka, India

[2] Department of Information Technology, Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India

[3] Department of Computer Science, PSG Institute of Technology and Applied Research, Coimbatore, Tamilnadu, India

[4] Department of Artificial Intelligence and Machine Learning, KPR Institute of Engineering and Technology, Tamil Nadu, Coimbatore, India

devices that are used in today's SCADA systems' power grids and networks to concurrently create energy in a huge number of networked nodes, they are highly intricate (Song et al. 2017; Moustafa et al. 2017).

Security and privacy issues present numerous significant difficulties when connecting CPS to the Internet. First, security concerns stem from the quick development of hacking methods, wherein attackers try to compromise the security of CPS data and equipment. Malware, for instance, might be used in cyberattacks to target network systems. Second, privacy concerns entail both passive and aggressive assaults that compromise sensitive information. During the time when the active assaults are attempting to collect, infer, and/or change confidential data, the passive assaults often nab crucial information from accessible data. To protect CPS against cyberattacks, however, is difficult.

As a result of the absence of cybersecurity tools like message authentication in many CPS systems, it could be difficult to identify inauthentic data injection attacks. It is difficult to protect against eavesdropping attempts since not all systems have universal encryption, especially those who use antiquated technologies. System states must be reviewed to detect replay attacks. Furthermore, the options for network traffic defences are often limited due to the operation's usage of dated technology. For attaining secrecy and integrity in CPS, many studies (Keshk et al. 2017; He et al. 2017) have been carried out. For information to be deemed private, both network and physical data must be secured from unauthorized users. Conversely, data must also be protected from unauthorized changes in order to be considered intact.

The security and privacy practices of CPS have been continuously enhanced to safeguard data integrity and confidentiality (Song et al. 2017). To prevent disclosing sensitive information, privacy-preserving strategies have been created (Fahad et al. 2014). These methods make an effort to safeguard private information while maintaining forecast accuracy. Finding the optimum compromise is still difficult, however. The interpretation of findings and the extraction of information are, on the one hand, less successful when the data are of low quality (high privacy level). For resolving these problems, machine learning (ML) approaches are presented. But a huge quantity of labelled data is required.

Protect cyber physical power systems against cyberattacks, many intrusion detection systems (IDS) have been developed (Keshk et al. 2017; Li et al. 2020). However, the difficulty of acquiring pertinent data is one of the major issues with establishing intrusion detection-based privacy (Fahad et al. 2014). The dataset's large number of characteristics has made it challenging as well. In order to speed up processing and provide more accurate privacy and detection techniques, feature selection (FS) removes unnecessary characteristics. Model performance and computational cost may be reduced by; it is desired to limit the amount of input characteristics.

Swarm Intelligence (SI), an artificial intelligence (AI) technique inspired by nature, has gained popularity. SI is a theoretical field that examines the complicated collective behavior of systems that are made up of a large number of simple agents. More specifically, these straightforward agents are capable of interacting both with other people and their immediate surroundings. Compared to traditional optimization methods, SI provides a number of benefits, according to Pham et al. (2021): Capacity to balance inquisitive and exploitative traits to generate high-quality answers, followed by (1) black-box optimization, (2) gradient-free operation, (3) and (4) ease and simplicity of implementation. It has been utilized effectively for FS in several applications and is becoming more and more popular for solving various optimization challenges. A unique meta-heuristic algorithm called the mayfly algorithm is based on the social behavior of biological groupings. By imitating mayfly flying behavior and mating behavior to find the global best solution, the program performs global and local search.

The study proposes an Optimized privacy preservation based anomaly detection (OPPAD) for CPS, it successfully detects cyber assaults on power systems and related networks while protecting original information. The key characteristics are chosen from the original data using a Mutation Mayfly Algorithm (MMA) approach in order to achieve the privacy preservation aim. Additionally, by applying a Gaussian Mixture Model (GMM), the relevant features are transformed into a representative feature, improving the performance of PPAD. The generated feature is sent into the Kalman Filter (KF) approach, which employs a dynamic threshold to detect abnormal activity while simulating the dynamics of both normal and attack events. Two open datasets are used to assess the framework: UNSW-NB15 for network data and the Power System for data on cyber power.

## 2 Literature review

Li et al. (2020) proposed DeepFed detect industrial CPS cyber risks. Using a CNN and a gated recurrent unit, develop a special deep learning-based intrusion detection model for industrial CPS. Second, a new framework for federated learning has been developed that enables many commercial CPS to work together to develop an extensive intrusion detection model while still protecting privacy. A Paillier cryptographic scheme for safe communication is also designed to safeguard model parameters during training. Extensive trials on an actual industrial CPS dataset show the proposed DeepFed scheme's great efficacy in identifying different forms of cyber threats to industrial CPS as well as its advantages over cutting-edge systems.