JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

2/2026

vol. 104

(*Contents continued on back cover*)

eISSN 1899-8852

Effects of Deformation of Main Reflector of Double Reflector Spherical Antenna on Its Aperture Field – ROT-54/2.6 Antenna Case

Arevik Sargsyan and Narek Hambardzumyan

National Polytechnic University of Armenia,
Yerevan, Armenia

https://doi.org/10.26636/jtit.2026.2.2528

Abstract — The aim of this study is to model the impact of main reflector deformations in a double-reflector spherical antenna system on the phase distribution of the electromagnetic field across the aperture and the associated gain loss. The study focuses on the antenna of the ROT-54/2.6 radio-optical telescope (Herouni radio telescope) – a spherical double-reflector system with a fixed primary reflector with a 54 m diameter, composed of 3 738 panels. An analytical model is developed to evaluate phase distortions induced by deviations from the spherical geometry. The model computes local phase shifts across the aperture and predicts gain degradation using Ruze's formula which relates the RMS surface error to efficiency losses. This approach is important for pre-alignment procedures and functional restoration of the antenna, enabling geometry corrections prior to full-scale observations. Based on terrestrial laser scanning (TLS) data, the methodology allows for a quantitative assessment of structural phase errors and corresponding gain degradation, confirming its suitability for practical diagnostics of large reflector systems.

Keywords — antenna, radio-optical telescope, ROT-54/2.6, terrestrial laser scanning

1. Introduction

The prolonged conservation period of the ROT-54/2.6 radio optical telescope has resulted in the accumulation of stochastic structural deformations caused by environmental factors. Verification of the actual geometric configuration of the primary spherical reflector is a key milestone of a project aiming to revitalize the Herouni National Space Center. Restoration of the telescope's operational capability requires a comprehensive alignment procedure based on a comparative assessment of the present electrodynamic performance against the original design specifications.

The ROT-54/2.6 radio-optical telescope is a dual reflector spherical system designed for precision measurements of radio emissions from deep space sources over a wavelength range of 3 – 200 mm. The primary reflecting element has the shape of spherical reflector (54 m in diameter) composed of 3 738 aluminum–manganese panels, each with an area of approximately 1 m^2. The panels are mounted on a supporting framework with adjustable stanchions that provide alignment capability with an accuracy of several centimeters, thereby enabling maintenance of the required spherical precision of the primary reflector.

The geometry of the reflector ensures that a constant distance is maintained from any point on the surface to a sphere of 27 m, which corresponds to the curvature radius and determines the key geometric parameters of the telescope, including its sub-reflector profile, focal position, suspension height of the corrective sub-reflector, and related parameters. Efficient concentration of electromagnetic energy in the focal region within the sub-reflector requires that the profile accuracy of both reflectors be maintained within an error budget not exceeding 50 – 70 μm, which ensures operability at frequencies up to 100 GHz [1]–[4].

The ROT-54/32/2.6 (ROT-54/2.6) telescope is a distinctive large aperture dual reflector spherical telescope that combines a 54 m physical primary reflector with an effective aperture of 32 m and an optical reflector of 2.6 m. Owing to its scale and potential millimeter band performance, restoration of this telescope is scientifically significant, as it is an important national research infrastructure component that doubles as a facility capable of contributing to international observational programs requiring geographically distributed instruments and access to long-term observation campaigns.

The telescope is potentially useful for long-term variability monitoring of compact radio sources, spectral studies of stellar and interstellar media, and participation in distributed interferometric observations where improved $u-v$ coverage is critical [5].

Relaunch of the millimeter band capability of the ROT-54/2.6 telescope depends, to a critical degree, on high-precision refurbishment, alignment, and calibration of its optical and radiotechnical subsystems. First and foremost, it requires that the geometric accuracy of the reflecting surface and the mutual conformity of the dual-reflector system be restored.

After an extended conservation period, accumulated deformations and misalignments have led to aperture phase errors, reduced gain, and loss of focusing capability, thus preventing achievement of the designed sensitivity and angular resolution. To remedy this, targeted corrective procedures are required. Therefore, quantitative diagnostics of the as-is reflector geometry, an explicit measurement-to-model link between geometric deviations and aperture-phase structure, the

Fig. 1. ROT-54/2.6 radio optical telescope.

development of corrective alignment and subsequent calibration algorithms are the necessary elements of the restoration workflow.

Modeling the impact of stochastic displacements of the primary-reflector panels on the radiation characteristics is a critical stage of the pre-alignment procedure. In principle, costly mechanical adjustment of each panel can be partially substituted by a hardware–software approach that implements real-time feed position correction.

This procedure, however, is the objective of a separate, dedicated study. Any deviation of the primary-reflector panels from the ideal spherical surface, caused by structural and thermodynamic factors, introduces phase errors in the reflected field and distorts the wavefront over the aperture. This, in turn, reduces directivity and compromises overall gain of the telescope.

The development of a pre-alignment framework, based on hybrid modeling and combining archival data with terrestrial laser scanning, enables to compensate for the deformations accumulated during the prolonged period of inactivity, thereby restoring proper field focusing at the aperture without requiring complete reassembly of the reflector's surface. The present study examines the quantitative influence of such deformations on the phase structure of the aperture field [6]–[9].

2. Results and Analysis

For the ROT-54/2.6 radio-optical telescope, the mathematical phase distribution model differs from that of conventional paraboloidal reflectors. The main difference is the presence of a fixed spherical primary reflector combined with a movable feed located at the focus of a corrective subreflector with a specially designed profile. In an ideal spherical system, the phase in the aperture plane $z = 0$ at a point with a given radial coordinate can be expressed as:

$$\Phi(\rho,\phi) = k\left(\sqrt{(R+\delta(\rho,\phi))^2-\rho^2} + \Delta L_{(corr)(\rho)} + \Delta z\cos\theta\right) \tag{1}$$

where:

- $k = \frac{2\pi}{\lambda}$ is the wave number,
- R is the curvature radius of the primary reflector (54 m),
- $\Delta L_{corr}(\rho)$ is the optical path length in the double-reflector feed system (Herouni antenna system) introduced to compensate for spherical aberration,
- $\Delta z\ \cos\theta$ stands for a compensating term describing the axial displacement of the secondary reflector along the optical axis to minimize phase error.

To assess the geometry of the primary reflector of a double reflector spherical antenna after an extended conservation period, it is appropriate to employ the terrestrial laser scanning (TLS) technique. In contrast to contact-based methods, TLS allows to acquire a highly redundant point cloud (up to 10^6 measurements) with sub-millimetre accuracy, without imposing mechanical loads on the fragile panel-alignment assemblies.

This capability is important for identifying local deformations induced by fastener corrosion and long-term foundation settlement during decades of inactivity. Terrestrial laser scanning is therefore one of the most effective techniques for the initial pre-alignment stage.

The approach yields a dense point cloud (a Digital Twin concept) that captures the as-is reflector geometry with an accuracy on the order of 0.5 mm, which is sufficient for verification of its current structural state. The subsequent transformation of the TLS point cloud into phase error parameters constitutes a key step in the digital restoration workflow for the ROT-54/2.6 radio optical telescope [10].

In the initial theoretical stage of the study, the following antenna parameters should be analyzed:

where:

- root mean square (RMS) error of the geometric profile of an individual panel for various perturbations of five control points on each panel,
- cumulative surface error of a group consisting of several panels,
- phase deviations introduced by these deformations into the wavefront over the aperture,
- antenna gain losses caused by the resulting aggregate phase dispersion [6].

For a quantitative assessment of the geometric accuracy of the j-th panel, we introduce the RMS deviation of its surface relative to the ideal spherical profile. Let measurements be performed at N_p control points on the panel (typically $N_p = 5$: four corner points and one central point), and let $\Delta r_{j,i}$ denote the deviation of the i-th point of panel j from

the nominal radial distance R_0:

$$\Delta r_{j,i} = r_{j,i} - R_0 \,, \tag{2}$$

where $r_{j,i}$ is the center of the measured distance from the sphere to the i-th point of the j-th panel and $R_0 = 27$ is the nominal radius of the spherical surface. The RMS profile error of the j-th panel is then defined as:

$$\sigma_j = \sqrt{\frac{1}{N_p} \sum_{i=1}^{N_p} \left(\Delta r_{j,i}\right)^2} \,. \tag{3}$$

where σ_j has the dimension of length and characterizes the typical magnitude of the deviations of a given panel from the ideal spherical surface.

The following notation is used:

- j – panel index, $j = 1, 2, \ldots, P$, where $P = 3738$ is the total number of primary reflector panels,
- i – control-point index, $i = 1, 2, \ldots, N_p$,
- N_p – number of control points per panel (typ. $N_p = 5$),
- $r_{j,i}$ – measured distance to point (j, i),
- R_0 – nominal (ideal) radial distance to the surface ($R_0 = 27$),
- $\Delta r_{j,i}$ – local deviation of point (j, i) from the ideal profile,
- σ_j – RMS profile error of the j-th panel.

To determine the overall surface error of the primary reflector, we introduce a global RMS deviation, σ_{group}, which relates the local RMS error of a representative deformed panel, σ_{pan}, to the number of such panels M and the total number of panels P:

$$\sigma_{group} = \sigma_{pan} \cdot \sqrt{\frac{M}{P}} = \sigma_{pan} \cdot \sqrt{f} \,, \tag{4}$$

where:

- σ_{group} – RMS surface error of the primary reflector (aperture-wide RMS),
- σ_{pan} – characteristic RMS profile error of a single deformed panel (if all M deformed panels exhibit the same error level),
- M – number of deformed panels,
- P – total number of primary reflector panels (for the ROT-54/2.6 radio-optical telescope $P = 3738$),
- $f = \frac{M}{P}$ – fraction of the aperture area associated with deformed panels.

This relationship shows that the contribution of each panel to the overall error is additive in power (i.e., additive in the squares of deviations). Consequently, σ_{group} increases with the square root of the number of deformed panels rather than linearly, reflecting the statistical nature of error accumulation.

To convert geometric surface deviations into wavefront phase errors, we use a relation that expresses the phase shift in terms of the measured radial error δz_i at the i-th control point:

$$\Delta\varphi_i = \frac{4\pi}{\lambda} \cdot \delta z_i \,, \tag{5}$$

where:

- $\Delta\varphi_i$ – phase error (phase shift) at the i-th point on the surface, expressed in radians,
- λ – operating wavelength,
- δz_i – deviation of the measured distance r_i from the ideal radius R_0,
- r_i – measured distance from the sphere to the i-th point on the surface,
- R_0 – nominal (ideal) distance from the center of the primary reflector to its surface (for ROT-54/2.6 $R_0 = 27$m) [11].

It is assumed that the measurements are performed for a spherical geometry such that the rangefinder measurement direction is aligned with the local surface normal and that the rays are considered in proximity of the optical axis. Under these conditions, the angular factor satisfies $\cos\theta \approx 1$.

The more general expression, which accounts for the incidence angle with the factor $\cos\theta$ is:

$$\Delta\varphi_i = \frac{4\pi}{\lambda} \cdot \delta z_i \cdot \cos\theta_i \,, \tag{6}$$

with $\cos\theta = 1$, it is reduced to Eq. (5). Thus, Eq. (5) provides a direct relationship between laser-measured deviation δz_i and phase distortion $\Delta\varphi_i$, which are subsequently used to calculate the RMS phase error, surface efficiency, and the related gain losses.

The phase change introduced by a deformed panel, for a wavelength $\lambda = 3$ cm and normal incidence ($\cos\theta \approx 1$), is given by:

$$\Delta\phi_{pan} = \frac{4\pi}{\lambda}\, \delta r_{pan} \,. \tag{7}$$

Substituting $\Delta\phi_{pan} = 2$ cm and $\lambda = 3$ cm, we obtain:

$$\Delta\phi_{pan} = \frac{4\pi}{3} \cdot 2 = \frac{8\pi}{3} \approx 8.38\,\text{rad} \,, \tag{8}$$

which is equivalent to approximately 480° (1.33 phase revolutions). Thus, even a 2 cm displacement of a single panel produces a big phase shift over the related local aperture region, although its contribution to the global antenna efficiency is determined by its fractional area.

The impact that cumulative phase errors exert on the antenna's gain is quantified by the Ruze formula, which relates the global RMS surface deviation σ to the relative efficiency η:

$$\eta = e^{-\left(\frac{4\pi\sigma}{\lambda}\right)^2} \,, \tag{9}$$

- η – relative gain efficiency (surface efficiency), $\eta = \frac{G}{G_0}$,
- G – actual antenna gain in the presence of surface errors,
- G_0 – ideal gain for a perfect (defect-free) surface,
- σ – total RMS surface deviation (in particular, σ_{group} may be substituted),
- λ – operating wavelength.

The exponential function indicates that even a moderate increase in the $\frac{\sigma}{\lambda}$ ratio results in a substantial reduction of η. In the limit $\sigma \to 0$, the formula yields $\eta \to 1$ (an ideal antenna). For σ comparable to $\frac{\lambda}{4\pi}$, the efficiency decreases approximately to $e^{-1} \approx 0.37$. With a further growth in σ, the impact of the distorted phase front becomes dominant and the actual gain degrades sharply [12].

Tab. 1. Estimated relative gain efficiency as a function of the number of deformed panels (Ruze model).

M	σ_{group}	η
1	0.032 cm	$0.983\ (\approx 98.3\%)$
10	1.0 mm	$0.839\ (\approx 83.9\%)$
50	2.24 mm	$0.416\ (\approx 41.6\%)$
100	3.16 mm	$0.173\ (\approx 17.3\%)$
500	7.07 mm	$1.5 \times 10^{-4}\ (\approx 0.015\%)$
1000	10 mm	$2.4 \times 10^{-8}\ (\approx 2.4 \times 10^{-6}\%)$

Consider the case in which a single panel of the main reflector is displaced as a rigid body along its local normal by an offset value such as:

$$\Delta r_{pan} = +2.0\,\text{cm}\ ,$$

with respect to the ideal spherical surface.

It is assumed that all $N_p = 5$ control points on this panel are assumed to have the same deviation:

$$\Delta r_{j,i} = \Delta r_{pan} = +2.0\ \text{cm}\ \ i = 1, \ldots, 5\ .$$

Then, the error of the RMS profile error of this panel σ_j is computed using the standard RMS expression:

$$\sigma_j = \sqrt{\frac{1}{N_p}\sum_{i=1}^{N_p}\left(\Delta r_{j,i}\right)^2}\ . \tag{10}$$

Substituting $\Delta r_{j,i} = \Delta r_{pan}$ for all five points, we obtain:

$$\begin{aligned}\sigma_j &= \sqrt{\frac{1}{N_p}\sum_{i=1}^{N_p}\left(\Delta r_{pan}\right)^2} = \sqrt{\frac{1}{N_p}N_p(\Delta r_{pan})^2} \\ &= |\Delta r_{pan}| = 2.0\,\text{cm}\ .\end{aligned} \tag{11}$$

Therefore, for a rigidly displaced panel, the surface error is numerically equal to the magnitude of the displacement [13] – [16].

We now consider an example that involves a larger number of deformed panels. Each deformed panel has the same RMS error $\sigma_{pan} = 2.0$ cm, and the total number of primary reflector panels is $P = 4000$. For a group of M-deformed panels, the global RMS surface deviation σ_{group} is estimated as:

$$\sigma_{group} = \sigma_{pan}\sqrt{\frac{M}{P}}\ . \tag{12}$$

Next, applying Ruze's formula, one can estimate relative efficiency η (ratio between actual gain and ideal gain) for different values of M at $\lambda = 3$ cm and $\sigma_{pan} = 2.0$ cm.

The calculation results are summarized in Tab. 1. These values illustrate that for a fixed displacement of 2 cm per panel, an increase in the number of deformed panels leads to a statistical growth of the global RMS surface error and an exponential decrease in antenna gain.

3. Conclusions

This analysis demonstrates that even relatively small geometric deformations of the main reflector panels of the ROT-54/2.6 radio-optical telescope antenna result in noticeable phase distortions of the wavefront over the aperture. The conversion of measured radial deviations δz_i to phase errors $\Delta\varphi_i$, using relation $\Delta\varphi_i = \frac{4\pi}{\lambda}\cdot\delta z_i$, establishes a direct link between laser measurement data and the electrodynamic characteristics.

The introduction of RMS estimates σ_j for individual panels and σ_{group} for an ensemble of deformed panels allows to quantitatively describe the accumulation of errors across the aperture. It is shown that the global RMS error σ_{group} increases as $\sqrt{\frac{M}{P}}$, reflecting the statistical nature of the summation of local errors. The application of Ruze's formula to calculate the efficiency factor demonstrates an exponential reduction in gain as the $\frac{\sigma_{group}}{\lambda}$ ratio increases.

Numerical examples for different values of M indicate that, when many dozens of panels are deformed, the gain losses reach several tens of percent. When the number of affected panels reaches the order of hundreds or more, the antenna effectively loses it focusing capability.

Therefore, maintaining the geometric accuracy of the panels at the submillimeter level is a necessary condition for preserving the designed gain and ensuring the operability of the ROT-54/2.6 radio-optical telescope over the specified frequency range.

References

[1] P.M. Herouni, "Issues in the Design Calculation of Spherical Dual-reflector Antennas", *Radiotekhnika i Elektronika*, vol. 19, pp. 3–12, 1964.

[2] P.M. Herouni, "The First Radio-optical Telescope", *Sixth International Conference on Antennas and Propagation (ICAP 89)*, Coventry, UK, 1989.

[3] P.M. Herouni, "Construction and Operation of Radio-Optical Telescope ROT-32/54/2.6", *URSI International Meeting of Mirror Antenna Construction*, Riga, Latvia, 1990.

[4] P.M. Herouni, "Measurements of the ROT-54/2.6 Characteristics", *VKAI-5*, Yerevan, Armenia, 1990.

[5] J.M. Martin and C. Rosolen, "Perspectives of the ROT 54/32/2.6 in Astronomy", *Astrophysics*, vol. 38, pp. 361–363, 1995 (https://doi.org/10.1007/BF02044713).

[6] A.S. Sargsyan, "Current Status and Prospects for Restoring the Herouni Reflector Radio Telescope Antenna", *Radiotekhnika*, vol. 87, pp. 158–166, 2023.

[7] A.S. Sargsyan, "Methodology for the Preliminary Stage of Alignment Works During the Deconservation of the ROT-54/2.6 Antenna", *Radiotekhnika*, vol. 87, no. 2, pp. 172–177, 2023.

[8] A.S. Sargsyan and V.A. Parfenov, "Development of an Alignment Concept for the ROT-54/2.6 Radio-optical Telescope", *XIII International Conference on Photonics and Information Optics*, Moscow, Russia, 2024 (in Russian).

[9] H. Kutterer and C. Hesse, "Automated Form Recognition of Laser Scanned Deformable Objects", *Geodetic Deformation Monitoring: From Geophysical to Engineering Roles*, vol. 131, pp. 103–111, 2006 (https://doi.org/10.1007/978-3-540-38596-7_12).

[10] C. Holst and H. Kuhlmann, "Challenges and Present Fields of Action at Laser Scanner Based Deformation Analyses", *Journal of Applied Geodesy*, vol. 10, pp. 17–25, 2016 (https://doi.org/10.1515/jag-2015-0025).

[11] N.S. Muzhikyan and A.S. Sargsyan, "Investigation of the Electromagnetic Field in the Focal Region of a Dual-reflector Spherical Antenna", *Vestnik NPUA*, vol. 2, pp. 83–89, 2015 (in Russian).

[12] J. Ruze, "Antenna Tolerance Theory – A Review", *Proceedings of the IEEE*, vol. 54, pp. 633–640, 1966 (https://doi.org/10.1109/PROC.1966.4784).

[13] P.F. Scott and M. Ryle, "A Rapid Method for Measuring the Figure of a Radio Telescope Reflector", *Monthly Notices of the Royal Astronomical Society*, vol. 178, pp. 539–545, 1977 (https://doi.org/10.1093/mnras/178.4.539).

[14] J.W.M. Baars, R. Lucas, J.G. Mangum, and J.A. Lopez-Perez, "Near-field Radio Holography of Large Reflector Antennas", *IEEE Antennas and Propagation Magazine*, vol. 49, pp. 24–41, 2007 (https://doi.org/10.1109/MAP.2007.4395293).

[15] V.N. Mitrokhin and E.O. Mozharov, "Radio-holographic Method for Monitoring the Profile of Parabolic Reflector Antennas Based on the Electromagnetic Field in the Near Zone", *Vestnik MGTU im. N.E. Baumana*, pp. 81–95, 2015 (in Russian).

[16] E.O. Mozharov and S.A. Rastvorov, "Analysis of the Surface Quality of Reflector Antennas Using a Geodetic Total Station", Antenny, no. 11, pp. 3–9, 2017.

Arevik Sargsyan, Ph.D.
Institute of ICTE (Information and Communication Technologies and Electronics)
https://orcid.org/0009-0003-5604-9137
E-mail: antenna@seua.am
National Polytechnic University of Armenia,
Yerevan, Armenia
https://polytech.am/en/home/

Narek Hambardzumyan, M.Sc.
Institute of ICTE (Information and Communication Technologies and Electronics)
https://orcid.org/0009-0000-5533-7696
E-mail: n.hambardzumyan@polytechnic.am
National Polytechnic University of Armenia,
Yerevan, Armenia
https://polytech.am/en/home/

Optimized Fuzzy Secure Scheme for Trust Assessment in IoMT

Olena Semenova, Olha Voitsekhovska, Andrii Dzhus, and Vladyslav Kuzniak

Vinnytsia National Technical University, Vinnytsia, Ukraine

https://doi.org/10.26636/jtit.2026.2.2494

Abstract — Rapid development of technologies associated with the Internet of Medical Things (IoMT) has enabled continuous patient monitoring, diagnosis, and integration of medical devices with various healthcare infrastructures. However, the increasing heterogeneity of IoMT systems and their connectivity-related features introduce also security risks, such as data tampering, unauthorized access, and unsafe behavior of the devices themselves. Traditional trust assessment techniques often fail to handle the uncertainty inherent in medical data and devices. This paper presents a fuzzy logic-based secure trust assessment scheme designed for IoMT, which integrates behavioral and communication indicators to compute trust scores for a device. The scheme employs a fuzzy logic-based approach and provides a trust level evaluation procedure suitable for resource-limited IoMT devices. A fuzzy inference system was developed specifically for this scheme and further optimized by applying evolutionary algorithms. The experimental results demonstrate an improved accuracy of the optimized model in evaluating the trust level of devices and show its enhanced accuracy compared to a classical trust mechanism.

Keywords — IoMT, fuzzy logic, trust management, security, optimization

1. Introduction

The emergence of IoMT in healthcare care has transformed the manner in which medical services are provided, as it is capable of significantly enhancing patient care through online monitoring, the use of wearable technology, and the ability to access medical consultations quickly and remotely. However, as IoT technologies continue to evolve, protecting sensitive health information has emerged as a significant challenge for researchers [1]. As data are collected, transmitted, and stored by medical devices, there is, unfortunately, a corresponding increase in cyber incidents, data breaches, and privacy violations associated with medical equipment [2].

The use of IoT devices may result in unauthorized access to confidential patient data, including email accounts, passwords, and private records [3]. Security, privacy, and safety are important factors and pose significant challenges in the implementation of IoT systems. IoT applications encompass numerous devices and generate substantial data volumes. Therefore, in order to ensure data security, it is essential to guarantee that the communicating IoT devices interact in a trustworthy manner [4].

Cryptography and access control are the two conventional approaches to safeguarding IoT networks. If properly implemented, they can be considered hard measures that ensure system security. However, since hacked network nodes might produce false or misleading information while still offering legitimate cryptographic credentials, cryptography alone is not capable of ensuring security in heterogeneous IoT systems. Similarly, typical centralized access control is inappropriate for distributed contexts and access control mechanisms are susceptible to internal harmful attacks. However, trust management, which is regarded a soft security mechanism, can address the aforementioned problems by improving, rather than replacing hard security procedures [5].

Trust management is employed to evaluate and ensure network reliability by assigning a trust value, i.e. its trust level, to each node. Consequently, the information sent by a node with a high trust level is considered reliable [6].

Therefore, trust management has emerged as an important components of IoT security. By analyzing behavioral patterns, data integrity, and communication quality, trust assessment mechanisms aim to quantify the reliability of devices. Traditional trust evaluation models – such as binary classification, threshold-based detection, and probabilistic schemes – offer a quite limited degree of effectiveness when applied in IoT systems. Furthermore, resource-limited medical devices of IoMT may experience communication errors or interruptions that should not be misinterpreted as malicious behavior. These challenges require efficient trust assessment techniques that are capable of differentiating between benign fluctuations and genuine threats.

Artificial intelligence (AI) techniques are a promising solution for assessing trust in IoMT networks, as they involve a data-centric evaluation of device-related and traffic behavior. Unlike traditional static or rule-based mechanisms, AI approaches can consider non-linear dependencies among medical data streams, allowing trust level estimation under complicated network conditions. Approaches based on fuzzy logic, neural networks, and evolutionary optimization offer advanced reasoning, parameter tuning, and efficient searching of complex parameter spaces – features which are essential for handling uncertainty in medical data communication.

Furthermore, AI-based trust modeling may provide continuous improvement as new traffic patterns or threat vectors emerge, ensuring that trust evaluation remains relevant to security challenges. This makes the fuzzy logic theory partic-

ularly suitable for implementation in IoMT, where decisions often depend on slight variations in physiological data.

This paper proposes a fuzzy logic-based trust assessment scheme for IoMT networks. The proposed model integrates several trust indicators concerning both behavioral anomalies and reliability of communication. The designed model computes the trust scores of a device. The resulting trust values may be utilized to establish secure interaction between devices or provide access control, thus increasing resilience against threats.

2. Problem Definition

The IoMT can be regarded as a set of connected medical devices, wearable sensors, implantable technologies, and clinical information systems that work together to ensure continuous provision of healthcare to the population. The complexity of IoMT networks stems from the heterogeneity of its devices: from low-power wearable monitors to complex systems and smart equipment. IoMT technology is defined by its vulnerable and unsafe nature, as medical devices operate in a sphere in which even small inaccuracies or delays can lead to severe consequences for patients' health.

As IoMT systems become increasingly connected, they are also exposed to emerging cybersecurity threats. Attackers can manipulate physiological data streams, impersonate medical devices, inject unauthorized control commands, or exploit vulnerabilities in wireless communication protocols. Furthermore, data collected by these devices are often noisy, incomplete, or suffer from sudden fluctuations and distortions caused by patient movement or environmental factors. These uncertainties complicate the discovery of benign anomalies and malicious actions. Finally, regulatory frameworks can impose strict requirements related to confidentiality and integrity, thus requiring the introduction of effective security mechanisms.

Although IoMT holds considerable potential, concerns about security and privacy have hindered its extensive implementation within the healthcare sector [7], [8]. This problem is exacerbated by the introduction of new technologies, including mobile devices, cloud services, and remote applications that are being integrated into the healthcare system [9].

The lack of attention to security and privacy in IoMT hinders the complete utilization of these technologies to address existing issues in healthcare. Thus, it is essential to define security and privacy within the healthcare sector.

Although these technologies improve data processing in the healthcare sector, they also significantly increase the risk of security and privacy breaches of medical information. The growing reliance on these technologies can lead to an increased vulnerability of health data, leaving health-related information open to various threats and misuse, which could result in sever consequences for both patients and organizations [10].

The need for effective methods capable of identifying attacks and malicious devices within IoT networks stems from their vulnerability to threats and attacks. The lack of adequate focus on security and privacy in healthcare IoT technologies is a major obstacle preventing these technologies from being effectively used to address current problems. Therefore, a need to investigate security-related factors exists.

Given these challenges, accurate assessment of the reliability of IoMT devices continues to remain a complex problem. Traditional trust assessment methods, which use deterministic thresholds or probabilistic evaluations, often fail to take into account the variability of wireless communication environments. Moreover, they are typically quite rigid when faced with incomplete information.

These limitations justify the need for a more uncertainty-aware trust assessment mechanism.

3. Literature Review

Researchers encounter several obstacles in the IoT area, such as guaranteeing a sufficient level of security while exchanging data, ensuring trust between IoT components, addressing concerns related to data confidentiality in IoT technologies, creating safe communication with various components on the edge network, and finding ways to save energy by applying reliable smart devices and infrastructure [11].

The degree of trust placed in engineering solutions depends on their capability to interprtet data in various psychological and economic contexts and varies rather considerably. Additionally, it differs with the contexts in which they are applied [12].

Trust is closely related to guaranteeing the security of a given system and the safety of its users. It involves not only security, but also other elements, including integrity, resilience, dependability, accessibility, and capability, making it more complex and challenging to provide [13].

In [14], trust is defined as a key feature for establishing trust between devices in order to guarantee secure services and applications.

An IoT device interacts with the physical environment to collect data and operates by relaying on communication technologies. However, IoT devices may become faulty, compromised, or can misbehave due to internal factors or external threats, such as cyberattacks. In such cases, the data collected and transmitted by these devices can become unreliable, which may significantly affect the decision making process, particularly in critical domains such as IoT-based healthcare. Establishing trust in devices and the data they generate can increase end-user confidence in IoT systems. Estimated trust status (trusted, uncertain, or untrustworthy) is to be used as a reputation indicator for healthcare applications [15].

In [16], a trust management mechanism based on architecture modeling is proposed. The IoT is decomposed into three layers, each of them controlled by a special purpose trust management system (self-organized, affective routing and multi-service). The final decision making process is conducted based on trust-related information.

To ensure data and information security, it is essential to verify that any IoT device that interacts with other system elements is trustworthy. To address these challenges, various methods have been proposed, for example, in [17], [18]. Several trust frameworks have been proposed to address the issue of node security to protect devices from being attacked or damaged, which can lead to unavailability of resources [19]–[21].

In [22], a centralized trust management scheme was created for lightweight IoT devices. This system facilitates service exchange between devices, as it manages trust certificates without performing trust calculations. In terms of cooperation and compatibility, additional observations of direct trust are quantified. Recommendations, meanwhile, are used to assess indirect trust.

The authors of [23] introduced a behavior-based reputation system to establish trust between nodes. They proposed an architecture that integrates software-defined networks within the IoT and a cross-layer authorization protocol in trust management. In [24], a dynamic trust management model was created that allows network nodes to autonomously assess the behavior of their peer nodes and dynamically assign rewards and penalties. This method identifies malicious nodes, categorizing them into three levels: mild, moderate, and severe.

Artificial intelligence methods are also widely used in trust assessment. Paper [25] considers the behavior of users in the trusted model to identify anomalous patterns. The established model takes into account specific indicators, such as security, authentication, operation, and efficiency, to assess the user's past behaviors and compare them with the current state of the their actions. The framework developed utilizes fuzzy logic to evaluate both comprehensive and direct trust values.

The technique introduced in [26] is based on fuzzy logic and aims to identify untrusted nodes. The authors created a reliable messaging method for IoT communication among nodes to ensure the security of the entire IoT system. However, the model suffers from certain limitations related to scalability, energy efficiency, and data storage.

A trust management scheme constructed on the principles of Bayesian learning and collaborative filtering was proposed in [27]. To quickly reflect behavioral changes, the scheme is regularly updated after a designated interval, applying a decay factor to the currently computed scores. Nevertheless, Bayesian inference presents certain limitations in trust calculations, including the challenge of trust subjectivity with the element of randomness.

The study described in [28] introduced a trust calculation model that is capable of yielding precise trust evaluations. The approach quantitatively assesses individual trust characteristics and categorizes them to derive the ultimate trust values. The investigation presented in [29] examined a trust model which offers an effective approach to routing protocols for lossy networks, allowing to categorize untrustworthy nodes. The designed model utilizes the logistic regression technique to assess the behavior of a specific node.

The investigation described in [30] proposed a trust-oriented model utilizing a decision tree algorithm to detect malicious activities within the Internet of Battlefield Things environment. In [31], the authors introduced conditional packet manipulation attacks, known as targeted insider attacks. The presented scheme maintains restricted trust performance metrics for every node, indicating the potential for initial attacks, such as forwarding packets with specific values.

The investigation presented in [32] introduced an adaptive trust protection scheme designed specifically for industrial IoT networks, using a deep neural network alongside a supervised learning algorithm. This approach successfully identified various types of attacks without the need for any prior knowledge of their characteristics and eliminated the need for manual intervention.

LSTM and multi-attribute rating techniques for trust management in IoT devices were proposed in [33]. A multi-attribute rating algorithm was applied to compute the trust values, while LSTM was utilized to determine the trust threshold based on behavioral changes.

Although previous studies presented a general examination of security- and privacy-related issues affecting IoT, a significant gap continues to exist in the literature as far as the layered structure of IoT is concerned, specifically within the healthcare context [34].

Paper [35] proposes a fuzzy trust management mechanism to prevent Sybil attacks in IoMT. Moreover, this mechanism can recognize untrustworthy nodes in the system. Study [36] proposes a blockchain-based fuzzy trust management framework to detect Sybil nodes in IoMT networks, while [37] discusses an intelligent trust cloud management method where individual trust clouds of IoMT devices are established by fuzzy trust recommending. The suggested trust classification scheme can determine whether an IoMT device is malicious and can be relied upon for secure clustering.

Although the number of published studies focusing on trust assessment in IoT networks is quite substantial, insufficient attention has been devoted to hybrid approaches that integrate several AI techniques and combine their advantages in order to improve model accuracy – a feature this paper focuses on.

4. Methodology

In this paper, fuzzy logic was chosen over other AI techniques because it does not require large training datasets and can operate effectively, since fuzzy logic deals with expert knowledge and linguistic rules, which makes it well suited for cases in which IoMT data may be limited or inprecise. Moreover, unlike black-box models (e.g. deep neural networks), fuzzy systems provide high interpretability and are transparent operationaly, while retaining low computational complexity.

At the foundation of the scheme lies the selection and integration of indicators that reflect the secure behavior of a specific IoMT device. The architecture of the proposed fuzzy logic-based trust assessment scheme for IoMT is shown in Fig. 1.

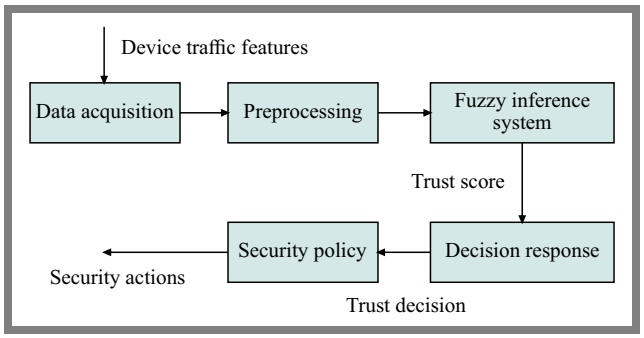

Fig. 1. Fuzzy-based secure trust assessment scheme.

The trust assessment scheme for IoMT medical devices comprises several functional units. The data acquisition unit collects the behavior characteristics of traffic from medical devices of the IoMT network. The preprocessing unit performs the data cleaning and normalization stage. Next, the fuzzy inference system processes the normalized numerical features and gives the trust score of each device. The decision response unit interprets the trust score produced by the FIS and determines the appropriate reaction, such as classifying devices as trusted, suspicious or malicious. By applying relevant security rules, the security policy unit implements this trust-related decision (access control, device isolation, and alert generation) to protect the IoMT network.

The trust assessment scheme can be used as part of a security management module integrated into IoMT gateways, edge servers, or organization network controllers to evaluate the trustworthiness of connected devices. Based on the calculated trust score, the scheme can control network access by prioritizing trusted devices for data transmission, and may restrict or isolate devices with suspicious behavior.

The core component of the proposed trust assessment scheme is the fuzzy inference system (FIS), which performs the decision-making process. It processes several indicators – behavioral and network characteristics of IoMT devices – and transforms them to a unified continuous trust score. To transform these features into a trust score, the FIS applies a fuzzification process that converts numerical indicator values into linguistic terms such as “low”, “medium” or “high”. These terms are represented by membership functions. Next, the inference stage takes place, where the fuzzy inference engine applies the rule base which encodes expert knowledge to produce fuzzy outputs. Then, defuzzification is performed to produce a single value trust score that represents the device’s current level of trustworthiness on a continuous numerical scale.

To evaluate the performance of the trust assessment phase, the FIS should be validated using a real dataset. In this study, the CICIoMT2024 dataset is applied, as it offers a comprehensive and up-to-date representation of network traffic and cyberattacks, which are specific for IoMT. This data set includes various attack scenarios and realistic benign traffic, thus allowing to objectively evaluate and validate the specific intrusion and attack detection methods [38].

The proposed FIS has four inputs, which correspond to selected features of the CICIoMT2024 dataset and determine essential traffic and security-related properties, enabling the FIS to model both normal and malicious patterns effectively. These chosen features are inter-arrival time, flow duration, tot_size, and SYN flag number.

The inter-arrival time feature measures the time difference between subsequent packets sent by a medical device, reflecting its communication behavior. This feature can indicate anomalies, such as irregular or suspicious transmission patterns that may indicate compromised or misbehaving devices.

The flow duration feature represents the total time of a given network flow, showing the duration of the period over which the device communicates during a session. Abnormal flow durations – either unusually short or excessively long – may indicate suspicious activity or potential security breaches. The Tot_size feature represents the total size of packets transmitted in a network flow, reflecting the volume of data exchanged by a device. Unusually large or small values can indicate abnormal behavior, such as data exfiltration or communication suppression.

The Syn flag number feature counts the TCP packets from a device, reflecting how often it attempts to establish communication. Abnormally high Syn counts may indicate suspicious behaviors such as scanning, flooding, or unauthorized connection attempts.

The output of the proposed FIS is the trust score, which represents the reliability or trustworthiness of an IoMT device evaluated based on its observed network behavior. In this study, the Mamdani-type FIS was selected due to its common rule-based structure and high interpretability, as well as a clear representation of expert knowledge in the trust assessment process. The Mamdani FIS represents a non-linear approach to mapping between a four-dimensional input vector $\mathbf{x} = [x_1, x_2, x_3, x_4]$ and a scalar output variable y. Each input variable $x_1, i = 1, \ldots, 4$, is characterized by three linguistic terms presented as Gaussian membership functions, while the output variable is described by five Gaussian membership functions. The Gaussian membership function corresponding to the j-th linguistic term of the i-th input can be expressed as:

$$\mu_{A_{ij}}(x_i) = \exp\left(- \frac{(x_i - c_{ij})^2}{2\sigma_{ij}^2} \right), \tag{1}$$

where c_{ij} and σ_{ij} are the center and standard deviation of the Gaussian function, respectively and $j = 1, 2, 3$.

Next, the k-th membership function of the output variable can be defined as:

$$\mu_{B_k}(y) = \exp\left(- \frac{(y - c_k)^2}{2\sigma_k^2} \right). \tag{2}$$

The fuzzy rule base designed for this case consists of 12 Mamdani type fuzzy if-then rules which encode expert knowledge about the system’s behavior. The r-th rule can be written as:

$$\begin{aligned} R_r : \text{if } x_1 \text{ is } A_{1j_1^r} \text{ and } x_2 \text{ is } A_{2j_2^r} \text{ and } x_3 \text{ is } A_{3j_3^r} \\ \text{and } x_4 \text{ is } A_{4j_4^r} \text{ then } y \text{ is } B_{k^r}\ , \end{aligned} \tag{3}$$

where $r = 1, \ldots, 16$, $j_i^r \in \{1, 2, 3\}$, and $k^r \in \{1, \ldots, 5\}$ are the indices of the previous and next membership functions, respectively.

The firing strength of the r-th rule is calculated using the minimum t-norm as:

$$\alpha_r = \min\left\{\mu_{A_{1j_1^r}}(x_1), \ldots, \mu_{A_{4j_4^r}}(x_4)\right\} . \tag{4}$$

Each fuzzy rule contributes to the output fuzzy set by modifying its consequent membership function according to its firing strength:

$$\mu_{B_r}^{\text{out}}(y) = \min\left\{\alpha_r, \mu_{B_{k^r}}(y)\right\} . \tag{5}$$

The aggregated output fuzzy set is obtained by applying the maximum operator over all rules:

$$\mu_{\text{agg}}(y) = \max_{r=1,\ldots,16} \mu_{B_r}^{\text{out}}(y) . \tag{6}$$

Finally, the final crisp output is calculated using the centroid defuzzification method:

$$y^* = \frac{\int y\mu_{\text{agg}}(y)dy}{\int \mu_{\text{agg}}(y)dy} . \tag{7}$$

To improve the accuracy of the FIS, evolutionary algorithms are employed to optimize the parameters of the membership functions and the structure of the fuzzy rule base.

First, the developed FIS is optimized by applying a genetic algorithm (GA). Here, a GA chromosome is encoded as a vector that includes all membership function parameters and the indices defining the fuzzy rules. The membership function parameters are encoded as:

$$\mathbf{z}_{\text{MF}} = \left[c_{11}, \sigma_{11}, \ldots, c_{43}, \sigma_{43}, c_1, \sigma_1, \ldots, c_5, \sigma_5\right] , \tag{8}$$

while the fuzzy rules are encoded as:

$$\mathbf{z}_{\text{R}} = \left[j_1^1, j_2^1, j_3^1, j_4^1, k^1, \ldots, j_1^{16}, j_2^{16}, j_3^{16}, j_4^{16}, k^{16}\right] , \tag{9}$$

where the previous indices j_i^r and subsequent indices k^r are integer-coded.

The complete chromosome can be written as:

$$\mathbf{z} = \left[\mathbf{z}_{\text{MF}}, \mathbf{z}_{\text{R}}\right]^{\cdot} , \tag{10}$$

For a given chromosome $\mathbf{z}$, the parameters of the fuzzy inference system are determined and its performance is evaluated through a fitness function expressed as the mean squared error between the desired output y^{ref} and the actual output y^*:

$$J(\mathbf{z}) = \frac{1}{N}\sum_{n=1}^{N}\left(y_n^{ref} - y_n^*(\mathbf{z})\right)^2 , \tag{11}$$

where N is the number of training samples.

The genetic algorithm iteratively minimizes $J(\mathbf{z})$ by applying selection, crossover, and mutation operators to evolve the chromosomes toward an optimal FIS configuration.

Another evolutionary algorithm, particle swarm optimization (PSO), is applied to the same FIS. In PSO, each particle represents a candidate solution with the same dimensionality and structure as the GA chromosome:

$$\mathbf{x}_p = \left[\mathbf{x}_{p,MF}, \mathbf{x}_{p,R}\right] \in \mathbb{R}^D , \tag{12}$$

where D is the total number of optimized parameters and denotes the particle index.

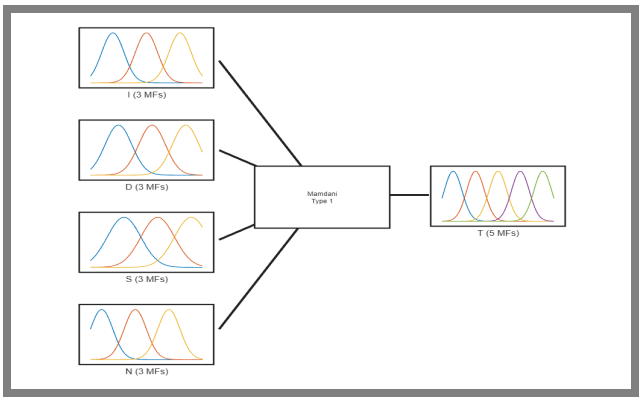

Fig. 2. Fuzzy inference system developed in Matlab.

Each particle is associated with a velocity vector $\mathbf{v}_p \in \mathbb{R}^D$, and its evolution in the search space is determined by:

$$\begin{aligned}\mathbf{v}_p(t+1) = \omega\mathbf{v}_p(t) + c_1 r_1\left[\mathbf{p}_p - \mathbf{x}_p(t)\right] \\ + c_2 r_2\left[\mathbf{g} - \mathbf{x}_p(t)\right] ,\end{aligned} \tag{13}$$

$$\mathbf{x}_p(t+1) = \mathbf{x}_p(t) + \mathbf{v}_p(t+1) , \tag{14}$$

where ω is the inertia weight, c_1 and c_2 are cognitive and social acceleration coefficients, respectively, r_1 and r_2 are vectors of random variables uniformly distributed in [0, 1], $\mathbf{p}_p$ denotes the personal best position found by particle p and $\mathbf{g}$ represents the global best position discovered by the swarm. During evaluation, the rule-related components of $\mathbf{x}_p$ are discretized to the nearest valid linguistic index. The fitness of each particle is computed using the same objective function $J(\cdot)$ as in the genetic algorithm.

To sum up, the proposed mathematical models provide a comprehensive description of a Mamdani-type fuzzy inference system and its optimization using two evolutionary algorithms and can be utilized to develop the required trust assessment FIS.

5. Simulations

Matlab can be used to examine and verify the operation of the developed FIS for trust assessment in IoMT. Running FIS simulations in Matlab enables fast model prototyping, structured performance testing, and convenient experimental analysis. Moreover, it is possible to integrate FIS with optimization toolboxes and machine learning techniques such as

	Rule	Weight	Name
1	If IT is L and FD is L and TS is L and FN is L then TS is VH	1	rule1
2	If IT is L and FD is M and TS is L and FN is L then TS is H	1	rule2
3	If IT is M and FD is L and TS is M and FN is L then TS is H	1	rule3
4	If IT is M and FD is M and TS is M and FN is L then TS is M	1	rule4
5	If IT is H and FD is M and TS is H and FN is M then TS is L	1	rule5
6	If IT is M and FD is H and TS is H and FN is M then TS is L	1	rule6
7	If IT is L and FD is H and TS is H and FN is H then TS is VL	1	rule7
8	If IT is H and FD is H and TS is M and FN is H then TS is VL	1	rule8
9	If IT is M and FD is M and TS is H and FN is L then TS is M	1	rule9
10	If IT is H and FD is L and TS is M and FN is M then TS is M	1	rule10
11	If IT is L and FD is M and TS is M and FN is H then TS is L	1	rule11
12	If IT is H and FD is H and TS is H and FN is H then TS is VL	1	rule12

Fig. 3. Rule base of the FIS.

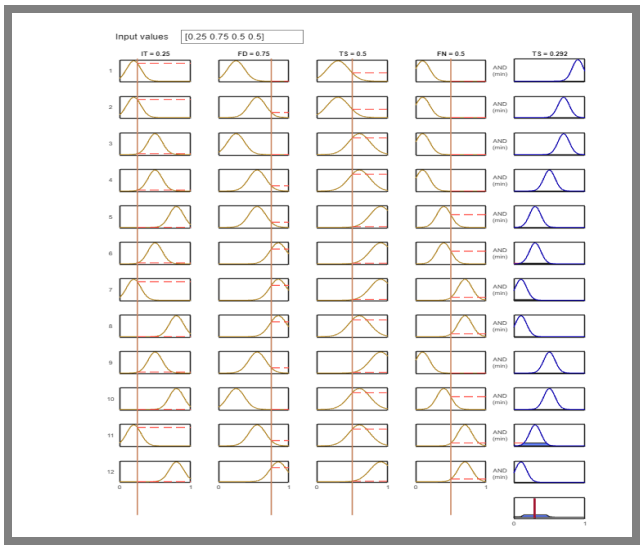

Fig. 4. FIS simulation results.

neural networks, which increases the effectiveness of fuzzy inference systems and promotes their improvement.

The initial phase of creating the FIS interface involved assigning input and output variables. The membership functions for the inputs and outputs were defined as well (Fig. 2).

The rule base was specified (Fig. 3). Following this, we allocated the input values and executed the simulation process to generate outputs, thus verifying the functionality of the proposed FIS.

To verify the operability of the developed FIS, a series of simulations was performed. Figure 4 illustrates a scenario with the following input values: the interarrival time value I_T was 0.25, the flow duration value F_D was 0.75, the total size value T_S was 0.5, and the Syn flag number value F_N was 0.5. The simulated FIS yielded the trust score of the device equal to 0.292. This means that this device has a low trust score and can be regarded malicious.

The GA was then applied to adjust both the parameters of the Gaussian membership functions and the structure of the fuzzy rule base, allowing the FIS to better reflect the nonlinear relationships within the features of the CICIoMT2024 dataset.

The convergence analysis of the GA-based optimization shows that the evolutionary search successfully refined the parameters of the proposed FIS within 86 iterations (Fig. 5). The convergence behavior verifies that the GA reached a near-optimal solution. After optimization, the Gaussian membership functions were better positioned around informative data regions. The GA also refined the rule base.

The Mamdani-type FIS was also optimized using the PSO tool. Representing each particle as a candidate FIS configuration and iteratively updating particle positions according to individual and global best performance values, PSO also adjusted the parameters of the Gaussian membership functions and refined the fuzzy rule base. The PSO-based optimization of the proposed FIS reached convergence after 310 iterations, demonstrating a gradual but steady improvement in the fitness value as the swarm explored the search space (Fig. 6).

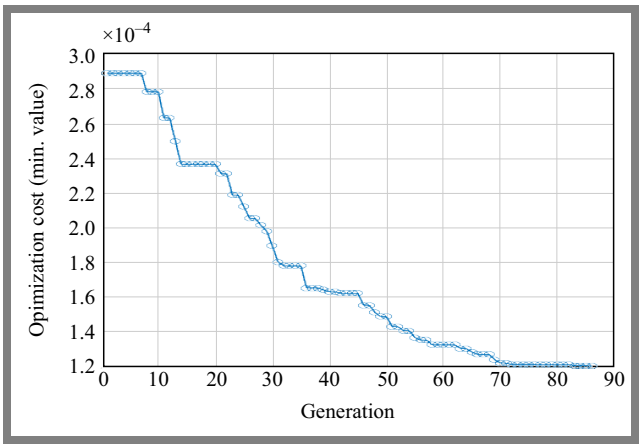

Fig. 5. FIS optimization with GA.

The performance of the original FIS, GA-optimized FIS, and the PSO-optimized FIS were validated in Matlab to ensure that the proposed trust assessment scheme demonstrates measurable improvement throughout the optimization stages. During validation, the FIS variants were evaluated according to a predefined fitness metric that reflects the accuracy of the trust estimate. Through this validation procedure, the authors verified whether GA and PSO optimization provided significant performance gains over the original FIS. The validation results show that both optimization algorithms improved the performance of the original FIS, while the PSO-optimized FIS showed the highest accuracy in estimating trust scores from IoMT traffic features (Fig. 7).

The original FIS produced comparatively less precise trust scores, caused by limitations of manually configured membership functions and fuzzy rules. The validation results indicate that optimization significantly improves the performance of the proposed FIS for trust assessment in IoMT. Despite the lower error, the GA-optimized FIS outperformed the original FIS. The PSO-optimized FIS achieved the best results, as it surpassed both the original and the GA-enhanced models. This improvement confirms that swarm-based optimization provided better parameter refinement and convergence.

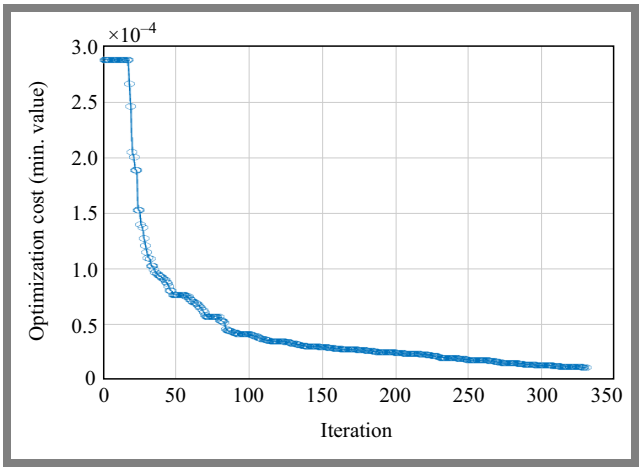

Fig. 6. FIS optimization with PSO.

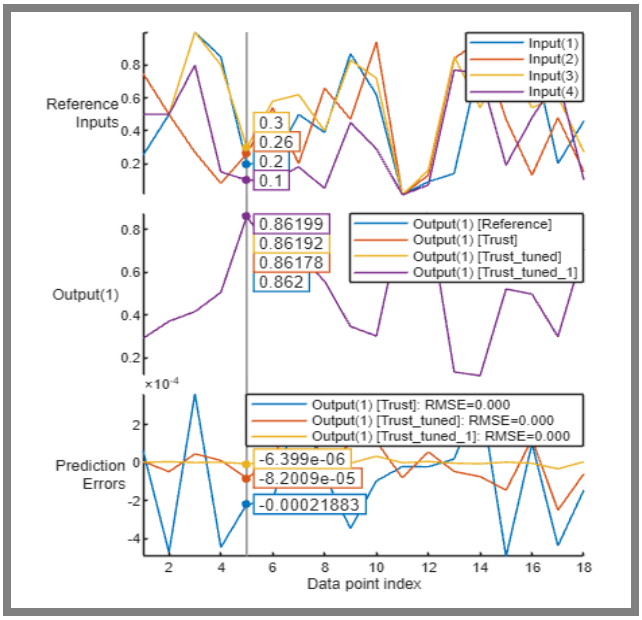

Fig. 7. FIS validation results.

6. Evaluation

To evaluate and compare the performance of the trust assessment models, simulations were performed in Matlab using traffic features extracted from the CICIoMT2024 dataset. Four models were examined: the original Mamdani type FIS, its GA-optimized and PSO-optimized variants, and a weighted sum trust scheme (WSTS), which is a traditional non-AI trust assessment method.

Figure 8 illustrates the trust scores across sample measures related to how the four models assign trust values to IoMT traffic samples. The weighted-sum method produces relatively smoother and less discriminative trust variations. The original FIS exhibits more adaptive trust fluctuations, as it has improved sensitivity to non-linear relations in the input data. GA-optimized FIS gives more stable high-trust scores for benign samples and lower trust scores for suspicious ones. The PSO-optimized FIS shows the clearest separation between trusted and untrusted samples.

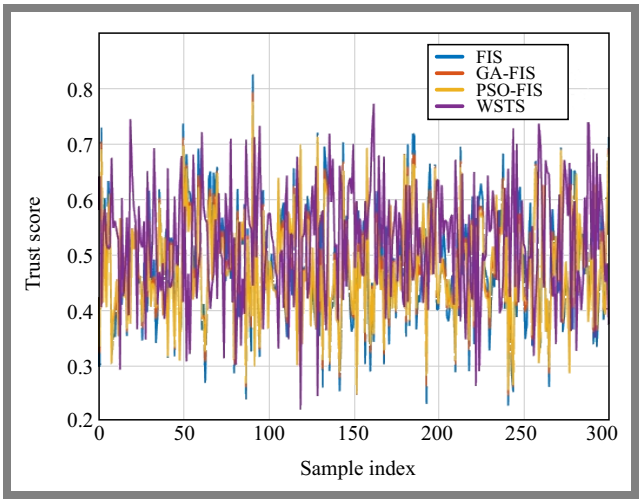

Fig. 8. Trust scores across samples.

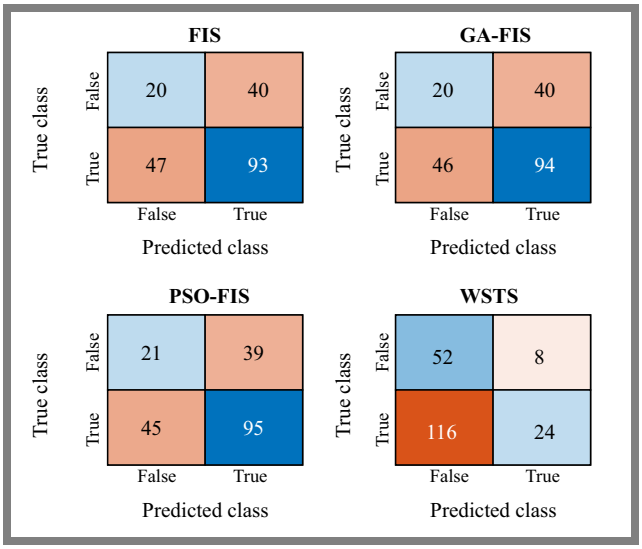

Fig. 9. Confusion matrices for models considered.

The confusion matrix plots confirm these trends, showing a reduced number of misclassified samples in both optimized models, where PSO-FIS shows the lowest false-negative rate (Fig. 9).

Receiver operating characteristic (ROC) curves and the corresponding area under the curve (AUC) values highlight the discriminatory strength of each method. The PSO-FIS curve was placed farthest from the random-guess diagonal line, indicating superior separability between trusted and untrusted samples, followed by GA-FIS, the original FIS, and finally WSTS (Fig. 10).

The simulation results demonstrate a significant advantage of the intelligent approach to trust assessment, as the developed fuzzy-based trust assessment model outperforms the traditional method in terms of accuracy and classification reliability.

The integration of fuzzy inference with optimization techniques leads to more precise modeling of complex and nonlinear relationships among IoMT traffic features, i.e., to improved discrimination between trusted and malicious devices.

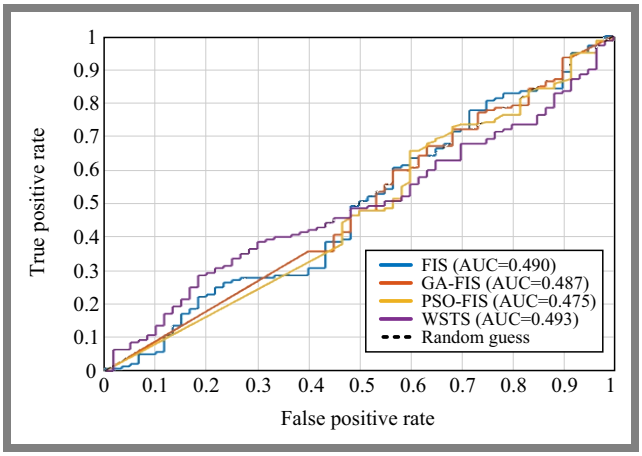

Fig. 10. ROC and AUC curves.

7. Discussion

The proposed fuzzy secure scheme for trust assessment can be implemented within a layered IoMT architecture, consisting of three layers: the perception layer, the edge/fog layer, and the cloud layer (Fig. 11). The trust assessment scheme is implemented at the edge layer. Deploying at the edge provides several advantages, such as reduced latency to transfer decisions, visibility of aggregated traffic, and sufficient computational capacity. Based on the calculated trust score, the edge/fog layer enforces security policies. Devices with high trust scores are allowed to communicate normally, while devices with low trust scores may be restricted or isolated.

The cloud layer performs the general analytics and model optimization. While trust decisions are made at the edge, the cloud environment can periodically update fuzzy rules or membership function parameters using GA or PSO techniques. The updated parameters are then transmitted back to the edge layer.

Depending on a device's current trust score, it may be assigned one of the five states. An IoMT device assigned with a very high trust score is considered to be in a highly trusted state. This means it exhibits a baseline behavior. The gateway routes its traffic to the intended destination, e.g., the local hospital server or remote cloud with prioritized quality of service. An IoMT device assigned with a high trust score is considered to be in a trusted state (reliable). Continuous monitoring persists, ensuring that the device remains within acceptable operational parameters without triggering punitive measures. Traffic is routed with standard priority. An IoMT device assigned with a medium trust score is considered to be in a suspicious state. The gateway executes preventive measures without severing the connection, recognizing that data availability is doubtful. Actions may include limiting the alert generation rate.

An IoMT device assigned with a low trust score is considered to be in a restricted state. This means that when anomalies become more severe, indicating a likely compromise, the device is to be quarantined. Medical telemetry is maintained only if this can be done safely; strict control actions and deep packet inspection are to be enforced. An IoMT device assigned with a very low trust score is considered to be in an isolation state. The gateway performs an immediate and aggressive isolation. Actions can include network segregation or traffic reduction.

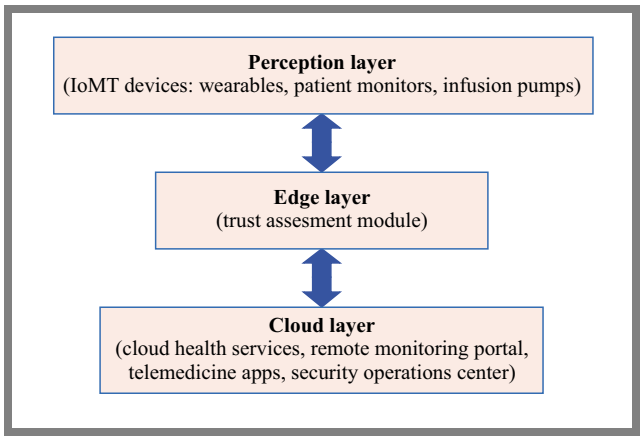

Fig. 11. IoMT layered architecture.

As this evaluation occurs directly at the edge gateway, suspicious behavior can be detected quickly without requiring continuous communication with cloud servers.

The developed optimized fuzzy secure scheme for trust assessment in IoMT can be deployed at the edge gateway, such as a smart router, as a JavaScript-based software module. The Node.js environment can be applied due to its open source nature and asynchronous architecture, as it is able to handle many network connections at once without slowing down. This makes it a good option for IoMT conditions as the gateway must constantly manage data streams from many various medical sensors at the same time.

The authors suggest that we divide the software into three parts. The first (feature extractor) unit runs a packet capture tool in Node.js, allowing it to monitor all the traffic flowing through the gateway's ports without interrupting it. It captures the four specific features and sends them to the second unit – the fuzzy inference engine, which is the core component of the JavaScript software module and reproduces the fuzzy inference system structure of the developed during the modeling stage through custom JavaScript functions to yield a trust score. The third (decision) unit processes the obtained trust score value and sends direct commands to the gateway's operating system to apply one of the five security actions.

Such an implementation has several advantages. It supports real-time analysis of device behavior, enables cross-platform deployment, and can be easily integrated with existing network monitoring tools and healthcare management systems. Consequently, this approach provides a practical solution to deploy the optimized fuzzy trust assessment scheme in IoMT networks.

8. Conclusions

The proposed fuzzy secure scheme for trust assessment in the IoMT provides an accurate trust evaluation as it produces continuous trust scores, not binary decisions, thus allowing for more flexible security-related decisions, such as partial access rather than complete acceptance or rejection. Furthermore, it ensures low computational complexity, making it suitable for resource-limited medical devices.

The core component of the scheme – a fuzzy inference system – was developed, analyzed, and validated. The initial stage was to build a mathematical framework for Mamdani-type FIS, its inputs being four network traffic features from the CICIoMT2024 dataset, and its output being a trust score for an IoMT device. The FIS was developed in Matlab. Simulations confirmed the correctness of the developed FIS and its ability to adequately assess trust levels considering the selected traffic features.

However, as its parameters were assigned manually, the developed FIS may not achieve a sufficiently high degree of accuracy. To increase its precision, the FIS was further optimized

and fine tuned using two approaches – genetic algorithms and particle swarm optimization.

Experimental results confirmed that both optimization methods yielded notable improvements in the accuracy of trust estimation. The PSO-optimized FIS produced the most accurate trust predictions. Finally, the comparative analysis of four models – the original Mamdani type FIS, its GA-optimized and PSO-optimized variants, and a weighted sum trust scheme – demonstrated that optimization is essential to maximizing the accuracy of fuzzy trust mechanisms in IoMT.

In general, this study confirms that the application of artificial intelligence techniques significantly improves trust assessment models by increasing the level of accuracy without sacrificing their complexity. The results demonstrate the feasibility of fuzzy logic as an effective approach to trust management in IoMT communications.

References

[1] N. Khatoon, S. Roy, and P. Pranav, "A Survey on Applications of Internet of Things in Healthcare", in: *Internet of Things and Big Data Applications,* Springer International Publishing, pp. 89–106, 2020 (https://doi.org/10.1007/978-3-030-39119-5_6).

[2] Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IoT) of Smart Home: Privacy and Security", *International Journal of Computer Applications*, vol. 182, pp. 3–8, 2019 (https://doi.org/10.5120/ijca2019918450).

[3] J.J. Hathaliya and S. Tanwar, "An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0", *Computer Communications*, vol. 153, pp. 311–335, 2020 (https://doi.org/10.1016/j.comcom.2020.02.018).

[4] W. Najib, S. Sulistyo, and Widyawan, "Survey on Trust Calculation Methods in Internet of Things", *Procedia Computer Science*, vol. 161, pp. 1300–1307, 2019 (https://doi.org/10.1016/j.procs.2019.11.245).

[5] G.J. Blinowski, "Risk-based Decision Making in IoT Systems", *Proc. of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017*, pp. 230–241, 2017 (https://doi.org/10.1007/978-3-319-67220-5_21).

[6] A.M. Konsta, A.L. Lafuente, and N. Dragoni, "A Survey of Trust Management for Internet of Things", *IEEE Access*, vol. 11, pp. 122175–122204, 2023 (https://doi.org/10.1109/access.2023.3327335).

[7] A. Chacko and T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare", *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 4, art. no. e2, 2018 (https://doi.org/10.4108/eai.13-7-2018.155079).

[8] P.K.D. Pramanik, G. Pareek, and A. Nayyar, "Security and Privacy in Remote Healthcare", *Telemedicine Technologies*, pp. 201–225, 2019 (https://doi.org/10.1016/b978-0-12-816948-3.00014-3).

[9] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and Privacy in IoT-Cloud-Based e-Health Systems – A Comprehensive Review", *Symmetry*, vol. 12, art. no. 1191, 2020 (https://doi.org/10.3390/sym12071191).

[10] I. Sadek, S.U. Rehman, J. Codjo, and B. Abdulrazak, "Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations", *Lecture Notes in Computer Science*, vol. 11862, pp. 3–17, 2019 (https://doi.org/10.1007/978-3-030-32785-9_1).

[11] S. Albishi, B. Soh, A. Ullah, and F. Algarni, "Challenges and Solutions for Applications and Technologies in the Internet of Things", *Procedia Computer Science*, vol. 124, pp. 608–614, 2017 (https://doi.org/10.1016/j.procs.2017.12.196).

[12] C. Fernandez-Gago, F. Moyano, and J. Lopez, "Modelling Trust Dynamics in the Internet of Things", *Information Sciences*, vol. 396, pp. 72–82, 2017 (https://doi.org/10.1016/j.ins.2017.02.039).

[13] Z. Yan, P. Zhang, and A.V. Vasilakos, "A Survey on Trust Management for Internet of Things", *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014 (https://doi.org/10.1016/j.jnca.2014.01.014).

[14] W. Najib, S. Sulistyo, and Widyawan, "Survey on Trust Calculation Methods in Internet of Things", *Procedia Computer Science*, vol. 161, pp. 1300–1307, 2019 (https://doi.org/10.1016/j.procs.2019.11.245).

[15] A. Rauf, R.A. Shaikh, and A. Shah, "Trust Modelling and Management for IoT Healthcare", *International Journal of Wireless and Microwave Technologies*, vol. 12, pp. 21–35, 2022 (https://doi.org/10.5815/ijwmt.2022.05.03).

[16] L. Gu, J. Wang, and B. Sun, "Trust Management Mechanism for Internet of Things", *China Communications*, vol. 11, pp. 148–156, 2014 (https://doi.org/10.1109/cc.2014.6821746).

[17] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A Survey on the Security of IoT Frameworks", *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018 (https://doi.org/10.1016/j.jisa.2017.11.002).

[18] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, vol. 5, pp. 586–602, 2017 (https://doi.org/10.1109/tetc.2016.2606384).

[19] U. Jayasinghe, N.B. Truong, G.M. Lee, and T.-W. Um, "RpR: A Trust Computation Model for Social Internet of Things", *2016 Int. IEEE Conferences on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Tolouse, France, 2016 (https://doi.org/10.1109/uic-atc-scalcom-cbdcom-iop-smartworld.2016.0146).

[20] F. Fei *et al.*, "A K-anonymity Based Schema for Location Privacy Preservation", *IEEE Transactions on Sustainable Computing*, vol. 4, pp. 156–167, 2019 (https://doi.org/10.1109/tsusc.2017.2733018).

[21] F. Jiang *et al.*, "Deep Learning Based Multi-channel Intelligent Attack Detection for Data Security", *IEEE Transactions on Sustainable Computing*, vol. 5, pp. 204–212, 2020 (https://doi.org/10.1109/tsusc.2018.2793284).

[22] I.U. Din *et al.*, "LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things", *IEEE Internet of Things Journal*, vol. 10, pp. 2776–2783, 2023 (https://doi.org/10.1109/jiot.2021.3081422).

[23] J. Chen *et al.*, "Trust Architecture and Reputation Evaluation for Internet of Things", *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 3099–3107, 2018 (https://doi.org/10.1007/s12652-018-0887-z).

[24] S.W.A. Hamdani *et al.*, "Dynamic Distributed Trust Management Scheme for the Internet of Things", *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 29, pp. 796–815, 2021 (https://doi.org/10.3906/elk-2003-5).

[25] M. Alruwaythi and K.E. Nygard, "Fuzzy Logic Approach Based on User Behavior Trust in Cloud Security", *2019 IEEE International Conference on Electro Information Technology (EIT)*, Brookings, USA, 2019 (https://doi.org/10.1109/eit.2019.8834173).

[26] M.D. Alshehri and F.K. Hussain, "A Fuzzy Security Protocol for Trust Management in the Internet of Things (Fuzzy-IoT)", *Computing*, vol. 101, pp. 791–818, 2018 (https://doi.org/10.1007/s00607-018-0685-7).

[27] P. Singh *et al.*, "Service Versus Protection: A Bayesian Learning Approach for Trust Provisioning in Edge of Things Environment", *IEEE Internet of Things Journal*, vol. 9, pp. 22061–22070, 2022 (https://doi.org/10.1109/jiot.2021.3082272).

[28] U. Jayasinghe, G.M. Lee, T.-W. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services", *IEEE Transactions on Sustainable Computing*, vol. 4, pp. 39–52, 2019 (https://doi.org/10.1109/tsusc.2018.2839623).

[29] K. Prathapchandran and T. Janani, "A Trust-based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression", *Journal of Physics: Conference Series*, vol. 1850, art. no. 012031, 2021 (https://doi.org/10.1088/1742-6596/1850/1/012031).

[30] P. Kannimuthu and J. Thangamuthu, "Decision Tree Trust (DTTrust)-based Authentication Mechanism to Secure RPL Routing Protocol on Internet of Battlefield Thing (IoBT)", *International Journal of Business Data Communications and Networking*, vol. 17, pp. 1–24, 2021 (https://doi.org/10.4018/ijbdcn.2021010101).

[31] L. Liu *et al.*, "A Detection Framework Against CPMA Attack Based on Trust Evaluation and Machine Learning in IoT Network", *IEEE Internet of Things Journal*, vol. 8, pp. 15249–15258, 2021 (https://doi.org/10.1109/jiot.2020.3047642).

[32] M.M. Hassan *et al.*, "A Robust Deep-learning-enabled Trust-boundary Protection for Adversarial Industrial IoT Environment", *IEEE Internet of Things Journal*, vol. 8, pp. 9611–9621, 2021 (https://doi.org/10.1109/jiot.2020.3019225).

[33] Y. Alghofaili and M.A. Rassam, "A Trust Management Model for IoT Devices and Services Based on the Multi-criteria Decision-making Approach and Deep Long Short-term Memory Technique", *Sensors*, vol. 22, art. no. 634, 2022 (https://doi.org/10.3390/s22020634).

[34] N.A. Azeez and C.V. der Vyver, "Security and Privacy Issues in e-health Cloud-based System: A Comprehensive Content Analysis", *Egyptian Informatics Journal*, vol. 20, pp. 97–108, 2019 (https://doi.org/10.1016/j.eij.2018.12.001).

[35] A. Almogren *et al.*, "FTM-IoMT: Fuzzy-based Trust Management for Preventing Sybil Attacks in Internet of Medical Things", *IEEE Internet of Things Journal*, vol. 8, pp. 4485–4497, 2021 (https://doi.org/10.1109/jiot.2020.3027440).

[36] S.E. Ali *et al.*, "BFT-IoMT: A Blockchain-based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things", *Sensors*, vol. 23, art. no. 4265, 2023 (https://doi.org/10.3390/s23094265).

[37] L. Yang *et al.*, "An Intelligent Trust Cloud Management Method for Secure Clustering in 5G Enabled Internet of Medical Things", *arXiv*, 2022 (https://doi.org/10.48550/ARXIV.2207.09057).

[38] S. Dadkhah *et al.*, "CICIoMT2024: A Benchmark Dataset for Multi-protocol Security Assessment in IoMT", *Internet of Things*, vol. 28, art. no. 101351, 2024 (https://doi.org/10.1016/j.iot.2024.101351).

Olena Semenova, Ph.D.
Department of Infocommunication Systems and Technologies
https://orcid.org/0000-0001-5312-9148
E-mail: semenova.o.o@vntu.edu.ua
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua

Olha Voitsekhovska, Ph.D.
Department of System Analysis and Information Technologies
https://orcid.org/0000-0001-8504-1204
E-mail: o_voytsekhovska@vntu.edu.ua
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua

Andrii Dzhus, M.Sc.
Department of Infocommunication Systems and Technologies
https://orcid.org/0009-0005-3583-5766
E-mail: dzhuz1988@gmail.com
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua

Vladyslav Kuzniak, M.Sc.
Department of Information Radioelectronic Technologies and Systems
https://orcid.org/0009-0001-1775-420X
E-mail: kuzniakvl@gmail.com
Vinnytsia National Technical University, Vinnytsia, Ukraine
https://vntu.edu.ua

Improving Performance of GNSS Acquisition Systems by Optimizing TM-CFAR Thresholds Using Metaheuristics

Elbahdja Ourfella, Sabra Benkrinah, and Naceur Aounallah

Kasdi Merbah University, Ouargla, Algeria

https://doi.org/10.26636/jtit.2026.2.2518

Abstract — Signal acquisition is one of the key signal processing tasks performed by global navigation satellite system (GNSS) receivers. It involves detecting the presence or absence of a signal by comparing it with a predefined threshold, which can be either fixed or adaptive. This study focuses on optimizing the threshold of the trimmed mean constant false alarm rate (TM-CFAR) detector under Rayleigh fading conditions, employing metaheuristic optimization techniques, due to their proven efficacy in solving complex optimization problems. Furthermore, two TM-CFAR detectors are applied to the data and pilot channels of the GNSS system. Their outputs are then combined using two logical fusion strategies: AND and OR rules. Simulation results demonstrate that the optimized thresholds improve the performance of the GNSS signal acquisition system.

Keywords — GNSS, metaheuristic optimization techniques, Rayleigh fading channel, signal acquisition, TM-CFAR detector

1. Introduction

Global navigation satellite systems (GNSS) include satellite constellations such as GPS, Galileo, Glonass or BeiDou, developed to deliver precise positioning and timing information to users worldwide [1], [2]. Among these, the Global Positioning System (GPS) is the earliest and remains the only fully operational system enjoying widespread adoption. It comprises a constellation of 32 satellites designed to provide continuous service regardless of weather conditions, with growing global demand [3]. However, as shown in Fig. 1, GNSS signals, particularly those from GPS, are susceptible to significant degradation due to power attenuation and multipath fading, especially under challenging visibility or environmental conditions.

GNSS signals typically comprise two distinct components: data and pilot channels. The data channel transmits the navigation message, whereas the pilot channel, carrying a minimum amount of or no data at all, is primarily utilized for precise pseudorange estimates. Signal acquisition is a fundamental process in ensuring the accuracy and reliability of GNSS-based positioning. Advancements in signal processing algorithms and optimization methodologies continue to enhance the performance of GNSS receivers, particularly in challenging signal environments.

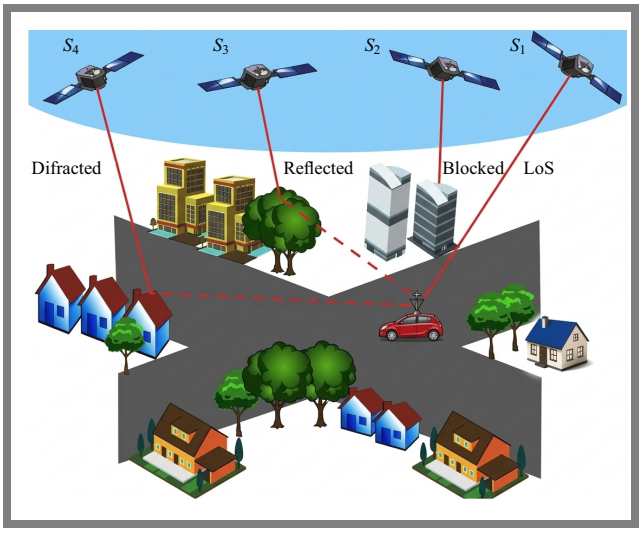

Fig. 1. GPS signal fading model.

In this context, the authors of [1] introduced an adaptive thresholding approach based on the cell-averaging constant false alarm rate (CA-CFAR) technique for the altBOC E5 signal under both Rayleigh and Gaussian fading conditions. Their findings indicated promising detection performance. In [2], an analytical formulation for the detection and false alarm probabilities in collective detection scenarios employing the CA-CFAR detector is proposed. To determine the optimal thresholds for CA-CFAR detectors, metaheuristic optimization techniques are applied in [4], in the context of Rayleigh fading channels. Four advanced metaheuristic algorithms, namely particle swarm optimization (PSO), biogeography-based optimization (BBO), firefly algorithm (FA), and simulated annealing (SA), are implemented and compared.

In satellite communication systems, multipath fading and interference make the signal environment non-homogeneous, reducing the effectiveness of the CA-CFAR detector. The TM-CFAR detector improves performance by ignoring the strongest and weakest signals in the reference window, thus helping to reduce the impact of random changes. This results

in a more precise detection threshold and a more stable false alarm rate. Therefore, TM-CFAR is more reliable than CA-CFAR in environments with interference and multipath effects [5].

This study explores the integration of the TM-CFAR detector which replaces its CA-CFAR counterpart during the acquisition phase of a GNSS receiver. By leveraging the enhanced robustness of TM-CFAR in non-homogeneous environments, the proposed approach aims to improve signal detection under challenging conditions. To optimize the detector's performance, metaheuristic optimization techniques are employed. This combination is expected to enhance the overall efficiency and reliability of the GNSS data acquisition process.

To achieve this objective, four different metaheuristic optimization algorithms are employed, and their performance is evaluated and compared in order to identify the most effective optimization strategy for enhancing the outcomes achieved with the use of the TM-CFAR detector. These include the following: particle swarm optimization (PSO), whale optimization algorithm (WOA), ant lion optimizer (ALO), and grey wolf optimizer (GWO).

The remainder of this paper is organized as follows. In Section 2, the proposed adaptive acquisition system operating in a Rayleigh-fading channel with the use of the TM-CFAR processor is presented. In Section 3, the system is analyzed and expressions for the detection and false-alarm probabilities as functions of the TM-CFAR parameters are provided. In Section 4, various metaheuristic optimization techniques are reviewed. In Section 5, the acquisition and detection performance of the proposed scheme are evaluated based on simulation results. Finally, concluding remarks are discussed in Section 6.

2. System Description

This study focuses on the signal acquisition phase, which is a critical stage in the GNSS receivers – see Fig. 2. This phase not only detects the presence or absence of the desired signal but also estimates its key parameters, such as code delay and Doppler frequency. The acquisition process is typically formulated as a joint detection and estimation problem, highlighting its importance in achieving accurate and reliable signal processing in GNSS systems [6].

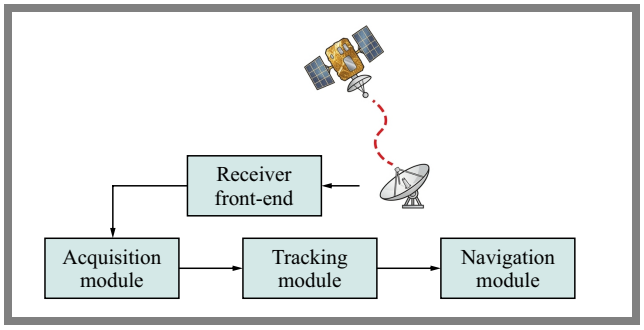

Fig. 2. GNSS receiver scheme.

The signal model under consideration comprises additive Gaussian noise, multiplicative noise, and the signal from the visible satellite. However, the analysis is simplified by assuming that multiplicative noise is sufficiently weak to be neglected, allowing the focus to remain on the effects of the additive noise and the satellite signal in the acquisition process [4], and it is described as follows:

$$r(t) = \sqrt{2C}\, c(t-\tau)\, \cos\left(2\pi F_D\, t + \phi\right) + n(t)\,, \qquad (1)$$

where C and $c(t)$ are the signal power and the spreading code, respectively. τ and F_D are the code delay and the Doppler frequency, respectively. ϕ is a uniformly distributed random phase in the interval $[0, 2\pi]$. Finally, $n(t)$ is the additive noise.

The signal described in Eq. (1) is initially multiplied by a locally generated carrier and spreading code. The resulting signal is then processed through incoherent integration to accumulate energy over time. Subsequently, the squared magnitude of the integrated output is computed to form the decision statistic.

The diagram of the proposed acquisition system is depicted in Fig. 3.

3. System Analysis

3.1. TM-CFAR Processor

In the presence of urban interference and multipath conditions, as well as to enhance detection performance, a constant false alarm rate technique is introduced at the detection and decision level. This technique offers a significant advantage due to its ability to adapt to varying ambient noise levels, enabling the reliable identification of visible GNSS satellites. Although CFAR techniques are well established in radar applications, their use in GNSS systems remains relatively limited.

In this work, two TM-CFAR detectors are implemented at two stages: at the output of the pilot channel and at the output of the data channel of the GNSS receiver.

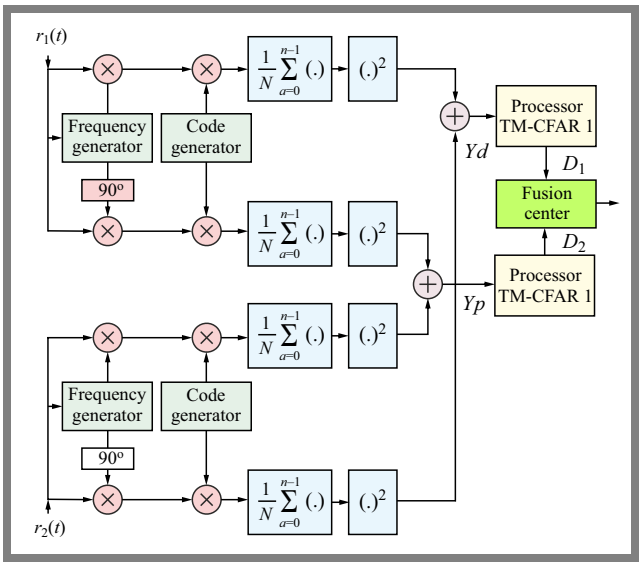

Fig. 3. Proposed adaptive acquisition system.

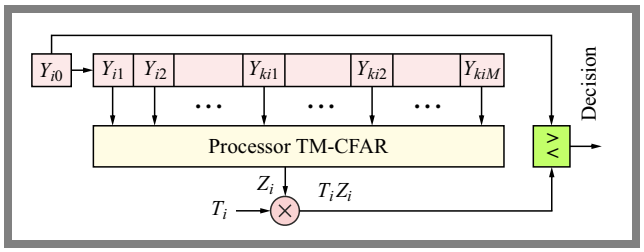

Fig. 4. Functional diagram of the TM-CFAR detector.

The functional diagram of the TM-CFAR detector, as shown in Fig. 4, consists of M cells that precede the cell under test (CUT). It comprises sorting, censoring and summation routines. First, the amplitudes of the samples, $Y_{i1}, Y_{i2}, \ldots, Y_{iM}, i = d, p$ for data and pilot channels, respectively, are ordered from the smallest value to the largest one as follows:

$$Y_{(i1)} \leqslant Y_{(i2)} \leqslant \cdots \leqslant Y_{(iM)} \, . \tag{2}$$

After censoring k_{i1} samples from the lower end and k_{i2} samples from the upper end of each detector, $i = d, p$, the noise power level Z_i is estimated by performing the arithmetic sum of the remaining reference cells content of each TM-CFAR detector [7]:

$$Z_i = \sum_{j=k_{i1}+1}^{M-k_{i2}} Y_{(ij)}, i = d, p \, . \tag{3}$$

With both detectors having the same number of reference cells M, the count of samples censored from the upper tail of each detector serves as an estimate of the number of samples containing multipath replicas.

Therefore, the values of k_{i1} and k_{i2}, $i = d, p$ are used to obtain the statistics Z_i $i = d, p$ and the scaling factors T_d and T_p that achieve the desired false alarm probabilities, P_{FA_i}, $i = d, p$ of the two adaptive detectors and, consequently, the overall desired false alarm rate P_{FA}.

Each factor T_i $i = d, p$ is determined according to the desired false alarm rate of the corresponding TM-CFAR detector. It is then multiplied by variable Z_i to obtain the adaptive threshold of each adaptive detector T_i Z_i.

3.2. Problem Definition and Formulation

In this section, we analyze the statistical detection process of the TM-CFAR detector in a GNSS acquisition system. To formulate the detection problem, we consider two cases:

- H_0 – the received signal contains only noise (signal absent),
- H_1 – the received signal contains the GNSS signal in addition to noise (signal present).

The probability density function (PDF) under the hypothesis H_1, $f_{Y_i/H_1}(y_i/H_1), i = d, p$, can be expressed as:

$$f_{Yi/H1}\left(y_i/H_1\right) = \frac{1}{1+\mu} \, e^{-\frac{y_i}{1+\mu}}, i = d, p, \; y_i \geqslant 0 \, , \tag{4}$$

where μ denotes the average signal-to-noise ratio (SNR) and y_i denotes the i-th received sample from either the pilot or data channel under hypothesis H_1. The PDF under hypothesis H_0 is given by:

$$f_{Yi/H_0}\left(y_i/H_0\right) = e^{y_i}, i = d, p, \; y_i \geqslant 0 \, . \tag{5}$$

In this situation, the false alarm probabilities P_{FAd} and P_{FAp} of the data and pilot channels can be calculated using the following expressions:

$$P_{FAd} = \prod_{i=1}^{M-k_{d1}-k_{d2}} Mv_i(T_d) \, , \tag{6}$$

$$P_{FAp} = \prod_{i=1}^{M-k_{p1}-k_{p2}} Mv_i(T_p) \, , \tag{7}$$

where

$$\begin{aligned} Mv_1(T_d) =& \frac{M!}{k_{d1}(M-k_{d1}-1)!(M-k_{d1}-k_{d2})} \\ & \times \sum_{i=0}^{k_{d1}} \frac{\binom{k_{d1}}{j}(-1)^{k_{d1}-i}}{\frac{M-i}{M-k_{d1}-k_{d2}}+T_d} \end{aligned} \, , \tag{8}$$

$$\begin{aligned} Mv_1(T_p) =& \frac{M!}{k_{p1}(M-k_{p1}-1)!(M-k_{p1}-k_{p2})} \\ & \times \sum_{i=0}^{k_{p1}} \frac{\binom{k_{p1}}{j}(-1)^{k_{p1}-i}}{\frac{M-i}{M-k_{p1}-k_{p2}}+T_p} \end{aligned} \, , \tag{9}$$

$$Mv_i(T_d) = \frac{a_{id}}{a_{id}+1}, \;\; id = 2, \ldots, M-k_{d1}-k_{d2} \, , \tag{10}$$

and

$$Mv_i(T_p) = \frac{a_{ip}}{a_{ip}+1}, \;\; ip = 2, \ldots, M-k_{p1}-k_{p2} \, , \tag{11}$$

with

$$a_{id} = \frac{M-k_{d1}-id+1}{M-k_{d1}-k_{d2}-i+1} \, , \tag{12}$$

and

$$a_{ip} = \frac{M-k_{p1}-ip+1}{M-k_{p1}-k_{p2}-i+1} \, . \tag{13}$$

The detection probabilities P_{Dd} and P_{Dp} of the data and pilot channels are obtained by replacing T_d and T_p with $T_d/(1+\mu)$ and $T_p/(1+\mu)$, in Eqs. (6) and (7), respectively.

The introduction of a fusion center, comprising two TM-CFAR detectors, aims to enhance the detection performance in any communication system. The fusion center will combine the results of the two TM-CFAR detectors, resulting in an increased probability of detection while maintaining a desired probability of false alarm. Two fusion methods are implemented in this present work: the AND rule and the OR rule [4].

For the "AND fusion rule", the global detection and false alarm probabilities are given by:

$$P_D = P_{Dd} \times P_{Dp} \, , \tag{14}$$

$$P_{FA} = P_{FAd} \times P_{FAp} \, . \tag{15}$$

For the "OR fusion rule", the global detection and false alarm probabilities are as follows:

$$P_D = 1 - \left[(1-P_{Dd}) \times (1-P_{Dp})\right] \, , \tag{16}$$

$$P_{FA} = 1 - \left[(1-P_{FAd}) \times (1-P_{FAp})\right] \, . \tag{17}$$

The optimization problem under consideration involves identifying a set of six unknown parameters: T_p, T_d, k_{p1}, k_{p2}, k_{d1}, and k_{d2} that significantly impact the performance of the system. Determining their optimal values is crucial to ensuring the desired system's behavior and maximizing its overall performance.

The objective function governing this optimization problem can be expressed as:

$$f(T_p, T_d, k_{d1}, k_{d2}, k_{p1}, k_{p2}) = \left|1 - P_D\right| + \left(\frac{1}{P_{FA0}} \times \left|P_{FA} - P_{FA0}\right|\right), \quad (18)$$

where P_{FA0} is the desired false alarm rate, and symbol $|\,.\,|$ gives the absolute value.

The goal is to minimize f by appropriately tuning the six unknown parameters. Classical optimization methods often exhibit limitations when addressing complex, non-linear, non-differentiable, or high-dimensional objective functions. In such cases, metaheuristic algorithms provide an effective alternative by offering flexible and computationally efficient mechanisms for global search and convergence.

3.3. Problem Solving Methodology

To solve the present optimization problem, several metaheuristic techniques are employed, including PSO, WOA, ALO and GWO. These population-based algorithms are capable of efficiently exploring the solution space and converging toward near-optimal solutions without requiring explicit gradient information or closed-form expressions of the objective function.

By applying these algorithms, the optimal values of T_p, T_d, k_{p1}, k_{p2}, k_{d1}, and k_{d2} can be effectively determined, thereby minimizing the objective function f and achieving the desired trade-off between detection performance and false alarm rate P_{FA}.

4. Optimization Techniques

4.1. Particle Swarm Optimization

PSO stands as a widely recognized stochastic swarm-based algorithm inspired by nature [8], [9]. The algorithm has attracted numerous researchers over the past decade due to its simplicity. The concept and formulation of the PSO algorithm were inspired by observations of the social behavior of bird flocks and fish schools [10].

In PSO, a group of particles (like a flock of birds) explores the problem space. Each particle shares its best position and fitness with others in the swarm, adding some randomness to decide its next move. This movement is influenced by each particle's past and the overall swarm's direction. After all particles update their positions in one iteration, the process repeats, exploring areas near the current best solutions. Eventually, the swarm tends to converge to the optimum of the objective function.

The rate of convergence depends heavily on the PSO variant and the control parameters. Particle speed and position updates follow the rules outlined in [8]:

$$V_{id}^{k+1} = \omega V_{id}^{k} + c_1 r_1^k (P_{best_{id}}^k - x_{id}^k) + c_2 r_2^k (G_{best_{id}}^k - x_{id}^k) \quad (19)$$

and

$$x_{id}^{k+1} = x_{id}^k + V_{id}^{k+1}, \quad (20)$$

where V_{id}^k and x_{id}^k represent the speed and the position of the i particle in d dimension at k time, $P_{best_{id}}^k$ is the best position visited so far by the i-th particle, and $G_{best_{id}}^k$ is the best position visited so far by any particle in the swarm, c_1 and c_2 are the cognitive and social acceleration coefficients, while r_1 and r_2 are two diagonal matrices of random values generated within the [0, 1] interval.

4.2. Grey Wolf Optimization

GWO stems from the social leadership and hunting technique of gray wolves. The algorithm incorporates a mathematical representation of the wolf pack hierarchy inspired by their social hunting behavior, observed in gray wolves in nature.

In this algorithm, the population is divided into four groups:

- alpha (α) – the leader of the pack, responsible for decision-making (e.g., hunting strategies). It represents the best solution in the optimization process.
- beta (β) – subordinate wolves that assist α in decision-making. They represent the second-best solution.
- delta (δ) – wolves that follow α and β, helping to control the pack. These represent the third-best solutions.
- omega (ω) – the lowest-ranking wolves that follow the other wolves. These represent the rest of the population.

The three strongest wolves α, β, and δ, are considered to guide the other wolves ω toward promising areas in the search space. The best solution is denoted as the α wolf, followed by β and δ wolves, while the remaining solutions are classified as ω wolves. The optimization process in GWO is guided by α, β, and δ, which lead the ω wolves toward the global optimum [9]. The hunting process starts with wolves encircling their prey. This process can be expressed as follows:

$$\vec{D} = \left|\vec{C} \cdot \vec{X}_{prey}(t) - \vec{X}(t)\right|, \quad (21)$$

$$\vec{X}(t+1) = \vec{X}_{prey}(t) - \vec{A} \cdot \vec{D}, \quad (22)$$

where $\vec{X}(t)$ denotes the current position of a wolf, $\vec{X}_{prey}(t)$ represents the position of the prey (best-known solution), and vector $\vec{D}$ represents the distance between the position of a wolf and the prey, weighted by a random coefficient $\vec{C}$.
$\vec{A}$ and $\vec{C}$ are defined as follows:

$$\vec{A} = 2\,\vec{a} \cdot \vec{r_1} - \vec{a}, \quad (23)$$

$$\vec{C} = 2 \cdot \vec{r_2}, \quad (24)$$

where $\vec{r_1}$ and $\vec{r_2}$ are random vectors in the range [0, 1], while $\vec{a}$ decreases linearly from 2 to 0 over the course of iterations, controlling the balance between exploration (searching new areas) and exploitation (refining known solutions).

To simulate the cooperative guidance of α, β, and δ wolves, each wolf updates its position according to the influence of these three leaders:

$$\begin{aligned}\vec{D}_\alpha &= \left|\vec{C}_1 \cdot \vec{X}_\alpha - \vec{X}\right|,\\ \vec{D}_\beta &= \left|\vec{C}_2 \cdot \vec{X}_\beta - \vec{X}\right|,\\ \vec{D}_\delta &= \left|\vec{C}_3 \cdot \vec{X}_\delta - \vec{X}\right|.\end{aligned} \tag{25}$$

The final position of each wolf is then calculated as the mean of these three influences:

$$\vec{X}(t+1) = \frac{\vec{X}_1 + \vec{X}_2 + \vec{X}_3}{3}\,. \tag{26}$$

This mechanism allows the population to converge on its prey (the optimal solution) while maintaining a good balance between exploration and exploitation. The fitness function measures the quality of each candidate solution based on the defined optimization goal.

The main steps of the GWO algorithm are described as follows:

1) Initialize the population of gray wolves randomly within the search space.
2) Evaluate the fitness of each wolf.
3) Identify α, β, and δ wolves based on their fitness values.
4) The positions of the wolves are updated in accordance with Eqs. (21) – (25).
5) Reduce parameter $\vec{a}$ linearly to shift from exploration to exploitation.
6) Repeat the process until the termination criterion (maximum iterations or convergence) is met.

The α wolf represents the algorithm's best solution upon completion of the optimization.

4.3. Ant Lion Optimizer

The ALO is a swarm intelligence-based metaheuristic algorithm. It models the interaction between ants and antlions in nature [10].

The algorithm is inspired by the hunting behavior of antlions, which trap prey in the pits they dig. In our study, this behavior is modeled to guide the optimization of TM-CFAR detection thresholds in the GNSS acquisition system. The algorithm adaptively explores the solution space and exploits promising regions to improve detection performance, avoid local optima, and ensure a reliable convergence toward optimal threshold values. The algorithmic process comprises five steps: starting with the random walk process of ants, followed by trap construction, then ant trapping in the traps created by antlions, ant capture, and finally reconstruction of traps.

The antlion life cycle consists of two stages: larvae and adults. The first method of ant capture involves moving ant larvae in a circular path to dig a cone-shaped pit in the sand. Then, antlions use their massive jaws to throw sand out of the cone. They then wait for insects to be trapped at the bottom of the cone. Once captured, the prey is drawn towards the cone and consumed by the antlions. Finally, the remains of the ants are discarded outside the conical pit, and the pit is improved for the next prey to be hunted [11].

4.4. Whale Optimization Algorithm

Inspired by the natural hunting behavior of humpback whales, WOA algorithm mimics the way these whales hunt by targeting groups of krill or small fish on the water's surface. They form spiral bubble nets to encircle and capture their prey while diving and ascending toward the surface. This behavior is modeled in WOA through three strategies: prey encircling, prey searching (exploration phase), and spiral bubble-net attacking (exploitation phase).

The position of the i-th whale at iteration t is given by:

$$X_i^t = (x_{i,1}^t, x_{i,2}^t, \ldots, x_{i,D}^t),\;\; i = 1, 2, \ldots, N\,, \tag{27}$$

where N and D represent the whale population size and the dimensionality of the problem, respectively.

The mathematical formulation of the WOA strategies is provided in [13].

5. Performance Evaluation

For the simulation outcomes, the detection probability has been calculated using the Monte Carlo simulation method. It is provided by the following equation:

$$P_D = \frac{\text{Number of detections}}{\text{Number of all tested signal cells}}\,. \tag{28}$$

The results obtained assume that the environment is a Rayleigh fading channel. Table 1 summarizes the parameter values used to obtain these results.

Firstly, search intervals are defined on T_p, $T_d \in [0, 5]$, k_{d1}, k_{d2}, k_{p1} and $k_{p2} \in [1, \frac{M}{2}]$, where M denotes the reference window size of each detector. The initial population consists of 30 particles, for the AND and OR fusion rules.

The results present four detector cases: identical, different, symmetric, and asymmetric, comparing fixed-threshold and TM-CFAR detectors. In addition, four optimization methods were selected to calculate the unknown parameters of the two TM-CFAR detectors (WOA, ALO, GWO, and PSO). The effects of the number of reference cells, SNR variations, and the desired P_{FA} on the performance of the system are then investigated. Considering a signal-to-noise ratio of 60 dB-Hz, the results are summarized in four tables with the corresponding detection probabilities. These tables clearly demonstrate

Tab. 1. Simulation parameters used to obtain the desired results.

Parameter	Value
Sampling frequency fs	40.92 MHz
P_{FA}	10^{-4}
Number of iterations	100 000
Population size	500
Number of interferers O	3, 6

Tab. 2. Parameters estimated using the four optimization algorithms based on the number of cells with the AND fusion rule.

Number of cells	PSO	GWO	ALO	WOA
$M = 8$	$T = 1.7023$	$T = 3.5138$	$T = 1.5288$	$T = 1.7647$
	$k_1 = 1$	$k_1 = 2$	$k_1 = 1$	$k_1 = 4$
	$k_2 = 2$	$k_2 = 3$	$k_2 = 2$	$k_2 = 1$
	$P_D = 0.9770$	$P_D = 0.9731$	$P_D = 0.9793$	$P_D = 0.9735$
	$T = 0.5522$	$T = 1.5391$	$T = 0.8132$	$T = 0.6057$
$M = 16$	$k_1 = 5$	$k_1 = 6$	$k_1 = 5$	$k_1 = 5$
	$k_2 = 4$	$k_2 = 6$	$k_2 = 4$	$k_2 = 4$
	$P_D = 0.9820$	$P_D = 0.9822$	$P_D = 0.9815$	$P_D = 0.9862$
	$T = 1.7034$	$T = 1$	$T = 0.651$	$T = 3.4978$
$M = 32$	$k_1 = 7$	$k_1 = 11$	$k_1 = 11$	$k_1 = 4$
	$k_2 = 13$	$k_2 = 13$	$k_2 = 13$	$k_2 = 16$
	$P_D = 0.9891$	$P_D = 0.9793$	$P_D = 0.9860$	$P_D = 0.9889$

Tab. 3. Parameters estimated using the four optimization algorithms based on P_{FA} with the AND fusion rule.

Probability of false alarm	PSO	GWO	ALO	WOA
$P_{FA} = 10^{-4}$	$T = 1.7034$	$T = 1.7393$	$T = 0.651$	$T = 3.4978$
	$k_1 = 7$	$k_1 = 7$	$k_1 = 11$	$k_1 = 4$
	$k_2 = 13$	$k_2 = 13$	$k_2 = 13$	$k_2 = 16$
	$P_D = 0.9891$	$P_D = 0.9793$	$P_D = 0.9860$	$P_D = 0.9889$
$P_{FA} = 10^{-6}$	$T = 4.1283$	$T = 1.7564$	$T = 0.5916$	$T = 0.5071$
	$k_1 = 10$	$k_1 = 9$	$k_1 = 2$	$k_1 = 3$
	$k_2 = 13$	$k_2 = 15$	$k_2 = 12$	$k_2 = 12$
	$P_D = 0.9850$	$P_D = 0.9700$	$P_D = 0.9803$	$P_D = 0.9833$
$P_{FA} = 10^{-8}$	$T = 0.7270$	$T = 1.9737$	$T = 1$	$T = 0.9914$
	$k_1 = 10$	$k_1 = 5$	$k_1 = 10$	$k_1 = 4$
	$k_2 = 8$	$k_2 = 14$	$k_2 = 8$	$k_2 = 9$
	$P_D = 0.9676$	$P_D = 0.9524$	$P_D = 0.9558$	$P_D = 0.9552$

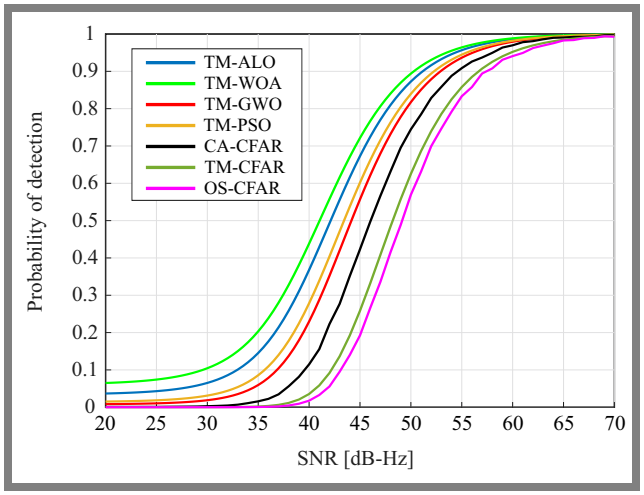

Fig. 5. Detection probability vs. SNR for three detectors: CA-CFAR, TM-CFAR and OS-CFAR, with and without optimization methods in a homogeneous environment.

a superior probability of detection when using the TM-CFAR detectors with optimization methods.

Tables 2–5 present the optimal values of the TM-CFAR parameters (T_d, T_p, k_{d1}, k_{d2}, k_{p1}, k_{p2}) in different scenarios. It has been observed that the best results are obtained when the parameters are identical (identical case). As a result, T_p and T_d are replaced by T and k_{d1}, k_{d2}, k_{p1}, k_{p2}, which take identical values k_1, k_2, for AND and OR fusion rules. Regarding the GNSS acquisition system, it is observed that the best results are obtained with a system that has the larger value of M. A degradation in detection performance is observed as the target false alarm probability decreases.

Furthermore, the influence of the AND and OR fusion rules is examined. It is evident that the best detection performance was achieved by a system utilizing the WOA and ALO algorithms followed by PSO and GWO for both OR and AND fusion rules. By comparing the results presented in Tabs. 2 and 3, a significant improvement in the probability of detection P_D

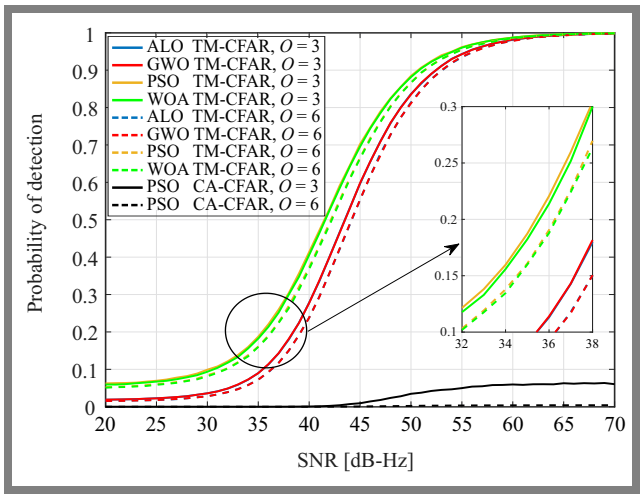

Fig. 6. Detection probability versus SNR for the TM-CFAR detector with optimization methods and the CA-CFAR detector.

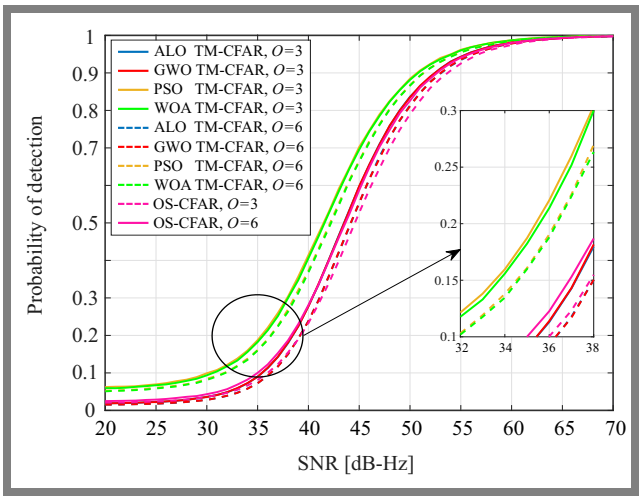

Fig. 7. Detection probability versus SNR for TM-CFAR and OS-CFAR detectors, with and without optimization methods.

is observed with the OR fusion rule, indicating that this rule offers better detection performance compared to the AND fusion rule.

Figure 5 presents the detection probability of TM-CFAR, CA-CFAR, and OS-CFAR detectors with and without optimization methods, when the number of reference cells is $M = 32$. CA-CFAR and OS-CFAR detectors are evaluated relative to the TM-CFAR detector under homogeneous conditions when optimization methods are employed. It is evident that CA-CFAR performs better than TM-CFAR in this environment. Moreover, the CA-CFAR algorithm outperforms both the TM-CFAR algorithm without optimization and the OS-CFAR algorithm.

Figure 6 compares CA-CFAR and TM-CFAR detectors in non-homogeneous environments with optimization techniques. It has been shown that the TM-CFAR algorithm surpasses its CA-CFAR counterpart in these environments. It should be noted that the problem addressed in this study focuses on the use of the TM-CFAR algorithm in non-homogeneous environments.

Figure 7 compares the TM-CFAR and OS-CFAR detectors with and without optimization techniques. It is demonstrated that the TM-CFAR algorithm surpasses the OS-CFAR algorithm.

Figure 8 shows the evolution of the total probability of detection P_D as a function of the variation in SNR for the AND fusion rule, using different optimization techniques, with a fixed number of reference cells $M = 32$, and in a situation in which the system contains two identical detectors. Based on this figure, it can be observed that the PSO technique provides the best performance compared to the remaining approaches.

Figure 9 illustrates the evolution of the overall probability of detection as a function of SNR, for the four cases: identical, non-identical, symmetrical and non-symmetrical. From this figure, we observe that the performance is better in the identical and symmetrical cases compared to the remaining scenarios.

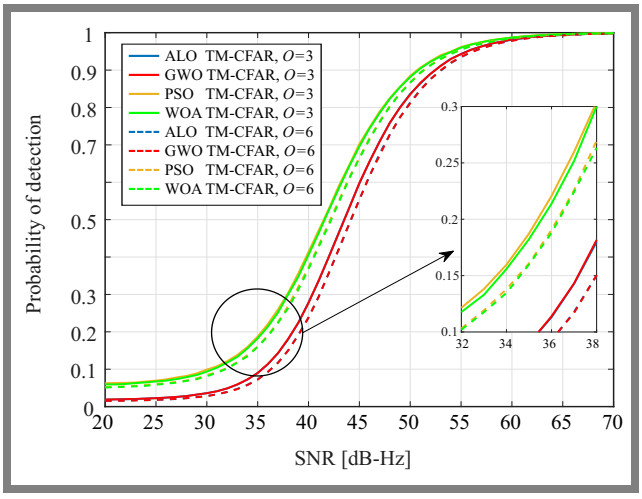

Fig. 8. Comparison between the four optimization algorithms of the TM-CFAR detector.

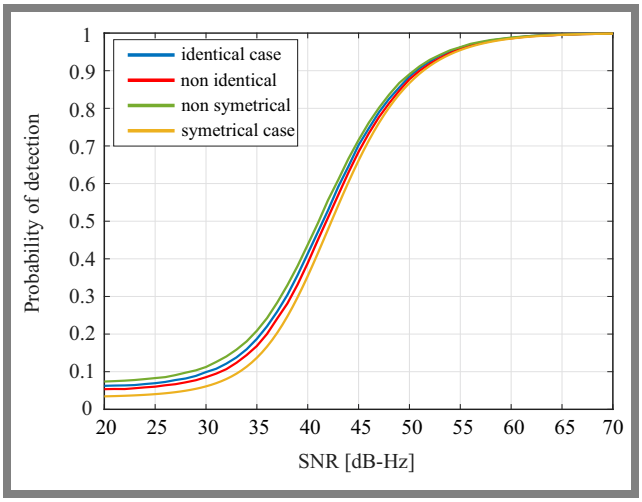

Fig. 9. Comparison of detection probability against SNR of the TM-CFAR detector for the four cases: identical, non-identical, symmetrical, and non-symmetrical, $P_{FA} = 10^{-4}$ and $M = 32$.

The evolution of the overall detection probability as a function of SNR variation is represented for the AND fusion rule

Tab. 4. Parameters estimated using the four optimization algorithms based on the number of cells with the OR fusion rule.

Number of cells	PSO	GWO	ALO	WOA
$M = 8$	$T = 3.5268$	$T = 2.7131$	$T = 3.5020$	$T = 3.5383$
	$k_1 = 1$	$k_1 = 1$	$k_1 = 1$	$k_1 = 1$
	$k_2 = 1$	$k_2 = 1$	$k_2 = 1$	$k_2 = 1$
	$P_D = 0.9987$	$P_D = 0.9986$	$P_D = 0.9988$	$P_D = 0.9987$
$M = 16$	$T = 1.5979$	$T = 3.6054$	$T = 3.6323$	$T = 5$
	$k_1 = 4$	$k_1 = 6$	$k_1 = 6$	$k_1 = 3.5563$
	$k_2 = 3$	$k_2 = 5$	$k_2 = 5$	$k_2 = 6$
	$P_D = 0.9994$	$P_D = 0.9992$	$P_D = 0.9992$	$P_D = 0.9992$
$M = 32$	$T = 0.5963$	$T = 1.5117$	$T = 0.9092$	$T = 0.8072$
	$k_1 = 6$	$k_1 = 7$	$k_1 = 6$	$k_1 = 6$
	$k_2 = 8$	$k_2 = 13$	$k_2 = 8$	$k_2 = 8$
	$P_D = 0.9998$	$P_D = 0.9996$	$P_D = 0.9995$	$P_D = 0.9996$

Tab. 5. Parameters estimated using the four optimization algorithms based on P_{FA} with the OR fusion rule.

Probability of false alarm	PSO	GWO	ALO	WOA
$P_{FA} = 10^{-4}$	$T = 0.5963$	$T = 1.5117$	$T = 0.9092$	$T = 0.8072$
	$k_1 = 6$	$k_1 = 7$	$k_1 = 6$	$k_1 = 6$
	$k_2 = 8$	$k_2 = 13$	$k_2 = 8$	$k_2 = 8$
	$P_D = 0.9998$	$P_D = 0.9996$	$P_D = 0.9995$	$P_D = 0.996$
$P_{FA} = 10^{-6}$	$T = 4.1283$	$T = 1.5834$	$T = 1.0286$	$T = 0.6289$
	$k_1 = 10$	$k_1 = 2$	$k_1 = 7$	$k_1 = 4$
	$k_2 = 13$	$k_2 = 10$	$k_2 = 4$	$k_2 = 6$
	$P_D = 0.9995$	$P_D = 0.9989$	$P_D = 0.9985$	$P_D = 0.9994$
$P_{FA} = 10^{-8}$	$T = 3.9342$	$T = 1.5500$	$T = 0.6495$	$T = 1.5285$
	$k_1 = 2$	$k_1 = 10$	$k_1 = 9$	$k_1 = 10$
	$k_2 = 12$	$k_2 = 6$	$k_2 = 1$	$k_2 = 6$
	$P_D = 0.9959$	$P_D = 0.9981$	$P_D = 0.9989$	$P_D = 0.9982$

in Fig. 10, for different values of P_{FA}, and a fixed value of the number of reference cells $M = 32$, in a system with two identical detectors. It can be seen from this figure that a decrease in false alarm probability P_{FA}, results in a significant degradation of detection probability.

Figure 11 shows the evolution of the probability of detection with respect to SNR for the AND fusion rules. It is shown that the higher the number of reference cells, the better the system and its detection performance.

To see the difference between the results obtained with the two fusion rules, i.e. AND and OR, more clearly, the variation in the total detection probability as a function of SNR for the two TM-CFAR detectors is presented.

The performance of the proposed system in terms of detection probability is shown in Fig. 12. It is evident from that figure that the system using the OR fusion rule outperforms the one employing the AND fusion rule in terms of detection probability.

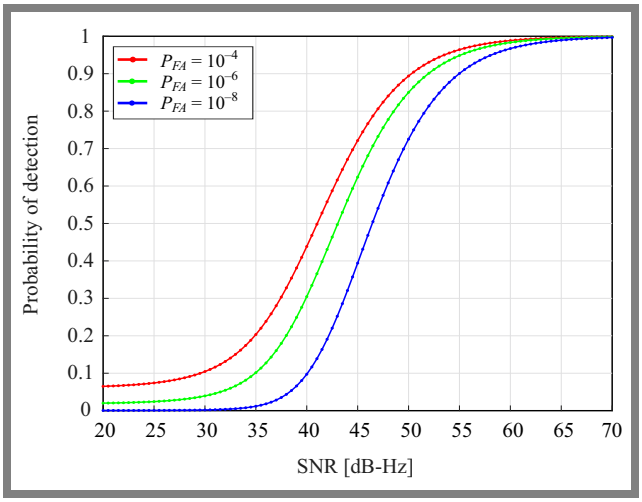

Fig. 10. Detection probability versus SNR of the TM-CFAR detector with different values of P_{FA}, in the case of $M = 32$.

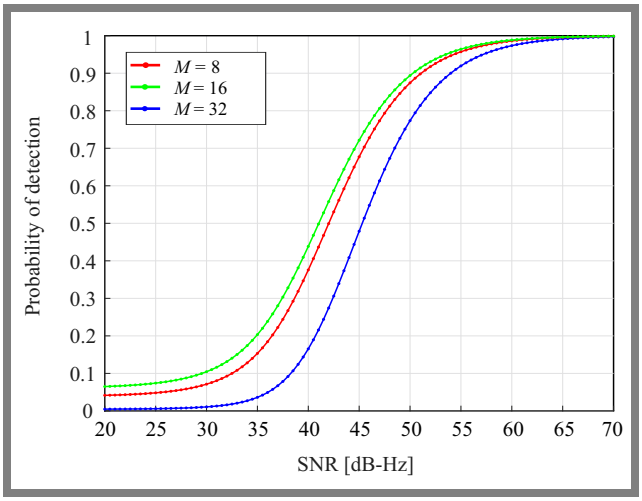

Fig. 11. Detection probability versus SNR of the TM-CFAR detector with different values of M, in the case of $P_{FA} = 10^{-4}$.

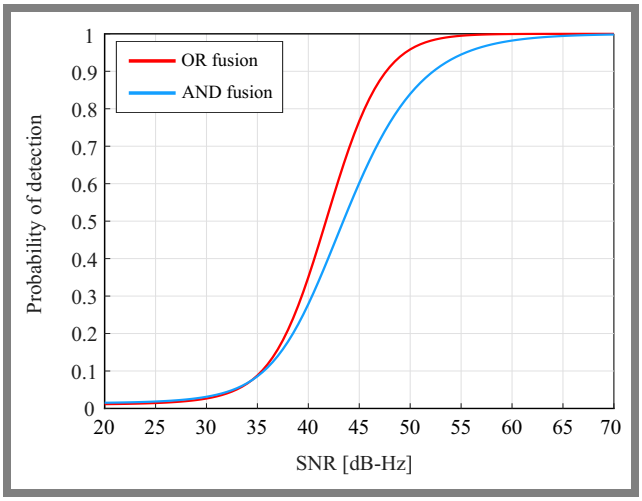

Fig. 12. Detection probability versus SNR of the TM-CFAR detector using PSO technique for AND and OR fusion rules in a scenario when $M = 32$ and with different detectors employed.

6. Conclusions

In this work, an attempt to enhance the efficiency of an approach based on metaheuristic optimization algorithms is presented to optimize the detection thresholds of TM-CFAR detectors. In this context, various simulations were performed, and the obtained results were compared and analyzed for different cases under consideration. The results indicate that applying these optimization methods enhances the performance of TM-CFAR detectors in non-homogeneous environments by enabling better estimation of scaling factors and estimated levels of noise power. Performance of the acquisition system is strongly influenced by the choice of fusion rules, as well as the use of identical or distinct detectors for the data and pilot channels.

The comparison of all optimization techniques revealed that PSO achieved the best performance in non-homogeneous environments. Furthermore, the OR fusion rule outperformed its AND counterpart, confirming the effectiveness of the proposed methods.

Acknowledgments

The presented work has been funded under the PRFU research project (no. A25N01UN300120220001) of the Algerian Ministry of Higher Education and Scientific Research (MESRS).

References

[1] K. Benachenhou, M. Hamadouche, and A. Taleb-Ahmed, "New Formulation of GNSS Acquisition with CFAR Detection", *International Journal of Satellite Communications and Networking*, vol. 35, pp. 215–230, 2017 (https://doi.org/10.1002/sat.1177).

[2] S. Dehouche and M. Hamadouche, "Enhanced Collective Detection for GNSS Weak Signals Acquisition in Rayleigh Channel", *International Journal of Satellite Communications and Networking*, vol. 36, pp. 332–351, 2018 (https://doi.org/10.1002/sat.1236).

[3] R. Grapenthin, "The Global Navigation Satellite System (GNSS): Positioning, Velocities, and Reflections", in: *Remote Sensing for Characterization of Geohazards and Natural Resources*, Springer, pp. 13–52, 2024 (https://doi.org/10.1007/978-3-031-59306-2_2).

[4] M.F. Hassani, A. Toumi, S. Benkrinah, and S. Sbaa, "Thresholding Optimization of Global Navigation Satellite System Acquisition with Constant False Alarm Rate Detection using Metaheuristic Techniques", *International Journal of Communication Systems*, vol. 37, art. no. 5938, 2024 (https://doi.org/10.1002/dac.5938).

[5] D. Ivković, A. Milenko, and Z. Bojan, "Detection of Very Close Targets by Fusion CFAR Detectors", *Scientific Technical Review*, vol. 66, pp. 50–57, 2016 (https://doi.org/10.5937/STR1603050I).

[6] K. Benachenhou, A. Taleb-Ahmed, and M. Hamadouche, "Performances Evaluation of GNSS ALTBOC Acquisition with CFAR Detection in Rayleigh Fading Channel", *IEEE Saudi International Electronics, Communications and Photonics Conference*, Riyadh, Saudi Arabia, 2013 (https://doi.org/10.1109/SIECPC.2013.6550786).

[7] D.U. Hai-Ming, M.A. Hong, and D.U. Bao-Qiang, "Adaptive TM-CFAR Detection Based on the Statistics ODV", *Journal of Beijing University of Posts and Telecommunications*, vol. 36, pp. 64–69, 2013 (https://journal.bupt.edu.cn/EN/Y2013/V36/I2/64).

[8] E.H. Houssein, A.G. Gad, K. Hussain, and P.N. Suganthan, "Major Advances in Particle Swarm Optimization: Theory, Analysis, and Application", *Swarm and Evolutionary Computation*, vol. 63, art. no. 100868, 2021 (https://doi.org/10.1016/j.swevo.2021.100868).

[9] J. Kennedy and E. Russell, "Particle Swarm Optimization", *IEEE International Conference on Neural Networks (ICNN'95)*, Perth, Australia, 1995 (https://doi.org/10.1109/ICNN.1995.488968).

[10] T.M. Shami *et al.*, "Particle Swarm Optimization: A Comprehensive Survey", *IEEE Access*, vol. 10, pp. 10031–10061, 2022 (https://doi.org/10.1109/ACCESS.2022.3142859).

[11] A. Sasithradevi, B. Chanthini, and S. Shoba, "A HybridOpt Approach for Early Alzheimer's Disease Diagnostics with Ant Lion Optimizer (ALO)", *Alexandria Engineering Journal*, vol. 109, pp. 112–125, 2024 (https://doi.org/10.1016/j.aej.2024.08.089).

[12] M.H. Nadimi-Shahraki, H. Zamani, Z.A. Varzaneh, and S. Mirjalili, "A Systematic Review of the Whale Optimization Algorithm: Theoretical Foundation, Improvements, and Hybridizations", *Archives of Computational Methods in Engineering*, vol. 30, pp. 4113–4159, 2023 (https://doi.org/10.1007/s11831-023-09928-7).

[13] L. Abualigah *et al.*, "Whale Optimization Algorithm: Analysis and Full Survey", in: *Metaheuristic Optimization Algorithms*, Morgan Kaufmann, pp. 105–115, 2024 (https://doi.org/10.1016/B978-0-443-13925-3.00015-7).

Elbahdja Ourfella, Ph.D. Student
LAGE laboratory
https://orcid.org/0009-0008-7843-4200
E-mail: ourfella.elbahdj@univ-ouargla.dz
Kasdi Merbah University, Ouargla, Algeria
https://www.univ-ouargla.dz

Sabra Benkrinah, Assoc. Prof.
LAGE laboratory
https://orcid.org/0000-0002-8292-2572
E-mail: benkrinah.sabra@univ-ouargla.dz
Kasdi Merbah University, Ouargla, Algeria
https://www.univ-ouargla.dz

Naceur Aounallah, Prof.
Department of Electronic and Telecommunications
https://orcid.org/0000-0001-9137-7900
E-mail: aounallah.naceur@univ-ouargla.dz
Kasdi Merbah University, Ouargla, Algeria
https://www.univ-ouargla.dz

Fairness-aware Joint Pattern and Power Design for Downlink PDMA Systems

Farhad E. Mahmood

University of Mosul, Mosul, Iraq

https://doi.org/10.26636/jtit.2026.2.2567

Abstract — Pattern division multiple access (PDMA) is recognized as a promising non-orthogonal multiple access technique for overloaded wireless systems, capable of being used for multiplexing multiple users over a limited set of resources. However, the real performance of PDMA is determined not only by the access principle itself, but also by the joint interaction between pattern design, transmit power allocation, and receiver interference cancellation. This paper proposes a fairness PDMA scheme for overloaded downlink systems based on joint pattern assignment, power allocation, and adaptive successive interference cancellation (SIC). The design aims to improve spectral efficiency and user fairness under real residual-interference conditions. Simulation results show that the proposed PDMA consistently outperforms orthogonal multiple access (OMA) and fixed-pattern PDMA techniques. At 30 dB, the proposed scheme achieves an average sum rate of approximately 14.5 bit/s/Hz under ideal SIC, compared with nearly 12 bit/s/Hz for OMA and approx. 8.5 bit/s/Hz for fixed-pattern PDMA. In terms of fairness, at an overload factor of $\lambda = 1.5$, the proposed method attains a Jain's fairness index of approx. 0.84, whereas OMA and fixed-pattern PDMA achieve nearly 0.58 and 0.44, respectively. These results confirm that an adaptive joint design allows to obtain both high throughput and balanced user performance in overloaded PDMA systems.

Keywords — NOMA, overloaded access, pattern design, PDMA, power allocation, SIC

1. Introduction

Growing demand for high spectral efficiency, low latency, and massive connectivity has rendered conventional orthogonal multiple access (OMA) insufficient for future wireless systems. In OMA, users are separated by orthogonal time, frequency, or code resources, which simplifies the receiver design but limits the number of users served. Therefore, non-orthogonal multiple access (NOMA) has been widely studied as a key enabling principle for fifth-generation (5G) wireless communication and beyond networks. Multiple users may share the same physical resource block and their mutual interference is handled by a structured transmitter design and receiver multi-user detection [1]–[3].

Among the main NOMA variants, pattern division multiple access (PDMA) is particularly attractive, as it combines resource-domain pattern mapping with power-domain superposition to improve access connectivity and spectral efficiency. In PDMA, each user is assigned to a sparse transmission pattern over a limited set of resource elements, and the overlap among users is controlled by a binary pattern matrix. This structure provides both diversity gain and overload capability, while still enabling practical multi-user separation through receivers based on successive interference cancellation (SIC), message passing, or hybrid detection [4]–[8]. In contrast to power-domain NOMA with a single resource block, PDMA allows users to be multiplexed jointly across multiple resources, turning the pattern matrix into a central design variable.

Although PDMA offers important advantages, its performance depends strongly on three coupled factors. The first is the structure of pattern matrix, controlling the diversity order of each user and the degree of crowding on each resource element. The second is the transmit power distribution, directly affecting both the achievable rate and the SIC decoding reliability. The third is the receiver operation, since real SIC is imperfect and residual interference may propagate through the detection chain. Therefore, a simple comparison between PDMA and OMA is insufficient for a high-quality study, because the real problem lies in how PDMA is designed and operated under realistic channel and interference constraints [9], [10].

Existing literature has already shown the importance of these issues. The authors of [5] studied the design of PDMA pattern matrices for uplink deployment scenarios and highlighted the decisive role of pattern structure in system performance. In [4], PDMA is introduced as a non-orthogonal access framework for 5G radio networks and its ability to exploit structured user multiplexing is demonstrated. Paper [6] further developed a joint transmitter and receiver design in which pattern mapping, power allocation, and hybrid detection are considered jointly. More recently, the authors of [11] investigated downlink power allocation optimization in PDMA and showed that imperfect channel state information (CSI) must be considered in practical deployments.

However, despite these important contributions, two limitations remain visible. First, many studies either use fixed or preselected PDMA patterns, which restricts the adaptability of the system under changing user demands. Second, fairness and residual SIC error are often not integrated explicitly into a unified design framework.

Motivated by these considerations, this paper proposes a fairness-aware downlink PDMA scheme in which the pattern matrix, user powers, and SIC decoding order are jointly updated in an alternating manner. Unlike a conventional

benchmarking paper that merely verifies that PDMA outperforms OMA, this work explicitly formulates the underlying joint design problem, captures residual interference during SIC, and studies the tradeoff among sum rate, BER, fairness, and overloaded access capability. The main idea is that the PDMA pattern should not remain fixed. Instead, it should adapt depending on channel strength, rate deficit, and interference congestion.

The main contributions of this paper are summarized as follows:

- a generalized downlink PDMA system model is established for overloaded operation, where multiple users share a limited number of resource elements through a sparse binary pattern matrix,
- a fairness-aware optimization framework is formulated in which the pattern matrix and the transmit-power vector are treated as coupled design variables under total-power, overload, and minimum-rate constraints,
- a residual-interference-aware SIC receiver model is incorporated in order to reflect non-ideal cancellation and to make the design more realistic,
- a low-complexity alternating algorithm is developed to update the pattern matrix, transmit powers, and decoding order iteratively,
- the proposed scheme is benchmarked against OMA and conventional fixed-pattern PDMA in terms of sum rate, BER, fairness index, overload behavior, and convergence characteristics.

The remainder of this paper is organized as follows. Section 2 presents the considered PDMA system model and the associated performance metrics. Section 3 develops the proposed fairness-aware joint design algorithm. Section 4 describes the simulation setup and discusses the numerical results. Finally, Section 5 concludes the paper.

2. System Model

Consider the downlink of a single-cell PDMA system in which one base station serves K users over N orthogonal resource elements, where $K > N$ is allowed in order to support overloaded transmission. Let $\mathcal{K} = \{1, 2, \ldots, K\}$ denote the user set and $\mathcal{N} = \{1, 2, \ldots, N\}$ denote the resource-element set. The overload factor is defined as:

$$\lambda = \frac{K}{N} , \tag{1}$$

where $\lambda > 1$ corresponds to non-orthogonal overloaded access.

2.1. Pattern Matrix Representation

The PDMA resource assignment is represented by a binary pattern matrix:

$$\mathbf{G} = [g_{n,k}] \in \{0, 1\}^{N \times K} , \tag{2}$$

where $g_{n,k} = 1$ indicates that user k occupies resource element n, while $g_{n,k} = 0$ means otherwise. The diversity order of user k is:

$$d_k = \sum_{n=1}^{N} g_{n,k} , \tag{3}$$

and the row weight of the n-th resource element is:

$$w_n = \sum_{k=1}^{K} g_{n,k} , \tag{4}$$

which measures how many users share the same resource element.

2.2. Transmit Signal Model

Let x_k be the information symbol of user k, normalized such that:

$$\mathbb{E}\{|x_k|^2\} = 1 , \tag{5}$$

and let p_k denote the power allocated to that user. The superposed transmit signal on resource element n is then:

$$s_n = \sum_{k=1}^{K} g_{n,k} \sqrt{p_k}\, x_k , \qquad n \in \mathcal{N} . \tag{6}$$

The total available transmit power is constrained by:

$$\sum_{k=1}^{K} p_k \leqslant P_{\mathrm{T}} , \qquad p_k \geqslant 0, \forall k , \tag{7}$$

where P_{T} is the base-station power budget.

2.3. Channel and Received Signal Model

Assume flat Rayleigh fading over each resource element. Let $h_{n,k} \in \mathbb{C}$ denote the channel coefficient from the base station to user k on resource element n and let $z_{n,k} \sim \mathcal{CN}(0, N_0)$ denote complex additive white Gaussian noise. Then the received signal at user k on resource n is:

$$y_{n,k} = h_{n,k} \sum_{j=1}^{K} g_{n,j} \sqrt{p_j}\, x_j + z_{n,k} . \tag{8}$$

Separating the desired term from the interference terms gives:

$$y_{n,k} = h_{n,k}\, g_{n,k}\, \sqrt{p_k} x_k + \sum_{\substack{j=1 \\ j \neq k}}^{K} h_{n,k}\, g_{n,j}\, \sqrt{p_j} x_j + z_{n,k} . \tag{9}$$

For user k, the effective composite channel gain over its assigned pattern is defined as:

$$\mu_k = \sum_{n=1}^{N} g_{n,k}\, |h_{n,k}|^2 . \tag{10}$$

Similarly, the effective interference coupling from user j to user k is:

$$\mu_{k,j} = \sum_{n=1}^{N} g_{n,j} |h_{n,k}|^2 . \tag{11}$$

2.4. Residual-Interference-Aware SIC

Let $\pi(1), \pi(2), \ldots, \pi(K)$ denote the SIC decoding order. Since practical cancellation is imperfect, a residual interference factor $\rho \in [0, 1]$ is introduced, where $\rho = 0$ corresponds

to ideal SIC and $\rho > 0$ models imperfect cancellation. Under this model, the effective SINR of user k is:

$$\gamma_k = \frac{p_k \, \mu_k}{\sum\limits_{j \in \mathcal{U}_k} p_j \, \mu_{k,j} + \rho \sum\limits_{j \in \mathcal{C}_k} p_j \, \mu_{k,j} + N_0} \, , \tag{12}$$

where $\mathcal{U}_k$ is the set of users not yet cancelled when decoding user k, and $\mathcal{C}_k$ is the set of already cancelled users.

Accordingly, the achievable rate of user k is:

$$R_k = \log_2 \left(1 + \gamma_k\right) \text{ [bit/s/Hz]} \, , \tag{13}$$

and the system sum rate becomes:

$$R_{\text{sum}} = \sum_{k=1}^{K} R_k \, . \tag{14}$$

To evaluate service uniformity, Jain's fairness index is adopted:

$$J = \frac{\left(\sum\limits_{k=1}^{K} R_k \right)^2}{K \sum\limits_{k=1}^{K} R_k^2} \, , \tag{15}$$

where values closer to one indicate more balanced user performance.

2.5. Joint Design Problem

The main objective is to jointly optimize the pattern matrix and transmit-power vector while preserving fairness. This leads to the following constrained optimization problem:

$$\begin{aligned} \max_{\mathbf{G},\mathbf{p}} \quad & \sum_{k=1}^{K} \omega_k R_k \\ \text{s.t.} \quad & \sum_{k=1}^{K} p_k \leqslant P_{\text{T}} \, , \\ & p_k \geqslant 0, \qquad \forall k \, , \\ & g_{n,k} \in \{0,1\}, \qquad \forall n, k \, , \\ & \sum_{k=1}^{K} g_{n,k} \leqslant W_{\max}, \qquad \forall n \, , \\ & R_k \geqslant R_k^{\min}, \qquad \forall k \, , \\ & \sum_{n=1}^{N} g_{n,k} = d_k, \qquad \forall k \, , \end{aligned} \tag{16}$$

where ω_k is a user-priority weight, $R_k^{\min}$ is the minimum required rate of user k, and $W_{\max}$ is the maximum allowable row weight. Because Eq. (16) includes both binary and continuous variables and the rates are interference-coupled, the problem is mixed-integer and non-convex.

3. Proposed Fairness-aware PDMA Scheme

3.1. Utility Function

To balance throughput and fairness, a weighted utility function is defined as:

$$\mathcal{J}(\mathbf{G}, \mathbf{p}) = \sum_{k=1}^{K} \omega_k R_k - \beta \sum_{k=1}^{K} \left[\max \left(0, R_k^{\min} - R_k\right) \right]^2 \, , \tag{17}$$

where $\beta > 0$ controls the penalty associated with rate-deficit violations. The second term prevents the optimizer from favoring only the strongest users.

Define the normalized rate-deficit factor of user k at iteration t as:

$$\Delta_k^{(t)} = \frac{\left(R_k^{\min} - R_k^{(t)} \right)^+}{R_k^{\min}} \, , \qquad (x)^+ = \max(x, 0) \, . \tag{18}$$

This factor quantifies how far the user is from its target rate.

3.2. Pattern Update

For fixed power allocation and SIC order, the pattern matrix is updated using a fairness- and interference-aware score. For user k on resource element n, define:

$$\Phi_{n,k}^{(t)} = \alpha_1 \frac{|h_{n,k}|^2}{\max\limits_{m \in \mathcal{N}} |h_{m,k}|^2} + \alpha_2 \Delta_k^{(t)} - \alpha_3 \frac{w_n^{(t)}}{W_{\max}} - \alpha_4 \mathcal{I}_{n,k}^{(t)} \, , \tag{19}$$

where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \geqslant 0$ are weighting coefficients and

$$\mathcal{I}_{n,k}^{(t)} = \sum_{\substack{j=1 \\ j \neq k}}^{K} g_{n,j}^{(t)} \, p_j^{(t)} \left| h_{n,k} \right|^2 \tag{20}$$

is the instantaneous interference cost on resource element n.

The updated pattern variable is then selected as:

$$g_{n,k}^{(t+1)} = \begin{cases} 1, & \text{if } n \text{ belongs to the best } d_k \text{ resources for user } k, \\ 0, & \text{otherwise.} \end{cases} \tag{21}$$

In this way, a user is assigned to resources that jointly offer high channel quality, low congestion, and strong fairness benefit.

3.3. Power Update

After updating the pattern matrix, the interference terms are frozen and the power vector is updated. The surrogate achievable rate of user k becomes:

$$\widetilde{R}_k^{(t+1)} = \log_2 \left(1 + \frac{p_k \, \mu_k^{(t+1)}}{I_k^{(t)} + N_0} \right) \, , \tag{22}$$

where

$$I_k^{(t)} = \sum_{j \in \mathcal{U}_k^{(t)}} p_j^{(t)} \mu_{k,j}^{(t)} + \rho \sum_{j \in \mathcal{C}_k^{(t)}} p_j^{(t)} \mu_{k,j}^{(t)} \, . \tag{23}$$

The resulting power-allocation subproblem admits a water-filling-like solution [12]:

$$p_k^{(t+1)} = \left[\frac{\omega_k + \beta \Delta_k^{(t)}}{\lambda_p^{(t)} \ln 2} - \frac{I_k^{(t)} + N_0}{\mu_k^{(t+1)}} \right]^+ \, , \tag{24}$$

where $\lambda_p^{(t)}$ is the Lagrange multiplier selected such that:

$$\sum_{k=1}^{K} p_k^{(t+1)} = P_{\mathrm{T}} \,. \tag{25}$$

Thus, users with stronger rate deficit and larger effective channel gain receive more power.

3.4. Adaptive SIC Ordering

Once the pattern matrix and power vector are updated, the SIC order is refined according to the effective composite received strengths [13]:

$$\Gamma_k^{(t+1)} = p_k^{(t+1)} \mu_k^{(t+1)} \,. \tag{26}$$

The decoding order is then determined such that:

$$\Gamma_{\pi(1)}^{(t+1)} \geqslant \Gamma_{\pi(2)}^{(t+1)} \geqslant \cdots \geqslant \Gamma_{\pi(K)}^{(t+1)} \,. \tag{27}$$

This step ensures that users with the strongest composite received signals are decoded first.

Accordingly, the proposed receiver adopts a strong first SIC rule, where users are ordered in descending values of $\Gamma_k^{(t+1)}$. This greedy ordering improve early stage decoding reliability because users with larger received power and effective channel gain are decoded before weaker users, hence, reducing error propagation under imperfect SIC.

3.5. Overall Algorithm

The complete procedure is summarized as follows:

1) Initialize a feasible pattern matrix $\mathbf{G}^{(0)}$, a feasible power vector $\mathbf{p}^{(0)}$, and a SIC order $\boldsymbol{\pi}^{(0)}$.
2) Compute the instantaneous SINR, achievable rate, and rate-deficit factor for each user.
3) Update the pattern matrix using the score in Eq. (19).
4) Update the power vector using Eq. (24).
5) Update the SIC order according to Eq. (27).
6) Repeat steps 2 – 5 until the utility variation $|\mathcal{J}^{(t+1)} - \mathcal{J}^{(t)}|$ falls below a threshold ε.

The dominant complexity per iteration is associated with score evaluation and sorting, yielding an overall complexity of:

$$\mathcal{O}(KN \log N + K \log K) \,, \tag{28}$$

which is significantly lower than exhaustive joint search.

4. Results and Discussion

4.1. Simulation Setup

The proposed method is evaluated in a single-cell downlink scenario under Rayleigh fading. The results compare four schemes: conventional OMA, fixed-pattern PDMA, the proposed fairness-aware PDMA under ideal SIC, and the proposed fairness-aware PDMA under imperfect SIC. Unless otherwise stated, the representative simulation parameters listed in Tab. 1 are used.

Tab. 1. Representative simulation parameters.

Parameter	Value
Number of users K	6
Number of resources N	4
Overload factor λ	1.5
Modulation	QPSK
Channel model	Rayleigh fading
Noise spectral density	AWGN
Total transmit power P_{T}	0 – 30 dBm
Maximum row weight $W_{\max}$	3
Residual SIC factor ρ	0, 0.05, 0.1
Minimum rate target $R_k^{\min}$	0.5 bit/s/Hz
Monte Carlo runs	10^4
Stopping threshold ε	10^{-4}

The performance metrics considered in this section are the achievable sum rate, user BER, Jain's fairness index, outage probability, and convergence behavior. The system is simulated over a wide transmit-SNR range in order to evaluate both low- and high-power operating regimes.

4.2. Sum Rate Performance

Figure 1 illustrates the average sum rate as a function of the transmit SNR. As expected, all schemes benefit from increasing transmit power, but the proposed fairness-aware PDMA achieves the highest throughput across the entire operating range. This behavior is explained by the joint adaptation of the pattern matrix and power vector.

In contrast, OMA is limited by strict orthogonal allocation, while fixed-pattern PDMA cannot exploit the changing channel and rate-deficit states of the users. The gain of the proposed method becomes more pronounced in the medium- and high-SNR regions, where resource sharing and dynamic interference management play a more pronounced role.

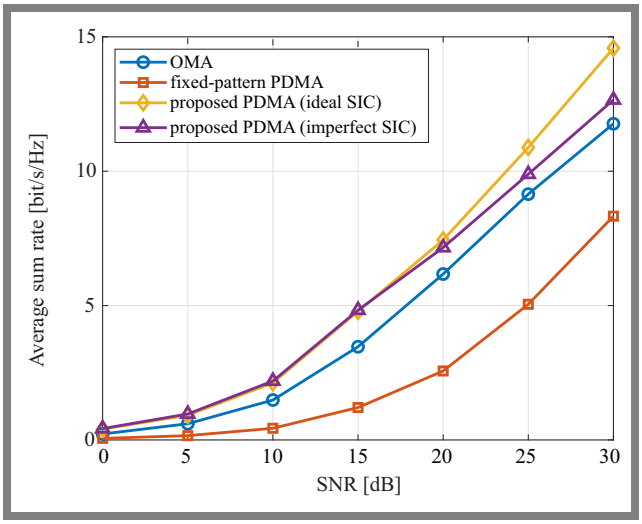

Fig. 1. SNR vs. average sum rate for OMA, fixed PDMA, proposed PDMA (ideal SIC), proposed PDMA (imperfect SIC).

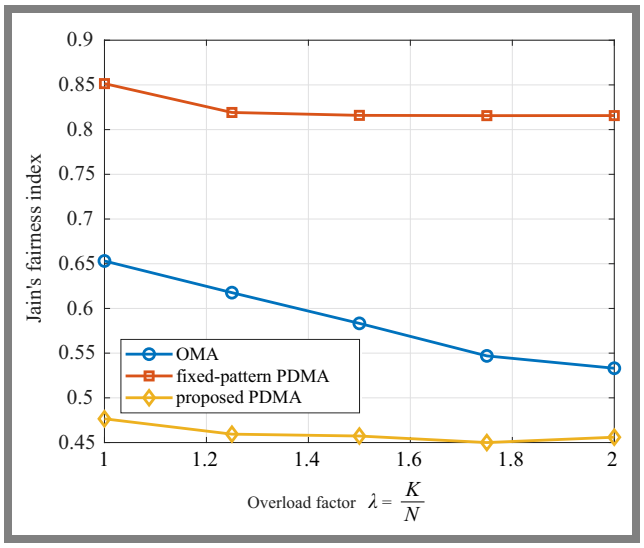

Fig. 2. Overload factor vs. Jain's fairness index.

4.3. Fairness and Overload Analysis

Figure 2 shows Jain's fairness index as a function of the overload factor. A key observation is that fairness generally degrades as more users are forced to share the same limited set of resources. However, the proposed design maintains a significantly higher fairness level than fixed-pattern PDMA, because the rate-deficit term in the utility function actively protects underserved users.

This is an important result, since overloaded access without fairness control often yields high aggregate throughput at the expense of weak users. The proposed method, therefore, offers a more balanced tradeoff between network efficiency and user service regularity.

4.4. Fairness and Overload Analysis

Figure 3 depicts BER performance under different SIC conditions. The results confirm that residual interference degrades the BER of all non-orthogonal schemes, especially in the moderate SNR region, where the cancelation process is more sensitive to ordering and power imbalance.

Nevertheless, the proposed fairness-aware PDMA remains more robust than fixed-pattern PDMA, since the adaptive ordering and interference-aware pattern assignment reduce the effective multi-user interference seen by the receiver. Under ideal SIC, the best BER performance is obtained, whereas a moderate performance loss is observed for $\rho > 0$. This behavior is consistent with the practical expectation that non-ideal cancellation introduces residual interference floors.

4.5. Sum Rate and Overload Analysis

Figure 4 shows the average sum rate as a function of the overload factor, defined by $\lambda = K/N$. One may observe that the proposed PDMA scheme achieves the highest sum-rate performance over the entire considered overload range. In particular, the proposed method benefits from moderate overload, as joint optimization of the pattern matrix and power allocation allows the available resource elements to be used

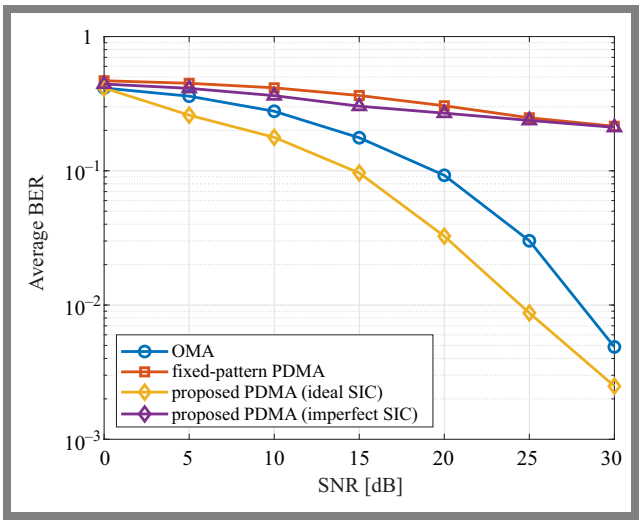

Fig. 3. SNR vs. average BER.

more efficiently. As the overload factor increases from $\lambda = 1$ to approx. $\lambda = 1.5$, the average sum rate of the proposed scheme increases, indicating that controlled non-orthogonal sharing can improve spectral efficiency when interference is properly managed.

However, for larger overload levels, a slight performance reduction is observed due to the stronger multi-user interference created by the denser resource sharing. Despite this reduction, the proposed method still maintains a clear advantage over both OMA and fixed-pattern PDMA.

In contrast, the OMA scheme shows a progressive decline in sum rate as the overload factor increases, since orthogonal allocation becomes less efficient when more users compete for the same limited resources. The fixed-pattern PDMA scheme also exhibits inferior performance, because it lacks the adaptability required to respond to changing interference and user-demand conditions.

Therefore, Fig. 4 confirms that the proposed fairness-aware PDMA design provides a more favorable tradeoff between overload capability and achievable throughput.

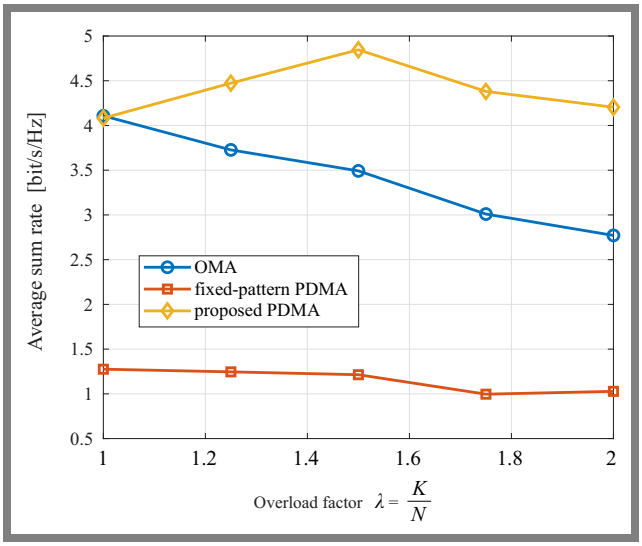

Fig. 4. Overload factor vs. average sum rate.

4.6. Discussion

The presented results lead to several important observations. First, the superiority of PDMA cannot be attributed solely to its non-orthogonal access principle. Instead, pattern matrix and power allocation must be designed jointly. Second, fairness-aware control is essential in overloaded regimes, since throughput-only designs tend to over-favor strong users. Third, residual SIC error cannot be ignored in realistic evaluations, because the practical benefit of PDMA depends on how well the receiver can suppress interference generated by the shared resources.

Finally, the proposed alternating framework offers a favorable complexity-performance tradeoff, making it more suitable for implementation than exhaustive joint optimization.

It is worth stressing that the proposed optimization framework assumes perfect CSI at the transmitter. Although this assumption is considered in many articles as a standard for isolating performance gains attributable to the joint pattern and power design, it may not reflect real conditions. In reality, CSI is usually estimated at the receiver and then fed back to the base station through a channel which introduces estimation errors. The impact of imperfect CSI on the proposed scheme is expected to manifest itself primarily in two ways: first, the pattern score in Eq. (19) would be computed based on noisy channel estimates, which leads to suboptimal pattern assignments; second, other power allocation techniques are required to fix the inaccurate channel estimated gain. Incorporating a robust optimization scheme to take into account the stochastic CSI uncertainty is a very promising future work beyond the 5G systems.

Overall, the results show that the proposed method transforms PDMA from a fixed access mechanism into an adaptive multi-user design framework. This shift is important for future beyond-5G systems, where connectivity density, fairness constraints, and interference dynamics are expected to be more demanding than in conventional orthogonal settings.

5. Conclusions

A fairness-aware joint pattern and power design for downlink PDMA systems has been discussed in this paper. The proposed method combines adaptive pattern allocation, power update, and SIC ordering in a unified framework for overloaded transmission. The numerical results show clear gains over the benchmark schemes. At 30 dB, the proposed PDMA reaches approx. 14.5 bit/s/Hz, while OMA and fixed-pattern PDMA achieve nearly 12 and 8.5 bit/s/Hz, respectively. In addition, at $\lambda = 1.5$, the proposed scheme improves the fairness index to approximately 0.84, compared with nearly 0.58 for OMA and 0.44 for fixed-pattern PDMA. These results demonstrate that the benefit of PDMA is maximized when pattern design and power allocation are optimized jointly rather than kept fixed.

References

[1] Z. Ding *et al.*, "A Survey on Non-orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends", *IEEE Journal on Selected Areas in Communications*, vol. 35, pp. 2181–2195, 2017 (https://doi.org/10.1109/JSAC.2017.2725519).

[2] Y. Liu *et al.*, "Non-orthogonal Multiple Access for 5G and Beyond", *Proceedings of IEEE*, vol. 105, pp. 2347–2381, 2017 (https://doi.org/10.1109/JPROC.2017.2768666).

[3] F.E. Mahmood, E.S. Perrins, and L. Liu, "Modeling and Analysis of Energy Consumption for MIMO Systems", *IEEE Wireless Communications and Networking Conference (WCNC)*, San Francisco, USA, 2017 (https://doi.org/10.1109/WCNC.2017.7925814).

[4] S. Chen *et al.*, "Pattern Division Multiple Access – A Novel Nonorthogonal Multiple Access for Fifth-generation Radio Networks", *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 3185–3196, 2017 (https://doi.org/10.1109/10.1109/TVT.2016.2596438).

[5] B. Ren *et al.*, "Pattern Matrix Design of PDMA for 5G Uplink Applications", *China Communications*, vol. 13, pp. 159–173, 2016 (https://doi.org/10.1109/CC.2016.7405732).

[6] Y. Jiang *et al.*, "Joint Transmitter and Receiver Design for Pattern Division Multiple Access", *IEEE Transactions on Mobile Computing*, vol. 18, pp. 885–895, 2019 (https://doi.org/10.1109/TMC.2018.2845364).

[7] M.M. Salim *et al.*, "Cooperative NOMA Meets Emerging Technologies: A Survey for Next-generation Wireless Networks", *IEEE Open Journal of the Communications Society*, vol. 6, pp. 9247–9286, 2025 (https://doi.org/10.1109/OJCOMS.2025.3626862).

[8] S.F. Kimaryo and K. Lee, "Uplink and Downlink Capacity Maximization of a P2P DMA-based Communication System", *IEEE Transactions on Wireless Communications*, vol. 23, pp. 14037–14051, 2024 (https://doi.org/10.1109/TWC.2024.3407828).

[9] S. Yan, K.C. Chou, H.H. Chen, and Q. Guo, "Real-time Downlink Resource Allocation in NOMA Systems: A Reinforcement Learning Approach", *IEEE Transactions on Vehicular Technology*, vol. 74, pp. 17779–17795, 2025 (https://doi.org/10.1109/TVT.2025.3575838).

[10] J. Liu and J. He, "Design and Analysis of CP-free OFDM PDMA Transmission System", *EURASIP Journal on Advances in Signal Processing*, vol. 2024, art. no. 68, 2024 (https://doi.org/10.1186/s13634-024-01154-y).

[11] J. Zeng *et al.*, "Downlink Power Allocation Optimization in Pattern Division Multiple Access", *IEEE Access*, vol. 9, pp. 14649–14659, 2021 (https://doi.org/10.1109/ACCESS.2021.3049493).

[12] O. Abdulghafoor *et al.*, "Efficient Power Allocation Algorithm in Downlink Cognitive Radio Networks", *ETRI Journal*, vol. 44, pp. 400–412, 2022 (https://doi.org/10.4218/etrij.2021-0013).

[13] M. Al-Ibadi and F.E. Mahmood, "Beam and Channel Tracking for 5G Communication Systems Using Adaptive Filtering Techniques: A Comparison Study", *Journal of Communications Software and Systems*, vol. 18, pp. 244–251, 2022 (https://doi.org/10.24138/jcomss-2021-0117).

Farhad E. Mahmood, Assistant Professor
Department of Communications and Intelligent Digital Systems Engineering, College of Engineering
https://orcid.org/0000-0002-5351-9768
E-mail: farhad.m@uomosul.edu.iq
University of Mosul, Mosul, Iraq
https://uomosul.edu.iq/en/

Evaluating AES Payload Encryption for Securing MQTT-based Smart Home Networks with Machine Learning-based Intrusion Detection

Mariusz Gajewski[1] and Wojciech Sałabun[1,2]

[1]*National Institute of Telecommunications, Warsaw, Poland,*
[2]*West Pomeranian University of Technology, Szczecin, Poland*

https://doi.org/10.26636/jtit.2026.2.2545

Abstract — The message queuing telemetry transport (MQTT) protocol is widely adopted in smart home IoT ecosystems despite its default configuration failing to offer adequate protection against eavesdropping or payload manipulation. This study addresses an important research gap and attempts to determine whether AES-128 payload encryption is capable of securing MQTT transmissions without degrading the effectiveness of machine learning-based intrusion detection systems (IDS). Three security configurations, namely TLS, payload encryption, and token-based authentication, deployed on the ESP32 microcontroller family, are compared and their impact on message latency is measured. Experimental results show that the AES-128 encryption overhead remains at below 25% of the message publication time on ESP32-S3. To evaluate the robustness of IDS under encryption, we apply a reproducible modification to the MQTTset benchmark dataset that replaces variable-length plaintext payloads with fixed-length ciphertext representations while simultaneously preserving feature semantics and labeling consistency. 5 out of 6 evaluated classifiers maintained their accuracy level at above 99% on the modified dataset, with tree-based and neural models showing no meaningful degradation. Only Naive Bayes proved unsuitable, with its accuracy dropping from 98.79% to 62.15% due to its independence assumptions being violated by cryptographic uniformity. These results confirm that AES-based MQTT payload encryption is a practical and efficient security measure for resource-constrained IoT environments, provided that appropriate classifiers are employed.

Keywords — AES, encryption, feature selection, machine learning, MQTT

1. Introduction

The proliferation of interconnected devices in home networks relies increasingly on standard communication protocols such as MQTT. This enables the integration of diverse devices, simultaneously facilitating efficient data aggregation and distribution. However, such connectivity raises significant security concerns, particularly given the limitations of available bandwidth, computing power, memory usage, and power supply constraints affecting the devices concerned. Although they are typically not targeted as frequently as enterprise infrastructures, home networks remain vulnerable to manipulation consisting, for instance, in impersonating a valid network endpoint, making data encryption essential. While gaining in popularity and being applied on a wide scale, the message queuing telemetry transport (MQTT) protocol does not provide built-in encryption at the application layer [1], [2].

Despite extensive research on securing MQTT communication and on machine learning-based intrusion detection systems (IDSs), interaction between MQTT payload encryption and protocol-level attack detectability remains insufficiently explored. In particular, it remains unclear whether encrypting application-layer data alters the statistical properties of MQTT traffic in a way that degrades the effectiveness of IDSs trained on protocol features. This uncertainty is especially critical for smart home environments, where resource-constrained devices must balance security, performance, and detection capability.

Most recent studies either assume plaintext payloads for IDS design or focus exclusively on cryptographic protection without validating its impact on anomaly detection. In contrast, this work explicitly investigates whether AES-based MQTT payload encryption may be deployed without sacrificing IDS performance, combining embedded-system measurements with a modified benchmark dataset to ensure fair and reproducible evaluation.

1.1. Research Problem and Objectives

Securing MQTT communication in smart home environments poses a fundamental design challenge. On the one hand, resource-constrained devices such as ESP32-based sensors have limited computational resources, making complex cryptographic mechanisms impractical. On the other hand, plaintext MQTT payloads are trivially susceptible to eavesdropping and manipulation by any party with access to the local network segment.

Transport layer security (TLS) addresses confidentiality at channel level but does not protect payload data end-to-end, e.g. when messages are relayed through an intermediary broker or stored for later processing. Lightweight payload-level

encryption, such as AES-128, may complement TLS by providing end-to-end content protection at a potentially lower computational cost. However, whether this added encryption layer is practically feasible on resource constrained microcontrollers, and at what latency cost, remains an open empirical question.

An equally critical concern arises at the intersection of encryption and intrusion detection. Machine learning-based IDSs trained on MQTT traffic typically rely on features derived from protocol-level fields, including packet lengths, timing patterns, and message types. When payload encryption transforms variable-length plaintext into fixed-length ciphertext, it alters the statistical distribution of these features. Therefore, it is unclear whether classifiers trained on plaintext traffic will retain their detection accuracy when applied to encrypted traffic. Existing benchmark datasets, such as MQTTset [3], contain plaintext payloads only and thus cannot be used directly to evaluate IDS robustness under encryption. A systematic methodology for adapting such datasets to reflect encrypted payloads, while preserving feature semantics and label consistency, is currently unavailable.

1.2. Contribution of This Work

This work addresses the problem of securing MQTT-based smart home communication while preserving the effectiveness of machine learning-based intrusion detection systems operating on protocol-level features. Unlike many existing studies that focus either on cryptographic protection or on intrusion detection in isolation, this paper considers their interaction under realistic resource constraints. As a result, the contributions of this study span both scientific insights into IDS behavior under encrypted traffic and engineering validation of lightweight security mechanisms on embedded platforms.

From a methodological and analytical perspective, this paper provides:

- a systematic investigation of how AES-based MQTT payload encryption influences the statistical characteristics of protocol-level features used by machine learning–based intrusion detection systems,
- a reproducible methodology for adapting an established benchmark dataset to reflect encrypted, fixed-length MQTT payloads while preserving feature semantics and labeling consistency,
- a comparative evaluation of classical and neural machine learning classifiers, revealing which algorithmic families remain robust under payload encryption and which are adversely affected by cryptographic transformations.

From an implementation and validation perspective, the paper delivers:

- a practical implementation and comparison of multiple MQTT security configurations, including TLS, authentication mechanisms, and AES-128 payload encryption, on ESP32 microcontrollers representing different processor architectures,
- detailed experimental measurements of connection setup time, message publication latency and encryption overhead under constrained computational and energy conditions,
- an end-to-end validation demonstrating that payload-level encryption can be integrated into MQTT-based smart home systems without compromising intrusion detection capabilities, provided that appropriate classifiers are employed.

The remainder of this paper is structured as follows. Section 2 reviews related work, Section 3 describes the approach developed by the authors and the experimental setup. Section 4 evaluates performance of the encryption method used. Section 5 presents and discusses performance of the proposed ML algorithm-based IDSs, while Section 6 concludes the study.

2. Related Works

As the number of networked devices continues to grow, home network security becomes an increasingly complex issue. This makes home network infrastructure an attractive target for attacks and a platform for launching attacks on other environments (e.g. botnets). A review of the literature describing attacks on home networks reveals a considerable number of scientific works focusing on the topic in question. Integration of existing solutions with monitoring and control systems presents additional challenges. MQTT is a popular solution used in this specific area. MQTT defines how IoT devices can publish and subscribe to data over the Internet.

The sender (publisher) and the receiver (subscriber) communicate via topics and are decoupled from each other. The MQTT broker filters incoming messages and distributes them correctly to the subscribers.

2.1. Home Network Threats Described in the Literature

The survey presented in [4] provides a systematic literature review of cybersecurity in Smart Home Internet of Things (SHIoT) environments. The authors catalog common attacks against SHIoT, including: (i) brute-force attacks, (ii) data breaches and monitoring, (iii) denial-of-service (DoS) attacks, (iv) data forgery, and (v) spam or malware. Paper [5] maps this classification to attacks targeting the MQTT protocol.

When analyzing vulnerabilities and potential attacks on the MQTT protocol, the authors also considered changes introduced in its subsequent versions, particularly the latest 5.0 iteration[1]. They also provide defense strategies and best practices for hardening MQTT-aware nodes. In this context, several approaches are selected:

- proper authentication and robust access control lists (ACLs) to restrict publish/subscribe capabilities per client and topic,
- end-to-end security considerations, including payload-level encryption or application-layer cryptographic protections to complement TLS and achieve true end-to-end confidentiality,

[1] https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

- secure broker and client deployment practices,
- monitoring, anomaly detection, and testing approaches to identify misconfigurations and vulnerable implementations before exploitation.

The authors also emphasize the role of modern techniques such as ML-based anomaly detection and cryptographic mechanisms in mitigating MQTT-specific threats.

Unfortunately, while the literature provides a comprehensive taxonomy of attacks targeting smart home and MQTT-based environments, it does not address how such threats can be effectively detected when application-layer data are protected using payload-level encryption.

2.2. Securing MQTT-based Networks

Effectively securing MQTT-based networks is essential, because MQTT is often used in IoT systems where devices are resource-constrained and widely distributed. Common approaches and best practices for securing MQTT deployments include the following:

- transport-layer encryption (TLS/mTLS),
- authentication and authorization of clients (publishers and subscribers),
- securing the topic structure,
- protecting the payload through encryption and/or digital signatures,
- hardening the software layer of MQTT-based systems and brokers (operating systems, hypervisors, etc.),
- monitoring system behavior and enforcing the principle of least privilege.

There is a substantial body of research addressing these aspects and proposing various security enhancements.

The proposed countermeasures include secure configuration practices for nodes and brokers, intrusion detection systems, and cryptographic mechanisms for protecting both MQTT sessions and data payload. Specifically, article [6] proposes a lightweight symmetric encryption algorithm optimized for MQTT constraints to enhance confidentiality and integrity of device-broker communication. In [7], an in-depth analysis of MQTT protocol security is presented, including experiments with different cryptographic integrations under IoT-specific constraints. In the study, AES-CBC, RSA, and ECC-AES are applied to encrypt the message payload, and the system is tested against attacks such as black-box penetration, man-in-the-middle (MiTM), identity spoofing, and denial-of-service (DoS).

The authors of [8] analyze the overhead associated with double encryption in end-to-end security models and propose improvements for streamlined secure MQTT communication with robust key management and authentication mechanisms. Similarly, a novel approach based on AugPAKE authentication and PRESENT encryption is proposed in [9] to achieve mutual authentication, confidentiality, and non-repudiation in MQTT-based applications.

Another approach is presented in [10], where the MQTT-TLS profile for authentication and authorization for the constrained environments (ACE) framework specified by the IETF [11] is implemented and evaluated. This work focuses on implementing the functionality of the authorization server for client registration, authorization policies and access tokens, as well as broker-side mechanisms enforcing authentication across different MQTT versions.

In contrast to the above approaches which primarily focus on strengthening confidentiality and authentication, the impact of MQTT payload encryption on protocol-level traffic characteristics and subsequent intrusion detection performance has received limited attention.

2.3. Anomaly/attack Detection of MQTT-based Networks

The field of anomaly and attack detection in MQTT-based IoT networks has experienced significant growth, driven by the proliferation of IoT devices and the security vulnerabilities inherent in the lightweight MQTT protocol. Despite its widespread adoption in industrial IoT, smart home, and medical IoT applications, MQTT faces critical security challenges. The protocol lacks encryption and authentication by default, making it vulnerable to various attack.

Previous research has extensively evaluated classical machine learning (ML) algorithms for MQTT attack detection. Studies comparing Naive Bayes, k-nearest neighbors (k-NN), decision trees, random forest, support vector machines, and logistic regression demonstrate varying degrees of effectiveness across different attack types. An overview of the application of classical ML methods for anomaly detection (one-class) and attack classification (multiclass) is provided, among others in [12]–[14]. These studies address the problem of detecting attacks in IoT networks using different communication protocols, including MQTT.

Moreover, deep learning approaches have shown strong potential for detecting MQTT intrusion. In particular, the authors of [15] proposed a deep neural network (DNN) architecture designed specifically for analyzing MQTT traffic, achieving accuracies of 99.92% for uni-flow, 99.75% for bi-flow, and 94.94% for packet-flow binary classification tasks. Their work compares DNN performance with traditional ML algorithms (Naive Bayes, random forest, k-NN, and decision trees) as well as sequence-based models such as LSTM and GRU, demonstrating the advantages of deep learning for MQTT attack detection.

Feature selection techniques, including chi-square statistics, correlation analysis, and wrapper methods, have also been shown to improve model efficiency while maintaining high detection accuracy.

Most studies rely on benchmark datasets containing MQTT traffic. Such datasets have gained popularity in research on IoT intrusion detection systems, because they provide a shared and reproducible basis for developing and evaluating detection methods. Benchmark datasets typically include both legitimate MQTT traffic and well-characterized attack scenarios (e.g., DoS, brute force, and malformed data), providing ground truth labels for supervised learning. Datasets such as MQTTset [3] and MQTTEEB-D [16] were specifically de-

signed to provide rich labeled MQTT flows for supervised and semi-supervised intrusion detection, including protocol-level features and realistic attack scenarios. More recently, MQTT_UAD was published in [17]. It is a publicly available dataset containing MQTT traffic under denial-of-service, man-in-the-middle, and intrusion attacks, enabling reproducible evaluation of classification models in MQTT-specific environments.

At a broader IoT scale, [18] introduces CICIoT2023 – a large-scale benchmark comprising traffic from 105 real IoT devices communicating via MQTT, CoAP, and RTSP protocols, with over 30 attack types spanning DDoS, reconnaissance, spoofing, and brute-force categories. While these datasets significantly advance the availability of labeled IoT traffic for IDS research, none of them includes encrypted MQTT payloads, leaving the question of IDS robustness under payload encryption unanswered.

3. Approach and Experimental Setup

The proposed approach assumes that the chosen security method represents a trade-off between effectiveness (understood as the level of security offered), operational speed, and cost-effectiveness, where cost-effectiveness is understood as energy consumption and computational resource utilization. In MQTT-based home networks, data-providing devices have limited technical capabilities and often rely on battery power supply. Deployment of complex cryptographic mechanisms to protect data transmitted by simple sensors, such as temperature or motion devices, is therefore disproportionate to the threat model. The primary security emphasis is placed on network access control at the wireless layer, while lightweight payload-level encryption is evaluated as a feature.

The general approach consists of two main phases. The former covers the verification of performance indicators for various security configurations and the selection of the optimal solution. The other addresses the mapping of the selected mechanism to protocol parameters at the TCP and MQTT levels, followed by the adaptation of an established benchmark dataset and the development of corresponding evaluation guidelines.

Data transmission times were measured across four scenarios for client-to-broker publication: plaintext transmission, authentication-only transmission, AES-128 encrypted payload transmission, and TLS-secured transmission. Peak current consumption was recorded during each operation to assess energy impact.

Figure 1 illustrates the complete interaction sequence between a publisher and a broker, including the optional data preparation phase introduced by payload encryption. Attack and anomaly detection performance was subsequently evaluated on the modified dataset, using supervised multiclass classifiers trained on protocol-level features, with their accuracy and F1 scores computed on identical train-test splits to ensure comparability with baseline results.

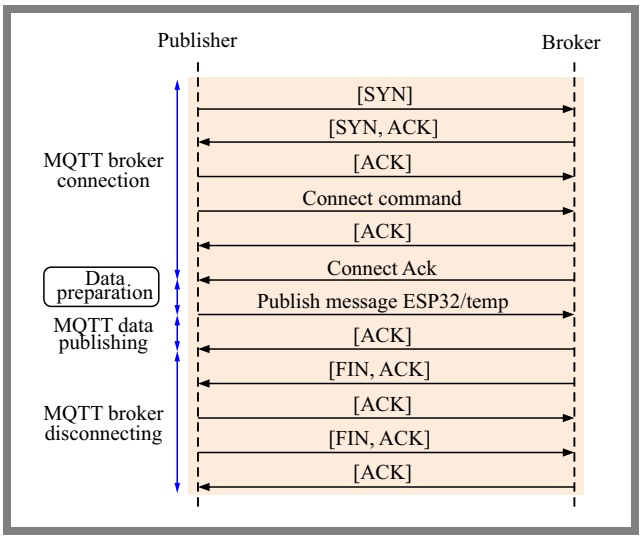

Fig. 1. Connection and MQTT data transmission time spans.

The diagram below outlines the standard process of connection, handshaking, data publishing, and disconnection, highlighting the key message exchanges and acknowledgements involved. The figure also shows an optional data preparation phase, which occurs only when MQTT messages are encrypted. The preparation time was therefore considered only in scenarios involving MQTT payload encryption.

4. Evaluation of Encryption Method Performance

Experimental evaluation was conducted on two microcontrollers from the ESP32 family: ESP32-S3 and ESP32-C3. The ESP32-S3 and ESP32-C3 are based on the Xtensa and RISC-V architectures, respectively. All measurements were conducted with the clock at 80 MHz to ensure comparable power conditions, although the ESP32-S3 supports speeds of up to 160 MHz. Identical library releases were used to implement WLAN, TLS, and MQTT on both devices, and the PSRAM external memory was disabled on the ESP32-S3 to ensure the same testing conditions. Timing measurements were determined for the following publication scenarios:

- plaintext publication without authentication,
- plaintext publication with authentication,
- TLS-secured plaintext publication without authentication,
- TLS-secured plaintext publication with authentication,
- AES-128 encrypted publication without authentication.

All timing measurements were performed directly on the ESP32 microcontrollers. Data were transmitted over Wi-Fi, with the ESP32 connected to a 2.4 GHz access point. The access point and the MQTT broker server were both connected via Ethernet to the same network switch. The ESP32 was located approximately 4 m from the access point, with no obstacles between the devices. Timing was measured using the `micros()` function, providing 1 µs resolution, which is adequate for operations on the millisecond scale. For each scenario, at least 500 measurement repetitions were executed,

Tab. 1. MQTT broker connection time.

Method	ESP32-S3		ESP32-C3	
	Mean [µs]	Std_dev [µs]	Mean [µs]	Std_dev [µs]
Plain	16 082.18	1 512.41	7 722.20	1 123.36
Auth	20 145.21	5 467.32	11 855.32	3 652.25
TLS	2 178 982.40	5 631.76	974 977.46	4 622.74
TLS_auth	2 188 194.09	10 181.12	1 623 887.00	16 832.54
Encrypted	19 160.12	2 737.36	13 171.94	1 729.27

Tab. 2. MQTT data publication time.

Method	ESP32-S3		ESP32-C3	
	Mean [µs]	Std_dev [µs]	Mean [µs]	Std_dev [µs]
Plain	2052.82	9.95	1105.60	4.45
Auth	2053.88	6.35	1105.95	6.41
TLS	1123.40	8.23	1144.50	6.23
TLS_auth	1103.95	7.06	2334.40	131.69
Encrypted	2100.60	8.57	2252.17	169.17

preceded by a series of 50 preliminary runs to minimize cold-start effects and stabilize cache memory contents.

The measurement campaign and MQTT result reporting were implemented using the base Arduino-esp32 library, which internally relies on ESP-IDF framework components for Wi-Fi, TCP/IP, and MQTT operations. AES-128 payload encryption was implemented using the AESLib library [19], a portable software-based AES implementation that operates across multiple hardware platforms and programming languages without relying on platform-specific hardware acceleration.

This choice favors implementation portability and reproducibility over platform-specific optimization. While absolute timing values are platform and implementation-specific, the relative overhead of AES-128 encryption compared with the connection setup and message publication is expected to remain consistent across implementations that use the same standard networking libraries, as the dominant latency contributors (Wi-Fi stack, TLS handshake, TCP operations) are governed by the vendor-provided framework.

For each scenario, mean execution time and standard deviation were recorded. All timing measurements were saved after successful network authentication and broker availability. The results are presented in Tab. 1.

Furthermore, the time required for data publication by the MQTT client running on the ESP32 was determined. The transmitted data consisted of floating-point values with two decimal places. The results are presented in Tab. 2.

Tab. 3. Data preparation (encryption) time.

Method	ESP32-S3		ESP32-C3	
	Mean [µs]	Std_dev [µs]	Mean [µs]	Std_dev [µs]
Plain	0.00	0.00	0.00	0.00
Auth	0.00	0.00	0.00	0.00
TLS	0.00	0.00	0.00	0.00
TLS_auth	0.00	0.00	0.00	0.00
Encrypted	397.00	5.26	495.22	6.47

Finally, the AES-128 encryption time was measured. The encryption process was performed after establishing the MQTT connection and before data publication. If encryption was not required for a given publication scenario, the encryption time was considered as zero.

As shown in Tabs. 1 – 3, the AES-128 encryption time is less than 50% of the publication time on the ESP32-C3 and less than 25% of the publication time on the ESP32-S3. It is also noteworthy that the time required to establish MQTT sessions is significantly longer than the time required for message publication or payload encryption.

Longer connection and publication times were observed for the ESP32-S3 compared to the ESP32-C3. This is likely caused by architectural differences between the two platforms. The ESP32-S3 features a dual-core Xtensa LX7 processor, whereas the ESP32-C3 employs a single-core RISC-V architecture. In the dual-core ESP32-S3, Wi-Fi-related tasks are typically pinned to core 0 by default within the Wi-Fi driver framework. In contrast, components such as the lightweight IP (lwIP) TCP/IP stack, operating at priority level 18, remain unpinned and may execute on either core. This configuration requires inter-core synchronization and task handoffs through the RTOS, which may increase latency in TCP transmission operations.

By contrast, the single-core ESP32-C3 executes all processes on a single core, eliminating inter-core synchronization overhead and potentially reducing networking latency at the same clock speed.

Considering the obtained data, we conclude that MQTT payload encryption ensures integrity and confidentiality of transmitted data within a local network. Assuming that the local Wi-Fi network is properly secured and access requires authentication, encrypting MQTT payload data further enhances communication security, although it increases the size of the transmitted data.

In the following sections, we demonstrate that increasing the payload size to 16 bytes (corresponding to the size of an AES-128 ciphertext for a two-digit floating-point value) does not degrade the effectiveness of machine learning algorithms used for anomaly and attack detection. Therefore, MQTT payload encryption appears to be a practical and promising approach for improving security in smart home networks.

5. Performance of the ML Algorithm-based IDS

We evaluated the detectability of anomalies and attacks in MQTT-based systems using a public MQTTset dataset, available at [2]. This dataset was chosen for the following reasons:

- It defines a typical IoT environment of smart home ecosystems, where data are primarily published by sensor devices. Therefore, the traffic patterns of publishers resemble those observed in smart home deployments. Although the dataset

[2] https://www.kaggle.com/datasets/cnrieiit/mqttset/data

is synthetic – as the network traffic was generated based on sensor behavior models – it has been recognized within the academic community as one of the representative datasets for IoT and smart home research. Additionally, the dataset includes packet capture (PCAP) files, enabling a detailed analysis of MQTT traffic across multiple layers of the OSI model.

- It uses plaintext MQTT communication (via the 1883 port with an MQTT broker), which enables a simple comparison of ML algorithm's performance on both the original and modified datasets under identical conditions.

The dataset MQTT set [3], because its vulnerability simulations focus on common and easily identifiable cyberattacks targeting MQTT traffic:

- *Flooding denial-of-service (DoS)* – aimed at saturating the MQTT broker by establishing multiple client connections and maximizing message transmission within each connection.
- *MQTT Publish flood* – in which a malicious IoT device establishes an MQTT connection and launches a DoS attack by periodically transmitting a lot of MQTT Publish messages within a single connection. The objective is to overload server resources such as connection slots, network bandwidth, thereby blocking normal communication.
- *SlowITe* – a DoS attack targeting the MQTT application protocol that requires minimal bandwidth and resources. It operates by initiating a large number of connections to the MQTT broker to occupy all available connection slots.
- *Malformed data* – generates and sends malformed packets to the broker to trigger exceptions in the target service. In the considered scenario, a sequence of malformed Connect or Publish packets is transmitted to the broker.
- *Brute-force authentication* – involves repeated attempts to guess user credentials used for MQTT authentication. Since DoS and DDoS attacks remain among the most common threats, the dataset reflects their characteristics as well as attacks targeting authorization mechanisms, malformed data, and violations of the MQTT protocol.

A limitation of this dataset is that it does not capture specification of wireless transmission, such as connection establishment delays caused by medium access. However, when focusing on anomaly and attack detection methods based on MQTT protocol-level features, this limitation does not restrict the usefulness of the dataset for further analysis.

Encrypting messages published by MQTT clients results in fixed-length payloads. This modification does not significantly affect anomaly and attack detection results when ML methods rely primarily on protocol-level features. To verify this assumption, we modified the MQTTset dataset accordingly.

As mentioned earlier, the modification involved assigning a new MQTT length value to Publish messages. Because the encrypted MQTT payload has a fixed size of 32 bytes, the MQTT message length depends only on the topic length.

Tab. 4. Effectiveness of classification model (16 bytes).

Algorithm	Accuracy	F1 score	Δ Accuracy	Δ F1 score
Neural network	0.9923	0.9908	-0.0010	-0.0025
Random forest	0.9971	0.9969	0.0028	0.0026
Naive Bayes	0.6215	0.7650	–0.3664	–0.2247
Decision tree	0.9971	0.9969	0.0191	0.0119
Gradient boost	0.9949	0.9947	0.0038	0.0030
Multilayer perceptron	0.9939	0.9936	0.0470	0.0299

Therefore, the modified MQTT length value was defined as the sum of the fixed payload size, the fixed MQTT topic length field (2 bytes), and the variable topic length.

Furthermore, each MQTT payload field was filled with a random string representing a 16-byte ciphertext encoded as 32 characters. This resulted in a modified dataset on which ML classifiers were applied to compare results with those obtained from the original dataset from [3]. Both datasets have the same feature schema, labeling strategy, and preprocessing pipeline to ensure comparability.

The modification was applied to the dataset containing MQTT network traffic extracted from PCAP traces. The dataset also includes related feature vectors enabling it to be used in ML classification tasks. Importantly, the modification affected only the subset representing legitimate traffic, while subsets describing anomalous or attack-related traffic remained unchanged.

For validation, supervised ML classifiers were trained separately on the original and modified datasets using identical architectures, hyperparameters, and train-test splits. Model performance was evaluated using accuracy and F1 score. Additionally, feature importance rankings were analyzed to determine whether enforcing fixed-length payloads altered the discriminative characteristics of the data.

Within the detection framework, the same widely applied multiclass classifiers as used in [3] were employed. In particular, the original study focused on decision tree (optimized), random forest, gradient boosting, multilayer perceptron (MLPC), a neural network implemented using Keras, and Gaussian Naive Bayes algorithms. To ensure comparability of results, we used the same classification algorithms and parameter settings.

Tables 4 and 5 present the classification performance for MQTT communication scenarios where publishers transmit encrypted 16- and 32-byte payloads, respectively.

Model performance was evaluated using accuracy and F1 score metrics. Accuracy represents the percentage of correctly classified instances, while the F1 score combines precision and recall. These metrics are based on the standard confusion matrix components: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN).

Despite the introduction of payload encryption, 5 of 6 algorithms maintained high classification performance with their

Tab. 5. Effectiveness of classification model (32 bytes).

Algorithm	Accuracy	F1 score	Δ Accuracy	Δ F1 score
Neural network	0.9922	0.9905	-0.0011	-0.0027
Random forest	0.9971	0.9969	0.0028	0.0026
Naive Bayes	0.6215	0.7650	–0.3664	–0.2247
Decision tree	0.9971	0.9969	0.0191	0.0119
Gradient boost	0.9949	0.9947	0.0038	0.0030
Multilayer perceptron	0.9955	0.9952	0.0486	0.0215

accuracy remaining within 5 percentage points of the baseline results. Random forest and decision tree classifiers showed slight performance improvements (accuracy Δ: +0.0028 to +0.0191), achieving accuracy of 99.71% on encrypted payloads. Gradient boosting maintained 99.49% accuracy with minimal variation (accuracy Δ: +0.0038). The neural network model showed only a negligible decrease in performance (accuracy Δ: –0.0010 for both payload lengths), while the multilayer perceptron improved to 99.39% and 99.55% for the 16-byte and 32-byte payload scenarios, respectively (accuracy Δ: +0.0470 and +0.0486).

In contrast, the Naive Bayes classifier exhibited a substantial performance degradation after the introduction of encrypted MQTT payloads. Its accuracy dropped from 98.79% to 62.15% in both scenarios.

This behavior can be explained by the conditional independence assumption underlying the Naive Bayes model, which assumes that features are statistically independent given the class label. AES-128 encryption produces a cryptographically uniform output, which violates these probabilistic assumptions. In contrast, tree-based models such as random forest and decision tree rely on recursive partitioning based on information gain or Gini impurity, making them less sensitive to feature distribution assumptions. Applying encryption to the MQTT payload shifts class separability to different feature subspaces rather than eliminating it, allowing tree-based models to adapt effectively.

Similarly, neural network architectures can learn non-linear feature transformations that generalize across both encrypted and unencrypted traffic patterns. The slight performance improvements observed for some classifiers suggest that cryptographic uniformity may reduce overfitting to noise patterns present in the original unencrypted data. Importantly, the negligible performance differences observed for 5 of 6 classifiers are not a limitation but rather a central finding of this study. The fact that accuracy and F1 score remain virtually unchanged after payload encryption confirms that these classifiers rely predominantly on protocol-level features, such as packet timing, message type distributions, and connection patterns, rather than on payload content.

This observation directly validates the premise underlying our dataset modification methodology. If features are properly selected at the protocol level, encrypting the application-layer payload does not degrade attack detectability. The sole exception, Naive Bayes, serves as a useful negative control, demonstrating that classifiers with strong distributional assumptions can indeed be affected by encryption-induced changes in feature statistics.

6. Conclusions

The use of MQTT payload encryption provides effective protection against eavesdropping and data integrity violations in home sensor networks. As demonstrated in this study, the implementation of the AES-128 algorithm on popular ESP32 microcontroller platforms efficiently handles the data encryption process. Moreover, the time required to perform encryption has a negligible impact on the overall data processing time of the microcontroller, particularly when compared with the time needed for radio communication over the Wi-Fi network. Consequently, the overall efficiency of MQTT-based communication is preserved.

Furthermore, the results obtained using the modified MQTTset dataset show that enforcing fixed-length encrypted payloads does not significantly affect the effectiveness of most ML classification methods. Consequently, the ability to detect attacks and traffic anomalies in MQTT is also preserved. An important exception is the Naive Bayes classifier, whose performance significantly deteriorates after the introduction of encrypted payloads. This behavior results from the strong conditional independence assumptions underlying the Naive Bayes model which are violated by the statistical properties of encrypted data. Consequently, Naive Bayes classifiers appear unsuitable for intrusion detection in environments where MQTT payload encryption is applied.

From an application perspective, the results demonstrate that AES-based MQTT payload encryption can be integrated into smart home IoT systems without compromising their intrusion detection capabilities, provided that appropriate classifiers, such as tree-based or neural network models, are employed.

References

[1] EMQX Team, "MQTT with TLS: Fortifying MQTT Communication Security", 2023 (https://www.emqx.com/en/blog/fortifying-mqtt-communication-security-with-ssl-tls).

[2] N.T. Dhokane *et al.*, "S-MQTT: A Secure MQTT Protocol with Merkle Tree Authentication and AES Encryption for IoT Communication Systems", *Ingénierie des Systèmes d'Information*, vol. 30, pp. 1963–1973, 2025 (https://doi.org/10.18280/isi.300803).

[3] I. Vaccari *et al.*, "MQTTset, a New Dataset for Machine Learning Techniques on MQTT", *Sensors*, vol. 20, art. no. 6578, 2020 (https://doi.org/10.3390/s20226578).

[4] L. Ayavaca-Vallejo and D. Avila-Pesantez, "Smart Home IoT Cybersecurity Survey: A Systematic Mapping", *2023 Conference on Information Communications Technology and Society (ICTAS)*, Durban, South Africa, 2023 (https://doi.org/10.1109/ICTAS56421.2023.10082751).

[5] S. Lakshminarayana, A. Praseed, and P.S. Thilagam, "Securing the IoT Application Layer from an MQTT Protocol Perspective: Challenges and Research Prospects", *IEEE Communications Surveys and*

Tutorials, vol. 26, pp. 2510–2546, 2024 (https://doi.org/10.1109/COMST.2024.3372630).

[6] R.A. Mahajan *et al.*, "Enhancing MQTT Security in the Internet of Things with an Enhanced Symmetric Algorithm", *Journal of Electrical Systems*, vol. 20, pp. 126–137, 2024 (https://doi.org/10.52783/jes.758).

[7] A. Al-Ani *et al.*, "Evaluating Security of MQTT Protocol in Internet of Things", *2023 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Regina, Canada, 2023 (https://doi.org/10.1109/CCECE58730.2023.10288857).

[8] H.Y. Chien, A.T. Shih, and Y.M. Huang, "Exploring MQTT Broker-based, End-to-end Models for Security and Efficiency", *Sensors*, vol. 25, art. no. 5308, 2025 (https://doi.org/10.3390/s25175308).

[9] I. Sahmi, A. Abdellaoui, T. Mazri, and N. Hmina, "MQTT-PRESENT: Approach to Secure Internet of Things Applications Using MQTT Protocol", *International Journal of Electrical and Computer Engineering*, vol. 11, pp. 4577–4586, 2021 (https://doi.org/10.11591/ijece.v11i5.pp4577-4586).

[10] M. Michaelides, C. Sengul, and P. Patras, "An Experimental Evaluation of MQTT Authentication and Authorization in IoT", *Proc. of the 15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH '21)*, pp. 69–76, 2021 (https://doi.org/10.1145/3477086.3480838).

[11] C. Sengul and A. Kirby, "RFC 9431. Message Queuing Telemetry Transport (MQTT). and Transport Layer Security (TLS). Profile of Authentication and Authorization for Constrained Environments (ACE) Framework", 2023 (https://doi.org/10.17487/RFC9431).

[12] J. Asharf *et al.*, "A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things Challenges, Solutions and Future Directions", *Electronics*, vol. 9, art. no. 1177, 2020 (https://doi.org/10.3390/electronics9071177).

[13] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, „Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges", *Cybersecurity*, vol. 2, art. no. 20, 2019 (https://doi.org/10.1186/s42400-019-0038-7).

[14] E. Jove *et al.*, „Intelligent One-class Classifiers for the Development of an Intrusion Detection System: The MQTT Case Study", *Electronics*, vol. 11, art. no. 422, 2022 (https://doi.org/10.3390/electronics11030422).

[15] M.A. Khan *et al.*, "A Deep Learning-based Intrusion Detection System for MQTT Enabled IoT", *Sensors*, vol. 21, art. no. 7016, 2021 (https://doi.org/10.3390/s21217016).

[16] A. Aqachtoul *et al.*, "MQTTEEB-D: A Real-world IoT Cybersecurity Dataset for AI-powered Threat Detection in MQTT Networks", *Data in Brief*, vol. 62, art. no. 111897, 2025 (https://doi.org/10.1016/j.dib.2025.111897).

[17] J. Aveleira-Mata *et al.*, "MQTT_UAD: MQTT under Attack Dataset. A Public Dataset for the Detection of Attacks in IoT Networks Using MQTT Protocol", *Data in Brief*, vol. 63, art. no. 112167, 2025 (https://doi.org/10.1016/j.dib.2025.112167).

[18] E.C.P. Neto *et al.*, "CICIoT2023: A Real-time Dataset and Benchmark for Large-scale Attacks in IoT Environment", *Sensors*, vol. 23, art. no. 5941, 2023 (https://doi.org/10.3390/s23135941).

[19] M. Sychra, "AESLib – Arduino and ESP AES library", *Arduino Docs*, 2023 (https://docs.arduino.cc/libraries/aeslib/).

Mariusz Gajewski, Ph.D.
Department of Cybersecurity
https://orcid.org/0000-0002-8084-6537
E-mail: M.Gajewski@il-pib.pl
National Institute of Telecommunications, Warsaw, Poland
https://www.gov.pl/web/instytut-lacznosci

Wojciech Sałabun, Prof.
Department of Advanced Information Technology
https://orcid.org/0000-0001-7076-2519
E-mail: W.Salabun@il-pib.pl
National Institute of Telecommunications, Warsaw, Poland
https://www.gov.pl/web/instytut-lacznosci
West Pomeranian University of Technology, Szczecin, Poland
https://www.zut.edu.pl

Hybrid Feature Selection Framework for Machine Learning-based Bot Detection on Social Media

Amina Guendouz, Fatima Boumahdi, Mohamed Abdelkarim Remmide, Abdelghani Foura, and Amina Madani

University of Blida 1, Blida, Algeria

https://doi.org/10.26636/jtit.2026.2.2541

Abstract — Nowadays, social media impact all aspects of our lives, making us vulnerable to fraud and scams. Bots are believed to be the most prevalent form of malware that may be found in social media environments. New detection methods are required to keep up with the pace of their continuous advancement. This paper offers an overview of machine learning-based bot detection methods. The study revealed that the effectiveness of machine learning (ML) models can be significantly hindered by redundant and irrelevant features present in the datasets, which can lead to performance degradation. A hybrid feature selection (FS) combining characteristics of the genetic algorithm (GA) and the mutual information (MI) approach is proposed to overcome this challenge. The proposed method is evaluated using the following approaches: random forest (RF), decision tree (DT), support vector machine (SVM), and logistic regression (LR). Compared to the state-of-the-art models, the proposed method is capable of efficiently identifying bots using only a small number of features. For the dataset used, we achieved a classification accuracy of 0.99 using 4 features only.

Keywords — bot detection, feature selection, machine learning, social media

1. Introduction

A bot is a software tool that imitates the behavior of a real person [1]. Bots can be used for negative as well as positive purposes [2]. Social bots that perform useful services [3], such as spreading news and interacting with users, are called benign bots.

However, most bots are used to carry out malicious activities [2], [4] such as running fabricated accounts, publishing fake posts and social spam, conducting phishing campaigns, spreading rumors to manipulate people, spamming, and web scraping to steal user information. Such activities not only annoy users but also negatively impact security of the public and specific individuals.

Bot detection is relied upon to classify social network accounts as human- or bot-operated based on an analysis of their features [1]. Various techniques, such as behavior analysis-based detection systems, anomaly-based systems, graph-based detection systems, and ML-based detection systems [4] have been used for this specific purpose.

According to [5], approaches based on supervised ML algorithms are the most common and have proven to be effective under many scenarios. Nevertheless, they still suffer from some weaknesses, especially with the continuous development of bots. Existing datasets and detection approaches must keep up with this evolution to enable more effective bot-human classification.

Real-life datasets can include a wide range of features. When building an ML algorithm, we must deal with all of them, even if not all are relevant. The inclusion of unnecessary features when training a model leads to increasing the degree of complexity of the model, thus decreasing its generalization capability, and reducing its overall accuracy.

Therefore, choosing the relevant set of features used to describe the entities to be classified is a critical step in building an ML model [5]. This step, known as feature selection (FS), aims to identify the optimal set of features for building a given ML model.

In this paper, we used two different bot detection methods: the traditional one, in which classification is performed directly after data preprocessing, and the new method, in which an FS task was added preceding the classification stage. Two FS algorithms are used: genetic algorithm (GA) and mutual information (MI), in addition to a hybrid approach including both above.

For classification purposes, four ML algorithms are explored for each method: random forest (RF), decision tree (DT), support vector machine (SVM), and logistic regression (LR). Finally, a comparative analysis of the methods is carried out according to three effectiveness criteria: accuracy, precision, and F1 score.

The remainder of the paper is organized as follows. Section 2 presents existing work focusing on the detection of social media bots. Section 3 explains the outlines of the proposed approach. Section 4 offers more details concerning the contribution made. Section 5 presents and discusses the results obtained. Finally, Section 6 concludes the work and provides a brief overview of potential future paths.

2. Related Works

In recent years, significant research efforts have been dedicated to identifying bots in social media. In this study, we focus on ML models and present a review of existing work focusing on this specific field. The proposed approaches are classified according to the ML models adopted and are categorized as: supervised, unsupervised, and semi-supervised.

2.1. Supervised ML

The widest range of works described in the literature relies on supervised ML models. The authors of [6] proposed SEBD: a stream-based evolving bot detection framework that consists of three phases: data collection, streaming using Kafka, as well as detection, in which they used "Bot-MGAT" to forecast the classification of every account. In a previous work [7], they proposed the Bot-MGAT framework that combines the multiview graph attention mechanism with a transfer learning approach to identify bots using profile features only.

In [8], a graph-based X platform (formerly Twitter) bot detection HOFA framework is proposed that combats the challenge of heterophilous disguise. HOFA incorporates modules such as Homo-Aug homophily-oriented graph augmentation and FaAt frequency adaptive attention, which are based on deep learning techniques such as MLPs and attention mechanisms.

A novel bot detection model that uses personal information to construct user profiles is presented in [9]. This initiative employs advanced techniques, such as deep contextualized word embedding using ELMO Glove (global vectors) and ELMO (embedding from the language model) for the textual analysis of tweets. During the pre-processing step, the user's profile is included into all X accounts using the content of the tweets in the data. Then, an ML model is used to identify social bots by analyzing personal information.

The authors of [10] focused on the detection and classification of social bots on the X platform. They also emphasized the importance of feature engineering methods and explainable ML in improving bot detection. The authors defined new bot categories and designed two additional datasets that include accounts which have been enriched with the categories of the newly identified bots. The dataset is balanced using the ADASYN algorithm to avoid bias. Several classification algorithms have been used thereafter for binary classification and for multiclass bot detection.

In [11], a new method is proposed to encode user accounts as low-dimensional feature vectors, identifying suspicious bot accounts, and generating embeddings for information retrieval purposes. The system uses a multilingual technique to effectively detect suspicious X accounts by analyzing a set of features, regardless of the account language. The work combines relevant metadata features along with text-based features transformed into vectors independently of the language of the input text.

Paper [12] introduced a multilayer ML approach. Beginning with a dataset that has been labeled, it carries out feature extraction using standard tests and correlation analysis. To overcome the limitation correlation, the *chi2* test on non-text attributes is applied to determine 5 strongest features. Then, the text attributes undergo feature engineering, followed by an initial classification procedure that generates a vector of predictions for each text attribute. The authors provide a comprehensive assessment of the effectiveness of several classification algorithms, along with an evaluation of two widely used strategies for enhancing text attributes: bag-of-words and n-gram model.

2.2. Unsupervised ML

Only a few researchers employed unsupervised ML algorithms for bot detection. Paper [13] proposes an approach that uses unsupervised ML algorithms for bot detection on social media. Initially, a set of features is chosen to distinguish between bots and genuine accounts. Subsequently, the efficacy of two clustering techniques, namely *dbscan* and *kmean*, is evaluated on six datasets using these features. The results demonstrated that *dbscan* achieved higher efficiency by obtaining a better level of accuracy.

2.3. Semi-supervised ML

Some scientists harness the idea of using a combination of supervised and unsupervised ML algorithms for bot detection. The authors of [14] addressed the issue of classifying bots as malicious or benign. They implemented four semi-supervised ML algorithms: semi-supervised Gaussian mixture model, S3VM (semi-supervised SVM), label propagation method being a graph-based SSML model that iteratively extends the labeling of all nodes on the graph until convergence is reached, and finally label spreading (LS). They identified significant features that may be used to differentiate between benign and malicious bots and showed that SVM achieved the best results in this classification.

In [15] and [16], an approach with graph-based features, obtained from flow-level data, is presented to enhance training and inference of ML models. The proposed BotChase is an anomaly-based bot detection system that can identify bots regardless of the protocol used. It is resistant to zero-day attacks and can handle large datasets properly. The authors suggest using feature normalization (F-Norm) in addition to graph-based features in BotChase and assess other machine learning algorithms.

2.4. Semi-supervised ML

Feature selection is a task that aims to select effective subsets from original features. In machine learning, the goal of FS techniques is to find the optimal set of features allowing to create optimized ML models. The FS process eliminates irrelevant features in such a way that it reduces the dimensionality of the data, accelerates the classification process, improves the model's comprehensibility, and increases its overall performance and accuracy [17], [18]. Despite the benefits brought by FS to the ML field, their use in bot detection models is restricted. To the best of our knowledge, what we present in this section is the only existing work in this field.

In [19], four ML algorithms are tested on a public dataset, and some expressive features based on simple user profile counters are proposed for the classification of bots on X. They focus on the use of features that are easy to obtain and constitute common profile attributes, as they can be retrieved in a single request using the X API. The choice of five characteristics was determined by empirical analysis based on previous experience in developing X bots. Research emphasizes that even with a limited number of features, it is feasible to identify bots with a certain degree of complexity.

In [20], four strategies are used to identify the appropriate characteristics: correlation attributes, information gain, cross-validation attribute evaluation, and evaluation of the wrapper subset. A public dataset available from Kaggle containing 18 features is used and different ML algorithms (RF, NB, SVM, and NN) are applied to evaluate performance.

If we take an in-depth look at the existing paper, we find that, despite the good results obtained, most of these works do not attach importance to model optimization. Actual experiments are performed on large datasets that include several features.

However, not all those features are relevant for bot detection. Introducing feature selection into the bot detection process seems to be a promising initiative. By carefully choosing the most optimal features and restricting the classification task to those features only, it is possible to obtain more significant results while simultaneously reducing execution time and minimizing complexity of the system.

Nevertheless, the analyzed research fails to consider this stage or, sometimes, performs it manually.

3. Proposed Methodology

As shown in Fig. 1, we took two different paths: the traditional one (without optimization) and one relying on the proposed method (with optimization). This was done to obtain a clear picture in the comparison step, highlighting the benefits of introducing the FS task.

After importing the data, our method goes through three main stages: (i) data pre-processing, (ii) classification, and (iii) obtaining and comparing the results.

3.1. Dataset and Pre-processing

In our experiment, we used a publicly available dataset from the X platform, originating from [21]. The dataset comprises a total of 8 386 records, categorically divided into two primary groups: 3 474 records representing human interactions and 4 912 records attributed to bot activity. It contains 69 features defined for each of these accounts. These features can be categorized into three groups: content, account information, and account use features (Fig. 2).

In search of better data quality and reliability, the data from the dataset was subjected to a pre-processing step. We removed missing values, eliminated duplicates, as well as identified and handled outliers. Additionally, we standardized formats and corrected inconsistencies in the data, preparing them for accurate and effective model training.

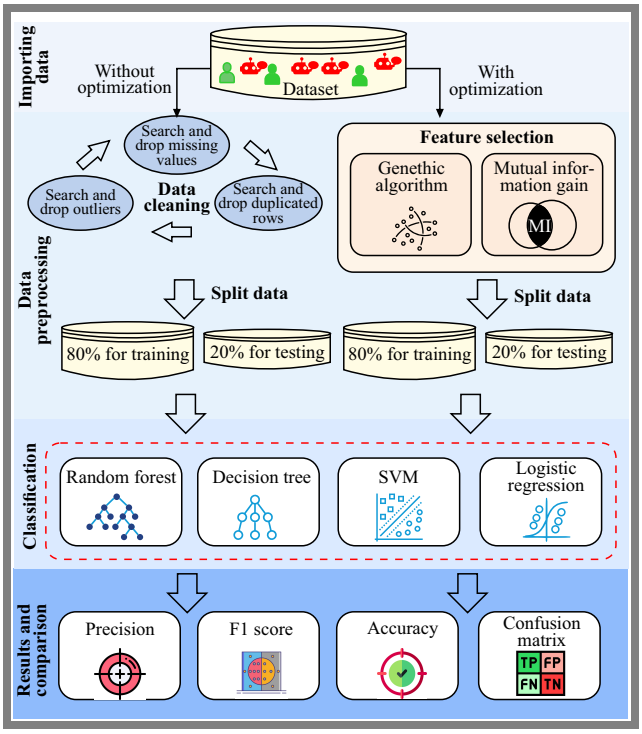

Fig. 1. Proposed bot detection methodology.

Content features	Account information	Account usage
statuses_count	ID	followers_count friends_count
favourites_count	default_profile	listed_count
min_tweet_length	default_profile_image	num_reply num_retweet min_
max_tweet_length	geo_enabled	favorite
avg_tweet_length	profile_use_background_image	max_favorite avg_favorite
min_urls max_urls	profile_background_tile	account_age
avg_urls min_hashtags	utc_offset	friends_followers_ratio
max_hashtags	protected	friends_followers_ratio_beq_50
avg_hashtags	verified	friends_followers_square_ratio
max_mentions	digits_name	2_followers_minus_friends 2_
avg_mentions	name_length screen_	followers_beq_100
max_retweets	name_length	lists_followers_ratio retweet_
avg_retweets	screen_name_length_	followers_ratio
description_length	name_length_ratio	favorites_followers_ratio
description_contains_bot	screen_name_contains_	lists_status_ratio
avg_urls_status_ratio	bot name_entropy	retweet_status_ratio
avg_mentions_status_ratio	screen_name_entropy	favorites_status_ratio
avg_favorite_status_ratio	profile_has_url	reply_status_ratio
	profile_pic_frec digits_	friends_account_age_ratio
	screen_name	followers_account_age_ratio
		favourites_account_age_ratio
		statuses_account_age_ratio
		lists_account_age_ratio
		friends_followers+friends_ratio

Fig. 2. Category of features of the X dataset (formerly Twitter).

3.2. Feature Selection and Classification

FS is introduced to find the optimal set of features that offer the best classification results. The dataset reduced to the selected features is then subjected to four classification algorithms to estimate the highest bot prediction score. We selected two algorithms (GA and MI) and used a hybrid solution comprising both.

The final stage of the proposed methodology is classification. The selected features from the previous step are the only ones considered for bot identification. The dataset is reduced to the selected feature subset. Then, it is divided into training and testing sets. We employ an 80:20 ratio to split raw and inte-

grated features, with 80% of the data set allocated for training classification algorithms and 20% for testing. The classification process involves the use of the test and train data sets for each feature subset generated from previous methods. This study uses four classifiers: random forest (RF), decision tree (DT), support vector machine (SVM), and logistic regression (LR).

4. Feature Selection Techniques

4.1. Genetic Algorithm

he genetic algorithm (GA) is inspired by the biological evolution process [22]. It is an optimization method that draws inspiration from the process of natural selection. This population-based search algorithm uses the idea of survival of the fittest. By iteratively applying genetic operators to members of the population, new populations are created. Chromosomes (population individuals), fitness function, and biologically inspired operators are key elements of GA [22]. Chromosomes are considered as possible solutions. The fitness function is used to dedicate a value to everyone in the population. After that, GA operators are applied to generate a new population.

The biologically inspired operators include selection, mutation, and crossover. Selection enables individuals to be chosen for processing in the next steps based on their fitness value. The crossover operator is a mechanism that combines two or more parents to generate new offspring solutions for the subsequent generation. During a mutation, certain pieces of the chromosomes will be randomly inverted based on probability.

The procedure of GA for FS is as follows: initial population generation, fitness function, selection, mutation, and crossover, with the next generation being produced in the final step (Fig. 3).

An initial population of solutions is randomly generated and the objective function is assessed for each member of this first generation. Chromosome genes are chosen from the dataset and without duplication. A chromosome (individual population) represents a subset of features from the original dataset. Each chromosome is a solution to the selection problem.

The fitness function serves as a tool allowing to discover the most effective features during classification (human-bot). It allows one to judge the ability of individuals (chromosomes) to survive through a fitness value and to compare them at each iteration. The fittest individuals are selected using an ML classifier. The classifiers used here are the same as those deployed in the classification phase. The fitness function computes accuracy for everyone, which represents, in this case, a feature subset. It returns the population members with the highest accuracy.

The creation of a new generation involves the selection of the fittest parents from the previous generation, followed by the application of crossover and mutation operators. The selection of individuals from the current generation, who will be the parents of the next generation, is determined randomly. However, the fittest individuals are more likely to be chosen.

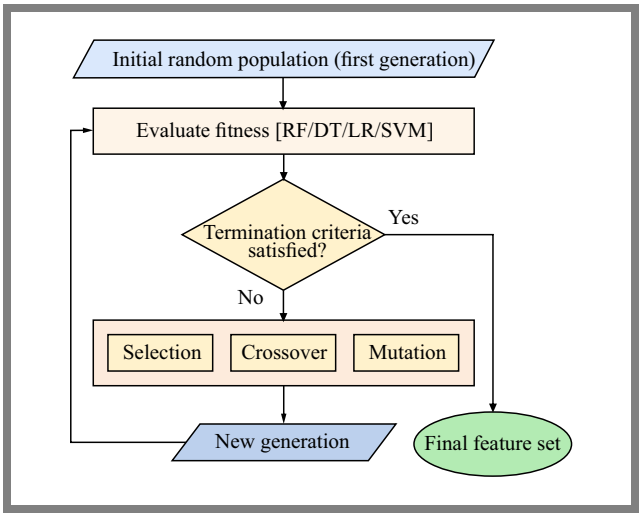

Fig. 3. Selection of features using genetic algorithm.

Suitability of a given solution is determined by its objective value, with higher objective values indicating better fitness.

A subset of the chosen solutions is utilized in a crossover operator that combines multiple parent solutions to generate new offspring solutions for the subsequent generation. The crossover operator typically produces offspring that inherit the shared traits of the parent solutions while simultaneously combining other characteristics in novel forms.

The next-generation solutions are subjected to a mutation operator, which introduces random variations within the solutions. The goal of the mutation operator is to ensure comprehensive exploration of the solution space, hence avoiding premature convergence to a local optimum.

Prior to classification, the new dataset is constructed using only the selected genes (features) from the previous step. However, once the GA converges, only the features represented by the best chromosome for a certain dataset is taken into consideration.

4.2. Mutual Information Algorithm

Mutual information relies on an elimination procedure to decrease the size of the input feature set while still preserving the discriminating class information for classification purposes. It estimates the level of information shared between two random variables. When the two variables are independent, the MI is zero. However, when the dependency of one variable on the other increases, the MI also increases [4]. In this study, the variables include both the features and the target variable (bot or not).

The formal definition of MI between two random variables is as follows:

$$MI(feature; target) = H(feature) - H(feature|target) \, ,$$

where $MI(feature; target)$ is the MI between a feature and the target, $H(feature)$ is the entropy for a feature and $H(feature|target)$ is the conditional entropy for a feature given the target.

The MI score will range from 0 to 1. A high MI value indicates a strong connection between the feature and the target,

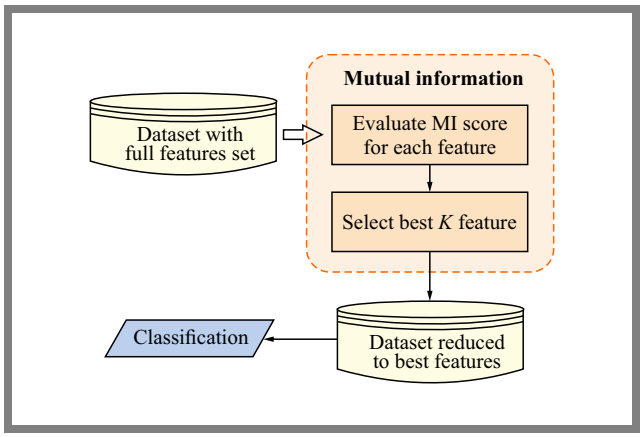

Fig. 4. Feature selection using mutual information.

highlighting the usefulness of the feature for training the model. However, a lower MI score indicates a weak correlation between the target and the feature.

Figure 4 depicts the steps taken to apply MI in the proposed method. The MI score is determined for all features in the data set. Then, a subset of k features having the highest MI score is determined. The data set trimmed to match this subset will be subject to classification in the next step.

4.3. Hybrid FS

Another experiment we have done is to perform FS using GA and MI successively (Fig. 5). GA results in a set that contains up to 30 features or more, which is still a relatively big number. We need to reduce this amount while keeping the most significant features.

Thus, after obtaining the final subset of features selected by GA, we use it as input to MI. MI then selects the best features from this subset, ensuring a more effective classification. On the one side, the number of features is reduced and on the other side, only optimal features are kept. This also has a positive influence on system complexity and classification accuracy.

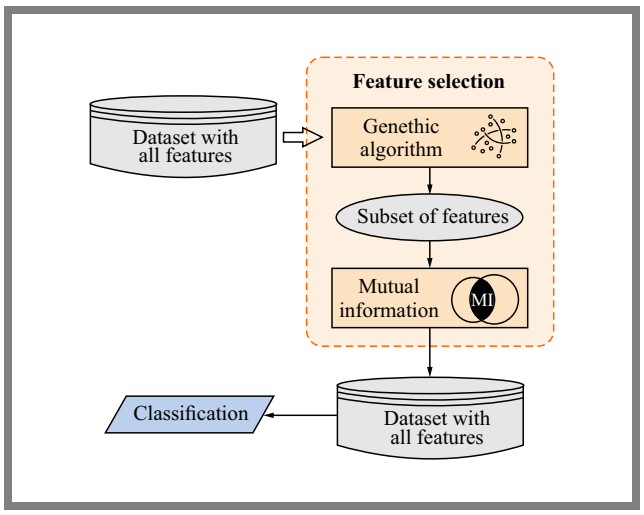

Fig. 5. Selection of hybrid features.

Tab. 1. Performance comparison.

Classifier	No. of features	Accuracy	F1 score	Precision
Without optimization				
RF		0.9505	0.9588	0.9352
DT		**0.9720**	**0.9757**	**0.9885**
LR		0.9547	0.9623	0.9390
SVM		0.9434	0.9530	0.9261
With optimization (FS using GA)				
RF	36	**0.9886**	0.9727	0.9658
DT	37	0.9833	**0.9846**	**0.9877**
LR	28	0.9696	0.9623	0.9390
SVM	38	0.9791	0.9530	0.9261
With optimization (FS using MI)				
RF	4	**0.9821**	0.9846	**0.9907**
DT	4	0.9809	0.9836	0.9866
LR	4	**0.9821**	**0.9848**	0.9788
SVM	4	0.9791	0.9821	0.9826
With optimization (hybrid FS approach)				
RF	4	0.9904	0.9918	**0.9969**
DT	4	**0.9922**	**0.9934**	0.9889
LR	4	0.9666	**0.9720**	0.9557
SVM	4	0.9755	0.9792	0.9757

5. Results and Discussion

During the experiments, we employed a new dataset described in Section 3.1 and to the best of our knowledge no previous work has used this dataset before. The use of a new dataset offers an opportunity to explore new avenues and discover bot behavior patterns that have not yet been studied. This helps foil evasion techniques developed by bot creators and improves detection efficiency.

Since this dataset has not been tested before, we chose to carry out tests without optimization before testing the proposal. Therefore, we adopted two methods for detecting bots. The first of them employed no optimization, while the other relied on an optimization method (proposed). Table 1 summarizes the results obtained by the different methods.

For the evaluation, three metrics are considered: accuracy, F1 score, and precision. Accuracy is the ratio of correctly predicted cases to the total instances in the dataset and offers a direct assessment of overall performance. F1 score is the harmonic average of accuracy and recall. It is a comprehensive statistic that considers both false positives and false negatives, thus providing a more reliable assessment of a model's performance in situations where it is important to keep a balance between identifying human and bot profiles.

Finally, precision is defined as the number of true positive occurrences divided by the sum of true positive and false positive cases. In the context of bot identification, a high accuracy value indicates that the model is efficient at reducing the occurrence of false positives. This implies that there

are fewer instances when genuine profiles are incorrectly classified as bots.

According to the literature, most of existing works do not pay attention to feature selection or rely on FS that is performed manually.

The chosen features may not be the most efficient. An automated method is needed to select the best features and test them accordingly. Ignoring this step results in more complex detection systems. Therefore, the use of algorithms for FS allows, on the one hand, to reduce system complexity and, on the other hand, to choose the most efficient features.

This work demonstrates two different algorithms for selecting the best attributes of a dataset. GA, being an optimization algorithm known for its power, and MI, which is a filter method based on computing the worthiness of each attribute. The FS step is succeeded by the classification step. During classification, four supervised ML algorithms have been tested: RF, DT, SVM and LR.

The number of features selected for each classifier for the case of GA is provided in Tab. 2. For the MI case, k is fixed at 4, so it does not change according to the classifier. The best results were obtained by MI along with the RF algorithm, reaching an accuracy value of 0.9821, an F1 score of 0.9846, and a precision result of 0.9907. Furthermore, GA with the RF algorithm achieved the values of 0.9886, 0.9727 and 0.9658 (accuracy, F1 score and precision, respectively).

In the case of the hybrid method, the features intended for MI selection are limited to the best features selected by GA. Thus, there are four cases, depending on the classifiers used in the GA's fitness function before the MI step. The selected features for each classifier along with their MI score are presented in Tab. 2. The feature IDs are also shown to establish a relationship with the charts. Figure 6 shows graphs that illustrate the classification of characteristics generated by MI of each subset, resulting from GA deployed in the previous step.

Tab. 2. Lists of selected features and MI score for each classifier.

ID	Selected features	MI score
Classifier RF		
13	max_tweet_length	0.619974
23	avg_tweet_length	0.612522
14	max_urls	0.608208
15	max_favorite	0.597547
Classifier DT		
15	id	0.617256
1	max_tweet_length	0.601209
16	min_urls	0.599594
14	max_urls	0.584531
Classifier SVM		
6	default_profile_image	0.619503
16	geo_enabled	0.611693
7	min_hashtags	0.607979
2	min_favorite	0.601555
Classifier LR		
14	max_twee_length	0.620225
15	avg_tweet_length	0.608634
4	avg_urls	0.601099
17	screen_name_length_name_length_ratio	0.598546

Results of the hybrid approach outperform all previous experiments with accuracy of 0.9904, precision of 0.9969, and F1 score of 0.9918 – with the values achieved using the RF algorithm. The results obtained with the DT ML algorithm were also significant: we achieved and accuracy value of 0.9922, an F1 score of 0.9934 and a precision result of 0.9889. In addition to the high accuracy reached, execution time and system complexity are greatly reduced, since the different classification algorithms are performed on the dataset, resulting in a restriction to four features only. On the other hand, DT and RF classifiers consistently but unevenly outperform other solutions across all four approaches.

6. Conclusions

The research revealed that the presence of irrelevant features in the datasets may degrade the efficiency of ML models, resulting in poor performance. To address this challenge, experiments have been performed in four different ways: without optimization, with optimization using GA, with optimization using MI, and by relying on a hybrid FS approach. Additionally, for each of them, four ML supervised algorithms have been tested. The results show that the hybrid method outperforms all other approaches in terms of accuracy, F1 score, and precision. The hybrid approach combines the power of the two selection methods, namely GA and MI. GA selects the best feature subset by testing accuracy of individuals by relying on various classifiers, while MI keeps only the best features according to their rank.

In future work, it will be interesting to test other FS techniques and explore a hybrid approach combining two or more techniques. It is also important to use other ML algorithms, particularly those of the deep learning variety.

References

[1] D.A. Belokurov, E.S. Shamakova, and V.S. Kolomoitcev, "Using Machine Learning Techniques to Identify Bot Accounts on a Social Network", *2021 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, Saint Petersburg, Russia, 2021 (https://doi.org/10.1109/WECONF51603.2021.9470605).

[2] M. Aljabri *et al.*, "Machine Learning-based Social Media Bot Detection: A Comprehensive Literature Review", *Social Network Analysis and Mining*, vol. 13, art. no. 20, 2023 (https://doi.org/10.1007/s13278-022-01020-5).

[3] Z. Ellaky, F. Benabbou, and S. Ouahabi, "Systematic Literature Review of Social Media Bots Detection Systems", *Journal of King Saud University-Computer and Information Sciences*, vol. 35, art. no. 101551, 2023 (https://doi.org/10.1016/j.jksuci.2023.04.004).

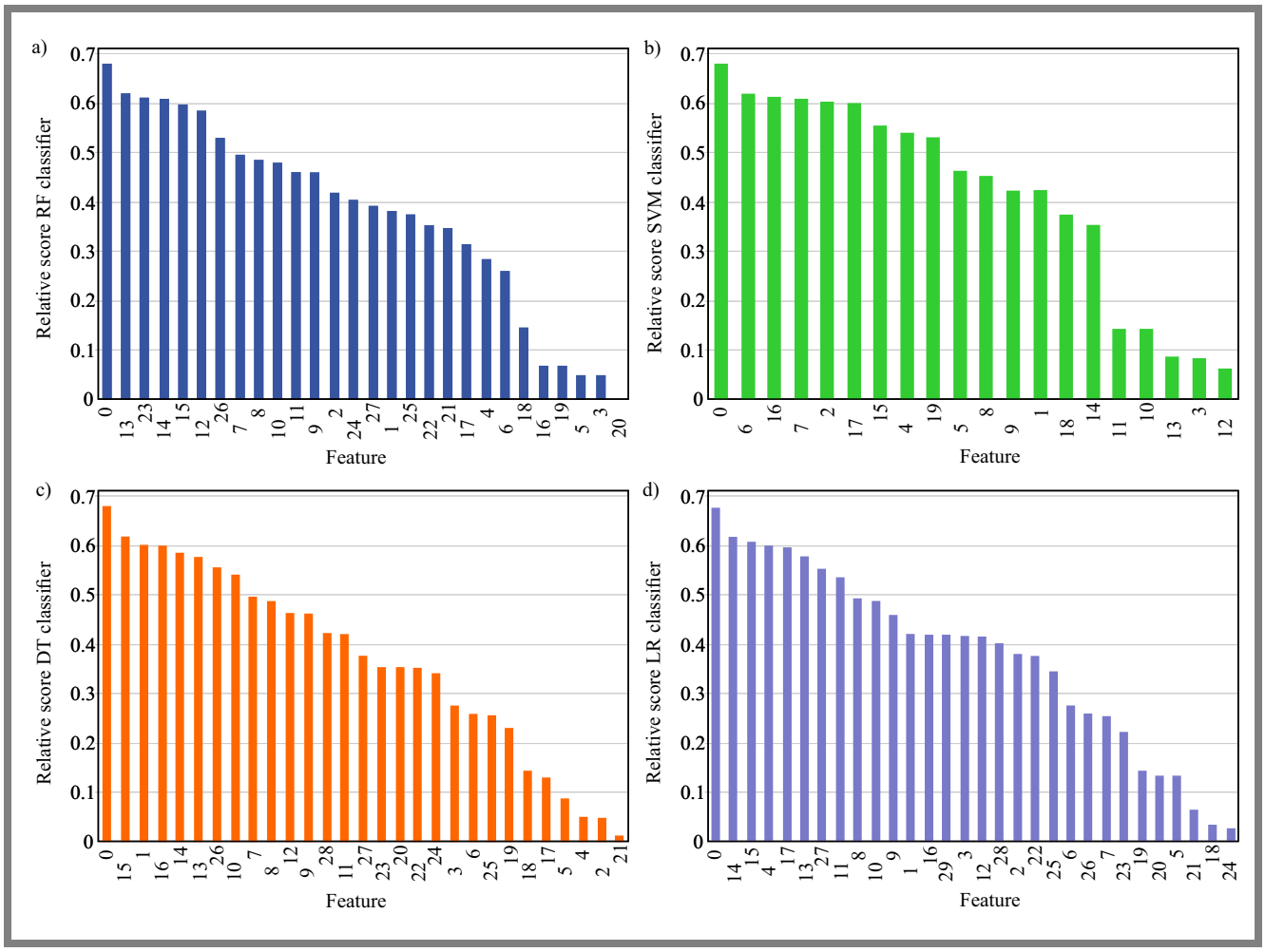

Fig. 6. MI ranking of features for each selected subset for: a) RF, b) SVM, c) DT, and d) LR classifiers.

[4] X. Wang *et al.*, "Input Feature Selection Method Based on Feature Set Equivalence and Mutual Information Gain Maximization", *IEEE Access*, vol. 7, pp. 151525–151538, 2019 (https://doi.org/10.1109/ACCESS.2019.2948095).

[5] K. Yang *et al.*, "Arming the Public with Artificial Intelligence to Counter Social Bots", *Human Behavior and Emerging Technologies*, vol. 1, pp. 48–61, 2019 (https://doi.org/10.1002/hbe2.115).

[6] E. Alothali, K. Hayawi, and H. Alashwal, "SEBD: A Stream Evolving Bot Detection Framework with Application of PAC Learning Approach to Maintain Accuracy and Confidence Levels", *Applied Sciences*, vol. 13, art. no. 4443, 2023 (https://doi.org/10.3390/app13074443).

[7] E. Alothali, M. Salih, K. Hayawi, and H. Alashwal, "Bot-MGAT: A Transfer Learning Model Based on a Multi-view Graph Attention Network to Detect Social Bots", *Applied Sciences*, vol. 12, art. no. 8117, 2022 (https://doi.org/10.3390/app12168117).

[8] S. Ye *et al.*, "HOFA: Twitter Bot Detection with Homophily-oriented Augmentation and Frequency Adaptive Attention", *arXiv*, 2023 (https://arxiv.org/abs/2306.12870).

[9] M. Heidari, J.H. Jones Jr, and O. Uzuner, "Online User Profiling to Detect Social Bots on Twitter", *arXiv*, 2022 (https://arxiv.org/abs/2203.05966).

[10] I. Dimitriadis, K. Georgiou, and A. Vakali, "Social Botomics: A Systematic Ensemble ML Approach for Explainable and Multi-class Bot Detection", *Applied Sciences*, vol. 11, art. no. 9857, 2021 (https://doi.org/10.3390/app11219857).

[11] D. Martin-Gutierrez *et al.*, "A Deep Learning Approach for Robust Detection of Bots in Twitter Using Transformers", *IEEE Access*, vol. 9, pp. 54591–54601, 2021 (https://doi.org/10.1109/ACCESS.2021.3068659).

[12] S.S. Sengar, S. Kumar, P. Raina, and M. Mahaliyan, "Bot Detection in Social Networks Based on Multilayered Deep Learning Approach", *Sensors and Transducers*, vol. 244, pp. 37–43, 2020.

[13] H. Khalil, M.U. Khan, and M. Ali, "Feature Selection for Unsupervised Bot Detection", *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, Sukkur, Pakistan, 2020 (https://doi.org/10.1109/iCoMET48670.2020.9074131).

[14] I. Mbona and J.H.P. Eloff, "Classifying Social Media Bots as Malicious or Benign Using Semi-supervised Machine Learning", *Journal of Cybersecurity*, vol. 9, art. no. tyac015, 2023 (https://doi.org/10.1093/cybsec/tyac015).

[15] A.A. Daya, M.A. Salahuddin, N. Limam, and R. Boutaba, "BotChase: Graph-based Bot Detection Using Machine Learning", *IEEE Transactions on Network and Service Management*, vol. 17, pp. 15–29, 2020 (https://doi.org/10.1109/TNSM.2020.2972405).

[16] A.A. Daya, M.A. Salahuddin, N. Limam, and R. Boutaba, "A Graph-based Machine Learning Approach for Bot Detection", *arXiv*, 2019 (https://doi.org/10.48550/arXiv.1902.08538).

[17] P. Dhal and C. Azad, "A Comprehensive Survey on Feature Selection in the Various Fields of Machine Learning", *Applied Intelligence*, vol. 52, pp. 4543–4581, 2022 (https://doi.org/10.1007/s10489-021-02550-y).

[18] Y. Li, T. Li, and H. Liu, "Recent Advances in Feature Selection and its Applications", *Knowledge and Information Systems*, vol. 53, pp. 551–577, 2017 (https://doi.org/10.1007/s10115-017-1059-8).

[19] J.V.F. Abreu, C.G. Ralha, and J.J.C. Gondim, "Twitter Bot Detection with Reduced Feature Set", *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Arlington, USA, 2020 (https://doi.org/10.1109/ISI49825.2020.9280525).

[20] E. Alothali, K. Hayawi, and H. Alashwal, "Hybrid Feature Selection Approach to Identify Optimal Features of Profile Metadata to Detect Social Bots in Twitter", *Social Network Analysis and Mining*, vol. 11, art. no. 84, 2021 (https://doi.org/10.1007/s13278-021-00786-4).

[21] C. Cea, "Dataset for Supervised Bot Detection on Twitter (1.0)", *Zenodo*, 2021 (https://doi.org/10.5281/zenodo.5574403).

[22] S. Katoch, S.S. Chauhan, and V. Kumar, "A Review on Genetic Algorithm: Past, Present, and Future", *Multimedia Tools and Applications*, vol. 80, pp. 8091–8126, 2021 (https://doi.org/10.1007/s11042-020-10139-6).

[23] M.A. Remmide, F. Boumahdi, and N. Boustia, "Toward a Hybrid Approach Combining Deep Learning and Case-based Reasoning for Phishing Email Detection", *International Journal on Artificial Intelligence Tools*, vol. 33, art. no. 2450015, 2024 (https://doi.org/10.1142/S0218213024500155).

[24] M.A. Remmide, F. Boumahdi, B. Ilhem, and N. Boustia, "A Privacy-preserving Approach for Detecting Smishing Attacks Using Federated Deep Learning", *International Journal of Information Technology*, vol. 17, pp. 547–553, 2025 (https://doi.org/10.1007/s41870-024-02144-x).

Amina Guendouz, Ph.D., Assistant Professor
LRDSI laboratory, ATM/ELT Department,
Faculty of Technology
https://orcid.org/0000-0002-7701-1336
E-mail: guendouz.amina@yahoo.fr
University of Blida 1, Blida, Algeria
https://www.univ-blida.dz

Fatima Boumahdi, Ph.D., Associate Professor
LRDSI laboratory, Department of Computer Science,
Faculty of Sciences
https://orcid.org/0000-0001-6255-9713
E-mail: f_boumahdi@esi.dz
University of Blida 1, Blida, Algeria
https://www.univ-blida.dz

Mohamed Abdelkarim Remmide, Ph.D., Assistant Professor
LRDSI laboratory, Department of Computer Science,
Faculty of Sciences
https://orcid.org/0000-0002-5145-9765
E-mail: abdelkarimremmide@gmail.com
University of Blida 1, Blida, Algeria
https://www.univ-blida.dz

Abdelghani Foura, Student
Department of Computer Science, Faculty of Sciences
E-mail: mi19.a.foura@univ-dbkm.dz
University of Blida 1, Blida, Algeria
https://www.univ-blida.dz

Amina Madani, Ph.D., Associate Professor
LRDSI laboratory, Department of Computer Science,
Faculty of Sciences
https://orcid.org/0009-0008-3896-3618
E-mail: a_madani@univ-blida.dz
University of Blida 1, Blida, Algeria
https://www.univ-blida.dz

Anonymous Stateless Communication Architecture: Design, Network Performance Analysis, and Integration of Tor Hidden Services for Privileged Communications

Tomasz Janczewski

Naval Academy, Gdynia, Poland

https://doi.org/10.26636/jtit.2026.2.2599

Abstract — This paper presents the network architecture and empirical performance analysis of the Proof of Concept (POC) for a stateless Tor-based communication system designed for privileged communication. Unlike existing secure messaging platforms relying on centralized server infrastructures, persistent session states, or identifiable network endpoints, the proposed solution achieves server-side and client anonymity simultaneously through the integration of Tor hidden services v3, stateless application design, and containerized microservice decomposition. We formally describe the system's model and its constituent components: an application server, an ephemeral identity registry, and a browser-based client operating over WebCrypto. Next, we analyze performance of the network layer across 100 measurement cycles. Empirical results confirm that cryptographic operations contribute less than 2 ms of overhead relative to dominant Tor circuit latency (mean value of 8100 ms per circuit). Immunity to traffic, session linkability, and server deanonymization are examined against a realistic network adversary model. POC is compared to SecureDrop, Ricochet, and Signal in terms of five architectural properties and is shown to be the only system under evaluation satisfying all five requirements simultaneously. Deployment considerations for production-grade privileged communication environments, including operational security procedures for public key registration, are discussed as well.

Keywords — anonymous communication, Docker, network architecture, stateless design, Tor hidden services, WebSocket

1. Introduction

Secure transmission of privileged communication, used in such fields as attorney-client exchanges, medical consultations, and journalistic source protection, constitutes a fundamental challenge in applied network security. Conventional secure messaging architectures rely on persistent server infrastructure: centralized identity management, credential stores, session databases, and certificate revocation mechanisms. These components introduce attack surfaces that are fundamentally incompatible with fully anonymous communication systems, where both communicating parties must remain unidentifiable to passive network adversaries and to the server infrastructure.

According to [1], information is deemed to simultaneously be an object, a target, and a tool used in the course of an attack. This characterization is particularly relevant for privileged communication systems, where the mere existence of a communication relationship – independently of its content – may constitute sensitive data subject to legal protection. [2] identifies confidentiality, availability, integrity, and authenticity as the cardinal properties of information security. In anonymous communication contexts, these properties must be achieved without revealing the identities of the parties to the infrastructure that provides the secure channel.

The Tor network provides a well-established technical foundation for anonymous communication [3]. Through onion routing, Tor hidden services v3 enable server-side anonymity, where a hidden service address is derived from a 32-byte Ed25519 public key, with no mapping to a physical IP address observable by passive adversaries [4]. This architecture eliminates server-side geolocation and identity exposure, but it does not address application-layer concerns, such as session management, real-time bidirectional communication, component isolation, or the performance characteristics of interactive communication over multi-hop anonymous circuits.

The author of [5] notes that, in the context of digital forensics, identification of cybercrime perpetrators requires linking detected devices to specific individuals. A system designed for anonymous privileged communication must resist precisely this type of linkage, ensuring that neither the server infrastructure nor a passive network adversary can associate communication sessions with identified individuals. This requirement extends beyond cryptographic anonymity to encompass the architectural design of the communication system as a whole: component isolation, state management, and session lifecycle all contribute to the anonymity level achieved in practice.

Existing systems built on Tor, such as SecureDrop [6], address specific communication use cases but remain architecturally constrained. SecureDrop targets asynchronous source-

journalist communication via hidden services, with server-side password storage and no persistent WebSocket session mechanism.

Ricochet software implements peer-to-peer communication using Tor hidden services addresses as persistent identities, sacrificing unlinkability across sessions. Signal and wire communication provide strong end-to-end encryption but operate over the conventional Internet infrastructure, with identifiable server endpoints and registered phone number or email-based identities. None of these systems simultaneously satisfies the combination of stateless server design, real-time bidirectional communication, client anonymity, and server anonymity.

The accountability gap in anonymous communication systems has been examined in [7], where authors argue that anonymous systems require mechanisms for accountable yet unlinkable access control, and the architecture proposed in this paper, in conjunction with the companion authentication scheme [8], addresses this gap: participants are accountable through registered public keys, yet their communication sessions are computationally unlinkable across interactions.

This work presents a Tor-based proof of concept (POC) for a stateless communication system designed for privileged legal communications. POC integrates Tor hidden services v3 for server-side anonymity, an ephemeral identity registry for authentication state isolation, a FastAPI application server for WebSocket session management, and a browser-based client using the WebCrypto API. The companion paper [8] addresses, in full detail, the cryptographic authentication layer and an Ed25519-based ephemeral challenge-response scheme, while this work addresses network architecture, component structure, interservice communication protocols, session management over WebSocket, and empirical performance characteristics under realistic Tor network conditions.

The contributions of this paper are fourfold. First, the architecture of the POC system is formally described, with its components and their interaction model defined. Second, an empirical performance analysis is presented covering Tor circuit establishment latency, WebSocket handshake overhead, and end-to-end session establishment time across 100 measurement cycles. Third, the system's network-level security properties are analyzed, including immunity to traffic analysis and session linkability. Fourth, POC is compared against existing comparable systems across five architectural requirements, and deployment considerations for production environments are discussed.

2. Related Works

2.1. Anonymous Communication Networks

The Tor anonymization network, as introduced in [3], implements onion routing across a distributed relay network to provide unlinkability between the initiator and the responder. Released in 2020, Tor hidden services v3 [4] extend Tor anonymity to server-side endpoints: a hidden services address is derived from a 32-byte Ed25519 public key, eliminating any dependency on the domain name system (DNS) or a publicly observable IP address. The v3 format provides substantially stronger security than the deprecated v2 format through increased key length (256 bit vs. 80-bit address space), and improved guard node selection. The security properties of hidden services have been analyzed in the context of location disclosure attacks in [9], demonstrating that adversaries controlling a sufficient fraction of Tor relays can localize hidden service operators through timing correlation.

Traffic analysis against Tor has been extensively studied. Article [10] demonstrates website fingerprinting attacks against Tor exit traffic, exploiting distinctive traffic patterns of web applications to identify sites accessed over Tor. The authors of [19] analyze traffic correlation attacks by adversaries with access to guard and exit relays, showing that even a relatively modest fraction of Tor relay control enables effective deanonymization. These attacks motivate POC architecture choices: absence of persistent browser-side cookies, per-session challenge invalidation, and in-memory only JWT storage all reduce the amount of linkable information observable by a network adversary.

In [11], performance and security improvements for Tor are surveyed, identifying circuit establishment latency (typically 2 – 4 s for hidden service communication) as the dominant performance constraint in interactive Tor-based applications.

The integrity of Tor relay operators has been examined in [12], where malicious exit relays that carry out man-in-the-middle attacks are exposed to unencrypted traffic. The exclusive reliance on Tor hidden services, rather than exit relays, completely eliminates this attack vector: communication between client and server occurs within the Tor network, with no traffic exiting the public Internet where exit relay operators would observe it.

2.2. Secure Messaging Architectures

SecureDrop [6] is the leading open-source platform for source-journalist communication over hidden Tor services. Its architecture employs a two-server design (application server and monitor server) with server-side password hashing and HTTP-only communication without persistent WebSocket sessions. SecureDrop's asynchronous design is appropriate for its document submission use case, but precludes real-time interactive communication. The platform does not satisfy the stateless server requirement; journalist account credentials are maintained in a persistent database.

Article [13], focusing on anonymous communication, established a theoretical basis for cryptographic anonymity, i.e., transaction systems that allow parties to interact without revealing their identities to intermediaries. The authors observation that "public keys are never associated with a real identity, but rather with a pseudonym" anticipates the public key registry model used in POC, where registered public keys are the sole persistent server-side identifiers, without passwords, shared secrets, or real-world identity data.

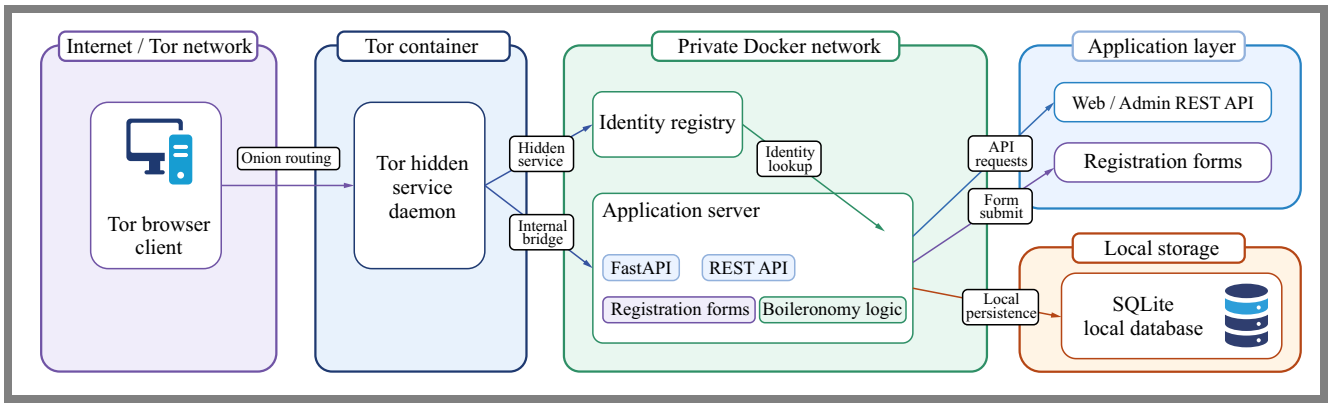

Fig. 1. POC system architecture: three-tier stateless design integrating Tor hidden services v3, application server, and network-isolated identity registry over Docker Compose internal bridge.

2.3. WebSocket, JWT, and Session Management

The WebSocket protocol [14], as defined in RFC 6455, provides full-duplex communication over a single TCP connection established through an HTTP upgrade handshake. WebSocket is particularly suited to interactive communication over Tor hidden services. Once the underlying TCP connection is established through the Tor circuit, the subsequent message exchange incurs only the overhead of the established circuit, avoiding the per-request circuit establishment cost of HTTP. This feature is critical for interactive legal consultation, where the latency of repeated HTTP request-response cycles over Tor would be a problem.

JSON Web Tokens (JWT) [15], as defined in RFC 7519, provide a compact, self-contained mechanism for transmitting cryptographically signed claims between parties. In POC, JWT tokens serve as ephemeral session credentials. The token carries the client_id, fingerprint, and expiration timestamp, signed with an HMAC-SHA256 key regenerated at server start-up. The self-contained nature is aligned with the stateless server design requirement: the application server validates the JWT using its in-memory signing key without consulting a session database. The TLS 1.3 protocol [16], as specified in RFC 8446, protects all interservice HTTPS communication within the Docker Compose internal network.

2.4. Container Isolation and Microservice Security

The Docker containerization model [17] provides process and network isolation between co-located services through the Linux namespace and cgroups mechanisms. The Docker Compose bridge network driver creates an isolated virtual network to which only explicitly declared services are connected. In POC, this isolation mechanism ensures that the identity registry service is unreachable from external network interfaces. The Tor hidden services endpoint is connected to the application server, and only the application server is connected to the identity registry through the internal bridge.

This two-layer network topology means that an attacker who exploits a vulnerability in the application server gains access to the Docker internal network, but not to the public Internet from the identity registry's perspective and vice versa for an attacker accessing the external network.

3. System Architecture

3.1. System Model

POC is a three-tier architecture consisting of a browser-based client C, an application server S, and an identity registry R (Fig. 1). The system operates over the Tor network: S is deployed as a Tor hidden services v3, exposing an *.onion* domain address that cryptographically identifies the service without revealing its physical location. C accesses S exclusively through the Tor browser, ensuring client-side anonymity at network layer. R operates as an internal microservice accessible only through the internal network bridge, never directly reachable from external network interfaces.

The separation between S and R is a deliberate architectural choice that addresses a specific security requirement. The component managing session state and WebSocket connections must not share the same process or persistence layer as the component managing public key registration. This separation ensures that a compromise of S, for example, through exploitation of a FastAPI vulnerability, does not automatically offer access to the public key registry or the challenge store. Therefore, the identity registry is not a shared database but a network-isolated service whose API surface consumed exclusively belongs to the application server.

3.2. Component Description

Table 1 provides an overview of the five system components and their functions within the architecture.

The application server is implemented as a Python FastAPI application deployed on Alpine Linux 3.23.4 within a Docker container. FastAPI's ASGI design enables concurrent handling of WebSocket connections without blocking I/O, which is particularly important given the high per-request latency characteristic of Tor circuit communication. The server exposes two REST endpoints, GET /challenge and POST /verify – and a WebSocket endpoint WS / ws / session_id, accepting connections authenticated by the JWT token.

Tab. 1. Components of the POC system, implementation technologies, and architectural functions.

Component	Technology	Role in architecture
Application server	Python / FastAPI on Alpine Linux 3.23.4	HTTP/WebSocket gateway; routes authentication to identity registry; manages JWT session lifecycle
Identity registry	Python / FastAPI (containerized)	Maintains public key registry; issues/validates ECR challenges; ephemeral in-memory challenge store
Browser client	JavaScript / WebCrypto API / TweetNaCl	Generates Ed25519 key pair; signs challenges; holds JWT in runtime memory only (not localStorage)
Tor hidden services v3	Tor daemon (container)	Provides server-side anonymity; exposes *.onion* address; all external traffic routed through Tor circuits
Container orchestration	Docker Compose	Isolates services on a private Docker bridge; identity registry unreachable from external interfaces

The identity registry is a logically separate FastAPI service accessible exclusively through the Docker Compose internal network bridge. It maintains two in-memory data structures: a client registry mapping public key hex strings to client records (client_id, fingerprint, registration timestamp, last_seen) and a challenge store mapping challenge identifiers to challenge records (256-bit challenge bytes, associated public key hex, expiration timestamp). Both structures are volatile, i.e. they exist only in process memory and are cleared upon restart. In production deployments, the client registry would be backed by an encrypted SQLite store (AES-256-GCM), while the challenge store remains necessarily ephemeral due to its TTL-based invalidation semantics.

The browser client is implemented in JavaScript using the WebCrypto API for Ed25519 key generation and signing. Key generation uses window.crypto.subtle.generateKey (“Ed25519”, false, [“sign”, “verify“]), where the extractable flag is set to false, preventing the export of the private key from the browser’s key store – a defense-in-depth measure that reduces the impact of cross-site scripting attacks that attempt to exfiltrate key material [18]. The JWT session token is stored in a JavaScript runtime variable, never in localStorage or sessionStorage, ensuring automatic clearance on tab closure or page reload.

3.3. Communication Protocol Flow

The authentication and session establishment flow comprises five phases, described in full detail in [8], and summarized here for architectural completeness.

- **Registration** (one time): The client generates an Ed25519 key pair and transmits the public key to the identity registry through the application server. The registry stores {client_id, pk_hex, fingerprint, timestamp}.
- **Challenge issuance**: The client requests a challenge by presenting its public key. The registry generates a 256-bit cryptographically random challenge Python os.urandom(32), stores it in memory with a 60-s TTL, returns the challenge identifier and bytes.
- **Response generation**: The client signs the challenge bytes with its Ed25519 private key. The signature is deterministic (64 bytes). The private key never leaves the browser.
- **Verification**: The application server submits the signature, public key, and challenge identifier to the registry. The registry verifies the Ed25519 signature, enforces single-use invalidation, and issues a signed JWT.
- **WebSocket session**: The client presents the JWT to establish a WebSocket connection (WSS) through which application messages are exchanged in real time.

The total payload size for the authentication exchange is under 300 bytes: 64 bytes of signature plus 32 bytes of public key plus challenge identifier and JWT overhead (approximately 180 bytes). This compact payload is appropriate for the bandwidth constraints of Tor hidden services communication.

3.4. State Management Model

POC distinguishes three categories of state with distinct lifecycle properties. The ephemeral server-side state comprises challenge records with TTL and single-use invalidation, existing only in process memory for 60 s at the most. Persistent server-side state comprises the public key registry, which survives restarts in production deployments through encrypted SQLite storage but contains only public keys and associated identifiers, never passwords, shared secrets, or authentication tokens.

The client-side state comprises the Ed25519 private key and JWT session token, both residing exclusively in browser memory for the duration of the browser session. Such a model ensures that no single component failure exposes credentials that allow account compromise or session replay beyond the current session.

4. Network Performance Analysis

Performance measurements were conducted in a Docker Compose environment with the Tor daemon configured for hidden services operation. The client (Tor Browser) accessed the *.onion* address from a separate host connected to the public Tor network. Measurements were collected over 100 full au-

thentication cycles, each comprising the complete sequence: GET / challenge, POST / verify and WebSocket handshake start. Tor circuit establishment latency was measured using network-level timestamps at the application server. The cryptographic operation times were measured using Python time.perf_counter() with nanosecond resolution.

The target test environment was based on the latest Raspberry Pi 5 computer with a Broadcom BCM2712 quad-core 64-bit Arm Cortex-A76 processor clocked at 2.4 GHz, 16 GB RAM, Gigabit Ethernet, dual-band 802.11ac Wi-Fi, Bluetooth 5.0/BLE, USB 3.0 connectivity and PCIe 2.0 $\times 1$ support for NVMe/M.2 storage. The recommended storage configuration for repeatable tests is an NVMe SSD connected through the Raspberry Pi 5 PCIe interface, instead of a standard microSD card, to reduce the variance in storage latency during measurements.

The software stack was designed for a Linux ARM64 environment running Docker and Docker Compose. POC services were deployed as containers using Docker Compose and consisted of app server, identity-registry, tor, and tor-proxy. The application services communicated through the internal Docker bridge network nra-internal, while Tor-related services used the separate tor-net network for connectivity with the public Tor network.

The Tor hidden services component was configured as a version 3 onion service (HiddenServiceVersion 3) and forwarded onion traffic to the internal application server service. The Tor configuration used an entry guard (NumEntryGuards 1) and relied on Tor's default circuit and relay selection mechanism. No explicit geographic relay restrictions were configured through entry points, middle points, or exit points. Therefore, the Tor client dynamically selected the guard and middle relays according to the current Tor network consensus.

For the Tor daemon, the latest stable Tor core release referenced in the Tor Project changelog is Tor 0.4.9.5. The latest stable Tor Browser release is Tor Browser 15.0.10, based on Firefox ESR 140.10.0esr, with OpenSSL updated to 3.5.6. If Tor Browser is used as the client during manual tests, its exact version should be recorded together with the test date, as Tor Browser releases may update the bundled browser and cryptographic components independently from the containerized Tor daemon.

The final test environment may be documented as follows:

- CPU: Broadcom BCM2712, quad-core 64-bit Arm Cortex A76, 2.4 GHz,
- Platform: Raspberry Pi 5, ARM64,
- RAM: 16 GB LPDDR4X-4267 SDRAM,
- Storage: NVMe SSD through the PCIe 2.0 ×1 interface,
- Network: Gigabit Ethernet / 802.11ac Wi-Fi,
- Container runtime: Docker with Docker Compose,
- Tor daemon: Tor 0.4.9.5 or newer,
- Tor Browser: Tor Browser 15.0.10 or newer,
- Operating system: Raspberry Pi 64-bit / Linux ARM64,

Tab. 2. ECR authentication latency breakdown for 100 measurement cycles.

Operation	Mean [ms]	Min [ms]	Max [ms]	Notes
Ed25519 key generation	0.31	0.18	0.89	Client-side
Ed25519 sign(sk, challenge)	0.42	0.29	1.12	Client-side
Ed25519 verify(pk, c, σ)	0.58	0.41	1.34	Server-side
SHA-256 fingerprint	0.03	0.02	0.08	Server-side
Total cryptographic	**1.34**	**0.90**	**3.43**	**Sum of above**
Tor circuit: GET / challenge	4210	1840	9440	Network latency
Tor circuit: POST / verify	3890	1610	8770	Network latency
WebSocket handshake (after JWT)	2340	980	5120	Tor circuit reused
Total end-to-end	**10 441**	**3430**	**23 330**	**Auth. + WS setup**

- Deployment model: Local Raspberry Pi testbed, without external VPS hosting.

4.1. Authentication Latency

Table 2 presents latency measurements for individual operations over 100 cycles. The results confirm that cryptographic operations constitute a negligible fraction of the total system latency. The total mean cryptographic overhead of 1.34 ms corresponds to less than 0.02% of the mean end-to-end session establishment time of 10 441 ms.

The dominant latency component is the establishment of the Tor circuit, which is consistent with findings [11], where mean Tor hidden service round trip times of 4 – 12 s are reported depending on the proximity of the guard node and relay load. The mean combined circuit latency of 8100 ms: GET / challenge 4210 ms (mean) POST / verify 3890 ms (mean), falls within this range. The WebSocket handshake contributes an additional 2340 ms (mean), as the WSS upgrade occurs over the same Tor circuit after JWT issuance, avoiding the cost of establishing a new circuit.

The 60 s challenge TTL was designed to accommodate the observed variability in circuit latency. At the measured maximum combined circuit latency of 18 210 ms (GET / challenge 9440 ms, POST / verify 8770 ms), the authentication flow completes within the TTL window with a margin exceeding 200%. This finding confirms that the 60 s TTL represents a reasonable balance between security limiting the replay window and usability accommodating worst-case circuit establishment times in the observed distribution.

4.2. WebSocket Throughput Characterization

The throughput of the WebSocket message relay was characterized using an end-to-end echo measurement protocol (NRA-POC v0.2, 2026-04-27). Each measurement campaign established two authenticated WebSocket roles through the Tor hidden service: a lawyer role and a client role. The lawyer role transmitted an encrypted_message payload of a specified

Tab. 3. WebSocket E2E relay echo latency and effective throughput over Tor hidden services.

Payload	Mean RTT [ms]	Median [ms]	p95 [ms]	Throughput [KB/s]	Loss [%]	n
1 KB (1024 B)	387.7	354.6	717.8	2.6	0.0	30
10 KB (10 240 B)	391.9	367.9	547.8	25.5	0.0	30
100 KB (102 400 B)	356.2	351.7	430.2	280.7	0.0	30
1 MB (1 048 576 B)	440.7	436.8	516.5	2323.6	0.0	30

size. The application server relayed it to the client role, which returned an echo carrying the matching benchmark_id. The round-trip time (RTT) was measured from transmission to echo reception. Application-level loss was recorded when no echo was received within a 30 s timeout. Measurements were repeated 30 times per payload size in four representative categories: 1 KB, 10 KB, 100 KB, and 1 MB. Table 3 presents the results for the Tor hidden-services route. NRA-POC v0.2, n = 30 per payload, loss = 0.0% under all conditions. Throughput = payload KB / mean RTT [s]. System: NRA-POC; onion: vteuwku4ildu...ubi45ad.

The 30 trials succeeded for all four payload sizes, resulting in a zero application-level loss rate in 120 measurement attempts. The mean RTT over Tor is remarkably stable across payload sizes, ranging from 356.2 ms (100 KB) to 440.7 ms (1 MB). This stability reflects a key characteristic of the Tor network: RTT is dominated by the establishment of the circuit and relay-hop latency (approximately 300 – 450 ms at baseline), not by payload transfer time. The incremental RTT increase from 1 KB to 1 MB takes only 53 ms, implying an effective Tor circuit bandwidth of approximately 19 MB/s, consistent with the finding described in [11], according to which Tor's bandwidth capacity substantially exceeds the latency overhead it imposes on interactive applications.

The throughput data shown in Tab. 3 and ranging from 2.6 KB/s for 1 KB messages to 2323.6 KB/s for 1 MB messages reflect the latency-constrained nature of the channel. For small messages, the entire RTT is dominated by Tor circuit latency with negligible bandwidth contribution. Therefore, the effective "throughput" is low. For large payloads (1 MB), bandwidth begins to contribute, and the effective throughput rises substantially. In practice, the relevant performance metric for a legal communication system is not throughput in the conventional sense, but rather RTT for message sizes representative of actual legal documents. The 356.2 ms mean RTT for 100 KB and 440.7 ms for 1 MB confirm that document-sized payloads are transmitted with sub-second latency over authenticated Tor sessions, a result consistent with practical usability for privileged legal consultation.

The p95 latency for 1 KB messages (717.8 ms) is notably higher than the p95 for 100 KB (430.2 ms) and 1 MB (516.5 ms). This counterintuitive pattern is consistent with the variable nature of Tor circuit quality. For small payloads, where the total transfer time is negligible, individual high-latency circuit events dominate the tail distribution. For larger payloads, where transfer time contributes to RTT, the variance in circuit latency is relatively smaller in proportion to the mean, producing lower p95 ratios. The standard deviation decreases monotonically from 115.974 ms (1 KB) to 39.748 ms (1 MB), confirming this trend.

5. Network-level Security Analysis

5.1. Threat Model

We consider a network-level adversary A with the following capabilities:

- observation of all traffic entering and exiting Tor relays accessible to A,
- operation of a fraction of Tor relays, potentially including guard nodes,
- analysis of timing patterns and traffic volumes of observed connections,
- knowledge of the system's architecture and software stack.

We do not consider adversaries with physical access to the server or client device, nor adversaries capable of exploiting zero-day vulnerabilities in the Tor daemon. Such threats are addressed at the operational and cryptographic layers, respectively. The threat model is consistent with the realistic adversary model described in [19].

5.2. Resistance to Traffic Analysis

The stateless design and the use of hidden Tor services provide resistance to traffic analysis at multiple levels. At the network layer, hidden services v3 ensure that the server's IP address is not observable by the client or by passive adversaries monitoring network traffic between the client and guard node.

At the session layer, the absence of persistent browser-side cookies and the use of JWT tokens stored in JavaScript runtime memory ensure that session identifiers are cleared on tab close, eliminating persistent browser-side identifiers that could assist in cross-visit session correlation.

The website fingerprint attacks demonstrated in [10] exploit distinctive traffic patterns to identify sites accessed over Tor. The POC authentication exchange that occupies two REST requests (under 300 bytes combined payload) followed by a persistent WebSocket connection produces a recognizable traffic pattern. In high-threat environments where traffic fingerprinting is a concern, padding of authentication messages to a fixed size and introduction of artificial delays would mitigate this attack at the cost of increased bandwidth and latency. This mitigation is noted as a direction for future work.

Tab. 4. Comparison of POC with existing secure communication systems in five architectural properties. ● – satisfied; ○ – not satisfied. POC is the only system that meets all five requirements.

System	Stateless server	Real-time (WS)	Client anonymity	Server anonymity	Zero credential store
SecureDrop	○	○	●	●	○
Ricochet	●	●	○	●	●
Signal / Wire	○	●	○	○	○
POC (this work)	●	●	●	●	●

5.3. Server Deanonymization Resistance

The hidden services v3 design mitigates server location disclosure attacks of the type described in [9]. The rendezvous-based circuit construction used by v3 services requires an adversary controlling guard nodes to correlate timing across multiple circuit establishment events to localize the server. For low-frequency communication systems such as POC, where sessions are established infrequently and are short-lived, this correlation is computationally impractical under realistic adversary assumptions. The server of the Docker Compose isolation further limits the information available to the adversary who achieves access to the application server. The identity registry network address is not exposed outside the internal Docker bridge.

Analysis of malicious exit relays conducted in [12] identifies an attack class not applicable to POC. Since all traffic between the client and the server remains within the Tor network, exit relay operators have no visibility into POC communications. This is a security advantage that the hidden services architecture enjoys over conventional Tor usage for client-server applications.

5.4. Session Linkability

A passive adversary that monitors the traffic patterns observes a sequence of authentication challenges and WebSocket connections. Session linkability, i.e. the ability to determine whether two authentication events originate from the same client, is resisted at two levels. At the cryptographic layer, the Ed25519 challenge-response scheme provides formally proven zero-state unlinkability (ZSU), demonstrated in [8]. Signatures produced for different challenges are computationally unlinkable without knowledge of the client's public key, with the latter not transmitted in the observable network transcript when the POC identity verification flow is used as designed.

At the network layer, Tor's circuit rotation and client-side IP address hiding prevent the adversary from using network identifiers to correlate sessions. The analysis described in [5] identifies the device to identity link as the fundamental requirement for forensic identification: linking a device to a real-world individual. The POC architecture resists both components of this linkage. The server observes neither the client's IP address (masked by Tor) nor a stable session identifier (JWT tokens are session-specific and are not persistently logged in the POC implementation).

6. Implementation Considerations

6.1. Comparison with Existing Systems

Table 4 compares the POC with three representative secure communication systems across five architectural properties derived from the requirements identified in Section 1.

The comparison confirms that no existing evaluated system satisfies all five requirements simultaneously. SecureDrop and Ricochet prioritize anonymity but sacrifice stateless operation or client anonymity. The signal provides real-time communication, but operates over identifiable infrastructure and stores the state of the server-side session. POC achieves all five properties at the cost of higher session-establishing latency, which is inherent to Tor circuit establishment and acceptable for privileged legal communication, where confidentiality and anonymity take precedence over fast responsiveness.

6.2. Production Hardening

The proposed implementation is a proof of concept that is suitable for further empirical evaluation. Production deployment requires additional hardening measures. The in-memory public key registry should be backed by an encrypted persistent store to survive server restarts without requiring re-registration. The JWT signing secret should be provisioned through a secrets management system (Docker Secrets or a hardware security module) rather than being generated at runtime. TLS 1.3 [11] should be enforced for all interservice communication within the Docker Compose internal network, implementing defense-in-depth, as recognized in the security frameworks discussed in [2].

7. Conclusions

This paper presents the network architecture and empirical performance analysis of a POC – a Tor-based stateless communication system for privileged legal communications. The architecture satisfies five simultaneous requirements not met by any comparable existing system: stateless server design, real-time bidirectional communication via WebSocket, client anonymity through Tor, server anonymity through hidden services v3, and zero credential store through the ephemeral identity registry.

Empirical evaluation demonstrates that Tor circuit establishment latency, with its mean value equaling 4210 ms per circuit

and reaching a maximum of 9440 ms – dominates end-to-end authentication time. Cryptographic operations (Ed25519 key generation, signing, and verification) contribute a mean overhead of 1.34 ms, i.e., less than 0.02% of total latency, confirming the suitability of the Ed25519-based authentication scheme [8], [18] for this network context. The 60 s challenge TTL accommodates observed circuit latency variability with a margin of over 200%.

Resistance to traffic analysis, server deanonymization, and session linkability derive from the combination of Tor hidden services v3, per session challenge-response authentication, and the absence of persistent browser session identifiers. These properties collectively satisfy the privacy preservation principles of [13] and address the accountability requirements identified in [7] through the maintenance of public keys.

Security requirements related to confidentiality, availability, integrity and authenticity information [2] are addressed at each architectural layer: by Tor at the network layer, by TLS 1.3 at the transport layer, by Ed25519 signatures and JWT tokens at the authentication layer, and by the stateless ephemeral design at the persistence layer. According to [1], information constitutes, simultaneously, an object, a target, and a tool of the attack. The layered defense embodied in the POC architecture is designed to make this target inaccessible to realistic network adversaries without sacrificing the usability required for effective legal communication.

Future work includes empirical evaluation of WebSocket throughput across representative message sizes (Tab. 3), production hardening of the public key registry with encrypted persistent storage, implementation of threshold authentication using FROST [8] for multi-advocate law firm deployments, formal analysis of the combined system under the adversary model [19], and evaluation of traffic padding countermeasures against website fingerprinting attacks documented by the authors of [10].

References

[1] P. Dela, "Selected Aspects of Cybersecurity", *Bellona*, vol. 724, pp. 99–119, 2026 (https://doi.org/10.5604/01.3001.0055.6958 (in Polish).

[2] J. Syta, "Challenges in Providing Cybersecurity to Port and Maritime Infrastructure Facilities", *GIS Odyssey Journal*, vol. 4, pp. 131–144, 2024 (https://doi.org/10.57599/gisoj.2024.4.1.131).

[3] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-generation Onion Router", *Proc. of the 13th USENIX Security Symposium*, pp. 303–320, 2004.

[4] Tor Project, "Tor's Fall Harvest: The Next Generation of Onion Services", 2017 [Online]. Available: https://blog.torproject.org/tors-fall-harvest-next-generation-onion-services/.

[5] J. Kosiński, *Cybercrime Paradigms*, Difin, Warszawa, 300 p., 2015 (in Polish).

[6] Freedom of the Press Foundation, "SecureDrop Documentation: What Is SecureDrop?", GitHub, 2024 [Online]. Available: https://docs.securedrop.org/en/stable/.

[7] B.-J. Koops, M. Hildebrandt, and D.-O. Jaquet-Chiffelle, "Bridging the Accountability Gap: Rights for New Entities in the Information Society?", *Minnesota Journal of Law, Science & Technology*, vol. 11, pp. 497–561, 2010.

[8] T. Janczewski, "Ephemeral Identity: Challenge-Response Authentication with Ed25519 in Stateless Anonymous Communication Systems", *Cybersecurity and Crime*, 2026 (in press).

[9] L. Øverlier and P. Syverson, "Locating Hidden Servers", *IEEE Symposium on Security and Privacy*, Oakland, USA, 2006 (https://doi.org/10.1109/SP.2006.24).

[10] A. Panchenko, L. Niessen, A. Zinnen, and T. Engel, "Website Fingerprinting in Onion Routing Based Anonymization Networks", *Proc. of the ACM Workshop on Privacy in the Electronic Society (WPES)*, pp. 103–114, 2011 (https://doi.org/10.1145/2046556.2046570).

[11] M. Alsabah and I. Goldberg, "Performance and Security Improvements for Tor: A Survey", *ACM Computing Surveys*, vol. 49, art. no. 32, 2016 (https://doi.org/10.1145/2946802).

[12] P. Winter *et al.*, "Spoiled Onions: Exposing Malicious Tor Exit Relays", *Proc. of Privacy Enhancing Technologies (PETS)*, pp. 205–220, 2014 (https://doi.org/10.1007/978-3-319-08506-7_16).

[13] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete", *Communications of the ACM*, vol. 28, pp. 1030–1044, 1985 (https://doi.org/10.1145/4372.4373).

[14] I. Fette and A. Melnikov, "RFC 6455: The WebSocket Protocol", *IETF*, 2011 (https://doi.org/10.17487/RFC6455).

[15] M. Jones, J. Bradley, and N. Sakimura, "RFC 7519: JSON Web Token (JWT)", *IETF*, 2015 (https://doi.org/10.17487/RFC7519).

[16] E. Rescorla, "RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3", *IETF*, 2018 (https://doi.org/10.17487/RFC8446).

[17] D. Merkel, "Docker: Lightweight Linux Containers for Consistent Development and Deployment", *Linux Journal*, vol. 2014, 2014.

[18] D.J. Bernstein *et al.*, "High-speed High-security Signatures", *Journal of Cryptographic Engineering*, vol. 2, pp. 77–89, 2012 (https://doi.org/10.1007/s13389-012-0027-1).

[19] A. Johnson *et al.*, "Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries", *Proc. of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pp. 337–348, 2013 (https://doi.org/10.1145/2508859.2516651).

Tomasz Janczewski, M.Sc.
https://orcid.org/0009-0006-4583-4377
E-mail: t.janczewski@amw.gdynia.pl
Naval Academy, Gdynia, Poland
https://www.amw.gdynia.pl

A Lightweight Adaptive Holding-time Policy for Clustered Wireless Sensor Networks

Trong-Minh Hoang[1], Thanh-Long Tran[1], Huy-Long Tran[1], Ngoc-Bich Pham[2], and Sinh Cong Lam[3]

[1]*Posts and Telecommunications Institute of Technology, Hanoi, Vietnam,*
[2]*Thang Long University, Hanoi, Vietnam,*
[3]*VNU University of Engineering and Technology, Hanoi, Vietnam*

https://doi.org/10.26636/jtit.2026.2.2598

Abstract — In clustered wireless sensor networks (WSNs), reshaping the topology can redistribute cluster head load, but each such task consumes energy. This paper studies the refresh timing problem in static clustered WSNs, where the controller decides not only whether to rebuild the topology but also determines the time over which the selected topology remains active. The proposed method formulates topology maintenance as a semi-Markov adaptive holding-time control problem. At each control epoch, the controller selects a refresh indicator, a target cluster count, and a holding time. The topology builder uses explicit cluster head election, nearest head member association, and intra-cluster chain forwarding with one-hop cluster head transmission to the base station. Under nominal deployment, the proposed controller reaches a half-node death (HND) point of 1969.1 ±8.4 rounds with 0.104 J of control energy, while periodic refresh with T = 10 reaches 1819.7 ±32.6 rounds and consumes 1.133 J. Across seven tested deployment scenarios, the proposed method gives a higher HND point with lower control energy than the tested refresh-enabled baselines. Therefore, the method is positioned as a lifetime overhead control mechanism, favoring lower control energy and longer mid-life operation, whereas periodic refresh remains preferable when delivery performance is the primary objective.

Keywords — adaptive holding time, energy efficiency, semi-Markov control, topology refresh, wireless sensor networks

1. Introduction

Clustered wireless sensor networks (WSNs) are used in environmental monitoring, smart agriculture, industrial sensing, and infrastructure supervision, as local data aggregation at cluster heads is capable of reducing the requirement for long-range radio transmissions from battery-powered sensor nodes to the base station [1]–[4]. In a clustered deployment, the operating bottleneck is not only the selected network topology, but also the process of updating that topology. Over subsequent communication rounds, residual energy, cluster head forwarding load, and member-to-cluster assignment may drift from the state used during the topology design phase, motivating a topology refresh before energy imbalance becomes severe.

A topology refresh is useful only when its reduction in data plane energy and energy offsets the added control energy cost. Frequent refreshes increase the overhead of status reporting, cluster head announcement, member reassociation, and schedule dissemination. Delayed refresh keeps an aging cluster assignment active after the residual energy distribution has changed, which can increase forwarding load on energy-depleted nodes. This paper studies clustered topology maintenance as a re-synchronization control problem, where the controller decides both the re-synchronization action and the holding time of the resulting topology.

Existing WSN clustering studies focus primarily on improving topology after reconfiguration. LEACH and HEED provide the classical baselines for cluster head rotation and energy-aware hybrid clustering [5], [6]. Recent studies further refine cluster operation through graph-based construction, energy-balanced routing, fuzzy or heuristic decision rules, and reinforcement learning-aided control [7]–[11]. These methods improve cluster head selection, forwarding load distribution, or route quality when the network decides to update its topology. The present papers address a narrower timing issue. The holding time of the selected topology is usually set to a fixed period or a one-step control clock, so its effect on control energy cost and residual energy drift is not explicitly controlled.

This paper makes the holding time of a topology control decision an explicit control variable. At each control epoch, the controller selects a refresh indicator, a target cluster count, and a holding time, rather than simply deciding whether to refresh the clustered topology. This converts topology maintenance into a variable duration control problem, where refresh responsiveness and control energy expenditure are handled within the same decision layer. The topology design module is kept explicit through cluster head election, nearest head member association, and intracluster chain forwarding, while the proposed controller operates above it to determine when to update the topology and for how long the updated topology should remain active.

The presented work is organized around three technical elements. First, clustered WSN topology maintenance is for-

mulated as an adaptive holding time problem with explicit control energy accounting, cluster head election, and member association. Second, a factorized semi-Markov controller separates the triggering of refresh, the selection of the cluster count, and holding time selection, making the action structure consistent with the operation sequence of clustered topology maintenance. Third, an evaluation examines nominal operation, fixed duration baselines, a holding-time-blind ablation, deployment changes, connectivity-based QoS proxies, imperfect state observation, cluster count sensitivity, and runtime complexity.

In the clustered WSN setting under consideration, exposing the topology holding time as a control variable reduces unnecessary topology refreshes, lowers the control energy cost, and improves the HND operating point relative to fixed period and holding-time blind refresh policies. This benefit is obtained at the cost of lower performance compared to the periodic refresh approach, which remains preferable when delivery performance is the primary objective. Therefore, the results should be interpreted as a lifetime overhead operating trade-off, and not as dominance over all lifetime or delivery metrics.

The remainder of the paper is organized as follows. Section 2 reviews clustering, adaptive topology refresh, and variable-duration control. Section 3 defines the network model, topology design, energy accounting, and the retention time objective. Section 4 presents the proposed control pipeline. Section 5 describes the experimental protocol. Section 6 presents the results and limitations, while Section 7 concludes the paper.

2. Related Works

Recent works on clustered WSNs first and foremost address the designed spatial structure developed after a topology update. LEACH rotates the cluster head role to distribute energy consumption among sensor nodes, while HEED incorporates residual energy and communication cost into the cluster head selection process to improve energy-sensitive cluster formation [5], [6].

Later studies refine this topology construction layer through graph-based clustering, energy-balanced path-tree design, dynamic clustering, and chain- or tree-based forwarding structures [7], [9], [10]. Stable clustering, redundancy-aware topology control, and energy-constrained cluster formation have also been studied to improve cluster head selection, member association, and forward load distribution [12]–[14].

These methods improve the topology installed after the network decides to update its structure. They do not directly control how long the installed topology should remain active before the next network state observation.

State-aware WSN control has also been studied through fuzzy inference, hedge algebra, and heuristic decision rules. These methods use residual energy, distance, load, or link-related descriptors to support cluster head selection and routing decisions under uncertain network conditions [15].

Fuzzy and heuristic WSN schemes further show that energy and load descriptors are useful inputs for distributed control when residual energy decreases unevenly across the network [8].

This line of work is relevant to the present paper, as it confirms the value of compact network state indicators. Its control object, however, is usually the cluster head choice, routing decision, or rule output inside a predefined update loop. The persistence time of the selected topology control decision is not treated as a separate operating variable.

Adaptive clustering and learning-based WSN control move beyond one-shot topology design by conditioning actions on the observed network state. Recent work on Q-learning-based routing, dynamic topology reconfiguration, and intelligent clustering adapts routing or cluster organization to residual energy evolution, traffic changes, or topology degradation [10], [11], [16]. These schemes are closer to the setting considered here, since the control action changes along with the network condition.

The remaining timing issue is more specific. In many adaptive schemes, the decision clock is still imposed by a fixed period or by a one-step update rule and, hence, the controller can choose what action to take but is not capable of determining how long the resulting topology control decision should persist.

This timing issue is important, because the cost of topology refresh and the effects of topology aging affect network performance over different time scales. A frequent refresh can correct cluster assignment and forwarding-load imbalance earlier, but it increases status reporting, cluster head announcement, member reassociation, and schedule dissemination overhead. A long holding time reduces the control energy cost, but the retained cluster assignment may drift from the current residual energy distribution. Therefore, fixing the update interval removes a degree of control freedom that is directly tied to the HND overhead operating point.

Semi-Markov decision processes and temporally extended actions provide the control structure needed for this degree of freedom. In a semi-Markov model, the selected action can remain active for a variable number of time steps, before the next decision is made [17]. The repetition follows the same principle by allowing the controller to choose both the action and its execution duration [18]. This mechanism aligns with clustered WSN topology maintenance, because a topology refresh incurs an immediate control energy cost, whereas the effect of the refreshed topology accumulates over several communication rounds.

This paper addresses a temporal control layer above clustered topology development. It does not replace the head election, member association, or the design of the forwarding structure. Instead, it treats the holding time of the installed topology as a controller output and evaluates whether this variable improves the HND overhead operating point at the expense of an explicit topology refresh cost. This separates the proposed problem from general WSN clustering and from learning-based routing methods that retain a fixed decision clock.

3. System Model and Problem Formulation

3.1. Network and Topology Model

Consider a static clustered WSN with N sensor nodes and one base station. The network evolves over discrete communication rounds indexed by t. Let V_t denote the set of alive nodes and let G_t denote the active clustered topology. The topology consists of the cluster head set H_t, the member association map, and the intra-cluster forwarding structure. In the evaluation model, each cluster uses a PEGASIS-style intracluster chain, and each cluster head forwards aggregated traffic to the base station through a one-hop uplink. This topology model is therefore a clustered chain-assisted structure, not an unrestricted multi-hop routing graph.

When a reconfiguration event is triggered, the topology builder first elects cluster heads from the alive node set. For each active node $i \in V_t$, the cluster head quality score is:

$$q_i(t) = 0.4\left(1 - \frac{d_{i,\mathrm{BS}}}{d_{\max}}\right) + 0.3\, c_i(t) + 0.3\,\frac{e_i(t)}{E_0}, \tag{1}$$

where $d_{i,\mathrm{BS}}$ is the distance from node i to the base station, $d_{\max}$ is the largest node-to-base-station distance in the deployment, $c_i(t)$ is the normalized centrality descriptor used by the topology builder, $e_i(t)$ is the residual energy, and E_0 is the nominal initial energy.

Equation (1) specifies the election rule used in the evaluation. A node obtains a higher score when it is closer to the base station, more central within the deployment, and has higher residual energy.

For a target cluster count C_n, the cluster head set is:

$$\mathcal{H}_{t_n} = \mathrm{Top}_{C_n}\left\{q_i(t_n) : i \in \mathcal{V}_{t_n}\right\}, \tag{2}$$

where Top_{C_n} returns the C_n highest scoring alive nodes, with $|\mathcal{H}_{t_n}| = \min(C_n, |\mathcal{V}_{t_n}|)$.

Equation (2) enforces the count of the requested cluster when enough alive nodes remain in the network. It also prevents depleted nodes from being selected as cluster heads.

Each non-head node is then associated with the nearest selected cluster head:

$$a_i(t_n) = \arg\min_{h \in \mathcal{H}_{t_n}} d_{i,h}, \qquad i \in \mathcal{V}_{t_n} \setminus \mathcal{H}_{t_n}. \tag{3}$$

Equation (3) defines the member association rule used after the cluster head election. Once the members are assigned, an intra cluster chain is constructed inside each cluster, and the resulting clustered topology remains active until the next refresh event.

3.2. Topology Age, State, and Composite Action

The topology age is updated as:

$$\tau_t = \begin{cases} 0, & \text{if a new topology is installed at round } t, \\ \tau_{t-1} + 1, & \text{otherwise.} \end{cases} \tag{4}$$

Equation (4) records the number of communication rounds during which the current clustered topology has remained active. A larger τ_t indicates that the retained cluster assignment and forwarding structure have been used for more rounds and may have drifted from the current residual energy distribution.

At the decision epoch n, the controller observes:

$$\begin{aligned}\mathbf{s}_n = \big[&\bar{e}_n, \sigma_{e,n}, e_n^{\min}, e_n^{\max}, \bar{e}_n^{\mathrm{ch}}, \sigma_{e,n}^{\mathrm{ch}}, \phi_n, C_n^{\mathrm{cur}}, \\ &\tau_n, \kappa_n, \hat{E}_{n-1}^{\mathrm{data}}, \hat{E}_{n-1}^{\mathrm{ctrl}}, \mathbb{I}(u_{n-1}=1)\big],\end{aligned} \tag{5}$$

where the entries describe the residual energy statistics, cluster head energy statistics, alive node ratio, active cluster count, topology age, energy imbalance and recent data/control energy.

Equation (5) supplies the controller with compact network state descriptors and the recent cost of topology maintenance. These descriptors are used to decide whether the current topology should be retained or updated.

The controller selects:

$$\mathbf{a}_n = (u_n, C_n, d_n), \tag{6}$$

where $u_n \in \{0,1\}$ is the refresh indicator, $C_n \in \mathcal{C}$ is the target cluster count, and $d_n \in \mathcal{D}$ is the holding time.

The next decision epoch is:

$$t_{n+1} = t_n + d_n. \tag{7}$$

Equation (7) makes the decision clock action dependent. The selected holding time determines how long the current control decision remains active before the state of the controller observes the network again.

3.3. Energy Accounting and Utility Interpretation

The round-level energy consumption is separated into data plane and control plane components:

$$E_t^{\mathrm{tot}} = E_t^{\mathrm{data}} + E_t^{\mathrm{ctrl}}. \tag{8}$$

Equation (8) makes topology refresh part of the network energy cost rather than treating the reconfiguration as a cost-free operation. The data plane component includes transmission, reception, and aggregation energy:

$$E_t^{\mathrm{data}} = \sum_{i \in \mathcal{V}_t} E_{i,t}^{\mathrm{tx/rx}} + \sum_{h \in \mathcal{H}_t} E_{h,t}^{\mathrm{agg}}. \tag{9}$$

Equation (9) collects the energy used for data forwarding and local aggregation. The second term captures the additional cost of aggregation at the selected cluster heads. When topology refresh is triggered at t_n, the control plane energy is formulated as cost:

$$E_{t_n}^{\mathrm{ctrl}} = u_n |\mathcal{V}_{t_n}| \left(e^{\mathrm{status}} + e^{\mathrm{config}}\right), \tag{10}$$

$E_t^{\mathrm{ctrl}} = 0$ for non-refresh rounds within the same holding segment.

Equation (10) models refresh overhead, as the status reporting and configuration dissemination costs are paid by the alive nodes when the clustered topology is rebuilt.

For a candidate decision (u, C, d), the idealized d-round utility can be written as:

$$\Delta_t(C,d) = \sum_{i=0}^{d-1}\left(E_{t+i}^{\mathrm{data,keep}} - E_{t+i}^{\mathrm{data,act}}(C)\right) - E_t^{\mathrm{ctrl}}(u,C). \tag{11}$$

Equation (11) is used only to interpret the refresh-timing trade-off. A refresh is useful when the data plane energy reduction obtained by rebuilding the topology is large enough to offset the one-time control plane cost. A shorter holding time improves responsiveness to residual energy drift, whereas a longer holding time gives more rounds over which the refresh cost can be amortized.

Theorem 1. *For a horizon of T communication rounds, if $d_n \geqslant d_{\min}$ for every control epoch, then the number of control opportunities satisfies:*

$$N_{\mathrm{ep}}(T) \leqslant \left\lceil \frac{T}{d_{\min}} \right\rceil, \tag{12}$$

and the cumulative control energy satisfies:

$$E_{\mathrm{ctrl}}^{\mathrm{cum}}(T) \leqslant N\left(e^{\mathrm{status}} + e^{\mathrm{config}}\right) \left\lceil \frac{T}{d_{\min}} \right\rceil. \tag{13}$$

Proof. Each decision epoch covers at least $d_{\min}$ communication rounds. Hence, over a horizon of T rounds, the number of control opportunities is upper-bounded by (12). At each refresh event, the control-plane charge is at most $N(e^{\mathrm{status}} + e^{\mathrm{config}})$ because no more than N nodes can be alive. This gives the cumulative control-energy bound in (13). □

Theorem 1 does not define an optimal policy. It states the structural role of the holding time. Increasing the minimum holding time directly limits the maximum refresh frequency and the worst-case accumulation of control plane energy.

Because each action remains active for d_n communication rounds, the segment reward is:

$$\bar{r}_n = \sum_{i=0}^{d_n-1} \lambda^i r_{t_n+i}, \qquad 0 < \lambda \leqslant 1, \tag{14}$$

and the long-horizon objective is:

$$J(\pi_{\boldsymbol{\theta}}) = \mathbb{E}_{\pi_{\boldsymbol{\theta}}} \left[\sum_{n=1}^{\infty} \gamma^{n-1} \bar{r}_n \right]. \tag{15}$$

Equations (14), (15) evaluate a topology control decision over its full holding segment, instead of only at the first communication round after refresh. This is the level at which topology aging, residual energy drift, and refresh overhead jointly affect the lifetime overhead trade-off.

4. Proposed Adaptive Holding-time Controller

4.1. Pipeline Overview

The proposed controller is organized as a four-block pipeline. The first block extracts compact state descriptors from the current network condition. The second block selects the factorized action (u_n, C_n, d_n). The third block rebuilds the clustered topology only when $u_n = 1$, using the topology-construction rules in Eqs. (1) – (3). The fourth block executes d_n rounds of data communication and returns the accumulated segment reward for the learning update.

This separation keeps the role of each module explicit. The learning policy controls refresh triggering, cluster-count selection, and holding time, while the cluster-head election and member-association rules remain fixed and are evaluated.

The reward in round t is:

$$r_t = \alpha\, \phi_t - \beta\, \hat{E}_t^{\mathrm{data}} - \gamma_c\, \hat{E}_t^{\mathrm{ctrl}} - \delta\, \kappa_t, \tag{16}$$

where ϕ_t is the alive-node ratio, κ_t is the energy-imbalance descriptor, and the energy terms are normalized by the initial network energy.

Equation (16) promotes node survival while penalizing the data plane energy, control plane energy, and residual energy imbalance. As a result, topology refresh is selected only when its expected benefit outweighs the additional control plane charge.

4.2. Factorized Policy and Learning Update

The policy is factored as follows:

$$\begin{aligned} \pi_{\boldsymbol{\theta}}\left(\mathbf{a}_n|\mathbf{s}_n\right) = \pi_{\boldsymbol{\theta}}^{(u)}\left(u_n|\mathbf{s}_n\right)\pi_{\boldsymbol{\theta}}^{(C)}\left(C_n|\mathbf{s}_n, u_n\right) \\ \times\, \pi_{\boldsymbol{\theta}}^{(d)}\left(d_n|\mathbf{s}_n, u_n\right). \end{aligned} \tag{17}$$

Equation (17) separates the refresh decision from the topology scale decision and the hold time decision. This structure follows the operating sequence for clustered topology maintenance. The controller first decides whether to update the current topology. When a refresh is selected, the target cluster count determines the new topology scale. The holding-time branch then determines how many communications rounds the resulting control decision remains active before the next control epoch.

The critical target is:

$$y_n = \bar{r}_n + \gamma\, V_{\psi}\left(\mathbf{s}_{n+1}\right), \tag{18}$$

and the critical loss is:

$$\mathcal{L}_{\mathrm{critic}} = \mathbb{E}\left[\, \left(V_{\psi}(\mathbf{s}_n) - y_n\right)^2 \right]. \tag{19}$$

Equations (18), (19) train the value estimator using the return accumulated over a complete holding segment, rather than only the immediate communication round after a refresh decision. This is consistent with the operating sequence for clustered topology maintenance, where a selected topology remains active for multiple rounds before the next control epoch.

The advantage estimate is as follows:

$$\hat{A}_n = \bar{r}_n + \gamma\, V_{\psi}(\mathbf{s}_{n+1}) - V_{\psi}(\mathbf{s}_n), \tag{20}$$

and the actor update follows::

$$\nabla_{\boldsymbol{\theta}} J \approx \mathbb{E}\left[\nabla_{\boldsymbol{\theta}} \log \pi_{\boldsymbol{\theta}}(\mathbf{a}_n|\mathbf{s}_n)\hat{A}_n\right]. \tag{21}$$

Equation (21) assigns credit to the complete control tuple (u_n, C_n, d_n) according to the multi-round network outcome produced by that tuple. This credit assignment is needed, because the control plane refresh cost is borne immediately, whereas the effect of the selected topology and holding time appears over subsequent communication rounds.

Algorithm 1 Adaptive holding-time topology control

Require: Deployment, energy parameters, cluster count set $\mathcal{C}$, holding-time set $\mathcal{D}$, actor parameters $\boldsymbol{\theta}$, critical parameters $\boldsymbol{\psi}$

for each training episode **do**
  Reset residual energy, alive node set, and initial clustered topology
  while the termination condition is not met **do**
    Design the control state $\mathbf{s}_n$ using Eq. (5)
    Sample the control tuple: $(u_n, C_n, d_n) \sim \pi_{\boldsymbol{\theta}}(\cdot|\mathbf{s}_n)$
    if $u_n = 1$ **then**
      Elect cluster heads using Eq. (1)
      Associate members using Eq. (3)
      Charge the control plane energy using Eq. (10)
    end if
    Execute d_n communication rounds under the active clustered topology
    Accumulate the segment reward $\bar{r}_n$
    Design the next control state $\mathbf{s}_{n+1}$
    Update the critic using Eq. (19)
    Update the actor using Eq. (21)
  end while
end for

4.3. Algorithm and Complexity

Algorithm 1 separates the timing decision from the topology construction rule. The actor selects whether to refresh, which cluster count to use, and how long the resulting control decision remains active. The topology builder is invoked only when $u_n = 1$. Otherwise, the network continues data communication under the retained clustered topology.

The complexity of topology construction per refresh event is:

$$\mathcal{O}_{\text{topo}} = \mathcal{O}\left(|\mathcal{V}_t| \log |\mathcal{V}_t| + |\mathcal{V}_t| C_n + \sum_{h \in \mathcal{H}_t} |\mathcal{C}_{h,t}|^2\right), \quad (22)$$

where the three terms correspond to cluster head ranking, nearest head member association, and intra-cluster chain construction, respectively. Equation (22) also shows that topology construction is paid only at refresh events, not during every data packet transmission.

The policy inference cost is proportional to the number of actor parameters:

$$\mathcal{O}_{\text{policy}} = \mathcal{O}(P_{\boldsymbol{\theta}}). \quad (23)$$

Tab. 1. Deployment scenarios used for evaluation.

ID	Nodes/field	BS position	Purpose
S0	100, 100 × 100	[150, 50]	Nominal
S1	50, 100 × 100	[150, 50]	Sparse density
S2	150, 100 × 100	[150, 50]	Dense density
S3	100, 150 × 150	[225, 75]	Larger field
S4	100, 100 × 100	[50, 50]	Centered BS
S5	100, 100 × 100	[200, 50]	Far BS
S6	100, 100 × 100	[150, 50]	Heterogeneous E_0

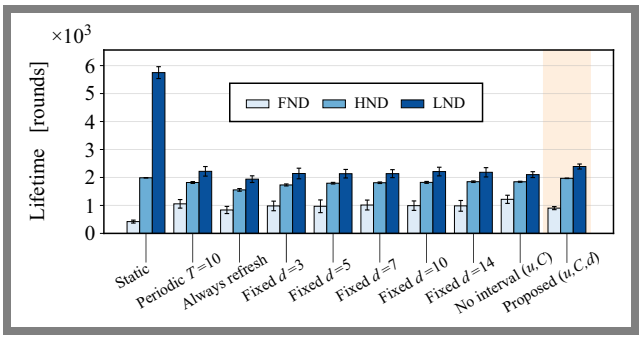

Fig. 1. Comparison of FND, HND and LND comparison under the nominal deployment.

Equation (23) applies only at control epochs and is incurred on the controller side. The sensor nodes do not execute the learning-based controller. They only receive and follow the disseminated topology configuration.

5. Experimental Design

The nominal setting uses $N = 100$ nodes in a 100×100 m field, a base station (BS) at $[150, 50]$, initial energy $E_0 = 0.5$ J, and 12 000 maximum rounds. The holding-time set is $\mathcal{D} = \{3, 5, 7, 10, 14\}$, and the baseline cluster count candidate set is $\mathcal{C} = \{3, 4, 5, 6, 7, 8\}$. Each main result is evaluated over 30 random seeds.

The baselines are static topology, periodic re-update with $T = 10$, always refresh, fixed-holding-time controllers with $d \in \{3, 5, 7, 10, 14\}$, a holding-time-blind adaptive controller (u, C) with fixed $d = 7$, and the proposed controller (u, C, d). A flat-action DQN baseline is also evaluated as an internal action factorization ablation. The evaluation scenarios are summarized in Tab. 1. They are designed to determine whether the result is limited to a single nominal deployment. The scenarios vary in node density, field size, base station location, and initial energy heterogeneity.

WSN performance is evaluated through lifetime (Fig. 1), topology maintenance overhead, and service-related metrics. Lifetime is measured based on first node death (FND), half-node death (HND), and last node death (LND). Overhead is measured based on control energy (CtrlE), refresh count, and average holding time. Service behavior is summarized by connectivity-based delivery, hop-count delay, throughput, coverage at HND, and Jain fairness at HND. These service-related metrics are treated as proxies, because the simulator does not include a full MAC layer scheduler, contention, retransmission, or stochastic physical layer decoding.

6. Results and Discussion

6.1. Nominal Lifetime Overhead Performance

Table 2 and Fig. 2 present the nominal comparison. The proposed controller attains 1969.1 ±8.4 rounds in HND with only 0.104 J control energy. Periodic refresh with $T = 10$ achieves 1819.7 ±32.6 rounds and consumes 1.133 J. Always

Tab. 2. Comparison of nominal lifetime and control energy (30 runs).

Method	FND	HND	LND	CtrlE [J]
Static	421.9 ±52.7	1988.3 ±2.1	5749.2 ±212.2	0.000
Periodic $T = 10$	1056.7 ±152.7	1819.7 ±32.6	2219.4 ±171.1	1.133
Always refresh	837.5 ±128.0	1556.0 ±47.1	1939.8 ±119.3	8.969
Fixed $d = 7$	1014.4 ±176.9	1811.5 ±27.0	2136.8 ±142.6	1.577
Fixed $d = 14$	984.8 ±191.9	1848.5 ±27.6	2184.9 ±166.3	0.803
No interval (u, C)	1218.4 ±145.9	1846.3 ±17.6	2101.6 ±105.1	1.651
Proposed (u, C, d)	903.6 ±54.6	1969.1 ±8.4	2391.5 ±89.1	0.104

refresh performs worse, because the topology is updated too aggressively and 8.969 J is spent on control energy.

The observation is metric-specific. The proposed controller does not maximize the FND, as the no-interval ablation reaches a higher FND point. Its advantage appears in HND, LND, and controlled energy. Compared to no-interval ablation, the proposed controller improves HND by 122.8 rounds and reduces the control energy by approximately 15.9×. This shows that the holding-time branch suppresses unnecessary topology refreshes and shifts the operating point toward longer mid-life and late-life network operation at lower control energy cost.

6.2. Fixed Holding Time and Factorization Effects

The fixed-holding-time baselines show the limitations of using a single designer-selected update period. The best fixed baseline in Tab. 2 is $d = 14$, which reaches 1848.5 HND rounds with 0.803 J of control energy. The proposed controller reaches 1969.1 HND rounds with 0.104 J of control energy. Therefore, the improvement is not explained by selecting a long holding time. The controller jointly decides whether to refresh the topology and how long the selected topology control decision should remain active, so the refresh is triggered only when the observed network state justifies the additional control plane charge.

The flat-action DQN ablation further examines the factorized action structure in Eq. (17). With the same state descriptors and reward, the flat-action DQN reaches 1930.5 ±15.9 HND but consumes 0.302 J of control energy, which is about 2.84× higher than the proposed factorized controller in the matched ablation setting. This result supports separating refresh triggering, cluster count selection, and hold-time selection. It is used only as an internal action-structure ablation, not as a substitute for external WSN clustering or routing baselines.

6.3. Cluster Head Election and Topology Verification

The topology construction verification checks the lower layer clustering process used in the evaluation model. Across the verified refresh events, no depleted node is selected as a cluster head. Every alive non-head node is associated with exactly one cluster, and the realized number of cluster heads matches the requested C_n whenever $|\mathcal{V}_t| \geqslant C_n$. The mean topology development time is 104.3 ms in the verification run, while the broader runtime profile in Subsection 6.8 reports a mean topology build time of 147.6 ms. In the evaluation model, a topology update is therefore executed within one control epoch. This timing result should not be interpreted as distributed reconfiguration latency in a physical WSN deployment.

This verification fixes the interpretation of the proposed controller. The learning policy does not depend on an unspecified clustering routine. It decides when to invoke the topology builder, which cluster count to request, and how long the resulting clustered topology should remain active. Cluster head election, member association, and intra-cluster chain construction are defined by the topology construction module described in Section 3.

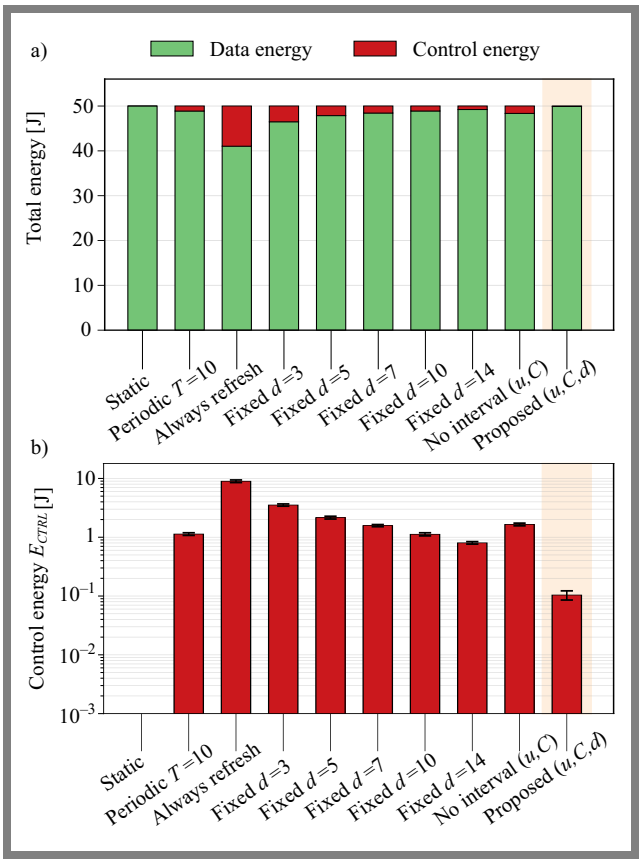

Fig. 2. Energy decomposition under nominal deployment.

6.4. Multi-scenario Validation

Table 3 and Fig. 3 show the validation for seven scenarios. The proposed method provides a better HND-CtrlE operating point than the best non-static refresh-enabled competitor. The largest gains occur when the field is enlarged, or the base station is moved farther away, because topology refresh becomes more expensive and holding-time control can amortize that cost.

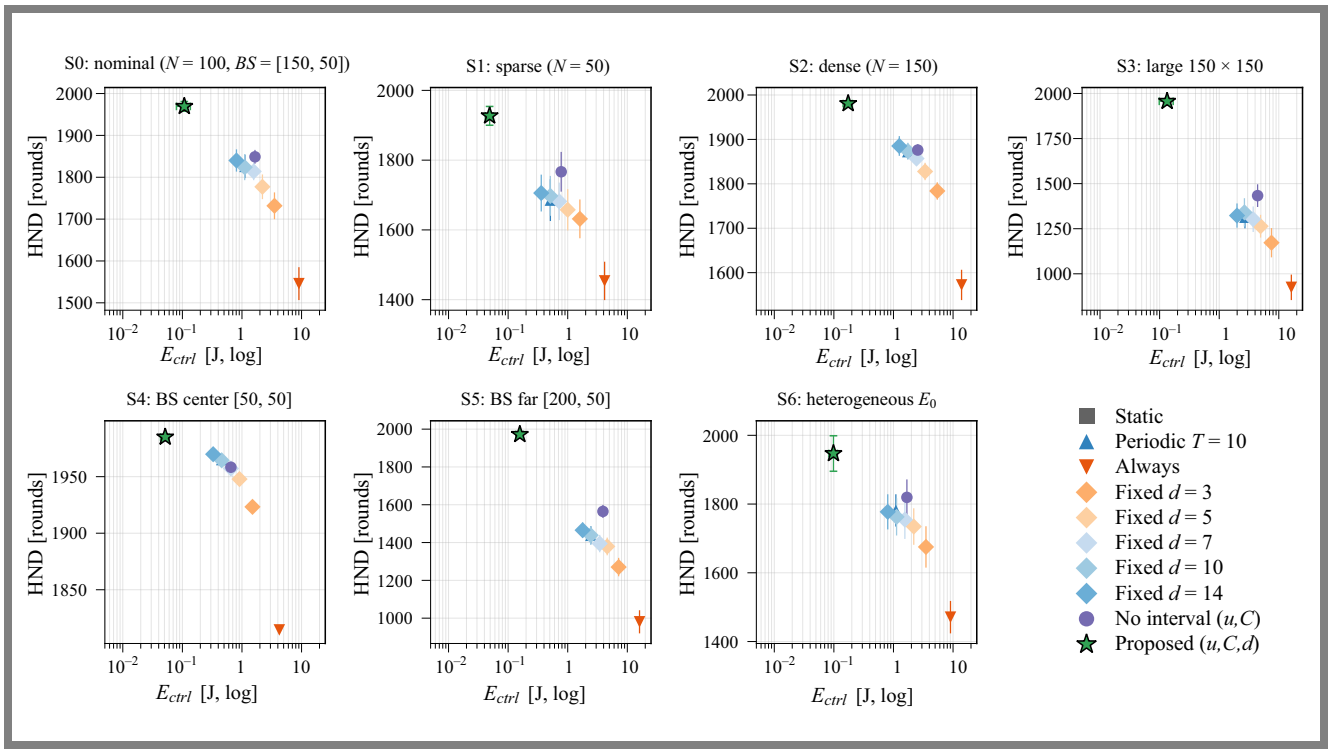

Fig. 3. HND versus control energy in seven deployment scenarios.

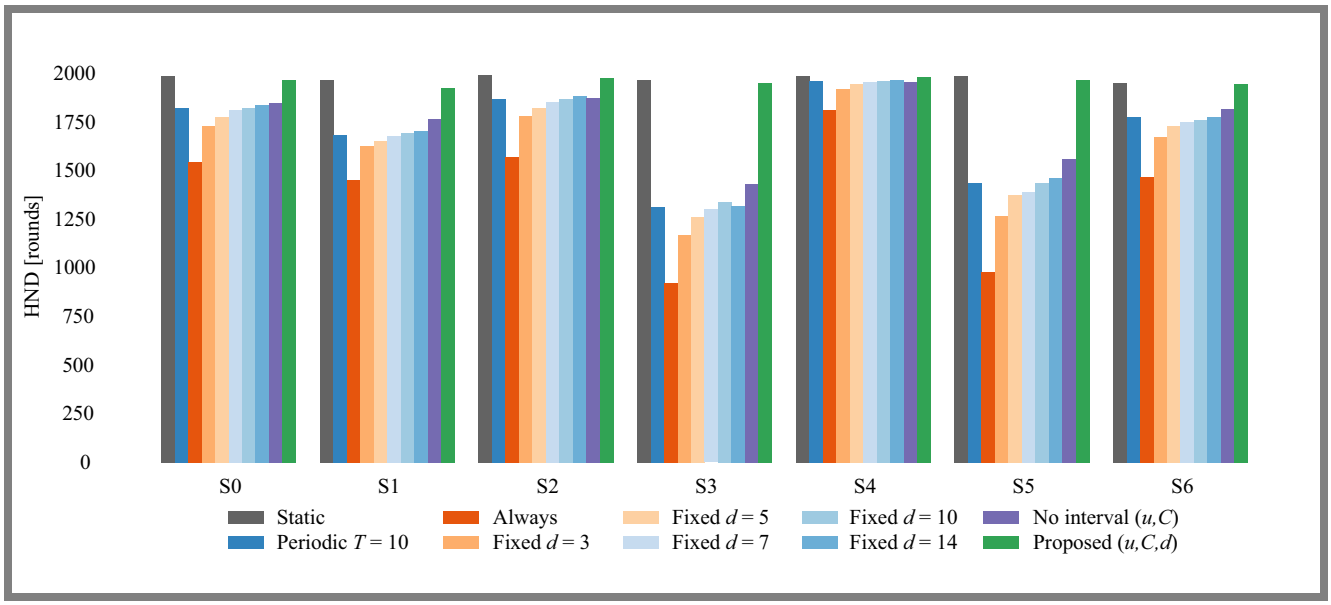

Fig. 4. Comparison of HNDs for tested scenarios.

The comparison also reveals where the gain is small. In S4, the base station is placed in the center of the field, reducing communication costs and making simple refresh policies more competitive. The HND gap is only 15.1 rounds. This indicates that adaptive holding time is most useful when refresh cost and topology staleness create a pronounced trade-off.

6.5. Connectivity-based Delivery, Coverage, and Fairness

Table 4 and Fig. 4 report the service-related proxies used to complement lifetime and overhead metrics. Periodic refreshes achieve a higher connectivity-based delivery value, because they update the clustered topology more frequently. The proposed controller refreshes less frequently, so the retained topology can age for more communication rounds. This produces a clear operating trade-off. The proposed method improves the overhead operating point, whereas periodic refreshing better preserves delivery-oriented performance.

The main limitation appears in S5, where the base station is farther from the sensing field. The proposed controller still improves the HND in this scenario, but its connectivity-based delivery value decreases to 0.352. This indicates that reduc-

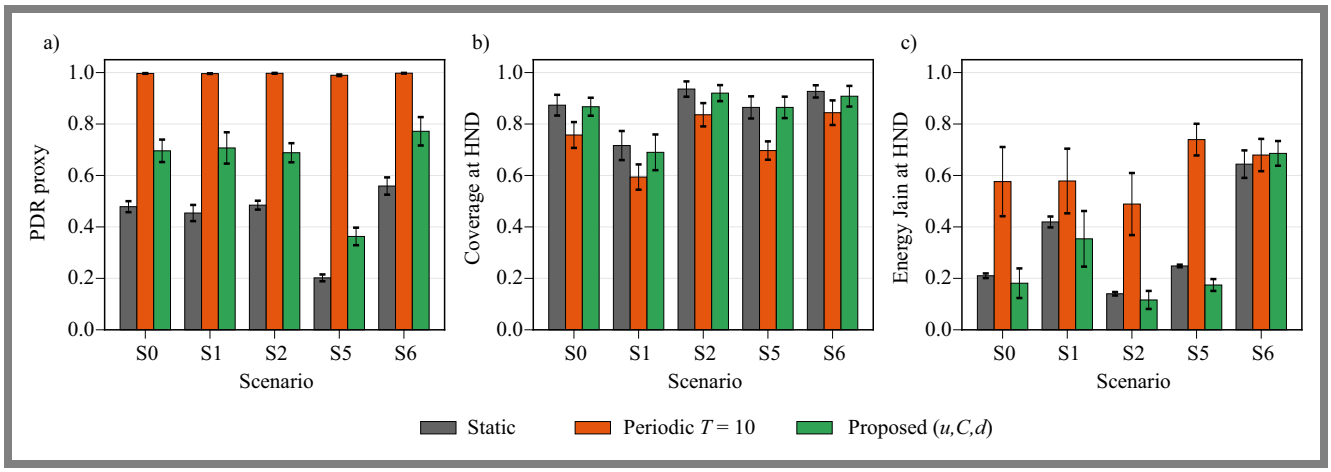

Fig. 5. Service-related proxy, coverage, and fairness.

ing the topology refresh frequency can extend the lifetime of the network while weakening delivery-oriented performance. For deployments where delivery performance is the primary objective, the controller would require a stronger delivery-oriented reward term, a different relay/base station placement, or a topology builder designed explicitly for delivery preservation.

6.6. Sensitivity to Imperfect Network-state Observation

Table 5 and Fig. 5 report the sensitivity of the proposed controller to residual energy observation noise and delayed network state information. The residual energy observation noise with $\sigma \in \{0.02, 0.05, 0.10\}$ changes HND by less than 0.2% relative to the clean proposed-policy reference. State-observation delay with $\Delta \in \{1, 2, 5\}$ control epochs keeps HND within 0.67% of the clean reference.

These results show limited sensitivity to the perturbation levels in the state vector. The evaluation covers residual energy observation noise and short state observation delays. It does not cover packet loss, node mobility, MAC contention, bursty traffic, or adversarial sensing errors. The result should therefore be interpreted as state observation sensitivity within the tested operating range, not as general robustness to all deployment impairments.

Tab. 3. Comparison of multi-scenario HND overhead against the best non-static refresh-enabled competitor.

Scen.	Proposed HND	CtrlE	Best competitor	HND gap
S0	1969.3	0.108	No interval	+120.5
S1	1927.0	0.049	No interval	+160.3
S2	1980.7	0.174	Fixed d =14	+95.5
S3	1956.6	0.134	No interval	+523.1
S4	1985.0	0.051	Fixed d =14	+15.1
S5	1972.0	0.157	Fixed d =14	+506.6
S6	1947.1	0.098	No interval	+127.7

Tab. 4. Delivery, coverage, and fairness under periodic refresh and the proposed controller.

Scen.	Method	Delivery	Cov.@HND	Jain@HND
S0	Periodic	0.996	0.743	0.528
S0	Proposed	0.700	0.869	0.192
S2	Periodic	0.997	0.829	0.538
S2	Proposed	0.700	0.929	0.117
S5	Periodic	0.989	0.691	0.738
S5	Proposed	0.352	0.867	0.175
S6	Periodic	0.998	0.844	0.679
S6	Proposed	0.772	0.908	0.686

Tab. 5. Sensitivity of the proposed controller to imperfect observation of the state of the network.

Perturbation	HND	CtrlE [J]	HND change
Clean	1967.3 ±10.7	0.109	0.00%
Noise $\sigma = 0.02$	1969.8 ±6.9	0.104	+0.13%
Noise $\sigma = 0.05$	1967.9 ±8.3	0.104	+0.03%
Noise $\sigma = 0.10$	1970.6 ±9.4	0.092	+0.17%
Delay $\Delta = 1$	1980.4 ±2.7	0.074	+0.67%
Delay $\Delta = 2$	1979.6 ±2.4	0.085	+0.63%
Delay $\Delta = 5$	1979.9 ±2.8	0.100	+0.64%

6.7. Cluster Count Selection Sensitivity

The cluster count sensitivity study explains how the controller constrains the choices for cluster count. The controller does not optimize a continuous cluster count. It selects C_n from a predefined finite candidate set. Table 6, Figs. 6 – 7 show that the baseline set $\mathcal{C} = \{3, 4, 5, 6, 7, 8\}$ gives the highest proposed-policy HND among the evaluated candidate sets.

Tab. 6. Sensitivity of the candidate set with cluster count for the proposed controller.

Set	Values	HND	CtrlE [J]	Avg. C
C_{base}	{3, 4, 5, 6, 7, 8}	1967.5 ±11.8	0.107	3.34
C_1	{4, 6, 8}	1863.2 ±38.4	0.829	5.22
C_2	{5, 8, 10}	1916.8 ±25.4	0.285	5.41
C_3	{6, 10, 14}	1921.3 ±23.9	0.191	6.13

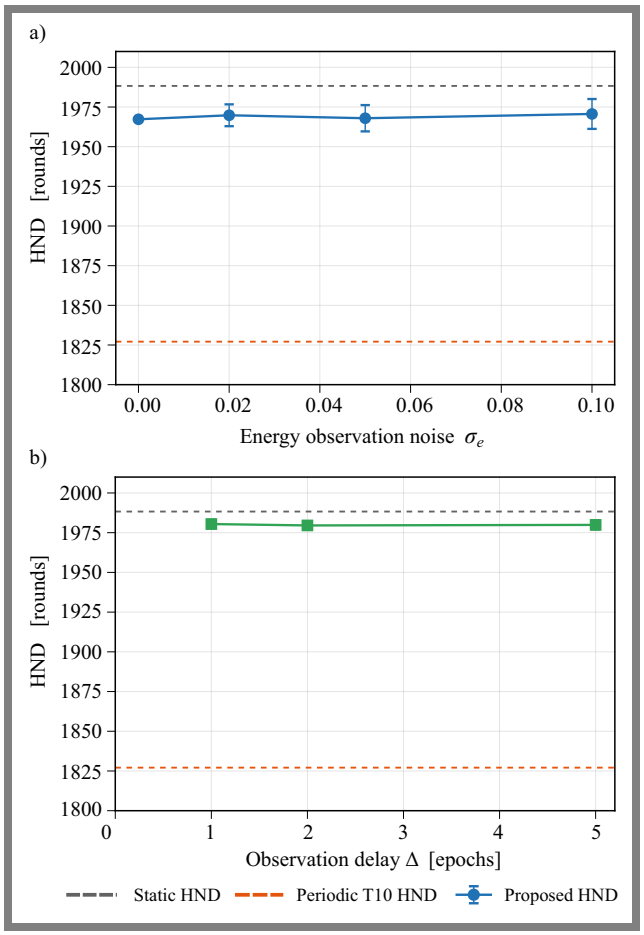

Fig. 6. HND of the proposed controller under residual energy observation noise and delayed network state observation.

The results indicate that the low cluster count options, especially the three- and four-groups, are useful under the evaluated deployment geometry and energy model. When the candidate set starts at 4 or 5 clusters, the controller is forced toward larger topologies, increasing control energy cost and reducing HND. The cluster count set is therefore an engineering design choice that should match the node density, the sensor field size, and the placement of the base station.

6.8. Training, Runtime, and Deployment Complexity

The controller uses a 13-dimensional state vector. Both the actor and critical models use two hidden layers with 256 units, LayerNorm, and ReLU activation. The actor has three output heads for the refresh indicator u, cluster count C, and holding time d. Adam is used with a learning rate of $3{\times}10^{-4}$ and a discount factor of 0.99. The implemented model has 73 741 actor parameters and 70 657 critic parameters, for a total of 144 398.

The runtime profile separates off-line training from online controller execution (Fig. 8). Policy inference takes 2476 ±797 µs per control call, with a 95-th percentile of 3628 µs. Topology construction takes 147.6 ±38.4 ms per refresh event, with a 95-th percentile of 197.4 ms. These values are measured on the controller side. The sensor nodes do not execute the learning-based controller. They only receive the topology configuration and follow the resulting cluster assignment and forwarding schedule.

7. Conclusions

This article studied clustered WSN topology maintenance from the perspective of adaptive holding time. The controller decides whether to refresh the topology, which cluster count to use after the refresh, and how long the resulting topology control decision should remain active. The lower layer topology builder is specified through cluster head scoring, nearest head member association, and chain-assisted intra-cluster forwarding with one-hop cluster head transmission to the base station.

The results show a consistent lifetime-overhead trade-off. Under nominal deployment, the proposed controller improves HND from 1819.7 ±32.6 rounds with periodic refresh to 1969.1 ±8.4 rounds, while reducing the control energy from 1.133 J to 0.104 J. Across the seven tested deployment scenarios, the proposed method provides a better HND overhead operating point than the tested refresh enabled baselines. The state observation tests also show limited sensitivity to the evaluated residual energy noise levels and short observation delays.

The operating gain is not universal across all metrics. The proposed controller does not maximize FND and does not preserve connectivity-based delivery or periodic refresh. In the far base station scenario, the delivery value is low even though HND remains high. Therefore, adaptive holding time should be interpreted as a lifetime overhead control mechanism for the considered clustered chain topology model, not as a general QoS-maximizing topology policy.

Future work should extend the evaluation to MAC layer packet scheduling, dynamic traffic, mobility, and external learning-based clustering baselines under matched topology and energy accounting models.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", *Computer Networks*, vol. 38, pp. 393–422, 2002 (https://doi.org/10.1016/S1389-1286(01)00302-4).

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless Sensor Network Survey", *Computer Networks*, vol. 52, pp. 2292–2330, 2008 (https://doi.org/10.1016/j.comnet.2008.04.002).

[3] M.M. Afsar and M.H. Tayarani-N, "Clustering in Sensor Networks: A Literature Survey", *Journal of Network and Computer Applications*, vol. 46, pp. 198–226, 2014 (https://doi.org/10.1016/j.jnca.2014.09.005).

[4] I. Daanoune, B. Abdennaceur, and A. Ballouk, "A Comprehensive Survey on LEACH-based Clustering Routing Protocols in Wireless Sensor Networks", *Ad Hoc Networks*, vol. 114, art. no. 102409, 2021 (https://doi.org/10.1016/j.adhoc.2020.102409).

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks", *Proc. of the 33rd Annual Hawaii International Conference on System Sciences*, pp. 3005–3014, 2000 (https://doi.org/10.1109/HICSS.2000.926982).

[6] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks",

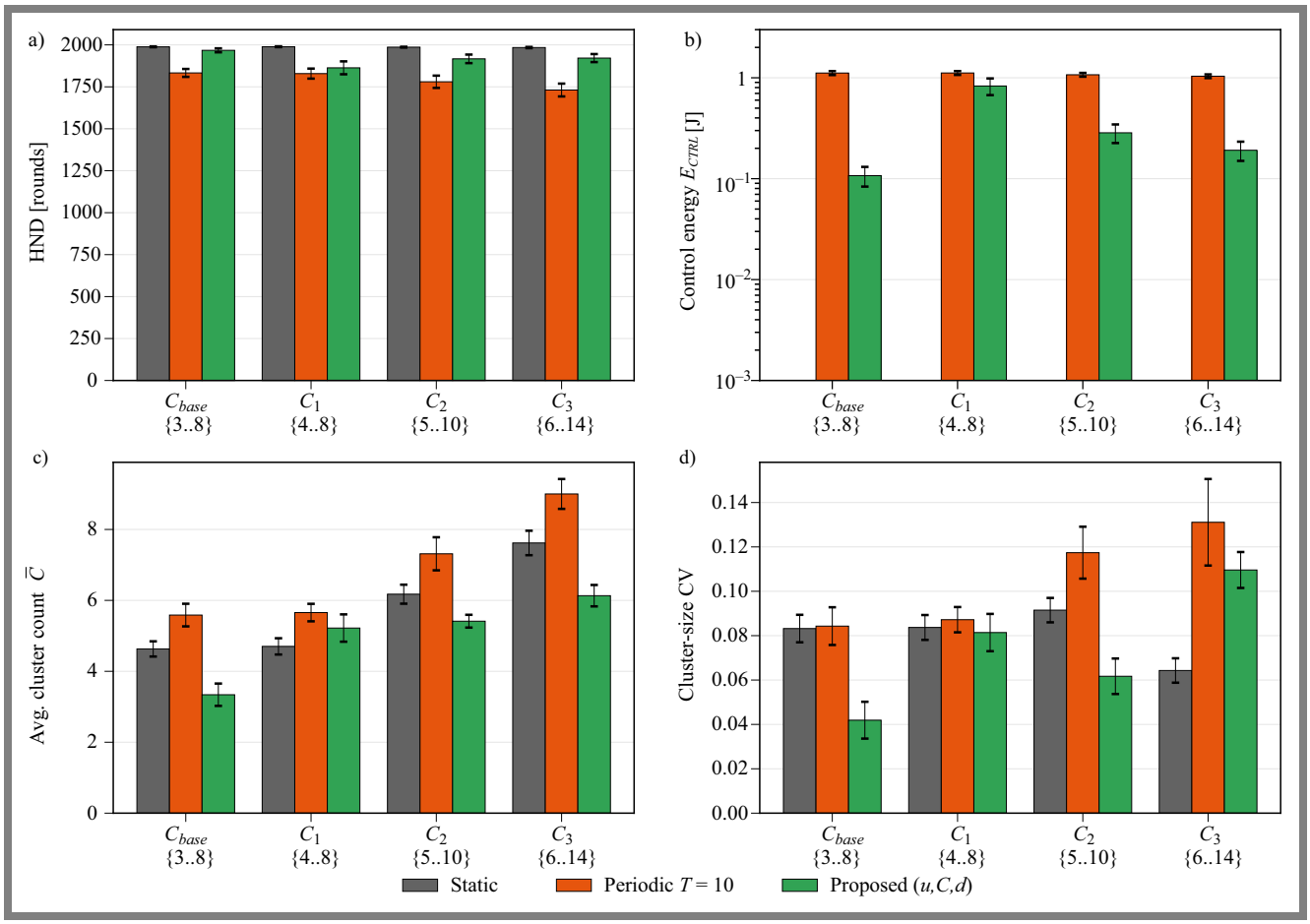

Fig. 7. Sensitivity of the cluster count candidate set. The proposed controller performs best with the evaluated baseline set, because it can select low cluster counts when fewer cluster heads are sufficient under this deployment model.

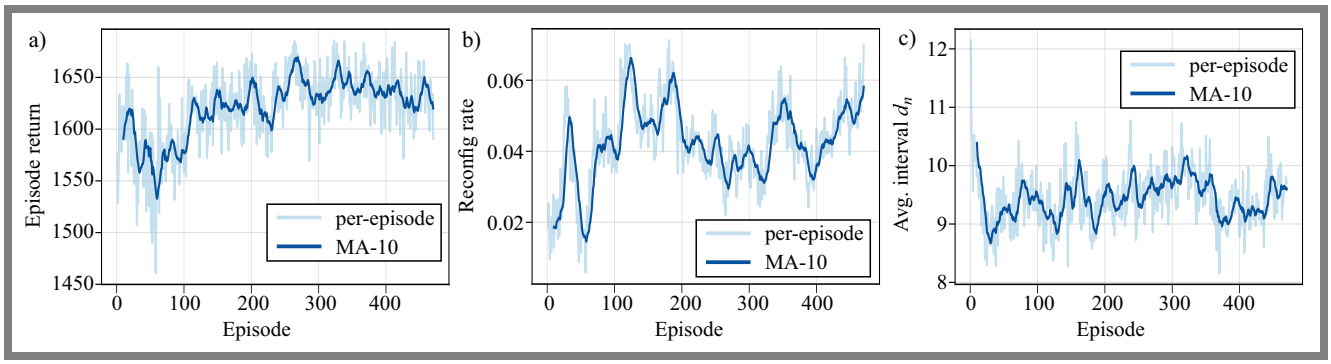

Fig. 8. Convergence of factorized policy.

IEEE Transactions on Mobile Computing, vol. 3, pp. 366–379, 2004 (https://doi.org/10.1109/TMC.2004.41).

[7] M. Saadati, S.M. Mazinani, A.A. Khazaei, and S.J.S.M. Chabok, "Energy Efficient Clustering for Dense Wireless Sensor Network by Applying Graph Neural Networks with Coverage Metrics", *Ad Hoc Networks*, vol. 156, art. no. 103432, 2024 (https://doi.org/10.1016/j.adhoc.2024.103432).

[8] M. Shokouhifar *et al*, "AI-driven Cluster-based Routing Protocols in WSNs: A Survey of Fuzzy Heuristics, Metaheuristics, and Machine Learning Models", *Computer Science Review*, vol. 54, art. no. 100684, 2024 (https://doi.org/10.1016/j.cosrev.2024.100684).

[9] B. Fan and Y. Xin, "EBPT-CRA: A Clustering and Routing Algorithm Based on Energy-balanced Path Tree for Wireless Sensor Networks", *Expert Systems with Applications*, vol. 259, art. no. 125232, 2025 (https://doi.org/10.1016/j.eswa.2024.125232).

[10] S. Najjar, M. David, W. Derigent, and A. Zouinkhi, "Dynamic Reconfiguration of Wireless Sensor Networks: A Survey", *Computer Networks*, vol. 262, art. no. 111176, 2025 (https://doi.org/10.1016/j.comnet.2025.111176).

[11] C. Wang, H. Hu, and X. Fan, "Intelligent Clustering and Routing Protocol for Wireless Sensor Networks Using Quantum Inspired Harris Hawk Optimizer and Deep Reinforcement Learning", *Ad Hoc Networks*, vol. 178, art. no. 103914, 2025 (https://doi.org/10.1016/j.adhoc.2025.103914).

[12] N. Mittal, U. Singh, and B.S. Sohi, "A Stable Energy Efficient Clustering Protocol for Wireless Sensor Networks", *Wireless Networks*, vol. 23, pp. 1809–1821, 2017 (https://doi.org/10.1007/s11276-016-1255-6).

[13] B. Zebbane, M. Chenait, and N. Badache, "A Distributed Lightweight Redundancy Aware Topology Control Protocol for Wireless Sensor

Networks", *Wireless Networks*, vol. 23, pp. 1779–1792, 2017 (https://doi.org/10.1007/s11276-016-1248-5).
[14] H.R. Farahzadi, M. Langarizadeh, M. Mirhosseini, and S.A.F. Aghda, "An Improved Cluster Formation Process in Wireless Sensor Network to Decrease Energy Consumption", *Wireless Networks*, vol. 27, pp. 1077–1087, 2021 (https://doi.org/10.1007/s11276-020-02485-y).
[15] T. Nguyen, T.-A. Nguyen, and T.-M. Hoang, "A Study on Multi-hop Routing Scheme for Wireless Sensor Networks", *JST: Smart Systems and Devices*, vol. 31, pp. 1–9, 2021 (https://doi.org/10.51316/jst.152.ssad.2021.31.2.1).
[16] Z. Zhang, J. Zhou, and J. Li, "Q-learning-based Semi-fixed Clustering Routing Algorithm in WSNs", *Ad Hoc Networks*, vol. 174, art. no. 103837, 2025 (https://doi.org/10.1016/j.adhoc.2025.103837).
[17] R.S. Sutton, D. Precup, and S. Singh, "Between MDPs and Semi-MDPs: A Framework for Temporal Abstraction in Reinforcement Learning", *Artificial Intelligence*, vol. 112, pp. 181–211, 1999 (https://doi.org/10.1016/S0004-3702(99)00052-1).
[18] A. S. Lakshminarayanan, S. Sharma, and B. Ravindran, "Dynamic action repetition for deep reinforcement learning", *Proc. of the AAAI Conference on Artificial Intelligence*, vol. 31, pp. 2133–2139, 2017 (https://doi.org/10.1609/aaai.v31i1.10918).

Trong-Minh Hoang, Ph.D.
https://orcid.org/0000-0001-8486-2940
E-mail: hoangtrongminh@ptit.edu.vn
Posts and Telecommunications Institute of Technology, Hanoi, Vietnam
https://ptit.edu.vn

Thanh-Long Tran, Ph.D.
https://orcid.org/0009-0006-5843-6044
E-mail: longtt.product@gmail.com
Posts and Telecommunications Institute of Technology, Hanoi, Vietnam
https://ptit.edu.vn

Huy-Long Tran, Ph.D.
https://orcid.org/0009-0008-2968-3905
E-mail: longth@ptit.edu.vn
Posts and Telecommunications Institute of Technology, Hanoi, Vietnam
https://ptit.edu.vn

Ngoc-Bich Pham, Ph.D.
https://orcid.org/0009-0002-3302-5813
E-mail: bichpn@thanglong.edu.vn
Thang Long University, Hanoi, Vietnam
https://thanglong.edu.vn

Sinh Cong Lam, Ph.D.
https://orcid.org/0000-0003-4546-3378
E-mail: congls@vnu.edu.vn (corresponding author)
VNU University of Engineering and Technology, Hanoi, Vietnam
https://uet.vnu.edu.vn

Analyzing Performance of Eigenvalue-based Spectrum Sensing within LoRaCog Framework

Batool Jaafar Bashar and Hikmat Abdullah

Al-Nahrain University, Baghdad, Iraq

https://doi.org/10.26636/jtit.2026.2.2576

Abstract — The CR technology enhances spectrum utilization by allowing access to unused licensed channels, while spectrum sensing allows secondary users to verify channel availability before the transmission. This study relies on the LoRaCog framework, a solution integrating the CR technology with LoRa LPWAN networks, to evaluate the performance of eigenvalue-based detection algorithms, such as maximum eigenvalue detection (MED), maximum to minimum eigenvalue (MME), energy-to-minimum eigenvalue (EME) and maximum-to-mean eigenvalue detection (MMED), with the comparisons based on energy detection (ED). The said algorithms were evaluated under three scenarios characterized by an increasing degree of complexity. These included the following: an ideal additive white Gaussian noise (AWGN) channel, followed by a multipath fading channel with noise uncertainty using a SISO receiver and, finally, a SIMO multiantenna receiver system. The simulation results for the AWGN channel showed that the ED algorithm achieved the best detection probability and the lowest sensing time. When multipath fading and noise uncertainty were introduced, eigenvalue-based algorithms achieved higher detection probabilities while maintaining comparable detection times. The MME algorithm achieved the highest detection probability when used with the SIMO multiantenna reception system.

Keywords — CR, eigenvalue-based detection, LoRa networks, LPWAN, spectrum sensing

1. Introduction

Many solutions have been proposed to address the challenges arising from inefficient spectrum management, among which the CR technology has emerged as a promising approach [1]. CR enables dynamic spectrum access by allowing secondary users (SUs) to opportunistically utilize frequency bands when primary users (PUs) are inactive, ensuring also that no interference is caused to licensed users [2], [3]. Spectrum sensing plays a crucial role in this mechanism by enabling SUs to determine whether a given frequency band is occupied before initiating transmission [4], [5].

Low-power wide-area networks (LPWANs) are among the primary wireless technologies that support applications of the Internet of Things (IoT). Among these, LoRa networks are distinguished by their ability to provide long-range communication while maintaining low power consumption. LoRa networks typically operate in unlicensed frequency bands. However, these bands have become increasingly congested due to the rapid growth in the popularity of IoT devices. Such congestion may lead to increased packet collisions and reduced communication reliability, particularly in dense deployment environments [6], [7].

Several studies have investigated integrating CR into LoRa networks using a cognitive LoRa framework (LoRaCog). In this framework, LoRa gateways are equipped with spectrum sensing capabilities, allowing them to monitor licensed channels and opportunistically access temporarily unused spectrum while preserving the existing LoRa infrastructure [8]. However, achieving reliable spectrum sensing in such environments remains a major challenge, particularly under low signal-to-noise ratio (SNR) conditions.

Because of its simplicity, energy detection (ED) is one of the most widely used spectrum-sensing techniques. However, its performance deteriorates significantly in low-SNR environments due to the SNR wall effect. To overcome these limitations, eigenvalue-based spectrum sensing algorithms have attracted considerable attention. These methods rely on the statistical properties of the covariance matrix of the received signal, allowing the detection of a primary user without prior knowledge of the signal structure or the noise power [2], [9], [10].

This study evaluates the performance of several eigenvalue-based spectrum sensing algorithms within the LoRaCog framework. The algorithms investigated include maximum eigenvalue detection (MED), maximum-to-minimum eigenvalue (MME), energy-to-minimum eigenvalue (EME), and maximum-to-mean eigenvalue detection (MMED). Performance of these algorithms is analyzed in terms of detection capability and sensing time. Furthermore, these algorithms are compared with the conventional ED technique under different channel conditions, including the ideal AWGN channel, multipath fading channels with noise uncertainty, and a SIMO multi-antenna reception system.

2. Literature Survey

Many studies have focused on improving spectrum utilization and scalability in LoRa and LPWAN networks operating in dense IoT environments. The authors of [11] discussed the

limitations of LoRaWAN networks, particularly spectrum congestion and scalability challenges within industrial, scientific, and medical (ISM) bands. The study highlighted the need for more flexible and efficient spectrum management approaches. In this context, in [8], the LoRaCog framework is introduced, integrating CR capabilities into LoRa networks by assigning spectrum sensing tasks to gateway nodes. This framework enables the dynamic utilization of licensed channels while preserving the existing LoRa infrastructure. Furthermore, in [12], the integration of CR technologies with LPWAN systems is reviewed and the main challenges related to spectrum sensing reliability, interference management, and energy efficiency in IoT environments are discussed.

The authors of [13] reviewed several aspects of the ED algorithm in CR networks and noted that it remains one of the most commonly adopted sensing techniques due to its ease of implementation. However, previous studies have shown that the effectiveness of this technique deteriorates significantly under low SNR conditions and in the presence of noise uncertainty. These limitations lead to reduced detection reliability and to the SNR wall effect [13], [14].

To address these limitations, many studies have focused on developing spectrum-sensing algorithms based on the eigenvalues of the received signal's covariance matrix. Paper [10] established the theoretical foundation for these techniques by demonstrating that the presence of a PU signal changes the eigenvalue distribution of the covariance matrix of the received signal. This property enables signal detection without requiring prior knowledge of the signal structure or noise power. Subsequently, several studies attempted to improve the reliability of eigenvalue-based sensing algorithms under different wireless channel conditions. For example, in [15], the development of eigenvalue-based sensing techniques is reviewed and the article reports that these methods provide greater reliability than conventional sensing approaches, particularly under noise uncertainty conditions.

More recent studies have further demonstrated the effectiveness of eigenvalue-based techniques in fading environments, where improved detection performance can be achieved at low SNR levels compared to conventional ED methods [16].

Recent works focus mainly on developing individual sensing algorithms or integrating spectrum sensing techniques with machine learning in conventional wireless communication environments. The number of studies covering multiple eigenvalue-based sensing algorithms in cognitive LoRa networks under realistic wireless channel conditions remains relatively limited.

3. Overview of the LoRa Cognitive Framework

This section provides an overview of the LoRa cognitive framework (LoRaCog) introduced in [8] – a solution integrating CR concepts into LoRa networks and enabling gateways to perform sensing to improve spectrum efficiency. The LoRaCog framework extends the traditional LoRaWAN architecture by enabling gateways to access licensed channels when they are temporarily unused by PUs. This extension aims to improve spectrum efficiency and mitigate spectrum congestion.

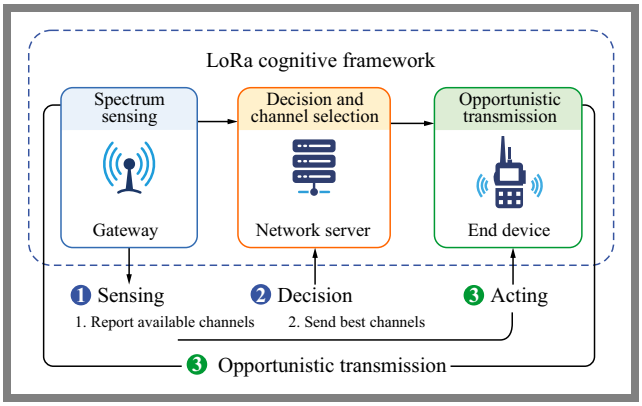

Fig. 1. Operational workflow of the LoRaCog framework.

The framework maintains the LoRaWAN network infrastructure, consisting of end devices (EDs), gateways (GWs) and the (NS). However, cognitive functions are integrated into this architecture by assigning spectrum sensing and decision-making tasks to specific components within the network, such as gateways, in order to optimize spectrum usage and improve overall network performance.

As shown in Fig. 1, the LoRaCog principle comprises three stages. First, spectrum sensing is performed at the gateway level, where the gateways monitor licensed channels and collect signal samples to detect the presence of a PU. Due to the availability of a stable power source, elevated deployment sites, and higher processing capabilities, gateways are suitable for implementing sensing algorithms. Then, the sensing results are sent to the NS, where the decision is made. Based on sensing reports from one or more gateways, the NS selects the channel, determines whether it is available for opportunistic access, and chooses the most suitable channel for transmission. Finally, the terminal devices that operate as SUs and benefit from gateway sensing transmit data based on NS information. These devices do not participate in the spectrum-sensing process due to their limited computational capabilities and strict energy consumption constraints. Instead, they rely entirely on the decisions before the uplink transmission begins.

4. System Model

At the beginning of the sensing process, a specific number of baseband samples of the received signal is collected. Let $x(n)$ represent the received sample in discrete time. The spectral sensing task can be formulated as a binary hypothesis test to determine whether the PU signal is present or absent in the observed frequency range [5].

$$H_0 : x(n) = n(n) \,, \tag{1}$$

$$H_1 : x(n) = s(n) + n(n) \,, \tag{2}$$

where $s(n)$ denotes the PU signal and $n(n)$ represents the additive noise component.

Noise is typically modelled as additive white Gaussian noise (AWGN) with zero mean and variance σ^2:

$$n(n) \sim CN\left(0, \sigma^2\right) . \tag{3}$$

In real wireless environments, the exact noise power may deviate from its nominal value due to hardware imperfections and environmental variations. This phenomenon is commonly referred to as noise uncertainty, which can be modeled as [2]:

$$\sigma_{eff}^2 = \sigma^2\left(1+\delta\right) , \tag{4}$$

where δ represents the uncertainty factor.

Because wireless channels often experience multipath fading, the received signal may contain several delayed replicas of the transmitted signal. The received signal can therefore be expressed in the following form:

$$x(n) = \sum_{k=0}^{L_h-1} h(k)\, s(n-k) + \eta(n) , \tag{5}$$

where $h(k)$ denotes the channel coefficient of the k-th propagation path and L_h represents the number of channel taps.

When multiple observation branches are considered, the received samples can be arranged in a vector form as follows.

$$x(n) = \left[x_1(n), x_2(n), \ldots, x_M(n)\right]^T . \tag{6}$$

To use the statistical properties of the received signal, the sample covariance matrix is estimated from the received samples:

$$R_x = \frac{1}{N}\sum_{n=1}^{N} x(n)\, x^H(n) . \tag{7}$$

Under the signal-present hypothesis, the covariance matrix can be expressed as:

$$R_x = R_s + \sigma^2 I , \tag{8}$$

where R_s denotes the covariance matrix of the signal component and I is the identity matrix.

The presence of the signal modifies the eigenvalue distribution of the covariance matrix, which forms the fundamental principle exploited by eigenvalue-based spectrum sensing algorithms [10].

5. Spectrum Sensing Algorithms

In this section, a summary of algorithms based on the eigenvalues of the covariance matrix is presented. The methods studied include maximum eigenvalue detection (MED), maximum–minimum eigenvalue detection (MME), energy with minimum eigenvalue (EME) and maximum-to-mean eigenvalue detection (MMED).

In the MED detector, the largest eigenvalue of the covariance matrix is used as the test statistic. Let the ordered eigenvalues of the covariance matrix be as follows:

$$\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_M . \tag{9}$$

The MED test statistic is defined as:

$$T_{\mathrm{MED}} = \lambda_1 . \tag{10}$$

The MED algorithm is among the simplest eigenvalue-based algorithms. It only requires calculating the largest eigenvalue and since it relies on a single eigenvalue, it is more prone to deterioration in its detection capability, especially at the SNR level [9].

The MME detector uses the ratio between the largest and smallest eigenvalues of the covariance matrix:

$$T_{\mathrm{MME}} = \frac{\lambda_1}{\lambda_M} . \tag{11}$$

Estimating multiple eigenvalues increases computational complexity and sensing time compared to simpler detectors [15].

The EME detector combines energy detection with eigenvalue normalization. The received signal energy is first computed as:

$$E = \frac{1}{N}\sum_{n=1}^{N} \left|x(n)\right|^2 . \tag{12}$$

The test statistic is then defined as:

$$T_{\mathrm{EME}} = \frac{E}{\lambda_M} . \tag{13}$$

Normalization improves the detector's robustness against noise uncertainties compared to conventional ED methods. However, the requirement of calculating eigenvalues increases the computational cost [15].

The MMED evaluates the ratio of the largest eigenvalue to the average eigenvalue of the sample covariance matrix. The test statistic is defined as:

$$T_{MMED} = \frac{\lambda_{max}}{\frac{1}{M}\sum\limits_{i=1}^{M}\lambda_i} , \tag{14}$$

where $\lambda_{\max}$ denotes the largest eigenvalue and λ_i represents the eigenvalues of the covariance matrix.

Under the noise-only hypothesis, the eigenvalues tend to be close to each other, whereas the presence of a signal increases the dominant eigenvalue relative to the average eigenvalue. Similar to other detectors based on eigenvalues, this method requires covariance matrix estimation followed by eigenvalue decomposition [15].

5.1. Complexity Analysis of Spectrum Sensing Algorithms

The computational complexity of the spectrum sensing algorithms depends mainly on the operations required for signal processing and statistical analysis. ED requires only energy computation on the received signal samples, resulting in a relatively low computational complexity of $O(N)$, where N represents the number of received samples [13]. In contrast, eigenvalue-based sensing algorithms require covariance matrix estimation followed by eigenvalue decomposition. Since the decomposition of an $M \times M$ covariance matrix typically requires $O(M^3)$ operations, the computational cost of MED, MME, EME, and MMED is mainly dominated by this process [10].

However, these algorithms provide improved sensing reliability under low SNR and noise uncertainty conditions, representing a trade-off between computational complexity and sensing performance [15].

6. Eigenvalue-based Spectrum Sensing

Three scenarios of variable difficulty were adopted to test the efficiency of eigenvalue-based spectral sensing algorithms. The first scenario assumes an ideal AWGN channel and a SISO wireless communication system. The second scenario considers multipath fading and noise power uncertainty while maintaining a SISO system, while the third scenario is a modification of the second one, using a SIMO wireless communication system to improve detection reliability and benefit from spatial diversity.

A numerical simulation framework based on the LoRaCog architecture was used, in which spectral sensing is performed at the gateway level rather than at the terminal nodes, according to the centralized architecture, thereby reducing power consumption in low power IoT devices. The gateway collects baseband signal samples from the surrounding wireless environment during each sensing period. After receiving the signal and completing the sample collection, the covariance matrix of the received signal is developed. This matrix represents the fundamental statistical structure on which the eigenvalue-based sensing algorithms are based.

Subsequently, eigenvalue analysis was performed, where the resulting values were arranged in descending order. Spectral sensing algorithms rely on these values to extract the statistical properties. When there is a signal from the PU, the largest eigenvalue increases significantly, while the remaining eigenvalues often reflect background noise due to statistical correlations induced by the organized signal across the received samples.

The traditional ED statistic in the system model is also computed and serves as a primary reference for comparison with eigenvalue-based algorithms.

In the next part, the detection threshold was determined to ensure the accuracy of the spectral sensing process. In this study, the threshold was not calculated from a theoretical distribution, but was estimated numerically from the empirical distribution of the test statistic under the null hypothesis of noise only. Noise samples were generated, and the test statistic was calculated for each algorithm. Then, the detection threshold was chosen based on the desired false alarm probability.

The threshold was derived using the inverse cumulative distribution function of the test statistic under the noise-only hypothesis, and it can be expressed as follows:

$$\gamma = F_T^{-1}\left(1 - P_f\right), \tag{15}$$

where F_T^{-1} refers to the inverse cumulative distribution function of the test statistic, and P_f represents the desired false alarm probability.

Tab. 1. Simulation parameters.

Parameter	Symbol	Value
Number of samples	N	1024
SNR range	SNR	$(-20:1:5)$ dB
Noise variance	σ^2	1
Noise uncertainty factor	δ	0.2
Covariance matrix size	M	50
Multipath channel taps	L_h	3 (SISO), 4 (SIMO)
Monte Carlo realizations	MC	1000
ROC realizations	MCROC	3000
Sampling frequency	F_s	1 MHz
Signal bandwidth	B	200 kHz

After determining the threshold, the process of testing the algorithms began under the assumption of the presence of both signal and noise at different SNR values to simulate the PU signal in the wireless channel. The detection probability was then calculated by comparing the test statistic with the corresponding threshold.

Performance evaluation relied on two types of analysis. The first focuses on studying the detection probability as the SNR varies to evaluate the performance under low SNR conditions, while the second uses receiver operating characteristic (ROC) curves to show the relationship between detection and false alarm probabilities at different threshold values.

In addition to evaluating the performance of the sensing algorithms, the execution time of each algorithm was measured. In the LoRaCog framework, since spectral detection is performed at the gateway level, processing time directly affects the detection delay of the system. Therefore, the average execution time extracted from the simulation reflects the computational complexity.

7. Simulation Results

The simulation environment was implemented using Matlab and, in all scenarios, the number of samples received was fixed at $N = 1024$, while the covariance matrix size was set to $M = 50$.

The simulation generated baseband signals and then passed them through a low-pass FIR filter with a sampling frequency of $F_s = 1$ MHz and a bandwidth of $B = 200$ kHz. This configuration was adopted to simulate narrowband wireless signals commonly used in low-power IoT applications. The performance of the sensing algorithms was evaluated in an SNR range of –20 dB to 5 dB with a step size of 1 dB. In multipath environments, the wireless channel was modeled with $L_h = 3$ propagation paths for the SISO system and $L_h = 4$ for the SIMO system. The SIMO scenario used $N_r = 3$ receiving antennas. The effect of noise uncertainty was incorporated using a noise uncertainty factor of $\delta = 0.2$.

The detection thresholds were numerically estimated using the empirical cumulative distribution function under the noise-only hypothesis with a target false alarm probability of $P_f = 0.1$. Monte Carlo simulation with 1000 iterations was used

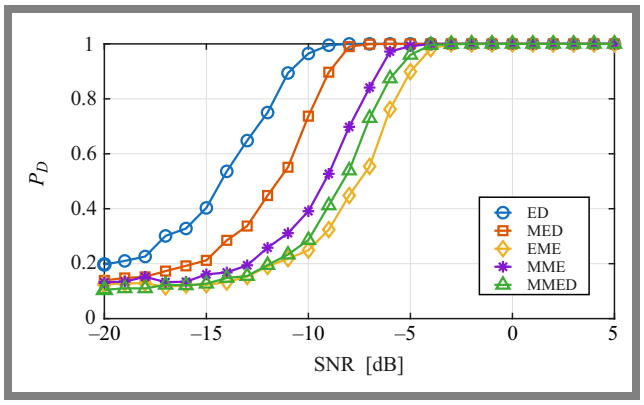

Fig. 2. Probability of detection versus SNR for spectrum detection algorithms under AWGN channel conditions.

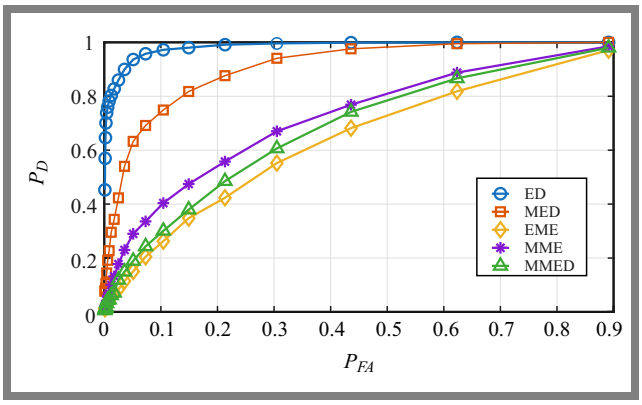

Fig. 3. ROC curves of P_D versus P_{FA} under AWGN channel conditions.

to analyze the probability of detection, while 3000 iterations were employed for ROC curve analysis.

Table 1 summarizes the simulation parameters used in this study.

The first scenario represents the ideal reference case, in which the received signal is affected only by AWGN with accurate knowledge of the noise power while employing the SISO receiver system. Figure 2 illustrates the relationship between the probability of detection of P_D and SNR, demonstrating the performance of the investigated spectrum detection algorithms under ideal channel conditions.

As the SNR increases, all evaluated algorithms exhibit gradual improvements in detection performance. However, the rate of improvement differs among the sensing techniques. The results indicate that ED achieves the highest sensing performance across most SNR ranges.

For instance, at SNR = –12 dB, ED achieves a detection probability of $P_D \approx 0.75$, whereas MED achieves 0.42. In contrast, the remaining eigenvalue-based techniques achieve detection probabilities below 0.20.

AWGN conditions with accurate noise power estimation, the statistical distinction between signal and noise becomes more evident, making the received signal energy a reliable indicator for signal detection and thereby improving sensing performance. Although MED performs worse than ED under AWGN conditions, its detection capability is influenced by the dominant eigenvalue of the covariance matrix, which becomes more pronounced in the presence of signal components.

At higher SNR levels, the performance gap between the evaluated techniques gradually decreases. At approximately SNR= –6 dB, all algorithms approach near-ideal sensing performance, where the probability of detection P_D approaches unity. This occurs because signal energy significantly exceeds the background noise energy, making signal detection easier regardless of the sensing technique employed.

To further analyze the sensing behavior under low SNR conditions, ROC curves were analyzed at SNR= –10 dB (Fig. 3).

The results obtained indicate that ED achieves superior sensing performance compared to eigenvalue-based techniques. At a false alarm probability of $P_{FA} = 0.05$, ED achieves

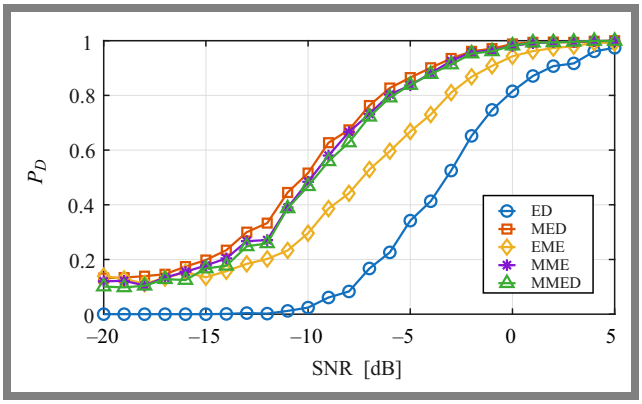

Fig. 4. Probability of detection versus SNR with multipath fading with uncertainty of noise.

$P_D \approx 0.92$, while MED and MME achieve 0.54 and 0.25, respectively. These observations further confirm the robustness of ED under ideal channel conditions and demonstrate its ability to achieve high detection performance while maintaining a low false alarm rate.

In the second scenario, more realistic operating conditions were considered by incorporating multipath fading effects and noise uncertainty while employing a SISO receiver system. Figure 4 illustrates the relationship between SNR and the probability of detection under these operating conditions.

The results show a noticeable degradation in the performance of the conventional ED technique. For example, at SNR = –10 dB, the detection probability decreases to $P_D \approx 0.021$, indicating a reduction in the sensing capability. This behavior can be attributed to the strong dependence of ED on accurate noise power estimation, where fluctuations in noise power increase the similarity between the two detection hypotheses, making the distinction between signal presence and signal absence more difficult.

At SNR = –10 dB, the obtained detection probabilities are: $P_D = 0.50$ (MED), $P_D = 0.4565$ (MME), $P_D = 0.4707$ (MMED) and $P_D = 0.2742$ (EME).

The eigenvalue-based sensing techniques maintain higher detection reliability under realistic channel conditions. MED benefits from the presence of dominant eigenvalues associated with signal components, whereas MME and MMED exploit eigenvalue ratios to enhance the separation between signal and

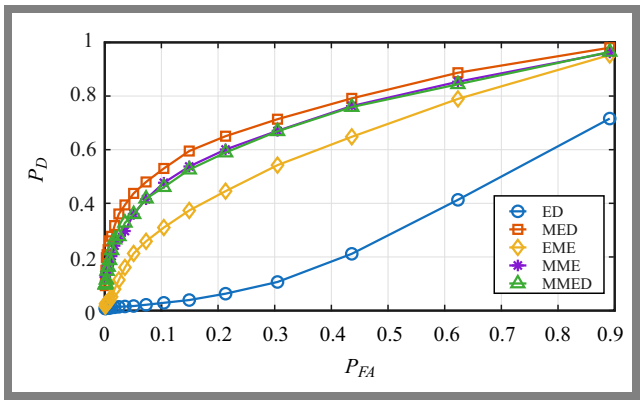

Fig. 5. ROC curves of P_D versus P_{FA} under multipath fading with noise uncertainty.

noise subspaces. EME also benefits from signal normalization using eigenvalues. However, its performance remains lower than that of the other techniques because of its sensitivity to variations associated with the minimum eigenvalue. The ROC curves for this case are presented in Fig. 5.

The ROC results further illustrate the behavior of the investigated sensing techniques under multipath fading and noise uncertainty conditions. At a false alarm probability of $P_{FA} = 0.1$, MED achieves a detection probability of $P_D \approx 0.68$, whereas ED remains below 0.05. The ROC curves of the eigenvalue-based techniques exhibit a steeper increase than those of ED, indicating a higher sensitivity to the presence of the primary user signal under realistic operating conditions. These observations indicate that eigenvalue-based sensing techniques preserve more reliable detection performance under realistic channel conditions and are less sensitive to noise power fluctuations than direct energy measurements.

The third scenario extends the previous environment by introducing spatial diversity through a SIMO receiver system with $N_r = 3$ receiving antennas while maintaining the same multipath fading conditions and noise uncertainty. Figure 6 illustrates the relationship between the probability of P_D detection and SNR for the sensing techniques investigated under spatial diversity conditions.

The results obtained indicate that all sensing techniques improve the detection performance compared to the previous SISO scenario. However, the improvement is more pronounced for eigenvalue-based sensing techniques. At SNR = –10 dB, the $P_D = 0.8045$ (MME), $P_D = 0.7813$ (MMED), $P_D = 0.6802$ (MED), and $P_D = 0.4972$ (EME).

In contrast, ED exhibits substantially lower performance under the same operating conditions, as spatial diversity provides a significant improvement in sensing reliability, particularly for eigenvalue-based sensing techniques. MED benefits from stronger dominant eigenvalues generated by multiple received observations, whereas MME and MMED use eigenvalue ratios more effectively as a result of the increased separation between signal and noise subspaces.

EME also benefits from the additional signal information provided by multiple antenna branches. However, its performance remains lower because of its sensitivity to variations associated with the minimum eigenvalue.

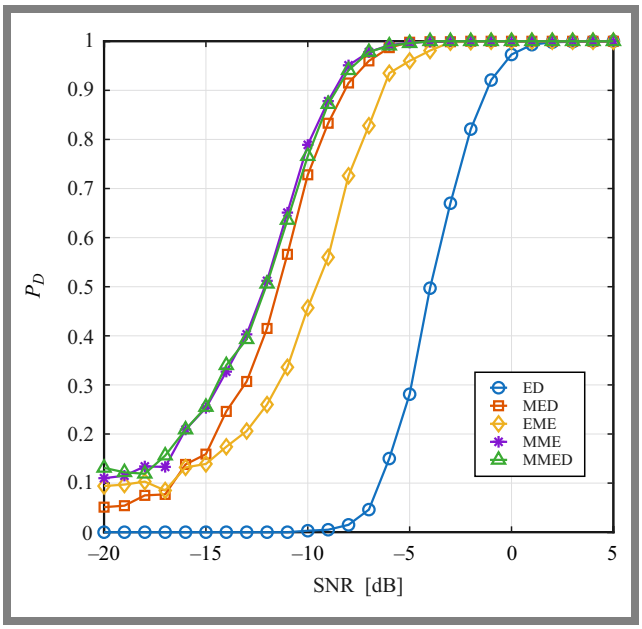

Fig. 6. Probability of detection versus SNR under the SIMO receiver system with multipath fading and noise uncertainty.

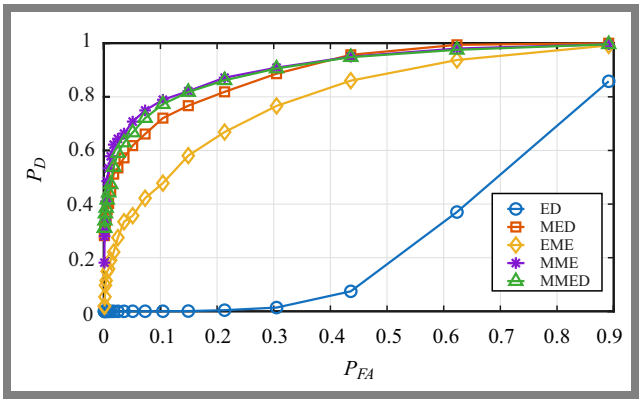

Fig. 7. ROC curves (P_D versus P_{FA}) under the SIMO receiver system with multipath fading and noise uncertainty.

The ROC curves obtained under SIMO operating conditions at SNR = –10 dB are presented in Fig. 7.

One may notice the superiority of MME under SIMO operating conditions. At a false alarm probability of $P_{FA} = 0.1$, both MME and MMED achieve detection probabilities exceeding 0.75, while MED achieves approximately 0.68. Furthermore, the ROC curves of MME and MMED exhibit steeper growth characteristics than those of the other techniques, showing a better sensitivity to the presence of the PU signal. These observations further confirm that spatial diversity improves the statistical separation between signal and noise components, thus enhancing sensing reliability.

The sensing time of the investigated spectrum-sensing techniques was also evaluated to analyze their computational requirements. The reported sensing time represents the total duration of the process, including both the observation interval required to collect the received samples and the time required to calculate the detection statistic.

The energy detection technique achieved the lowest sensing time of 1.084 ms. This low-sensing delay is primarily attributed to its simple implementation, as it relies only on direct energy calculations without additional processing. In contrast, eigenvalue-based sensing techniques require covariance matrix estimation and eigenvalue decomposition, resulting in higher computational costs and longer sensing times.

The average detection time of the eigenvalue-based techniques was 2.655 ms. EME, MME, and MMED exhibit similar sensing times, since they share the same fundamental computational stages which constitute the dominant computational burden in eigenvalue-based sensing techniques.

Although eigenvalue-based techniques require higher computational cost, the improved sensing reliability achieved under low SNR and realistic channel conditions may justify the additional processing overhead. Since spectrum sensing in the LoRaCog architecture is performed at gateway nodes rather than at resource-constrained end devices, the additional computational burden of eigenvalue-based sensing techniques is more manageable.

The improved sensing reliability observed under low SNR and noise uncertainty conditions may help reduce channel access failures and improve spectrum utilization in dense IoT environments. However, practical implementation of SIMO-based sensing approaches may require additional RF chains, multiple antenna elements, and increased processing capabilities at the gateway level, resulting in higher hardware cost, energy consumption, and implementation complexity.

8. Conclusions

In this study, four eigenvalue-based spectrum sensing algorithms were analyzed within the LoRa cognitive framework to evaluate their performance using the conventional ED algorithm as a reference in different operating environments and to assess their suitability.

The results indicate that the ED algorithm achieves the best sensing performance under ideal AWGN channel conditions and exhibits the shortest sensing time. However, ED performance deteriorates significantly in the presence of noise uncertainty and multipath propagation effects. On the contrary, a noticeable improvement in performance was observed under the same conditions when eigenvalue-based algorithms were employed. These algorithms demonstrated higher reliability in non-ideal wireless environments because they rely on the statistical properties of the received signal rather than on accurate knowledge of the noise power.

In the final scenario, where spatial diversity was simulated through signal reception using multiple antennas, the MME detector outperformed the other algorithms investigated in terms of detection probability. These findings demonstrate the effectiveness of using the eigenvalue distribution of the covariance matrix when multiple signal observation branches are available.

Regarding computational sensing time, although eigenvalue-based algorithms require a relatively high computational effort due to covariance matrix construction and eigenvalue analysis, the required sensing time remains within approximately 1 to 3 ms, which is considered acceptable for gateway level sensing operations within the system.

References

[1] F. Hu, B. Chen, and K. Zhu, "Full Spectrum Sharing in Cognitive Radio Networks Toward 5G: A Survey", *IEEE Access*, vol. 6, pp. 15754–15776, 2018 (https://doi.org/10.1109/ACCESS.2018.2802450).

[2] Y. Arjoune and N. Kaabouch, "A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions", *Sensors*, vol. 19, art. no. 126, 2019 (https://doi.org/10.3390/s19010126).

[3] M.U. Muzaffar and R. Sharqi, "A Review of Spectrum Sensing in Modern Cognitive Radio Networks", *Telecommunication Systems*, vol. 85, pp. 347–363, 2024 (https://doi.org/10.1007/s11235-023-01079-1).

[4] A. Nasser *et al.*, "Spectrum Sensing for Cognitive Radio: Recent Advances and Future Challenge", *Sensors*, vol. 21, art. no. 2408, 2021 (https://doi.org/10.3390/s21072408).

[5] T. Yucek and H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications", *IEEE Communications Surveys & Tutorials*, vol. 11, pp. 116–130, 2009 (https://doi.org/10.1109/SURV.2009.090109).

[6] Z.K. Farej and A.Y. Adel, "Review on LoRa Communication Technology, Its Issues, Challenges and Applications in Healthcare System", *European Journal of Computer Science and Information Technology*, vol. 12, pp. 1–17, 2024 (https://doi.org/10.37745/ejcsit.2013/vol12n8117).

[7] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range Communications in Unlicensed Bands: The Rising Stars in the IoT and Smart City Scenarios", *IEEE Wireless Communications*, vol. 23, pp. 60–67, 2016 (https://doi.org/10.1109/MWC.2016.7721743).

[8] F. Salika *et al.*, "LoRaCog: A Protocol for Cognitive Radio-based LoRa Network", *Sensors*, vol. 22, art. no. 3885, 2022 (https://doi.org/10.3390/s22103885).

[9] M.K. Giri and S. Majumder, "Eigenvalue-based Cooperative Spectrum Sensing Using Kernel Fuzzy C-means Clustering", *Digital Signal Processing*, vol. 111, art. no. 102996, 2021 (https://doi.org/10.1016/j.dsp.2021.102996).

[10] Y. Zeng and Y.C. Liang, "Eigenvalue-based Spectrum Sensing Algorithms for Cognitive Radio", *IEEE Transactions on Communications*, vol. 57, pp. 1784–1793, 2009 (https://doi.org/10.1109/TCOMM.2009.06.070402).

[11] M. Bor, U. Roedig, T. Voigt, and J.M. Alonso, "Do LoRa Low-power Wide-area Networks Scale?", *Proc. of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*, pp. 59–67, 2016 (https://doi.org/10.1145/2988287.2989163).

[12] A.J. Onumanyi, A.M. Abu-Mahfouz, and G.P. Hancke, "Cognitive Radio in Low Power Wide Area Network for IoT Applications: Recent Approaches, Benefits and Challenges", *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 7489–7498, 2020 (https://doi.org/10.1109/TII.2019.2956507).

[13] K. Arshid *et al.*, "Energy Detection Based Spectrum Sensing Strategy for CRN", *2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS)*, Dalian, China, 2020 (https://doi.org/10.1109/ICAIIS49357.2020.9752316).

[14] A.S.S. Musuvathi *et al.*, "Efficient Improvement of Energy Detection Technique in Cognitive Radio Networks Using K-nearest Neighbour (KNN) Algorithm", *EURASIP Journal on Wireless Communications and Networking*, vol. 2024, art. no. 10, 2024 (https://doi.org/10.1186/s13638-024-02338-8).

[15] K.P. Patil, A.S. Lande, and M.H. Naikwadi, "A Review on the Evolution of Eigenvalue Based Spectrum Sensing Algorithms for Cognitive Radio", *Network Protocols and Algorithms*, vol. 8, pp. 58–77, 2016 (https://doi.org/10.5296/npa.v8i2.9349).

[16] S. Samala, S. Mishra, and S.S. Singh, "Machine Learning and an Eigenvalue-based Technique to Improve Cooperative Spectrum Sensing in Generalized α-$\varkappa$-μ Fading Channel", *Journal of Communications*, vol. 19, pp. 222–228, 2024 (https://doi.org/10.12720/jcm.19.5.222-228).

Batool Jaafar Bashar, Master's Student
Department of Information and Communication Engineering
https://orcid.org/0009-0004-5529-6467
E-mail: batool.jafar.ie25@nahrainuniv.edu.iq
Al-Nahrain University, Baghdad, Iraq
https://nahrainuniv.edu.iq/en

Hikmat Abdullah, Professor
Department of Information and Communication Engineering
https://orcid.org/0000-0002-1133-2057
E-mail: hikmat.abdullah@nahrainuniv.edu.iq
Al-Nahrain University, Baghdad, Iraq
https://nahrainuniv.edu.iq/en

Federated Learning for Low-rate DDoS Detection in Multi-controller Software Defined Networks: A Meta Analysis

Rikie Kartadie[1,2], Eko Marpanaji[1], and Agus Maman Abadi[1]

[1]*Universitas Negeri Yogyakarta, Indonesia,*
[2]*Universitas Teknologi Digital Indonesia, Yogyakarta, Indonesia*

https://doi.org/10.26636/jtit.2026.2.2552

Abstract — Multi-controller SDN environments suffer from a blind spot when it comes to detecting low-rate DDoS attacks. Each controller sees only its own traffic slice, meaning that an LDDoS campaign looking, at every controller, like background noise is still capable of draining the network. Federated learning (FL) is a reasonable answer to this challenge, due to such controllers sharing model updates rather than raw logs. However, the published literature on FL-based detection is fragmented enough that the results have not been systematically compared up to date. We analyze 39 papers published between 2020 and 2026. 35 of those reported quantitative results, with the pooled mean detection precision equaling 98.25% (SD ±0.91) and the mean F1 score amounting to 97.98% (SD ±1.10). Federated models averaged an accuracy score of 98.33%, compared to 98.06% for centralized approaches – a 0.27 pp gap that is practically negligible. LSTM and hybrid CNN + RNN architectures ranked the highest in terms of the most metrics. Four aggregation strategies were mentioned repeatedly: weighted aggregation, asynchronous FL, personalized FL, and standard FedAvg. The widest gap we identified was in the datasets. No available benchmark simultaneously models multi-controller SDN topology, low-rate attack patterns, and heterogeneous traffic distributions across various controllers. Until that changes, high-accuracy scores on CICIDS2017 or CICDDoS2019 should be interpreted with some caution.

Keywords — federated learning, intrusion detection systems, low-rate distributed denial-of-service, SDN security, software-defined networking

1. Introduction

Software-defined networking (SDN) has changed the way in which large-scale networks are managed. By separating the control plane from the data plane, SDN allows operators to configure routing, security policies, and traffic engineering from a central point, rather than by adopting the device-by-device approach. In cloud and IoT deployments, this matters greatly, as networks are too large and too dynamic for per-device management to be deployed at scale.

Many production SDN deployments now run multiple controllers rather than one instance only, thus distributing the control workload geographically and improving fault tolerance. However, such a design choice creates a security problem that has received less attention than it actually deserves [1], [2].

Low-rate distributed denial of service attacks (LDDoS) is the main problem here. A volumetric DDoS is easy to notice. As traffic volume spikes, the anomaly detectors are triggered. LDDoS works in the opposite manner. It sends short, periodic bursts timed to match TCP retransmission timeouts, gradually draining the target's capacity to serve legitimate requests.

No obvious spikes are identified. In a multi-controller SDN environment, the situation is even worse, as each controller observes only the traffic in its own domain. An LDDoS attack targeting the entire network may appear as a hardly noticeable background fluctuation for any single controller [3]–[5].

Federated learning (FL) addresses part of this problem. Controllers can train local detection models and share only model parameters, not raw traffic logs. This preserves privacy in administrative domains and makes collaborative detection feasible without centralizing sensitive network data [6], [7]. The catch is that the amount of literature on FL-based intrusion detection has been growing faster than the community's ability to compare the results of specific studies. Different articles use different architectures, aggregation protocols, and various datasets. Nobody has pooled the numbers.

This paper does that. We reviewed 39 studies published between 2020 and 2026, extracted performance metrics from the 35 that reported quantitative results, and calculated pooled statistics across architecture groups and learning paradigms. Four questions define the scope of the analysis.

1) Which deep learning architectures produce the highest pooled detection performance for LDDoS in federated SDN environments?
2) How do FL aggregation strategies handle data heterogeneity when traffic distributions differ between controllers?
3) What does the quantitative performance gap between federated and centralized detection actually look like?
4) Do the benchmark datasets used in this literature adequately represent LDDoS conditions in multi-controller SDN deployments?

Tab. 1. PRISMA-aligned study selection process.

Stage	Records, N	Decision criteria
Initial identification (keyword search)	187	Terms: federated learning, SDN, DDoS, intrusion detection, LDDoS
After duplicate removal	141	Cross database deduplication (IEEE Xplore, ACM DL, Springer, Scopus)
After title/abstract screening	73	Excluded: unrelated to FL or SDN security ($n = 68$)
After full-text eligibility assessment	39	Excluded: no quantitative results, purely theoretical, non-SDN environment ($n = 34$)
Included in meta-analysis	39	Satisfied all inclusion criteria; 35 empirical + 4 survey/review

Note: Record counts reflect the complete screening process from initial identification to final inclusion.

1.1. Research Design

This study uses a systematic meta-analysis research design following evidence synthesis procedures adapted from preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines, commonly adopted in computer science research [8]. The methodology combines systematic literature identification with quantitative cross-study synthesis, producing pooled descriptive statistics, group-level comparisons, and dataset coverage analysis.

Four databases were searched: IEEE Xplore, ACM Digital Library, Springer, and Scopus. The searches targeted titles, abstracts, and author provided keywords, and were limited to publications from January 2020 to March 2026. The following Boolean string was applied consistently across all databases:

```
("federated learning" OR "federated deep learning"
OR "FL") AND ("software-defined network*" OR
"SDN") AND ("intrusion detection" OR "IDS" OR
"attack detection") AND ("DDoS" OR "LDDoS" OR
"low-rate DDoS" OR "low-rate distributed denial of
service").
```

The wildcard operator (*) was used where a given database supported it in order to capture morphological variants such as networks and networking. Table 1 shows how the records were filtered at each stage.

Studies were included if they proposed or evaluated an FL-based IDS, targeted DDoS or LDDoS detection in an SDN or SDN-enabled environment, reported quantitative experimental results, and provided enough methodological detail to extract the model architecture and aggregation mechanism. Papers that were purely theoretical, lacked experimental evaluation, or operated in non-SDN contexts were excluded.

The selection process comprised four steps:

1) First, we identified publications using keywords related to learning.
2) Then we removed duplicates.
3) Next, we checked the titles and abstracts.
4) Finally, we assessed the text for eligibility.

Table 1 shows how many records were left at each stage following the PRISMA guidelines. The framework diagram is presented in Fig. 1.

1.2. Data Extraction and Analytical Procedure

For each included study, we extracted seven categories of information: publication location and year, network environment (SDN, SDN-IoT, telecom), deep learning architecture, federated learning aggregation mechanism, data set used for evaluation, reported detection metrics (accuracy, precision, recall, F1 score) and, where available, system efficiency indicators such as model size or convergence time.

Accuracy values stated as percentages were converted to decimal form for consistency. Where a study did not report a metric, the value was recorded as "–" rather than estimated. No imputation was applied.

The analysis was carried out in three steps. First, we computed pooled descriptive statistics, mean, standard deviation, minimum, and maximum values across all 35 empirical studies for precision, recall, and F1 score. Second, we grouped the studies by architecture type and by learning paradigm (federated vs. centralized) to identify systematic performance differences. Third, we assessed how well the benchmark datasets used in these studies actually reflect LDDoS conditions in multi-controller SDN environments, using three criteria: presence of low-rate attack patterns, simulation of multi-controller topology, and heterogeneity of traffic across controllers.

Because the reviewed studies use different data sets and evaluation setups, the synthesis is of the descriptive nature. Statistical pooling across incompatible experimental designs would not be meaningful.

2. Results

2.1. Deep Learning Architectures for LDDoS Detection

Analysis of the 35 empirical studies reporting quantitative results produced the combined descriptive statistics shown in Tab. 2.

In all studies, the pooled mean detection precision was 98.25% (SD = ±0.91; range: 96.40 – 99.93%), the mean precision was 97.96% (SD = ±0.94%), the mean recall was 98.21% (SD = ±0.89%), and the mean F1 score was 97.98% (SD = ±1.10%; range: 94.21 – 99.96%).

Recurrent architectures, particularly LSTM and Bi-LSTM, are the most frequently adopted models appearing in approx-

Tab. 2. Pooled performance statistics for all empirical studies (N = 35).

Metric	No. of studies	Mean [%]	Std Dev [±]	Min [%]	Max [%]
Accuracy	35	98.25	0.91	96.40	99.93
Precision	35	97.96	0.94	96.00	99.96
Recall	35	98.21	0.89	96.70	99.97
F1 score	35	97.98	1.10	94.21	99.96

Note: Excludes 4 survey/review studies that did not report original quantitative results.

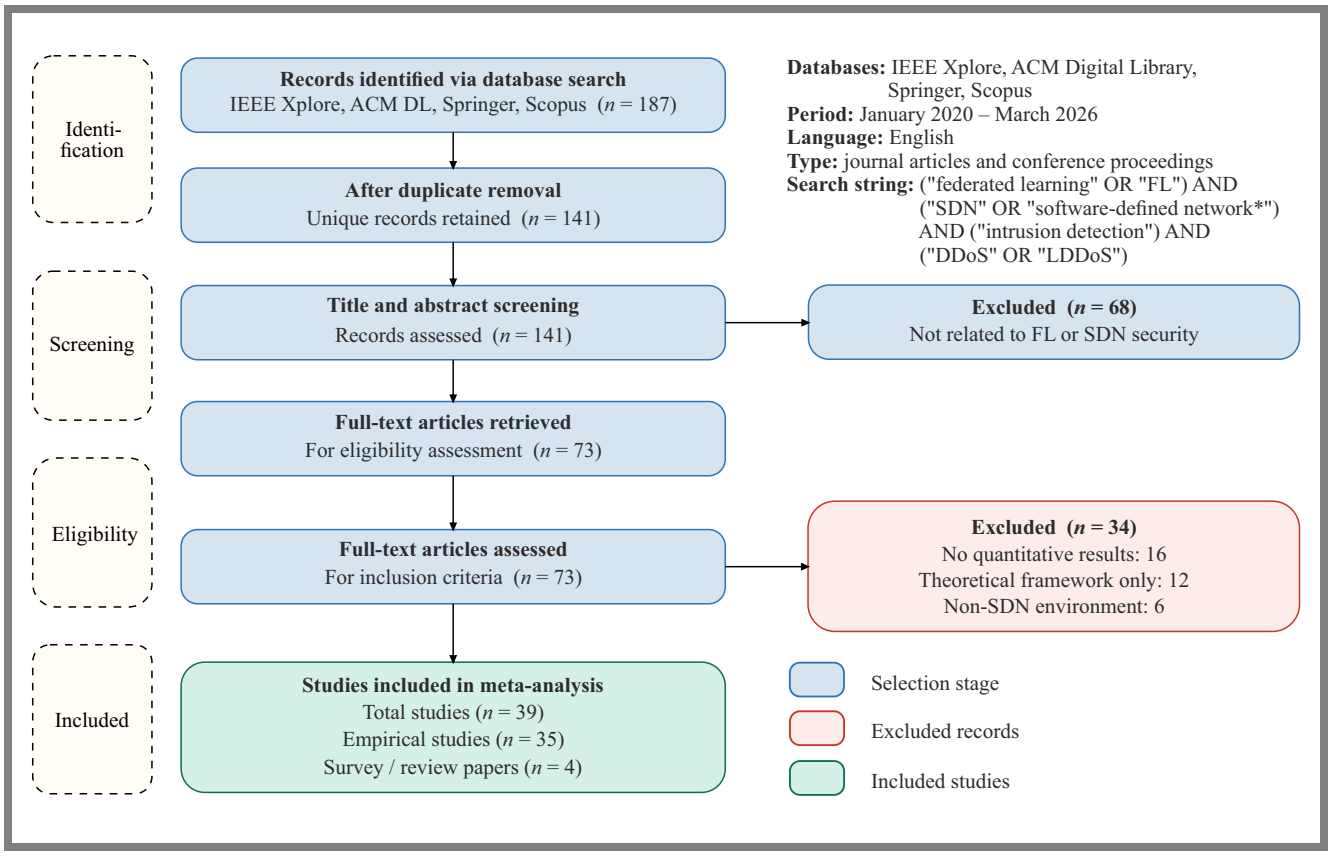

Fig. 1. Prisma framework diagram.

imately 20% of empirical studies (n = 7 of 35; see Tab. 3). This adoption pattern is consistent with the temporal nature of LDDoS attacks which exploit periodic traffic bursts rather than volumetric anomalies, requiring models capable of capturing sequential dependencies. Table 3 presents group-level performance comparisons disaggregated by architecture type.

The hybrid CNN + RRN architectures achieved the highest mean F1 score of 98.54% (±0.67; Tab. 3), followed by the LSTM / Bi-LSTM models at a mean F1 score of 97.89% (±1.55; Tab. 3). CNN-only architectures showed strong classification accuracy (mean: 99.23%) but a lower mean F1 score of 98.59%, which is consistent with prior findings according to which purely spatial models are less effective in detecting stealthy temporal attack patterns.

Graph neural network (GNN) architectures, represented by two studies, demonstrated a mean accuracy of 97.75% with a mean F1 of 97.70%, suggesting promising but early-stage applicability. Transformer-based architectures reported in [9] achieved accuracy of 99.50% and a 99.40% F1 score, indicating a strong potential to capture long-range temporal dependencies in LDDoS traffic.

2.2. Federated Learning Strategies for Handling Data Heterogeneity

The reviewed works report four primary federated learning strategies to mitigate heterogeneous traffic distributions across SDN controllers:

1) weighted aggregation,
2) asynchronous federated learning,
3) FL customized / entire FL,
4) standard FedAvg.

Weighted aggregation strategies, which dynamically adjust the contribution of model updates from individual controllers, are reported in approximately 31% of FL-based studies ($n \approx$ 9 studies). The authors of [10] demonstrated that an asynchronous FL framework (AsyncFL-bLAM) with Bi-LSTM and an attention mechanism achieved a mean F1 score on CAIDA LDDoS data, specifically addressing the synchronization delay problem in multi-controller SDNs. Work [11] showed that the adaptive FLAD framework converges significantly faster than the standard FedAvg, while achieving a 97.01% F1 score. Personalized strategies reported in [12] achieved a 98.82% F1 score on CICDoS2017 / CICDDoS2019 with asynchronous aggregation in a multi-controller SDN scenario.

2.3. Performance Trade-offs Between Federated and Centralized Detection

Table 4 presents a quantitative comparison between federated and centralized learning approaches described in the 35 studies that clearly specified their learning paradigm.

FL-based systems achieved a mean precision of 98.33% (SD = ±0.86) and a mean F1 score of 97.98% (SD = ±1.16), compared to 98.06% (SD = ±0.99) and 97.97% (SD = ±0.97) for centralized approaches. The 0.27% accuracy gap sug-

Tab. 3. Performance comparison by the deep learning architecture group.

Architecture group	No. of studies	Mean acc [±SD, %]	Min acc [%]	Mean F1 [±SD, %]	Min F1 [%]	Primary dataset
LSTM / Bi-LSTM	7	98.63 (±0.36)	97.8	97.89 (±1.55)	94.21	CAIDA, CICDDoS, Edge-IIoT
GRU / Bi-GRU	2	99.15 (±0.35)	98.8	98.55 (±0.85)	97.70	InSDN, CICDDoS2019
CNN (1D / 2D)	4	98.92 (±0.66)	97.8	98.76 (±0.62)	97.70	CICIDS2017, CICDDoS2019
Hybrid CNN+RNN	7	98.68 (±0.61)	98.1	98.54 (±0.67)	97.95	CICIDS2017, CICDDoS2019
Transformer-based	1	99.50 (±–)	99.5	99.40 (±–)	99.40	CICDDoS2019
Graph neural networks	2	97.75 (±0.15)	97.6	97.70 (±0.10)	97.60	CICIDS2017, InSDN
Other FL models	5	97.86 (±0.63)	96.8	97.61 (±0.59)	96.80	CAIDA, CICIDS2017

Note: Studies may appear in multiple architecture groups where hybrid models are employed. SD = standard deviation. "–" indicates a single study group (SD not computable).

Tab. 4. Quantitative comparison: federated learning versus centralized learning.

Approach	No. of studies	Mean acc [±SD,%]	Min acc [%]	Mean F1 [±SD,%]	Min F1 [%]
Federated learning	24	98.33 (±0.86)	96.8	97.98 (±1.16)	94.21
Centralized learning	11	98.06 (±0.99)	96.4	97.97 (±0.97)	96.4

Note: Studies classified as FL involve at least one FL aggregation mechanism across distributed clients. Centralized studies are trained on aggregated data sets without FL.

gests that FL achieves performance comparable to centralized training while preserving data privacy across SDN controller domains. However, federated approaches introduce additional communication overhead from model parameter exchange. The authors of [3] directly compared federated and centralized IDS in the InSDN dataset, reporting that the federated model (98.80% accuracy) closely approached centralized performance (99.10%), with a gap of only 0.30 percentage points.

2.4. How Well Do Benchmark Datasets Represent Real Life?

Table 5 shows the types of benchmark data sets that were used in the studies we analyzed. It also shows how well these datasets represent real-life LDDoS detection scenarios in multi-controller SDN environments.

Table 6 provides a structured overview of all 39 studies included in this meta-analysis. For each study, the table lists the first author, the deep learning architecture used, the federated learning aggregation strategy, the primary evaluation dataset, the best reported accuracy and the F1 score, the scope of the experimental study, and type of the study under consideration. This summary serves as primary evidence for the cross-study comparisons presented in Subsections 2.1 through 2.4. Studies classified as survey or review papers (type S) do not report original experimental results and are included for contextual reference only. Performance values marked "–" were not reported by the original study authors and were not estimated or imputed.

As shown in Tab. 6, the reviewed studies span a range of deep learning architectures, aggregation mechanisms, and evaluation datasets, reflecting the methodological diversity existing in the field. Most empirical studies ($n = 35$) report a precision level greater than 97%, with performance differences between architecture groups examined in detail in Subsection 2.1. Studies specifically addressing low-rate DDoS detection in multi-controller SDN environments (scope: LDDoS-SDN) represent a small but methodologically distinct subset, $n = 4 : [4, 12, 15, 36]$, a limitation discussed further in Subsection 2.4.

CICIDS2017 is the most used dataset (51.4% of empirical studies), followed by CICDDoS2019 (40.0%). However, both data sets were originally designed for centralized network monitoring and primarily contain volumetric DDoS variants. Only the CAIDA LDDoS dataset provides authentic low-rate attack traffic patterns, yet it is used in only 8.6% of reviewed studies and does not simulate the multi-controller SDN topology.

The InSDN dataset, used by 14.3% of studies, is the only benchmark that explicitly simulates the SDN topology, though it does not model multi-controller distributed visibility. These findings indicate that 93.7% of the reviewed studies employed

Tab. 5. Distribution of benchmark data sets and evaluation of LDDoS representativeness.

Dataset	Frequency N	Coverage [%]	LDDoS representation in SDN environment
CICIDS 2017	18	51.4	Partial – volumetric DDoS dominant; limited LDDoS patterns
CICDDoS 2019	14	40.0	Partial – multiclass DDoS; not SDN/controller-specific
InSDN	5	14.3	Moderate – SDN-specific topology; binary classification
Edge-IIoTset	4	11.4	Partial – IoT focus; no multi-controller simulation
CAIDA LDDoS	3	8.6	High – real LDDoS traffic; not multi-controller SDN
NSL-KDD	4	11.4	Low – general IDS dataset; no LDDoS or SDN specificity
Custom / other	6	17.1	Variable – domain-specific; limited reproducibility

Note: Percentage values are calculated over 35 empirical studies (studies may use multiple datasets, so the frequencies add up to > 35). LDDoS representativeness evaluated against three criteria: a) presence of low-rate attack patterns, b) multi-controller SDN topology simulation, and c) heterogeneous traffic distribution.

datasets that only partially represent the operational conditions of LDDoS detection in multi-controller SDN environments.

3. Discussion

3.1. Architecture Effectiveness

The spread of the F1 score, varying from 94.21% to 99.96% across 35 studies, is wider than the mean of 97.98% might suggest. That variance matters. It reflects real differences in how the studies were set up: which dataset and how many attack classes were considered, whether the task was binary or of the multiclass type. A single pooled mean is useful for broad comparisons of paradigms, but it may obscure cases where a particular architecture fails badly on stealthy traffic. Table 2 shows both the mean and the spread; both are worth becoming acquainted with.

The appearance of LSTM and Bi-LSTM models in 20% of empirical studies (n=7 of 35; Tab. 3) comes as no surprise. LDDoS attacks are fundamentally temporal events. They have the form of short bursts occurring at regular intervals and are designed to exploit TCP retransmission timeouts. CNN-based architectures capture spatial feature relationships well and achieve high accuracy on binary tasks, but their lower F1 scores on multiclass scenarios (Tab. 3) suggest that they can miss the periodicity that defines LDDoS. Recurrent models are built for that periodicity; it is what they were designed to capture.

The transformer result from [9] (99.40% F1) and the GNN result from [31] (97.60% F1) are both encouraging. Each of them originates from a single study. The numbers are real, but a single study cannot determine whether an architecture is generalized. Additional replication across datasets and SDN configurations is required before either approach receives a recommendation.

3.2. Federated vs. Centralized Performance

The 0.27 percentage point accuracy gap between federated (98.33%) and centralized (98.06%) approaches, as shown in Tab. 4, is small enough to be treated as noise in most deployment contexts. Federated learning does not sacrifice much detection performance in exchange for keeping traffic data local. This trade-off looks reasonable.

What it gives up is simplicity. Every aggregation round requires controllers to exchange model parameters with a central server. In large-scale deployments with many controllers and constrained inter-domain links, the communication cost compounds over training. None of the reviewed studies report actual bandwidth figures, making it hard to identify how significant this cost is in practice. This type of reporting should be standard in future work.

3.3. Dataset Representativeness Limitations

CICIDS2017 and CICDDoS2019 cover 51.4% and 40.0% of the evaluated studies, respectively (Tab. 5). Both of them were captured in centralized environments with volumetric attack traffic as the dominant threat class. A model trained on these datasets is essentially learning to separate high-volume attack flows from normal traffic. LDDoS attacks do not generate high-volume flows; this is the very point behind their use. A model tuned on CICIDS2017 may never see the kind of signal an LDDoS attack actually produces.

CAIDA LDDoS contains really low-rate attack traffic and is the most relevant data set in the corpus, but only 8.6% of studies used it and it does not simulate the distributed SDN topology. InSDN is the only benchmark with an SDN-specific capture environment, but it lacks multi-controller partitioning. Consequently, 93.7% of the reviewed studies were evaluated on data that do not match the deployment scenario their methods claim to address. The high accuracy figures in those studies should be interpreted accordingly.

3.4. Limitations and Threats to Validity

Publication bias is a real concern here. Studies finding that federated learning performed poorly or failing to converge are less likely to appear in indexed databases. As a result, the pooled accuracy figures shown in Tab. 2 probably lean towards the optimistic side.

Heterogeneity between studies is a deeper problem. The 35 empirical studies use different datasets, different attack mixes, different numbers of controllers, and different evaluation protocols. The pooling of their results gives a rough picture of the field, but cannot substitute for a controlled comparison. The synthesis should be read as a structured overview, not as experimental evidence.

Two narrower issues need to be taken into consideration as well: some metric values were not reported by the studies' authors and appear as "–" in Tab 6. Those gaps are real and affect coverage of certain architecture groups. The search also covered four databases (IEEE Xplore, ACM Digital Library, Springer, Scopus), making it thorough but not exhaustive. Relevant work in domain-specific venues may have been missed.

4. Conclusions

The central finding is straightforward: federated learning works for LDDoS detection in multi-controller SDN environments, and it does not sacrifice much accuracy in the process. Across 39 studies published between 2020 and 2026, federated models averaged an accuracy score of 98.33% versus 98.06% for centralized approaches. The observed gap of 0.27 percentage points is, for practical purposes, negligible.

As far as the architecture is concerned (question no. 1), LSTM-based and hybrid CNN+RNN models led the field on most metrics. Neither result is surprising. LDDoS traffic has temporal structure-periodic bursts, not volume spikes, and recurrent architectures are built to capture exactly that. Hybrid CNN+RNN models achieved the highest mean F1 score among groups with more than two studies (98.54%, ±0.67; Tab. 3). Transformer and GNN architectures showed

Tab. 6. Summary of all 39 reviewed studies: architecture, aggregation strategy, dataset, and reported performance.

Study	Architecture	Aggregation strategy	Dataset	Acc [%]	F1 [%]	Scope	Type
[1]	Hybrid CNN+LSTM	FedAvg	CICIDS2017	98.71	98.50	DDoS-SDN	E
[2]	GRU	FedAvg	CICIDS2018	98.30	97.90	DDoS-IoT	E
[3]	CNN+LSTM	FedAvg/Cent.	InSDN	98.80	98.70	DDoS-SDN	E
[4]	LSTM	FedAvg	Edge-IIoTset	98.50	97.80	LDDoS-SDN	E
[5]	CNN (2D)	FedAvg	CICIDS2017	99.23	98.59	DDoS-SDN	E
[6]	Survey	N/A	Multiple	–	–	IDS-general	S
[7]	Bi-LSTM	Centralized	NSL-KDD	98.90	98.60	IDS-general	E
[8]	Survey	N/A	Multiple	–	–	IDS-general	S
[9]	Transformer	FedAvg+CL	CICDDoS2019	99.50	99.40	DDoS-SDN	E
[10]	Bi-LSTM+Attn.	AsyncFL (bLAM)	CAIDA LDDoS	98.55	98.55	LDDoS-SDN	E
[11]	CNN (1D)	Adaptive FL (FLAD)	CAIDA LDDoS	97.10	97.01	DDoS-gen.	E
[12]	LSTM	Async FedAvg	CICDDoS2019	99.10	98.82	DDoS-SDN	E
[13]	Multi-model FL	Multi-model Agg.	CICIDS2017	98.00	97.95	DDoS-SDN	E
[14]	XGBoost+LSTM	Centralized	Custom	97.80	97.50	IDS-general	E
[15]	MLP	Weighted Agg. FL	Custom	97.10	97.00	DDoS-SDN	E
[16]	CNN+Attention	FedAvg	CICIDS2017	98.40	98.20	DDoS-IoT	E
[17]	Hybrid DL	Centralized	CICIDS2017	99.10	99.00	DDoS-SDN	E
[18]	Multi-agent DL	Adaptive FL	CICIDS2018	98.40	98.30	IDS-general	E
[19]	LSTM	FedAvg (robust)	N-BaIoT	97.60	97.40	DDoS-IoT	E
[20]	Hybrid CNN+RNN	Centralized	CICDDoS2019	99.20	99.10	DDoS-SDN	E
[21]	CNN (1D)	Centralized	NSL-KDD	98.50	98.30	DDoS-IoT	E
[22]	Survey	N/A	Multiple	–	–	IDS-general	S
[23]	CNN (1D)	Centralized	NSL-KDD	99.20	–	IDS-general	E
[24]	RNN	FedAvg	Custom (telecom)	96.80	96.70	DDoS-tel.	E
[25]	Survey	N/A	Multiple	–	–	IDS-general	S
[26]	CNN+RNN	Centralized	CICIDS2017	98.10	97.80	DDoS-gen.	E
[27]	Hybrid DL	Centralized	CICIDS2017	98.80	98.60	DDoS-SDN	E
[28]	GRU	FedAvg	CICDDoS2019	98.80	98.35	DDoS-SDN	E
[29]	CNN+LSTM	Adaptive FL	CICDDoS2019	98.20	98.00	DDoS-SDN	E
[30]	ML (SVM/RF)	Centralized	Custom (SDN)	96.10	–	LDDoS-SDN	E
[31]	GNN (GowFed)	FedAvg	CICIDS2017	97.60	97.60	DDoS-SDN	E
[32]	LSTM	FedAvg	CICDDoS2019	98.90	98.80	DDoS-SDN	E
[33]	ML (framework)	Centralized	Custom (SDN)	96.40	–	DDoS-SDN	E
[34]	CNN+LSTM (MFFLR)	Centralized	Custom (SDN)	97.40	97.20	LDDoS-SDN	E
[35]	G-Network	Decentralized FL	CICIDS2017	97.00	96.90	IDS-general	E
[36]	CNN+XAI	FedAvg + XAI	CICIDS2018	97.80	97.70	IDS-SDN	E
[37]	GNN (ensemble)	Multi-view FL	N-BaIoT	97.90	97.80	DDoS-IoT	E
[38]	Survey	N/A	Multiple	–	–	DDoS-SDN	S
[39]	Autoencoder+FL	FedAvg	CICIDS2018	98.20	98.10	DDoS-SDN	E

Note: Scope: LDDoS-SDN=low-rate DDoS in multi-controller SDN [4, 15, 32, 36]; DDoS-SDN=general DDoS in SDN; DDoS-IoT=DDoS in IoT network; DDoS-tel.=telecom cloud; DDoS-gen.=general DDoS (non-SDN); IDS-general=generic IDS without SDN focus; IDS-SDN=IDS with SDN component. Type: E=empirical; S=survey/review. Acc and F1: best values per study; "–"= not reported.

strong individual results, but each appeared in only one or two studies, which is not enough to draw firm conclusions.

As far as aggregation strategies (question no. 2) are concerned, weighted aggregation, asynchronous FL, and personalized FL all appeared repeatedly and each of them addressed a different version of the heterogeneity problem, unequal data distributions, synchronization delays, and domain-specific traffic patterns, respectively. The standard FedAvg remained a common baseline. Evidence suggests that asynchronous and adaptive strategies tend to outperform FedAvg when con-

trollers operate under genuinely different conditions, though direct comparisons within single studies are limited.

The data set situation (question no. 4) is the field's clearest weak point. No available benchmark simultaneously models low-rate attack patterns, multi-controller SDN topology, and heterogeneous traffic distributions. CICIDS2017 and CICDDoS2019 dominate the literature despite not being designed for LDDoS or distributed SDN scenarios. Until better evaluation data is available, the accuracy figures reported on these benchmarks overstate how ready these methods are for deployment.

Three things would improve future work in this area the most. A benchmark dataset built for LDDoS detection in multi-controller environments, with distributed traffic capture and varied attack periodicity, would make cross-study comparison genuinely meaningful. Studies should routinely report communication overhead and convergence time alongside detection metrics; right now, those numbers rarely appear in the literature. Pre-registering the analysis protocol before data extraction would also reduce the risk of post-hoc decision making that inflates reported performance.

References

[1] X. Zhou, X. Mao, and Y. Chen, "A DDoS Attack Detection Method Combining Federated Learning and Hybrid Deep Learning in Software Defined Networking", *The Computer Journal*, vol. 68, pp. 1463–1475, 2025 (https://doi.org/10.1093/comjnl/bxaf049).

[2] A. Alhasawi and S. Alghamdi, "Federated Learning for Decentralized DDoS Attack Detection in IoT Networks", *IEEE Access*, vol. 12, pp. 42357–42368, 2024 (https://doi.org/10.1109/access.2024.3378727).

[3] M. Shamim *et al.*, "A Comparison Study on federated Learning and Centralized Learning-based Intrusion Detection System for Software Defined Networking", *2025 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC)*, Seoul, South Korea, 2025 (https://doi.org/10.1109/ITC-CSCC66376.2025.11137775).

[4] Z. Alashhab *et al.*, "Low-rate DDoS Attack Detection Using Deep Learning for SDN Enabled IoT Networks", *International Journal of Advanced Computer Science and Applications*, vol. 13, 2022 (https://doi.org/10.14569/ijacsa.2022.0131141).

[5] Z. Lv *et al.*, "DDoS Attack Detection Based on CNN and Federated Learning", *International Conference on Advanced Cloud and Big Data*, Xi'an, China, 2022 (https://doi.org/10.1109/cbd54617.2021.00048).

[6] V. R *et al.*, "A Comprehensive Tutorial and Survey of Applications of Deep Learning for Cyber Security", *TechRxiv*, 2020 (https://doi.org/10.36227/TECHRXIV.11473377.V1).

[7] S. Muthunambu *et al.*, "A Novel Eccentric Intrusion Detection Model Based on Recurrent Neural Networks with Leveraging LSTM", *Computers Materials and Continua*, vol. 78, pp. 3089–3127, 2024 (https://doi.org/10.32604/cmc.2023.043172).

[8] A. Khraisat *et al.*, "Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions", *ACM Computing Surveys*, vol. 57, pp. 1–38, 2024 (https://doi.org/10.1145/3687124).

[9] M. Fan *et al.*, "DDoS Attack Detection in SDN-assisted Federated Learning Environment Based on Contrastive Learning", *IEEE Access*, vol. 13, pp. 108798–108814, 2025 (https://doi.org/10.1109/access.2025.3582445).

[10] Y. Liu *et al.*, "An Asynchronous Federated Learning Arbitration Model for Low-rate DDoS Attack Detection", *IEEE Access*, vol. 11, pp. 18448–18460, 2023 (https://doi.org/10.1109/ACCESS.2023.3247512).

[11] R. Doriguzzi-Corin and D. Siracusa, "FLAD: Adaptive Federated Learning for DDoS Attack Detection", *Computers & Security*, vol. 137, art. no. 103597, 2023 (https://doi.org/10.1016/j.cose.2023.103597).

[12] Y.S.N. Fotse, V.K. Tchendji, and M. Velempini, "Federated Learning Based DDoS Attacks Detection in Large Scale Software-defined Network", *IEEE Transactions on Computers*, vol. 74, pp. 101–115, 2024 (https://doi.org/10.1109/tc.2024.3474180).

[13] A.A. Al-Ameer and W.S. Bhaya, "Intelligent Intrusion Detection Based on Multi Model Federated Learning for Software Defined Network", *International Journal of Safety and Security Engineering*, vol. 13, pp. 1135–1141, 2023 (https://doi.org/10.18280/ijsse.130617).

[14] R. Amin, G. El-Taweel, A. Ali, and M. Tahoun, "A Hybrid Extreme Gradient Boosting and Long Short-term Memory Algorithm for Cyber Threats Detection", *Mendel*, vol. 29, pp. 307–322, 2023 (https://doi.org/10.13164/mendel.2023.2.307).

[15] K. Ramya *et al.*, "An Efficient Infiltration and Denial of Service Detection Using Dynamic Weighted Aggregation Federated Learning", in *Recent Trends in Network Security*, 2024 (https://doi.org/10.1201/9781003565024-13).

[16] N.T. Cam and N.G. Trung, "An Intelligent Approach to Improving the Performance of Threat Detection in IoT", *IEEE Access*, vol. 11, pp. 44319–44334, 2023 (https://doi.org/10.1109/access.2023.3273160).

[17] J. Malik *et al.*, "Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN", *IEEE Access*, vol. 8, pp. 134695–134706, 2020 (https://doi.org/10.1109/ACCESS.2020.3009849).

[18] M. Moradi *et al.*, "A Multi Agent Adaptive Deep Learning Framework for Online Intrusion Detection", *Cybersecurity*, vol. 7, art. no. 9, 2024 (https://doi.org/10.1186/s42400-023-00199-0).

[19] R. Yang *et al.*, "Dependable Federated Learning for IoT Intrusion Detection Against Poisoning Attacks", *Computers & Security*, vol. 132, art. no. 103381, 2023 (https://doi.org/https://doi.org/10.1016/j.cose.2023.103381).

[20] A. Elubeyd and D. Yiltas-Kaplan, "Hybrid Deep Learning Approach for Automatic dos DDoS Attacks Detection in Software Defined Networks", *Applied Sciences*, vol. 13, art. no. 3828, 2023 (https://doi.org/10.3390/app13063828).

[21] M. Aswad *et al.*, "Deep Learning in Distributed Denial of Service Attacks Detection Method for Internet of Things Networks", *Journal of Intelligent Systems*, vol. 32, 2023 (https://doi.org/10.1515/jisys-2022-0155).

[22] H. Zhang *et al.*, "Survey of Federated Learning in Intrusion Detection", *Journal of Parallel and Distributed Computing*, vol. 195, art. no. 104976, 2024 (https://doi.org/10.1016/j.jpdc.2024.104976).

[23] U. Qazi, A. Almorjan, and T. Zia, "A One-dimensional Convolutional Neural Network (1D-CNN) Based Deep Learning System for Network Intrusion Detection", *Applied Sciences*, vol. 12, art. no. 7986, 2022 (https://doi.org/10.3390/app12167986).

[24] A.A Maiga, E. Ataro, and S. Githinji, "Secured Federated Learning for DDoS Detection in Heterogeneous Telecom Cloud Networks Using Recurrent Neural Networks", *International Journal of Electrical and Electronics Engineering*, vol. 10, pp. 54–64, 2023 (https://doi.org/10.14445/23488379/ijeee-v10i12p106).

[25] A. Adedeji, A.M. Abu-Mahfouz, and A.M. Kurien, "DDoS Attack and Detection Methods in Internet Enabled Networks: Concept, Research Perspectives, and Challenges", *Journal of Sensor and Actuator Networks*, vol. 12, art. no. 51, 2023 (https://doi.org/10.3390/jsan12040051).

[26] M. Elsayed *et al.*, "DDoSnet: A Deep Learning Model for Detecting Network Attacks", *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"*, Cork, Ireland, 2020 (https://doi.org/10.1109/WoWMoM49955.2020.00072).

[27] M.W. Nadeem, H.G. Goh, Y. Aun, and V. Ponnusamy, "Detecting and Mitigating Botnet Attacks in Software-defined Networks Using Deep Learning Techniques", *IEEE Access*, vol. 11, pp. 49153–49171, 2023 (https://doi.org/10.1109/access.2023.3277397).

[28] J. Mateus, G.A.L. Zodi, and A. Bagula, "Federated Learning-based Solution for DDoS Detection in SDN", *2024 International Conference on Computing, Networking and Communications (ICNC)*, Big Island, USA, 2024 (https://doi.org/10.1109/icnc59896.2024.10556115).

[29] S.S. Kiruthika, S. Kumar, R. Fernandes, and S. Adari, "Network Flow Based Abnormal Behavior Feature Extraction for DDoS Attack Classification Using Adaptive Federated Learning Model", *Journal on Emerging trends in Modelling and Manufacturing*, vol. 9, 2023 (https://doi.org/10.46632/jemm/9/2/5).

[30] F. Perez Diaz *et al.*, "A Flexible SDN-based Architecture for Identifying and Mitigating Low-rate DDoS Attacks Using Machine Learning", *IEEE Access*, vol. 8, pp. 155859–155872, 2020 (https://doi.org/10.1109/ACCESS.2020.3019330).

[31] A. Belenguer, J.A. Pascual, and J. Navaridas, "GowFed: A Novel Federated Network Intrusion Detection System", *Journal of Network and Computer Applications*, vol. 217, art. no. 103653, 2023 (https://doi.org/10.1016/j.jnca.2023.103653).

[32] Y.S.N. Fotse, V.K. Tchendji, and M. Velempini, "Federated Learning Based DDoS Attacks Detection in Large Scale Software Defined Network", *IEEE Transactions on Computers*, vol. 74, pp. 101–115, 2024 (https://doi.org/10.1109/tc.2024.3474180).

[33] A. Kadam *et al.*, "SDN-driven Security Framework for DDoS Attack Detection and Mitigation", *International Journal for Science Technology and Engineering*, vol. 12, pp. 620–625, 2024 (https://doi.org/10.22214/ijraset.2024.65142).

[34] J. Wang, L. Wang, and R. Wang, "MFFLR-DDoS: An Encrypted LR-DDoS Attack Detection Method Based on Multi Granularity Feature Fusions in SDN", *Mathematical Biosciences and Engineering*, vol. 21, pp. 4187–4209, 2024 (https://doi.org/10.3934/mbe.2024185).

[35] M. Nakip, B.C. Gul, and E. Gelenbe, "Decentralized Online Federated G-network Learning for Lightweight Intrusion Detection", *2023 31st International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Stony Brook, USA, 2023 (https://doi.org/10.1109/MASCOTS59514.2023.10387644).

[36] K. Oki, Y. Ogawa, K. Ota, and M. Dong, "Evaluation of Applying Federated Learning to Distributed Intrusion Detection Systems through Explainable AI", *IEEE Networking Letters*, vol. 6, pp. 198–202, 2024 (https://doi.org/10.1109/lnet.2024.3465516).

[37] D.C. Attota, V. Mothukuri, R.M. Parizi, and S. Pouriyeh, "An Ensemble Multi-view Federated Learning Intrusion Detection for IoT", *IEEE Access*, vol. 9, pp. 117734–117745, 2021 (https://doi.org/10.1109/access.2021.3107337).

[38] A.A. Wabi, I. Idris, O.M. Olaniyi, and J.A. Ojeniyi, "DDoS Attack Detection in SDN: Method of Attacks, Detection Techniques, Challenges and Research Gaps", *Computers & Security*, vol. 139, art. no. 103652, 2023 (https://doi.org/10.1016/j.cose.2023.103652).

[39] J. Ma and W. Su, "Collaborative DDoS defense for SDN-based AIoT with Autoencoder-enhanced Federated Learning", *Information Fusion*, vol. 117, art. no. 102820, 2024 (https://doi.org/10.1016/j.inffus.2024.102820).

Rikie Kartadie, S.T., M.Kom.
Doctoral Program in Engineering Science
https://orcid.org/0000-0003-1947-353X
E-mail: rikie@utdi.ac.id
Universitas Negeri Yogyakarta, Indonesia
https://www.uny.ac.id
Universitas Teknologi Digital Indonesia,
Yogyakarta, Indonesia
http://www.utdi.ac.id

Eko Marpanaji, Ph.D., Assoc. Professor
Doctoral Program in Engineering Science
https://orcid.org/0009-0001-6613-4920
E-mail: eko@uny.ac.id
Universitas Negeri Yogyakarta, Indonesia
https://www.uny.ac.id

Agus Maman Abadi, Ph.D., Professor
Department of Mathematics Education
https://orcid.org/0000-0002-5488-3043
E-mail: agusmaman@uny.ac.id
Universitas Negeri Yogyakarta, Indonesia
https://www.uny.ac.id

Information for Authors

Journal of Telecommunications and Information Technology (JTIT) is published quarterly since 2000. It comprises original contributions, dealing with a wide range of topics related to telecommunications and information technology. **All papers are subject to peer review.** Topics presented in the JTIT report primary and/or experimental research results, which advance the base of scientific and technological knowledge about telecommunications and information technology.

JTIT is dedicated to publishing research results which advance the level of current research or add to the understanding of problems related to modulation and signal design, wireless communications, optical communications and photonic systems, voice communications devices, image and signal processing, transmission systems, network architecture, coding and communication theory, as well as information technology.

We encourage submissions from a diverse range of authors from across all countries and backgrounds.

Manuscript

Latex files are preferred and Editorial Office provides a style to prepare the material along with the documentation. We also accept Microsoft Word and PDF files. A typical article is 10 pages long (approximately 6,000 words) and must include the following contents:

- Authors' names and affiliations in the following format:
  First name and surname (last name), academic title,
  Position held,
  ORCID number,
  E-mail address from the University's domain,
  Faculty and name of the University,
  Link to University website.
- Abstract (150-200 words). The abstract should contain statement of the problem, assumptions and methodology, results and conclusion or discussion on the importance of the results. Abstracts must not include mathematical expressions or bibliographic references.
- Keywords related to the content of the article. About four keywords or phrases in alphabetical order should be used, separated by commas.
- The content of the article in a typical structure, i.e.: introduction, related work, conducted research, conclusions, references.

Figures, Tables and Photos

Together with the article, please send files with graphics with the highest resolution available, 150 dpi or more in bitmap resolution (jpg, png) and vector (cdr, svg, ps, pdf) formats are welcomed.

References

We use four main citation styles for a journal article, for an Internet article, for a conference paper, and for a book. Below are examples of citations. In each item, the DOI number or link to the PDF of the cited article should be provided.

[1] R.K. Meyers and A.H. Desoky, "An implementation of the blowfish cryptosystem", *2008 IEEE International Symposium on Signal Processing and Information Technology*, 2008 ((https://doi.org/10.1109/ISSPIT.2008.4775664).

[2] K. Nowicki and T. Uhl, *Ethernet End-to-End*, 1st ed. Germany, Shaker-Publisher, 2008 (ISBN: 978383832271404).

[3] C. Shorten and T.M. Khoshgoftaar, "A survey on image data augmentation for deep learning", *Journal of Big Data*, vol. 6, no. 1, pp. 1–48, 2019 (https://doi.org/10.1186/s40537-019-0197-0).

[4] S. Wong *et al.*, "Traffic forecasting using vehicle-to-vehicle communication", *3rd Annual Conference on Learning for Dynamics and Control*, pp. 917–929, 2021 (https://arxiv.org/pdf/2104.05528).

Submission

The paper with full PDF version and anonymous PDF version for the blind review process should be submitted on the JTIT website https://www.jtit.pl/jtit/about/submissions.

Reviewing Process

The article is initially approved by the Editor-In-Chief and if the decision is positive, is then sent to the reviewers. Depending on the subject of the article, it takes few weeks. In the next step, reviews are showed to authors who have 2 weeks to correct the article. Finally, the corrected text can be re-presented to the reviewer for reevaluation, which will take another 2 weeks.

As a result, after about 3 months, we are able to send the text for publication in the upcoming issue of JTIT.

When the reviews are inconsistent, additional corrections are necessary, or the reviewer expects additional verification because the corrections ordered by the author are insufficient or additional problems arise, the review of the article may be extended by another month or more.

Editorial Work

Positively reviewed and corrected article is next prepared by the editorial office for publication. At the end of this process the author receives an copyedited version for approval.

Licensing

Manuscript submitted to JTIT should not be published or simultaneously submitted for publication elsewhere. By submitting a manuscript the author grants license to the National Institute of Telecommunications, for the use of the paper in the fields of exploitation: reproducing and fixing the paper, distributing the paper by means of introduction to trade, letting for use or rental of the original or copies, and distributing the paper by means of public exhibition, screening, presentation and broadcast as well as rebroadcast, and making the paper publicly available in such a manner that anyone could access it at a place and time selected thereby, or by making it available in a way not allowing selection of time or place, including by means of Internet or other networks.

Ghostwriting Declaration

We require formal declaration that the process of writing the paper was not influenced by any third party. In the article, all the contributions of other people are clearly indicated. The theories presented, methods used, analysis and research, as well as the copyrights to the drawings, photographs and other figures belong to the authors or are clearly credited in the text. The author must also indicate whether his work has received financial support and if the realization of the whole project was possible thanks to the permission and cooperation with scientific institutions, associations and others.

Other Information

- The JTIT being an Open Access Journal (OAJ) has no article processing charges (APCs). The published articles can be downloaded freely without payment.
- JTIT supports open access and using continuous publishing "publish-as-you-go" scheme. This means that we no longer wait to accumulate several articles into a quarterly issue before publication. Rather, articles are continuously added to current issues after acceptation. Publish-as-you-go reduces publication lag for our authors, and make the newest research available quickly. After completing the review process, an article is published online in the current issue with DOI registration. When the issue period ends, a new issue is activated. So accepted articles are published without waiting for the quarterly issue end.

National Institute of Telecommunications

Editorial Office

National Institute
of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland
https://www.gov.pl/web/instytut-lacznosci

phone +48 22 512 81 83
fax +48 22 512 84 00

e-mail: journal@jtit.pl
www.jtit.pl

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY 2/2026 vol. 104