GOCE DELCEV UNIVERSITY, STIP, NORTH MACEDONIA

FACULTY OF ELECTRICAL ENGINEERING

ETIMA 2025

THIRD INTERNATIONAL CONFERENCE

24-25 SEPTEMBER, 2025

TECHNICAL SCIENCES APPLIED IN ECONOMY, EDUCATION AND INDUSTRY

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“, ШТИП
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

GOCE DELCEV UNIVERSITY, STIP
FACULTY OF ELECTRICAL ENGINEERING

ТРЕТА МЕЃУНАРОДНА КОНФЕРЕНЦИЈА
THIRD INTERNATIONAL CONFERENCE

ЕТИМА / ETIMA 2025

ЗБОРНИК НА ТРУДОВИ
CONFERENCE PROCEEDINGS

24-25 септември 2025 | 24-25 September 2025

ISBN: 978-608-277-128-1
DOI: https://www.doi.org/10.46763/ETIMA2531

Главен и одговорен уредник / Editor in Chief
проф.д-р Сашо Гелев
Prof.d-r Saso Gelev

Јазично уредување / Language Editor
Весна Ристова (македонски) / Vesna Ristova (Macedonian)

Техничко уредување / Technical Editing
Дарко Богатинов / Darko Bogatinov

Издавач / Publisher
Универзитет „Гоце Делчев", Штип / Goce Delcev University, Stip
Електротехнички факултет / Faculty of Electrical Engineering

Адреса на организационен комитет / Adress of the organizational committee
Универзитет „Гоце Делчев", Штип / Goce Delcev University, Stip
Електротехнички факултет / Faculty of Electrical Engineering
Адреса: ул. „Крсте Мисирков" бр. 10А / Adress: Krste Misirkov, 10A
Пош. фах 201, Штип - 2000, С. Македонија / PO BOX 201, Stip 2000, North Macedonia
E-mail: conf.etf@ugd.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

62-049.8(062)
004-049.8(062)

МЕЃУНАРОДНА конференција ЕТИМА (3 ; 2025 ; Штип)
Зборник на трудови [Електронски извор] / Трета меѓународна конференција ЕТИМА 2025, 24-25 септември 2025 ; [главен и одговорен уредник Сашо Гелев] = Conference proceedings / Third international conference, 24-25 September 2025 ; [editor in chief Saso Gelev]. - Текст во PDF формат, содржи 357 стр., илустр. - Штип : Универзитет "Гоце Делчев", Електротехнички факултет ; Stip : "Goce Delchev" University, Faculty of Electrical engineering, 2025

Начин на пристапување (URL): https://js.ugd.edu.mk/index.php/etima/en. - Наслов преземен од екранот. - Опис на изворот на ден 30.10.2025. - Трудови на мак. и англ. јазик. - Библиографија кон трудовите

ISBN 978-608-277-128-1

а) Електротехника -- Примена -- Собири б) Машинство -- Примена -- Собири
в) Автоматика -- Примена -- Собири г) Инфоматика -- Примена -- Собири

COBISS.MK-ID 67297029

Трета меѓународна конференција ЕТИМА
24-25 Септември 2025
Third International Conference ETIMA
24-25 September 2025

ОРГАНИЗАЦИОНЕН ОДБОР
ORGANIZING COMMITTEE

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Маја Кукушева Панева / Maja Kukuseva Paneva
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Дарко Богатинов / Darko Bogatinov
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Трета меѓународна конференција ЕТИМА
24-25 Септември 2025
Third International Conference ETIMA
24-25 September 2025

ПРОГРАМСКИ И НАУЧЕН ОДБОР
SCIENTIFIC COMMITTEE

Георги Иванов Георгиев / Georgi Ivanov Georgiev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Антон Белан / Anton Beláň
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Ивелина Стефанова Балабанова / Ivelina Stefanova Balabanova
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Бојан Димитров Карапенев / Boyan Dimitrov Karapenev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Влатко Чингоски / Vlatko Cingoski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Божо Крстајиќ / Bozo Krstajic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Милован Радуловиќ / Milovan Radulovic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Гоце Стефанов / Goce Stefanov
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Мирјана Периќ / Mirjana Peric
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Ана Вучковиќ / Ana Vuckovic
Електронски факултет,
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Мирослава Фаркаш Смиткова / Miroslava Farkas Smitková
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Петер Јанига / Peter Janiga
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Јана Радичова / Jana Raditschová
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Александар Туџаров / Aleksandar Tudzarov
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Владимир Талевски / Vladimir Talevski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Владо Гичев / Vlado Gicev
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Марија Чекеровска / Marija Cekerovska
Машински факултет,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Mechanical Engineering,
Goce Delcev University, Stip, North Macedonia;

Мишко Џидров / Misko Dzidrov
Машински факултет,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Mechanical Engineering,
Goce Delcev University, Stip, North Macedonia;

Александар Крстев / Aleksandar Krstev
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Ванчо Аџиски / Vancho Adziski
Факултет за природни и технички науки,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Natural and Technical Sciences,
Goce Delcev University, Stip, North Macedonia;

Томе Димовски / Tome Dimovski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Зоран Котевски / Zoran Kotevski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Никола Рендевски / Nikola Rendevski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Илија Христовски / Ilija Hristovski
Економски факултет,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Economy,
University St Climent Ohridski, North Macedonia;

Христина Спасовска / Hristina Spasovska
Факултет за електротехника и информациски технологии,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Роман Голубовски / Roman Golubovski
Природно-математички факултет,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Mathematics and Natural Sciences,
Ss. Cyril and Methodius University, North Macedonia;

Маре Србиновска / Mare Srbinovska
Факултет за електротехника и информациски технологии,
Универзитет „Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Билјана Златановска / Biljana Zlatanovska
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Александра Стојанова Илиевска / Aleksandra Stojanova Ilievska
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Мирјана Коцалева Витанова / Mirjana Kocaleva Vitanova
Факултет за информатика,
Универзитет „Гоце Делчев“, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Ивана Сандева / Ivana Sandeva
Факултет за електротехника и информациски технологии,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Наташа Стојковиќ / Natasa Stojkovik
Факултет за информатика,
Универзитет „Гоце Делчев“, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

PREFACE

The Third International Conference “Electrical Engineering, Technology, Informatics, Mechanical Engineering and Automation – Technical Sciences in the Service of the Economy, Education and Industry” (ETIMA’25), organized by the Faculty of Electrical Engineering at the “Goce Delchev” University – Shtip, represents a significant scientific event that enables interdisciplinary exchange of knowledge and experience among researchers, professors, and experts in the field of technical sciences. The conference was held in an online format and brought together 78 authors from five different countries.

The ETIMA conference aims to establish a forum for scientific communication, encouraging multidisciplinary collaboration and promoting technological innovations with direct impact on modern life. Through the presentation of scientific papers, participants shared the results of their research and development activities, contributing to the advancement of knowledge and practice in relevant fields.
The first ETIMA conference was organized four years ago, featuring 40 scientific papers. The second conference took place in 2023 and included over 30 papers. ETIMA’25 continued this scientific tradition, presenting more than 40 papers that reflect the latest achievements in electrical engineering, technology, informatics, mechanical engineering, and automation.

At ETIMA’25, papers were presented that addressed current topics in technical sciences, with particular emphasis on their application in industry, education, and the economy. The conference facilitated fruitful discussions among participants, encouraging new ideas and initiatives for future research and projects.

ETIMA’25 reaffirmed its role as an important platform for scientific exchange and international cooperation. The organizing committee extends sincere gratitude to all participants for their contribution to the successful realization of the conference and its scientific value.

We extend our sincerest gratitude to all colleagues who, through the presentation of their papers, ideas, and active engagement in discussions, contributed to the success and scientific significance of ETIMA’25.

The Organizing Committee of the Conference

ПРЕДГОВОР

Третата меѓународна конференција „Електротехника, Технологија, Информатика, Машинство и Автоматика – технички науки во служба на економијата, образованието и индустријата“ (ЕТИМА’25), организирана од Електротехничкиот факултет при Универзитетот „Гоце Делчев“ – Штип, претставува значаен научен настан кој овозможува интердисциплинарна размена на знаења и искуства меѓу истражувачи, професори и експерти од техничките науки. Конференцијата се одржа во онлајн формат и обедини 78 автори од пет различни земји.

Конференцијата ЕТИМА има за цел да создаде форум за научна комуникација, поттикнувајќи мултидисциплинарна соработка и промовирајќи технолошки иновации со директно влијание врз современото живеење. Преку презентација на научни трудови, учесниците ги споделуваат резултатите од своите истражувања и развојни активности, придонесувајќи кон унапредување на знаењето и практиката во релевантните области.

Првата конференција ЕТИМА беше организирана пред четири години, при што беа презентирани 40 научни трудови. Втората конференција се одржа во 2023 година и вклучи над 30 трудови. ЕТИМА’25 продолжи со истата научна традиција, презентирајќи повеќе од 40 трудови кои ги отсликуваат најновите достигнувања во областа на електротехниката, технологијата, информатиката, машинството и автоматиката.

На ЕТИМА’25 беа презентирани трудови кои обработуваат актуелни теми од техничките науки, со посебен акцент на нивната примена во индустријата, образованието и економијата. Конференцијата овозможи плодна дискусија меѓу учесниците, поттикнувајќи нови идеи и иницијативи за идни истражувања и проекти.

ЕТИМА’25 ја потврди својата улога како значајна платформа за научна размена и интернационална соработка. Организациониот одбор упатува искрена благодарност до сите учесници за нивниот придонес кон успешната реализација на конференцијата и нејзината научна вредност. Конференцијата се одржа онлајн и обедини седумдесет и осум автори од пет различни земји.

Изразуваме голема благодарност до сите колеги кои со презентирање на своите трудови, идеи и активна вклученост во дискусиите придонесоа за успехот на ЕТИМА’25 и нејзината научна вредност.

Организационен одбор на конференцијата

СОДРЖИНА / TABLE OF CONTENTS:

Трета меѓународна конференција ЕТИМА
Third International Conference ETIMA
UDC: 004.728.056:004.491
https://www.doi.org/10.46763/ETIMA2531311s

A REVIEW OF RESOURCE OPTIMIZATION TECHNIQUES IN INTRUSION DETECTION SYSTEMS

Goce Stevanoski[1], Aleksandar Risteski[2], Mitko Bogdanoski[1]
[1]Military Academy General Mihailo Apostolski, Skopje, North Macedonia,
email: goce.stevanoski@ugd.edu.mk
email: mitko.bogdanoski@ugd.edu.mk
[2]Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University, Skopje, North Macedonia,
email: acerist@feit.ukim.edu.mk

Abstract

Intrusion Detection Systems (IDS) are critical components in ensuring the security of modern network infrastructures, providing real-time detection and mitigation of malicious activities. However, these systems are often challenged by limited computational resources, high false-positive rates, and inefficiencies in handling large volumes of data. Resource optimization techniques have emerged as a vital area of research aimed at enhancing the efficiency and accuracy of IDS implementations. This review systematically analyzes various resource optimization strategies employed in IDS. The paper discusses the applicability, advantages, limitations, and performance impacts of these techniques across different intrusion detection scenarios. Finally, future research directions are proposed, highlighting the potential integration of advanced machine learning methods and real-time adaptive optimization methods to further improve IDS efficiency and reliability.

Keywords

IDS, single-objective, multi-objective, resources, optimization

Introduction

An Intrusion Detection Systems (IDS) can be network-based (monitoring network traffic) or host-based (monitoring activities on a host). Modern IDS often employ machine learning (ML) and deep learning (DL) to improve detection of novel threats. However, these sophisticated techniques can be computationally intensive. The deployment context of an IDS greatly influences its resource requirements. In enterprise or cloud environments, IDS may have powerful servers available, whereas in IoT, edge, or fog scenarios, the IDS components may reside on embedded devices, wireless sensors, or gateway nodes with limited hardware capabilities. With the proliferation of networked devices and high-speed data flows, modern IDS face significant challenges, including handling large volumes of data under limited computational resources and minimizing false alarm rates. Traditional IDS often struggle with high false-positive rates and performance bottlenecks when are working on packet-level analysis in high-speed networks[1]. These resource constraints are even worse in emerging environments such as the Internet of Things (IoT), edge, and fog computing, where devices may have limited processing power, memory, and energy supply. Ensuring timely and accurate intrusion detection in such resource-constrained settings requires innovative optimization techniques.

This paper provides a comprehensive review of resource optimization techniques in IDS from the last five years, covering both traditional network environments and resource-constrained domains like IoT, edge, and fog computing. We categorize optimization approaches into single-objective (optimizing one primary metric or goal) and multi-objective (simultaneously optimizing trade-offs between two or more goals) strategies. A comparative summary of key approaches is provided in Table 1. Finally, we outline future research directions, including the integration of advanced machine learning and real-time adaptive optimization, to guide further improvements in IDS efficiency and reliability.

1. Literature review

Recent years have witnessed extensive research into resource optimization for IDS, aiming to improve detection accuracy and efficiency despite constraints. A prominent trend is the incorporation of optimization algorithms – especially metaheuristic and evolutionary algorithms – into IDS design[1]. Techniques like genetic algorithms (GAs), particle swarm optimization (PSO), and other nature-inspired algorithms have been employed to tune IDS parameters, select important features, and balance detection performance against resource usage. In fact, a systematic review of IDS literature (2018–2023) identified GAs among the top methods used alongside machine learning models to enhance IDS performance[2]. The popularity of such algorithms underlines the growing focus on optimizing IDS configuration for better trade-offs between security and resource consumption.

Sharma et al. (2024) conducted a systematic review of multi-objective optimization algorithms for IDS in IoT networks, reflecting the growing interest in this area[3]. They note that a wide variety of metaheuristic optimizers – Moth-Flame Optimization, Crow Search, Vortex Search, Red Fox Optimization, multi-objective variants of algorithms like PSO and evolutionary strategies – have been used to tackle IDS optimization with multiple goals. Notably, many studies in their survey treat feature selection as a multi-objective problem, confirming that this is a fruitful formulation for IDS. The use of multi-objective functions for computational efficiency in IoT was proposed for future studies by Al-Shurbaji et al. (2025) in their research on Deep Learning-Based IDS for detecting IoT botnet attacks. They emphasize that MOO helps in balancing the objectives for efficiency with selection of optimal feature subset [4].

The problem with low computational power is addressed by N. Dai and S. Uludag (2024) where IoT devices are optimized for better resource optimization in inference time and memory consumption [5]. They are showing that there is a trade-off between the models' performances and the resources usage. Better performance often needs higher resources consumption. In conclusion they emphasize that high-performing models tend to consume more resources. Hoseinpur F. (2022) in his dissertation besides the research on how to enhance security and privacy in fog computing by designing lightweight and efficient IDS, they explore how to efficiently utilize computing resources in fog computing to enhance the quality of services and effectively facilitate the deployment of security mechanisms [6]. They have proposed an analytical model to formulate resource management problems from a communication cost perspective based on a greedy principle. The model minimizes the communication cost and demonstrates near-optimal efficiency. Their work was not extended to other resources costs.

Several studies have reviewed the application of optimization techniques but have not addressed resource optimization, despite its significance in IDS research. For example, Houssein et al. in their paper have made a very comprehensive and in-depth analysis of metaheuristic algorithms and their applications in wireless sensor networks. One downside in their work is that they

haven't addressed the utilization of the algorithms for efficient resource optimization, which was already big topic to the day [7]. Manzoor et al. with their review on resource allocation techniques (RAT) in cloud environments have presented that RAT are targeting MOO for resource optimization[8]. Directing their work in the cloud computing area, they have pointed out that one of the most research algorithms or resource optimization is Genetic algorithm. Although in conclusion they did not consider their findings regarding optimization algorithms and left them out of recommendations for future research. Therefore, our work can contribute to future research in this area.

Table 1. Comparison of various resource optimization techniques in IDS.

Study (Year)	Opt. type	Algo. family	Application in IDS	Optimization Goal	Categorization	Opt. techniq.	Environment / Dataset
Dickson & Thomas (2020)[1]	Single objective	Bio-Inspired	Hyperparameter Tuning	Threshold optimization	Meta-Heuristic	PSO	Enterprise network (NSL-KDD dataset)
R. Manivannan & S. Selvaraj (2025)[9]	Single objective	Bio-Inspired	Feature Selection	Reduce resources	Meta-Heuristic	FOX	CICIDS-2017
Einy et al. (2021)[10]	Multi objective	Bio-Inspired	Feature Selection	Reduce resources	Meta-Heuristic	MOPSO	MANET / Wireless (KDD Cup 99 dataset)
Ahsan et al. (2025)[11]	Single objective	Bio-Inspired	Hyperparameter Tuning	Maximize detection accuracy	Meta-Heuristic	GWO	
N. Savanović et al. (2023) [12]	Single objective	Bio-Inspired	Hyperparameter Tuning	Maximize detection accuracy	Meta-Heuristic	Firefly Algorithm	
H. G. A. Umar et al. (2025)[13]	Single objective	N/A	Lightweight and Efficient Model Design	Reduce resources	N/A	DNN-KDQ	CIC-IDS2017
B. O.George and B. Pranggono (2025)[14]	Single objective	N/A	Lightweight and Efficient Model Design	Reduce resources	N/A	AE and FL techniques	N-BaIoT
Y. Chen et al. (2021)[15]	Multi objective	Evolutionary	Hyperparameter Tuning	Reduce resources	Meta-Heuristic	MOEA/D	AWID and the CIC-IDS2017
M. Stehlik et al. (2013)[16]	Multi objective	Evolutionary	Resource Optimization	Balance multiple conflicting goals	Meta-Heuristic	NISGA-II and SPEA2	Simulated environment with OMNeT++
S. Subramani et al. (2023)[17]	Multi objective	Bio-Inspired	Feature Selection	Balance multiple conflicting goals	Meta-Heuristic	IMOPSO	KDD Cup 1999, NSL-KDD, CIDD
M. Fatima et al. (2024) [18]	Multi objective	N/A	Feature Selection	Reduce resources	N/A	Ensemble Feature Selection	TON_IoT, BoT-IoT, UNSW-

							NB15, CIC-IDS2017/2018
P. T. Cong et al. (2024)[19]	Multi objective	Bio-Inspired	Hyperparameter Tuning	Reduce resources	Meta-Heuristic	PSO	NSL-KDD, CIC-IDS2017
S. Latif et al. (2024)[20]	Multi objective	Bio-Inspired	Hyperparameter Tuning	Reduce resources	Meta-Heuristic	Genetic Algorithm (GA)	Edge-IIoTset
N. O. Aljehane et al. (2024) [21]	Multi objective	Bio-Inspired	Hyperparameter Tuning, Feature Selection	Reduce resources	Meta-Heuristic	GJO and SSA	NSL-KDD, CIC-IDS2017
A. Alshahrani & J. A. Clark (2023) [22]	Multi objective	Bio-Inspired	Lightweight and Efficient Model Design	Reduce resources	Meta-Heuristic	Genetic Algorithm (GA)	Simulated environment
N. Kashyap et al. (2020)[23]	Multi objective	Evolutionary	Resource Optimization	Balance multiple conflicting goals	Meta-Heuristic	NSGA-II	Simulated environment
S. P. Singh (2022)[24]	Multi objective	Bio-Inspired	Resource Optimization	Balance multiple conflicting goals	Meta-Heuristic	MODE	Simulated environment

2. Resource optimization in IDS

Intrusion detection systems (IDS) must function within the limits of processing time, memory, storage, and energy across various environments. This challenge becomes particularly difficult with IoT networks and wireless sensor networks. Resource optimization in IDS can be tackled through multiple approaches. Broadly speaking, these strategies include: (1) Feature Selection and Dimensionality Reduction – selecting a subset of informative features from traffic data to reduce processing load without compromising accuracy; (2) Algorithm and Model Optimization – tuning ML/DL models or using efficient classifiers to balance accuracy and speed; (3) Parameter Tuning – adjusting detection thresholds or algorithm parameters (e.g., updating anomaly detection sensitivity) to achieve optimal performance; (4) Architectural Optimization – distributing IDS components (e.g., on edge vs. cloud) to offload work from constrained nodes; and (5) Multi-objective Optimization (MOO) – using algorithms that seek trade-offs (e.g., maximize detection rate while minimizing false alarms and resource usage).

In the following sections, we dive into single-objective and MOO techniques, providing examples of each and how they apply in both normal and constrained environments.

3. Single-objective optimization approaches

Single-objective optimization techniques focus on improving one primary metric or goal of the IDS, often treating other requirements as constraints. This section discusses common single-objective optimization strategies, including feature selection, hyperparameter tuning, and lightweight model design.

Feature Selection and Dimensionality Reduction

Feature selection is a critical optimization for IDS, especially to handle high-dimensional data. By removing irrelevant or redundant features, an IDS can operate faster and more efficiently, which is valuable both in traditional networks and in IoT devices with limited resources. The challenge is to select features that preserve or improve detection capability.
A variety of algorithms have been applied for IDS feature selection. Genetic Algorithms (GA), which simulate evolution to search for optimal feature subsets, were among the early approaches and continue to be popular[2]. In recent work, R. Manivannan & S. Selvaraj have proposed a novel ARNN-FOX model for efficient intrusion detection and classification based on single objective optimization. They have proved that the model optimization on feature selection and dynamically tune on hyperparameters can provide a scalable and adaptable solution for modern IDS in various environments[9].

Hyperparameter Tuning

Besides selecting features, optimizing the internal parameters of IDS models can greatly improve both performance and efficiency [13]. Hyperparameter tuning involves finding the best configuration for algorithm parameters that yield the highest detection performance. This is often treated as a single-objective optimization problem where the objective is to maximize a metric like detection rate, precision, or F1-score on validation data. Therefore, metaheuristic algorithms have been effectively used to tune hyperparameters for IDS. For instance, Grey Wolf Optimization (GWO) algorithm was utilized to optimize the hyperparameters of a deep neural network for anomaly detection, resulting in an IDS that achieved over 99% detection accuracy[11]. Similarly, Firefly Algorithm (FOA) was used by Savanovic et al. (2022) to fine-tune the hyperparameters of classifiers like KNN and XGBoost in an IoT IDS, yielding excellent results (accuracy of 99.98% on UNSW-NB15 dataset) when the optimization was effective[12]. These examples illustrate that tuning an IDS model's settings via intelligent search can significantly boost accuracy, which is a key single-objective goal. Threshold optimization is another single-objective task common in IDS. Many IDS generate a score or likelihood for each event, and a threshold is used to decide if it is an attack. Setting this threshold is crucial: too low can trigger many false positives, too high can miss attacks. Optimization techniques like PSO have been used to automatically find the threshold that maximizes a combination of true positives and true negatives. Anne Dickson and Thomas (2020) demonstrated this by optimizing the operating point of a classifier's ROC curve using PSO[1]. In their experiment on the NSL-KDD dataset, they identified the optimal trade-off point which yielded a True Positive rate of 99.5% while keeping the False Positive rate at only 2%. This effectively improved detection rates and solved the false alarm minimization problem using swarm intelligence. The approach was shown to generalize both traditional networks and IoT scenarios, indicating its usefulness in resource optimization (fewer false alarms mean less wasted processing on benign traffic).

Lightweight and Efficient Model Design

Another category of single-objective optimization focuses on creating lightweight IDS models that meet resource constraints. Here the goal is typically to minimize resource usage (model size, runtime, or energy) while maintaining acceptable accuracy. This is especially relevant for deployment on edge and IoT devices. A notable technique in this category is the use of model compression and knowledge distillation. Umar and Yasmeen (2025) introduced a deep learning IDS framework called DNN-KDQ, which integrates Knowledge Distillation and post-training

Quantization to produce a compact model suited for energy-constrained edge computing[13]. Their objective was to simultaneously optimize high detection performance and low computational footprint. The results were impressive: the distilled and quantized DNN model achieved a test accuracy of 99.43% while reducing model size from 196.8 KB to 20.2 KB – an almost 90% reduction. This compression led to a 63% reduction in inference latency and significantly lower energy consumption, without compromising detection accuracy. By using adaptive sampling and sliding windows for preprocessing, the DNN-KDQ framework further ensures that only the most relevant data segments are analyzed, saving energy. This example underscores how advanced ML techniques can be leveraged to create IDS that meet strict resource limits as a single optimization objective (in this case, minimizing resource usage given a high accuracy target). Other approaches in efficient model design include using simpler classifiers or shallow models in environments where deep learning would be too costly. For example, Olanrewaju-George and Pranggono (2020) explored federated learning for IDS, which trains models across distributed IoT devices without centralizing data[14].

In summary, single-objective optimizations in IDS have yielded substantial benefits to IDSs which perform better with equal or fewer resources. However, focusing on one objective at a time may neglect other aspects. This motivates multi-objective approaches, discussed next, which explicitly consider trade-offs.

4. Multi-objective optimization approaches

In many cases, IDS optimization is inherently a multi-objective problem. Security practitioners seek to maximize detection rates and minimize false positives, while also keeping computational cost low. These goals can conflict: pushing accuracy to the maximum might require more features or complex models, increasing resource usage; conversely, strict resource limits might reduce accuracy. In IDS research, multi-objective algorithms (typically evolutionary or swarm-based) have been applied to balance detection efficacy against factors like false alarm rate, number of features, or processing time.

Multi-Objective Feature Selection and Tuning

Feature selection can naturally be framed as a multi-objective problem: one objective to maximize detection accuracy, and another to minimize the number of features (or equivalently minimize computational cost). The MOO implementation in a IDS had been proposed by various authors for different cases. In that respect, Subramani et al. (2023) and Cong et al. (2024), have proposed and implemented an intelligent Multi Objective PSO based Intrusion Detection System (IMOPSO-IDS) for detecting the intruders present in the IoT based sensor networks that are working in the cloud environment [17], [19]. The proposed system was focused on developing a more efficient approach for feature selection in data. The use of MOO in feature selection was presented by Fatima et al. (2024), which have made an extensive study discussing feature selection enabled lightweight IDS tailored for resource-constrained IoT devices [18]. They have a special focus on the emerging Ensemble Feature Selection (EFS) techniques with and aim to pave the way for the effective design of futuristic FS/EFS-enabled lightweight IDS for IoT networks, and by addressing the critical need for robust security measures in the face of resource limitations.

Chen et al. (2022) have demonstrated a new multi-objective evolutionary convolutional neural network for IDS in Fog infrastructure to detect network intrusions in the IoT environment. There the Multi-objective evolutionary algorithm based on decomposition (MOEA/D) algorithm is used for modifying and evolving the CNN model which simplifies the tuning

process of DL [25]. Sharma et al. (2024), is proposing the future work on multi-objective optimizers to be conducted in various optimizing tasks such as resource management, parameter estimation, scheduling. They have done study in which they have demonstrated that AI techniques have significantly improved detection efficiency. During their work they define that optimization techniques can be used for hyper parameter optimization in ML and DL methods, additionally emphasizing that there are issues with computational time and memory usage, since the whole process needs more computational resources.

Beyond feature selection, multi-objective formulations have been applied to simultaneously optimize detection performance and resource usage metrics. Stehlík et al. (though slightly older work in concept) showed that using multi-objective evolutionary algorithms (like NSGA-II and SPEA2) to parametrize an IDS for wireless sensor networks yields better trade-offs between detection accuracy and energy consumption than single-objective tuning[16]. This idea is increasingly relevant for IoT, where one must often find a compromise between security level and device longevity or latency.

Metaheuristic Algorithms for Multi-Objective IDS

Most multi-objective IDS optimizations leverage metaheuristic algorithms, which are well-suited for exploring complex search spaces and finding trade-off solutions. Evolutionary algorithms and nature-inspired algorithms have been adapted to multi-objective versions. For example, a recent work by Latif et al. applied a GA to tune hyperparameters of a deep ensemble IDS (combining CNN models) and achieved perfect classification scores (100% accuracy, precision, recall) on a benchmark dataset[20]. While such an ideal result may reflect an easy dataset or potential overfitting, it exemplifies that evolutionary multi-objective search can potentially find extremely high-performing configurations that manual tuning might miss.

In IoT scenarios, novel bio-inspired algorithms have been tailored for MOO in IDS. We have already noted PDO in IoT-IDS. Additionally, algorithms like Golden Jackal Optimization (GJOA) and Salp Swarm Algorithm (SSA) have been combined to address separate objectives in a complementary way. Aljehane et al. (2023) employed GJOA to identify the most significant features (objective: feature reduction) and SSA to fine-tune the hyperparameters of an LSTM-based detector (objective: accuracy maximization) in an IoT network IDS[21]. This dual-optimizer approach led to an outstanding detection performance (≈99.7% accuracy with F1-score ~98.9% on the CIC-IDS2017 dataset). The success of such hybrid optimization suggests that complex IDS could benefit from modular MOO.

Alshahrani et al. (2023) in one of the authors in one of the author's PhD publications "Optimizing IDS Configurations for IoT Networks using AI Approaches" [22] [26] are working on IDS in a resource-constrained environment and are emphasizing that IDS's deployment in that environment is a challenging task. They are using a meta-heuristic-based optimization method, namely a Genetic Algorithm (GA), to discover optimal IDS placements and configurations for Low Power and Lossy Networks (LLNs). In the work authors target an approach that seeks to optimize and balance the detection rate, F1 score, coverage, feasibility cost and deployment cost. The work has proved that using a fitness approximation is a valid approach to be used as a surrogate model to accelerate the convergence of the genetic algorithm to optimal or excellent IDS configurations. Stating that for future work research should be conducted on multi-objective framework for optimizing IDS configurations in resources-constraint environments and are proposing use of Non-dominated Sorting Genetic Algorithm (NSGA-II) in the future work. The usage of NSGA II algorithm in IoT was demonstrated in

[23] and [24] where it is shown the usability of NSGA II algorithm in finding solution for service composition problems and delivering efficiency in energy consumption.

5. Discussion and future directions

Resource optimization techniques have improved IDS performance in both traditional and constrained environments. Single-objective methods like feature selection and model compression help in deploying faster IDS on low-power devices. Multi-objective methods provide a way for handling trade-offs in IDS security and efficiency. Despite these advances, several open challenges and promising directions remain:

- Real-Time Adaptive Optimization. Future IDS are expected to operate in dynamic environments where network conditions and attack patterns evolve continuously. A promising direction is the development of adaptive optimization methods that can adjust IDS parameters on the fly. For instance, using reinforcement learning or online evolutionary algorithms, an IDS could self-tune its thresholds or feature set in real time based on feedback. This real-time adaptation would further reduce the need for manual reconfiguration and keep the IDS optimal as conditions change[13]. Early research in this vein includes adaptive threshold control using Q-learning and online feature selection algorithms that periodically revise the chosen features as new data comes in. Integrating such approaches could fulfill the vision of an autonomously optimizing IDS.

- Advanced Machine Learning Integration. As attacks become more sophisticated, IDS will likely incorporate cutting-edge ML techniques (deep neural networks, graph-based models for IoT device interactions, etc.). Optimizing these complex models for resource efficiency is crucial. Techniques like neural architecture search (NAS) could be employed in the IDS context to find neural network structures that offer the best accuracy-speed trade-off under given constraints[11]. Combining NAS with MOO (e.g., objectives: maximize detection, minimize FLOPs) is a potential research avenue.

- Energy-Aware IDS for IoT and Edge. Given the rise of battery-powered sensors and IoT deployments, energy efficiency will remain a key optimization goal. Future research should explore energy-aware intrusion detection, where algorithms explicitly account for energy consumption as an optimization objective alongside detection metrics. This might involve scheduling IDS tasks (e.g., only activating heavy analysis during certain times or when suspicion is high), or designing cooperative detection schemes where edge devices offload computations to slightly more powerful fog nodes in an optimal way.

- Scalability and Distributed Optimization. In large-scale networks or IoT ecosystems, a single IDS module might not suffice; instead, multiple IDS agents work collaboratively (e.g., hierarchical IDS in edge–fog–cloud). Optimizing resource usage in such distributed IDS is complex – one must decide how to partition the detection tasks and how agents should share information. Future research could employ MOO to determine the optimal placement of detection modules (e.g., which intrusion checks to run on-device vs on cloud) considering latency, bandwidth, and detection accuracy as objectives. Evolutionary algorithms could potentially evolve configurations of federated IDS that yield the best trade-off between detection performance and communication cost.

- Security of Optimization Techniques: An often-overlooked aspect is that optimization algorithms themselves might introduce vulnerabilities if not carefully applied. For instance,

an adversary could exploit an adaptive IDS by manipulating inputs to drive the optimization toward a weaker configuration (an instance of adversarial machine learning).

In conclusion, resource optimization in IDS is a rich and evolving field. As networks expand and diversify (with billions of IoT devices coming online) and as cyber threats continue to grow in sophistication, IDS must become not only more accurate but also smarter in how they use resources.

Conclusions

This review presented an analysis of resource optimization techniques in IDS, covering recent advances in both single-objective and multi-objective approaches. We discussed how feature selection, hyperparameter tuning, and model compression methods can significantly reduce resource usage and improve speed for IDS in traditional and constrained settings. We also presented multi-objective evolutionary and swarm algorithms that balance conflicting goals such as maximizing detection accuracy while minimizing false positives and computational cost. Future research is poised to further integrate machine learning advancements with optimization. We anticipate more AI-driven adaptive IDS that continually self-optimize in operation, and the adoption of multi-faceted objectives that incorporate security, efficiency, and even privacy considerations into a unified optimization framework. The evolution of IDS will probably follow a path of intelligent resource management, ensuring that increased security does not come at the expense of impractical resource demands. By leveraging the techniques reviewed in this paper and pursuing the proposed future directions, the community can develop IDS that are not only effective against attacks but also efficient and scalable for the next generation of cyber-physical systems and ubiquitous networks.

References

[1] Dickson, Alex/Thomas, Charly: “Improved PSO for optimizing the performance of intrusion detection systems”. Journal of Intelligent & Fuzzy Systems 38(5), 2020, pp. 6537–6547.

[2] Issa, Mustafa M./Aljanabi, Mohammed/Muhialdeen, Hawraa M.: “Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations”. Journal of Intelligent Systems 33(1), 2024, pp. 1–24.

[3] Sharma, Saurabh/Kumar, Vinod/Dutta, Kunal: “Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review”. Internet of Things and Cyber-Physical Systems 4, 2024, pp. 258–267.

[4] Al-Shurbaji, Taha et al.: “Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review”. IEEE Access 13, 2025, pp. 11792–11822.

[5] Dai, Na/Suludag, Serdar: “Performance Tradeoff in ML-Based Intrusion Detection Systems: Efficacy vs. Resource Usage”. In: IEEE (ed.): 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC). IEEE: Piscataway 2024, pp. 1030–1031.

[6] Hoseinpur, Fatemeh: Towards security and resource efficiency in fog computing networks. 2022. https://urn.fi/URN:ISBN:978-952-335-886-7

[7] Houssein, Essam H./Saad, Mohammed R./Djenouri, Youcef/Hu, Gang/Ali, Ahmed A./Shaban, Hassan: “Metaheuristic algorithms and their applications in wireless sensor networks: review, open issues, and challenges”. Cluster Computing 27(10), 2024, pp. 13643–13673.

[8] Manzoor, Muhammad F./Abid, Adnan/Farooq, Muhammad S./Azam, Nabeel A./Farooq, Umar: “Resource Allocation Techniques in Cloud Computing: A Review and Future Directions”. Elektronika ir Elektrotechnika 26(6), 2020, pp. 40–51.

[9] Manivannan, Rajesh/Senthilkumar, S.: “Intrusion Detection System for Network Security Using Novel Adaptive Recurrent Neural Network-Based Fox Optimizer Concept”. International Journal of Computational Intelligence Systems 18(1), 2025, pp. 37.

[10] Einy, Shayan/Oz, Cagatay/Navaei, Yashar D.: “Network Intrusion Detection System Based on the Combination of Multiobjective Particle Swarm Algorithm-Based Feature Selection and Fast-Learning Network”. Wireless Communications and Mobile Computing 2021(1), 2021, pp. 6648351.

[11] Ahsan, Mohammad S./Islam, Shoriful/Shatabda, Swakkhar: “A systematic review of metaheuristics-based and machine learning-driven intrusion detection systems in IoT”. Swarm and Evolutionary Computation 96, 2025, pp. 101984.
[12] Savanović, Nikola et al.: “Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning”. Sustainability 15(16), 2023, pp. 12563..
[13] Umar, Halima G. A. et al.: “Energy-efficient deep learning-based intrusion detection system for edge computing: a novel DNN-KDQ model”. Journal of Cloud Computing 14(1), 2025, pp. 32.
[14] Olanrewaju-George, Bukola/Pranggono, Bernardi: “Federated learning-based intrusion detection system for the internet of things using unsupervised and supervised deep learning models”. Cyber Security and Applications 3, 2025, pp. 100068
[15] Chen, Yang/Chen, Shuai/Xuan, Min/Lin, Qiang/Wei, Wei: “Evolutionary Convolutional Neural Network: An Application to Intrusion Detection”. In: IEEE (ed.): 2021 13th International Conference on Advanced Computational Intelligence (ICACI). IEEE: Piscataway 2021, pp. 245–252.
[16] Stehlik, Milan/Saleh, Ahmed/Stetsko, Andriy/Matyas, Vashek: “Multi-Objective Optimization of Intrusion Detection Systems for Wireless Sensor Networks”. In: MIT Press (ed.): Advances in Artificial Life, ECAL 2013. MIT Press: Cambridge 2013, pp. 569–576.
[17] Subramani, S./Selvi, M.: “Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks”. Optik (Stuttgart) 273, 2023, pp. 170419.
[18] Fatima, Maryam/Rehman, Obaid/Rahman, Ijaz M. H./Ajmal, Anum/Park, Seong J.: “Towards Ensemble Feature Selection for Lightweight Intrusion Detection in Resource-Constrained IoT Devices”. Future Internet 16(10), 2024, pp. 368.
[19] Cong, Pham T./Van Huong, Pham/Minh, Le Q.: “A Multi-Objective Approach to Improve Hyperparameters of CNN for Network Intrusion Detection Problem”. In: IEEE (ed.): 2024 1st International Conference on Cryptography and Information Security (VCRIS). IEEE: Piscataway 2024, pp. 1–6.
[20] Latif, Sarmad/Boulila, Wadii/Koubaa, Anis/Zou, Zhigang/Ahmad, Jawad: “DTL-IDS: An optimized Intrusion Detection Framework using Deep Transfer Learning and Genetic Algorithm”. Journal of Network and Computer Applications 221, 2024, pp. 103784.
[21] Aljehane, Nada O. et al.: “Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security”. Alexandria Engineering Journal 86, 2024, pp. 415–424. doi: 10.1016/j.aej.2023.11.078.
[22] Alshahrani, Ali/Clark, John A.: “On Optimal Configuration of IDS for RPL Resource-Constrained Networks Using Evolutionary Algorithm”. In: Springer (ed.): Advances in Intelligent Systems and Computing. Springer: Cham 2023, pp. 514–535.
[23] Kashyap, Nikhil/Kumari, Anupama C./Chhikara, Rakesh: “Multi-objective Optimization using NSGA II for service composition in IoT”. Procedia Computer Science 167, 2020, pp. 1928–1933.
[24] Singh, Shailendra P./Dhiman, Gaurav/Viriyasitavat, Wattana/Kautish, Sandeep: “A Novel Multi-Objective Optimization Based Evolutionary Algorithm for Optimize the Services of Internet of Everything”. IEEE Access 10, 2022, pp. 106798–106811.
[25] Chen, Yang/Lin, Qiang/Wei, Wei/Ji, Jichuan/Wong, Ka-Chun/Coello, Carlos A. Coello: “Intrusion detection using multi-objective evolutionary convolutional neural network for Internet of Things in Fog computing”. Knowledge-Based Systems 244, 2022, pp. 108505.
[26] Alshahrani, Ali: Optimising IDS Configurations for IoT Networks using AI Approaches. University of Sheffield: Sheffield 2023. https://etheses.whiterose.ac.uk/id/oai_id/oai:etheses.whiterose.ac.uk:3323