中国科学院上海微系统与信息技术研究所
Shanghai Institute of Microsystem and Information Technology Chinese Academy of Sciences

Toward Deep Learning based Intrusion Detection System: A Survey

Oral Presentation For
2024 6th International Conference on Big Data Engineering

Zhiqi Li

July/26/2024

Contents

01 **Introduction & Contributions**

02 **Related Works**

03 **Analysis & Discussion**

04 **Challenges & Future Works**

Part 01

Introduction & Contributions

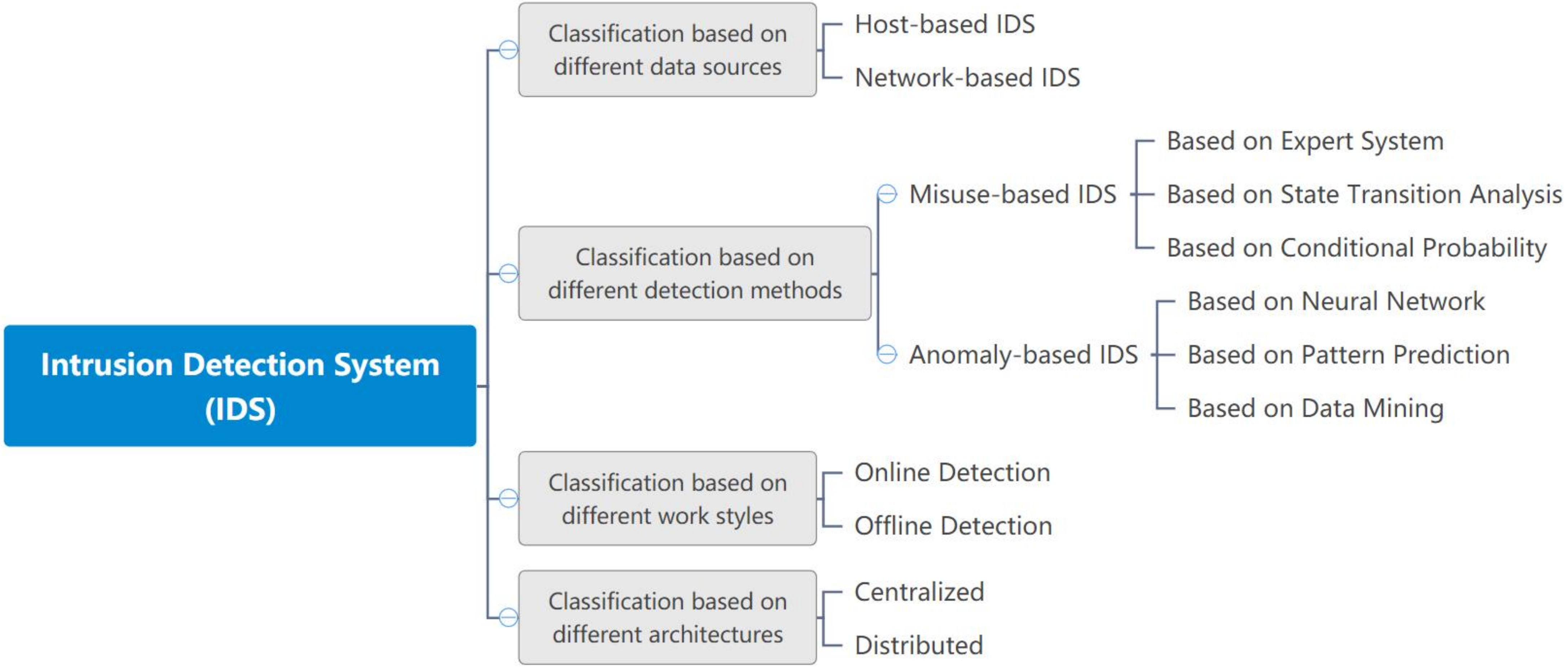
Introduction

Intrusion Detection System (IDS)

A type of security management software or hardware to detect **anomalous activities** or potential **malicious behaviors**.

It detects possible intrusions or attacks by analyzing network traffic, system logs, or host activities.

Classification of IDS



Intrusion Detection System (IDS)

- Classification based on different data sources
  - Host-based IDS
  - Network-based IDS
- Classification based on different detection methods
  - Misuse-based IDS
    - Based on Expert System
    - Based on State Transition Analysis
    - Based on Conditional Probability
  - Anomaly-based IDS
    - Based on Neural Network
    - Based on Pattern Prediction
    - Based on Data Mining
- Classification based on different work styles
  - Online Detection
  - Offline Detection
- Classification based on different architectures
  - Centralized
  - Distributed

Contributions

1. A review of recent works on DL-based IDS proposed within the past few years is presented, accompanied by a analysis and discussion.

2. The advancements in DL-based IDS development over recent years are provided.

3. Some insightful suggestions are proposed for future works.

Part 02

Related Works

Related Works

Computer Networks

Composing of multiple computers with independent functionalities interconnected via communication channels.

Internet of Things

Comprising various information devices, including the wireless sensor network (WSN) composed of sensors.

Related Works for Computer Networks

- Z. Wang et al. introduced a DNN, named **EFS-DNN**, based on integrated feature selection. It was used to detect attacks in networks characterized by heavy traffic data *(Z. Wang et al., 2022)*.
  They integrated a feature selection module based on a **light gradient enhancer (LightGBM)** to enhance the robustness of the optimal subset selection process.

- T. Zhang and S. Bao introduced a **DNN** model to detect computer network intrusion *(T. Zhang and S. Bao, 2022).*
  They identified intrusion patterns and normal user behaviour as a set of parameters in IDS, and used **immune genetic algorithms** to thoroughly explore and refine these parameter sets, making the model real-time.

Zehong Wang, Jianhua Liu, Leyao Sun. 2022. EFS-DNN: An ensemble feature selection-based deep learning approach to network intrusion detection system. Secur. Commun. Netw. 2022 (April 2022), 2693948.

Tuqian Zhang, Shumei Bao. 2022. A novel deep neural network model for computer network intrusion detection considering connection efficiency of network systems. In Proceedings of the 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (February 2022), 962–965.

Related Works for Computer Networks

- T. Kim et al. introduced a method to enhance the processing of NIDS data sets using **vision-based** deep learning technology *(T. Kim et al., 2023)*.

  By applying various image conversion techniques, they converted the NIDS dataset into a **two-dimensional** representation and merged it into a **three-channel RGB** color image.

- X. Yuan et al. proposed a **hybrid** IDS architecture that combines traditional and DL models to improve the robustness against adversarial attacks *(X. Yuan et al.,2023)*.

  They proposed a detector with **local intrinsic dimensionality**, and improved the limited attack portability between the DL and ML models to enhance the robustness of the model to identify malicious traffic.

Taehoon Kim, Wooguil Pak. 2023. Deep learning-based network intrusion detection using multiple image transformers. Appl. Sci. 2023, 13 (February 2023), 2754.

Xinwei Yuan, Shu Han, Wei Huang, Hongliang Ye, Xianglong Kong, Fan Zhang. 2023. A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system. Comput. & Secur. 137 (December 2023), 103644.

Related Works for Computer Networks

- E. Qazi et al. developed a hybrid intrusion detection system based on DL by using **convolutional recurrent neural networks** *(E. Qazi et al.,2023).*

  They used **CNN** for local feature acquisition and **deep RNN** for feature extraction to improve the efficiency.

- M. Soltani et al. introduced a **deep learning**-based framework for IDSs to adapt to emerging threats *(M. Soltani et al.,2023)*.

  ① They adopted a deep learning-driven approach to open **set identification** to detect unfamiliar samples, including some new attacks and threats.

  ② It was combined with a **clustering algorithm** to organize these new samples into clusters, simplifying the labeling process and reducing the burden on expert teams.

  ③ These **clusters** were used to **update** the model so that it can adapt to changing traffic patterns.

Emad U. H. Qazi, Muhammad H. Faheem, Tanveer Zia. 2023. HDLNIDS: Hybrid deep-learning-based network intrusion detection system. Appl. Sci. 2023, 13 (April 2023), 4921.

Mahdi Soltani, Behzad Ousat, Mahdi J. Siavoshani, Amir H. Jahangir. An adaptable deep learning-based intrusion detection system to zero-day attacks. J. Inform. Secur. Appl. 76 (June 2023), 103516.

Related Works for IoT

Scheme	Description	Dataset	Accuracy	Advantages	Disadvantages
SMO+DBN ***(H. Bhor et al.,2021)***	It was designed by combining Taylor series with Spider Monkey Optimization (SMO) algorithm.	KDD CUP 99	90%	High accuracy and low false alarm rate.	Low hidden neurons led a high false alarm rate (>10%).
CPMA ***(L. Liu et al.,2021)***	A detection framework based on ML in IoT platforms using an SVM classifier.	-	96%	High accuracy.	Small relay nodes led a low accuracy rate.
NSBPSO ***(S. Baniasadi et al.,2022)***	A novel optimization approach employs a neighborhood search-based PSO algorithm.	UNSW-NB15 and Bot-IoT	98.86%	High accuracy.	High computational costs.
GNN ***(Y. Zhang et al.,2022)***	A framework for intrusion detection based on GNNs and a network constructor with refinement regularization.	gas pipeline dataset	97.2%	Good performance on small or unbalanced class datasets.	The efficiency performance needs to be tested and improved.

Harsh N. Bhor, Mukesh Kalla. 2021. TRUST- based features for detecting the intruders in the Internet of Things network using deep learning. Comput. Intell. 38, 2 (July 2021), 438–462.

Liang Liu, Xiangyu Xu, Yulei Liu, Zuchao Ma, Jianfei Peng. 2021. A detection framework against cpma attack based on trust evaluation and machine learning in IoT network. IEEE IoT J. 8, 20 (January 2021), 15249–15258.

Sahba Baniasadi, Omid Rostami, Diego Martín, Mehrdad Kaveh. 2022. A novel deep supervised learning-based approach for intrusion detection in IoT systems. Sensors (Basel) 22, 12 (June 2022), 4459.

Yichi Zhang, Chunhua Yang, Keke Huang, Yonggang Li. 2022. Intrusion detection of Industrial Internet-of-Things based on reconstructed graph neural networks. IEEE Trans. Netw. Sci. Eng. 10, 5 (September

Related Works for IoT

Scheme	Description	Dataset	Accuracy	Advantages	Disadvantages
ML-IDS ***(Y. Saheeda et al., 2022)***	A ML-based IDS is proposed to detect anomalous behavior on insecure IoT networks.	UNSW-NB15	99.9%	Low communication overhead and keyless encryption.	It needs to test for additional attack types.
IMIDS ***(Y. Saheeda et al., 2022)***	An intelligent IDS can against cyber threats in IoT using CNN. An attack data generator is proposed and powered by a conditional GAN.	UNSW-NB15 and CICIDS2017	96.69% and 95.92%	High network attacks detection F-score with 97.22%.	Low detection accuracy for Fuzzers & Backdoor attacks (77.60% & 37.08%).
DRL-IDS ***(S. Tharewal et al., 2022)***	A proximal policy optimization method based on light GBM's feature selection method using PPO2 algorithm.	A real dataset	99.09%	DL observation and decision-making fusion.	The detection capability for distributed industrial IoT needed to be enhanced.
CL ***(C. Liu et al., 2021)***	K-means and random forest algorithms were used for binary classification and they are implemented on Spark platform.	NSL-KDD and CIS-IDS2017	85.24% and 99.91%	Improved accuracy, faster preprocessing speed, and less training time.	Training on more attack types to expand detection capabilities.

Yakub K. Saheeda, Aremu I. Abiodunb, Sanjay Misrac, Monica K. Holonec, Ricardo C.-Palaciosc. 2022. A machine learning-based intrusion detection for detecting Internet of Things network attacks. Alexandria Eng. J. 61, 12 (March 2022), 9395–9409.

Kim-Hung Le, Minh-Huy Nguyen, Trong-Dat Tran, Ngoc-Duan Tran. 2022. IMIDS: An intelligent intrusion detection system against cyber threats in IoT. Electronics 11, 4 (February 2022), 524.

Sumegh Tharewal, Mohammed W. Ashfaque, Sayyada S. Banu, Perumal Uma, Samar M. Hassen, Mohammad Shabaz. 2022. Intrusion detection system for Industrial Internet of Things based on deep reinforcement learning. Wirel. Commun. Mob. Comput. 2022 (March 2022), 9023719.

Chao Liu, Zhaojun Gu, Jialiang Wang. 2021. A hybrid intrusion detection system based on scalable k-

Related Works for IoT

- A. Awajan proposed a DL-based intrusion detection system tailored for IoT devices *(Albara Awajan,2023)*.
  Utilizing a four-layer deep **fully connected (FC) network** architecture, the malicious traffic targeting connected devices could be efficiently identified. Notably, it offered a protocol-independent solution, simplifying deployment complexities.

- S. Soliman et al. proposed an intelligent IDS to identify attacks in IIoT *(S. Soliman et al.,2023)*.
  They used the synthetic minority **over-sampling technique** to mitigate issues of overfitting and underfitting that could lead to biased classification.

Albara Awajan. 2023. A novel deep learning-based intrusion detection system for IoT networks. Computers 12, 2 (February 2023), 34.

Sahar Soliman, Wed Oudah, Ahamed Aljuhani. 2023. Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alexandria Eng. J. 81 (September 2023), 371–383.

Related Works for IoT

- N. Khan et al. presented a deep learning-based intelligent IDS algorithm aimed at overcoming the limitations of existing systems, which often focused solely on one layer of the three-layer IoT architecture *(N. Khan et al.,2023)*.

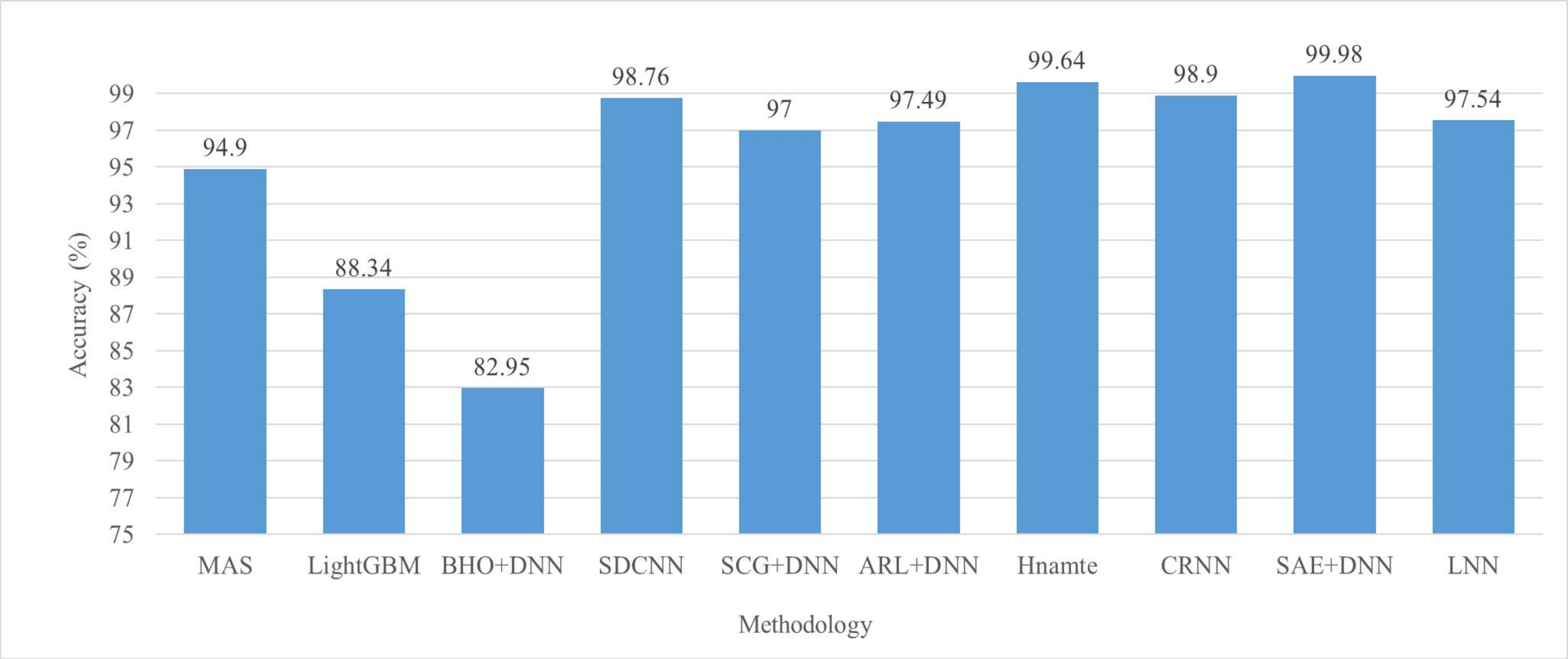
  Their approach integrated a **RNN and Gated Recurrent Unit (DNN-GRU)**, enabling classification of attacks across the network. The model's training and testing utilized the ToN-IoT dataset, curated for three-layer IoT systems, offering diverse attack scenarios compared to publicly available datasets.

Noor W. Khan, Mohammed S. Alshehri, Muazzam A. Khan, et al. 2023. A hybrid deep learning-based intrusion detection system for IoT networks. Math. Biosci. Eng. 20, 8 (June 2023), 13491–13520.

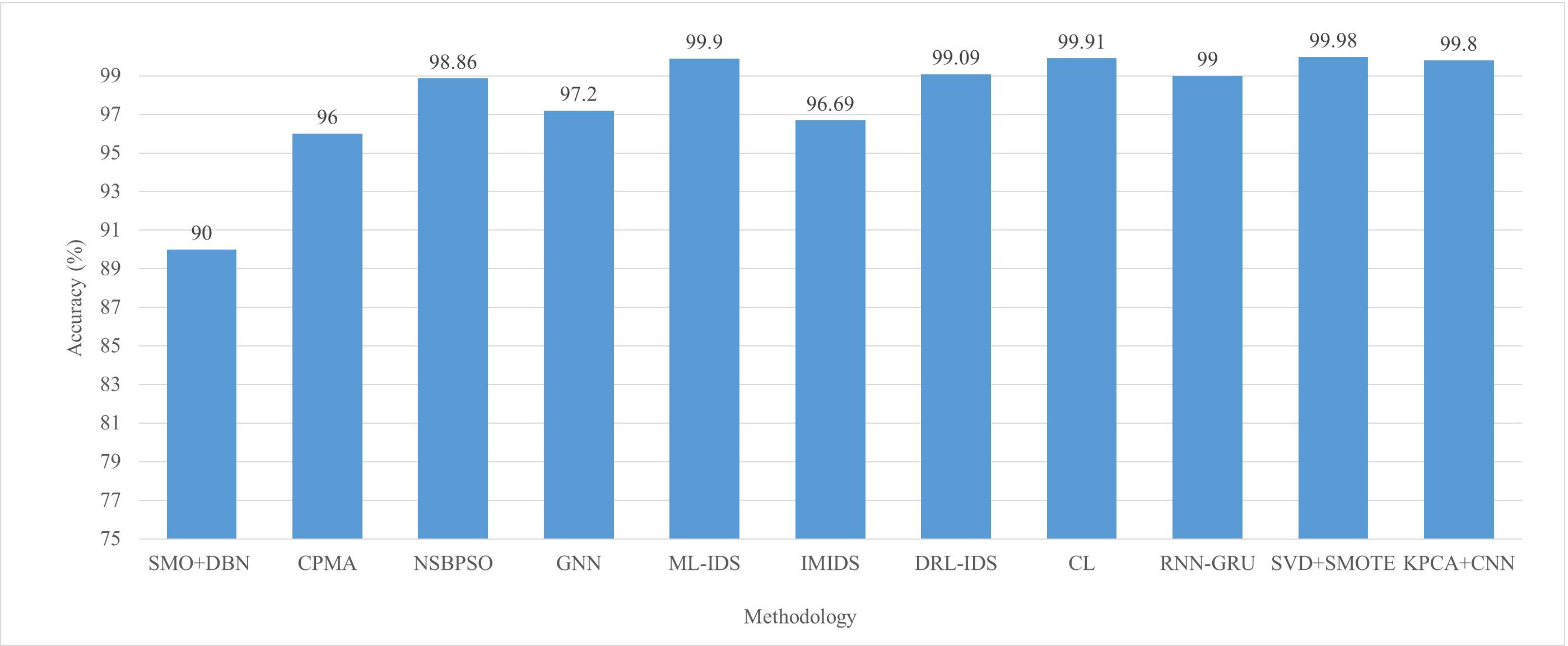
Part 03

Analysis & Discussion

Accuracy Performance Comparison of IDS for Computer Network



Accuracy Performance Comparison of IDS for Internet of Things



Accuracy Performance Comparison of IDS in WSN

Scheme	Dataset	Precision	Recall	Accuracy
SLnO+NN	-	92%	93%	95%
ACO-DNN	NSL-KDD	99.6%	96.6%	99.5%
VGRD	NSL-KDD	95%	91.5%	95.5%
RNN	WSN-DS	-	-	99.8%

Part 04

Challenges & Future Works

Challenges & Future Works

Challenges

1. The results obtained from DNN-based attack detection may lack interpretability

2. Low adaptability to various network topologies

3. Internal Threat

Future Works

1. Explainable Artificial Intelligence (XAI)

2. Collaborative learning and cooperative detection

3. Nodes Trust Evaluation

Acknowledgment

This work was funded in part by the National Natural Science Foundation of China (Grant no. 62071450), in part by the Shanghai Natural Science Foundation (Grant no. 21ZR1461700), and in part by the Key Research and Development Task Special Project of the Xinjiang Uygur Autonomous Region (Grant no. 2022B01009).

Q & A