ISSN: 2821-157X | htpps://www.jasd.khadu.ir

Journal of Aerospace Defense

Volume 4, Issue 3
Autumn2025
P.P 102-115.

Research Paper;

Designing an extended IP with variable FP granularity for time-series traffic-based anomaly detection and enhancing the security of aerospace defense networks

Gohar Varamini[1]
1. Department of Electrical Engineering, Bey. C., Islamic Azad University, Beyza, Iran.
Gohar.Varamini@iau.ac.ir

Article Information

Accepted:
2025/12/12

Recceived:
2023/08/18

Keywords:

Keywords:/
Anomaly Detection
Traffic Control
Time Series Analysis
Fast Proxy

Corresponding Author:
Gohar Varamini

Email:
Gohar.Varamini@iau.ac.ir

Abstract

Abstract

In the field of network anomaly detection in the Internet Protocol (IP) architecture, a variety of methods have been proposed. Since the network behavior is reflected in the communication traffic, anomaly detection should be possible by analyzing the communication traffic flows correctly. In large-scale IP networks, traffic flows are allocated and encapsulated by headers along with the communication operator, and it is difficult to observe and accurately detect the occurrence of anomalies in individual communication flows in the form of coarser information, and the flow obtained by flow measurement protocols (IP Information Export) is the result of combining different communication flows with different characteristics.

In this study, an anomaly detection method based on time series traffic flows is proposed. First, the composite traffic flows are implemented using a system called Fast Proxy, which can decompose traffic flows into individual flows with very fine granularity and detect anomalies in the decomposed flows based on a simple correlation analysis and dynamic threshold configuration. The proposed method detects anomalies caused by service failures with almost 100% accuracy and even achieves an accuracy of about 80% to 90% in more difficult detection cases, such as small traffic fluctuations or noisy conditions.

Varamini, Gohar;.(1404). Title: Design and implementation of wide IP traffic with variable granularity for anomaly detection and optimization of defense-security networks., Volume3 (Issue4), Page 102-115

ISSN: 2821-157X | htpps://www.jasd.khadu.ir

فصلنامه علمی دفاع هوافضایی
دورهٔ ٤ ، شمارهٔ ۳.
پاییز١٤٠٤
صفحات١١٥-١٠٢

مقاله پژوهشی؛

طراحی IP گسترده با دانه‌بندی متغیر FP به منظور تشخیص ناهنجاری مبتنی بر ترافیک سری زمانی و افزایش امنیت شبکه های دفاع هوا فضایی

گوهر ورامینی [1*]

۱. دانشیار، گروه مهندسی برق، دانشگاه آزاد اسلامی، بیضا، ایران. **رایانامه:Gohar.Varamini@iau.ac.ir**

اطلاعات مقاله

تاریخ دریافت:
١٤٠٤/٠٥/٢٧

تاریخ پذیرش:
١٤٠٤/٠٩ /٢١

کلیدواژه‌ها:

فونت و سایز کلیدواژه‌ها:
تشخیص ناهنجاری
کنترل ترافیک
تحلیل سری زمانی
پروکسی سریع

نویسنده مسئول:
گوهر ورامینی

ایمیل:
Gohar.Varamini@iau.ac.ir

چکیده

چکیده (Abstract):

در زمینه تشخیص ناهنجاری شبکه در ساختار پروتکل اینترنت(IP) ، مقیاس بزرگ و گسترده روش های متنوعی ارائه شده است. از آنجا که رفتار شبکه در ترافیک ارتباطی منعکس می گردد، تشخیص ناهنجاری با تحلیل صحیح جریان‌های ترافیک ارتباطی می بایست امکان پذیر شود. در شبکه‌های IP گسترده، جریان‌های ترافیک توسط هدرها همراه با اپراتور ارتباطی اختصاص و کپسوله‌سازی شده و به صورت اطلاعاتی درشت‌دانه‌تر مشاهده و تشخیص دقیق وقوع ناهنجاری‌ها در جریان‌های ارتباطی منفرد دشوار است و جریانی که توسط پروتکل‌های اندازه‌گیری جریان (IP Information Export) به دست می‌آید، حاصل ترکیب سازی ارتباطی مختلف با ویژگی‌های متفاوت است. در این مطالعه، یک روش تشخیص ناهنجاری مبتنی بر جریان‌های ترافیک سری زمانی پیشنهاد شده است. ابتدا، جریان‌های ترافیک ترکیب سازی شده با استفاده از سیستم پیاده‌سازی شده به نام پروکسی سریع (Fast Proxy)که می‌تواند جریان‌های ترافیک را با دانه‌بندی بسیار ریز تجزیه و به جریان‌های منفرد تبدیل و ناهنجاری‌ها را در جریان‌های تجزیه شده بر اساس یک تحلیل همبستگی ساده و پیکربندی آستانه پویا تشخیص دهد. روش پیشنهادی ناهنجاری‌های ناشی از خرابی سرویس را با دقت تقریباً ١٠٠٪ تشخیص و حتی در موارد تشخیص دشوارتر، مانند نوسانات کوچک ترافیک یا شرایط نویزی، به دقتی در حدود ٨٠٪ تا ٩٠٪ دست یابد.

استناد: ورامینی، گوهر؛(۱۴۰۵). عنوان: طراحی IP گسترده با دانه‌بندی متغیر FP به منظور تشخیص ناهنجاری مبتنی بر ترافیک سری زمانی و افزایش امنیت شبکه های دفاع هوا فضایی. *دفاع هوافضایی*، دوره ۴(شماره۳)، صفحات۱۰۲-۱۱۵.

۱–مقدمه

به منظور ایجاد بهره‌برداری پایدار و همراه با ضریب اطمینان بالا از شبکه‌های پروتکل اینترنت (IP) گسترده به عنوان یک زیرساخت اجتماعی، اندازه‌گیری و تحلیل دقیق ترافیک ارتباطی شبکه و تشخیص ناهنجاری‌ها، مانند خرابی‌ها یا حملات امنیتی، ازاهمیت بسیار زیادی برخوردار است. در واقع ترافیک ارتباطی از جریان‌های منفرد و تکی تشکیل شده است[۱]. به طور کلی، جریان‌ها با استفاده از پنج شناسه ۵ تایی (5-tuple) شناسایی و تشخیص داده می‌شوند که عبارتند از: آدرس IP مبدأ، آدرس IP مقصد، شماره پورت مبدأ، شماره پورت مقصد و نوع پروتکل[۲] این جریان‌ها را می‌توان با استفاده از پروتکل‌های اندازه‌گیری جریان به نام پروتکلx NetFlow وIPFIX جمع‌آوری کرد[۳].

فناوری امنیت اطلاعات به دلیل ویژگی‌های پردازش موازی با ابعاد بالا، توجه زیادی را به خود جلب کرده است و تحقیق در مورد پنهان‌سازی اطلاعات و الگوریتم رمزگذاری به عنوان موضوع اصلی در این زمینه تبدیل شده است[۱]. مطالعات در این زمینه با ارائه فناوری رمزگذاری فاز تصادفی دوگانه بر اساس سیستم ۴ f روش رمزگذاری نوری از حوزه فوریه به حوزه کسری تکامل قابل توجهی یافته است [۲]. استراتژی رمزگذاری تکراری آبشاری که پیشنهاد شده بود، کارایی رمزگشایی را از طریق کدگذاری الگوی دو فازی بیشتر بهبود بخشید و محدودیت‌های رمزگذاری خطی سنتی را شکست و امنیت سیستم را به طور قابل توجهی بهبود بخشیدند[۳].

الگوریتم های فراابتکاری (Metaheuristic Algorithms) یکی از انواع روش‌های جستجو هستند که با عنوان روش‌های بهینه‌سازی نیز شناخته می‌شوند[۴]. این الگوریتم‌ها به منظور یافتن راه‌حلی مناسب به منظورمسائل بهینه‌سازی پیچیده و دشوار طراحی شده‌اند که با الگوریتم‌های سنتی قابل حل نیستند. به عبارتی، در دنیای واقعی ممکن است با مسائلی مواجه که برای حل آن‌ها منابع محدودی (مانند توان محاسباتی و زمان) در اختیار باشد[۵]. در این شرایط الگوریتم های فراابتکاری می‌توانند به عنوان ابزاری مناسب تلقی شوند و راه‌حل‌های خوبی را با تلاش محاسباتی کمتری نسبت به سایر الگوریتم‌ها پیدا کنند[۶].

الگوریتم های فراابتکاری را می‌توان به عنوان روش‌های جستجو محسوب کرد که به منظور یافتن راه‌حل مناسب در مسائل بهینه‌سازی پیچیده طراحی شده و از آن‌ها می‌توان به خوبی در شرایط حساس و حیاتی بهره گرفت که اطلاعات ناقص، ناکافی یا منابع محدود (مانند قدرت محاسباتی و زمان) در اختیار است[۷]. ظهور الگوریتم های فراابتکاری به منظور حل چنین مسائل بهینه‌سازی، به عنوان یکی از برجسته‌ترین دستاوردهای دو دهه اخیر در پژوهش های عملیاتی تلقی می‌شود [۸].

اگرچه پروتکلx Flowعملاً اطلاعات جریان را در اینترنت جمع‌آوری و دسته بندی می کند، اما در شبکه‌های IP گسترده و در مقیاس بزرگ با محدودیت‌هایی روبرو است[۴]. هدرهای بسته‌های داده ها توسط هدرهای اضافی اختصاص داده شده توسط اپراتورهای ارتباطی کپسوله‌سازی می‌شوند و رفتار ترافیک کاربر در حالتی درشت‌دانه‌تر مشاهده می‌شود. به عنوان مثال، کپسوله‌سازی توسط پروتکل تونل‌زنی لایه در جهت احراز هویت کاربرPPPoE استفاده می‌شود و چندین برچسب توسط مسیریابی قطعه‌ای با استفاده از سوئیچینگ برچسب چندپروتکلی (SR-MPLS) به عنوان هدرهای بیرونی برای کاربران شبکه خصوصی مجازی (VPN)یا کنترل انعطاف‌پذیر شبکه توسط مهندسی ترافیک اضافه می گردد. در نتیجه، پروتکلx Flow اطلاعات دقیق به ازای هر جریان را به دست نمی‌آورد[۵]، بلکه اطلاعاتی حجیم تر از هدرهای بیرونی کسب می‌کند.به دلیل محدودیت پروتکلx Flowدر شبکه‌های IP گسترده و در مقیاس بزرگ، جریان‌ها به عنوان اطلاعات کلان که چندین سرویس بر روی آن‌ها ترکیب سازی شده‌اند مورد اندازه‌گیری قرار می گیرند[۶].

اگرچه هر سرویس بسته به الگوی استفاده خود ویژگی‌های ترافیکی متفاوتی دارد، این تفاوت‌ها از طریق این ترکیب سازی قابل تشخیص نیستند. در نتیجه، تشخیص دقیق ناهنجاری‌های ارتباطی برای یک جریان خاص از نتایج اندازه‌گیری بسیار دشوار می‌شود[۷].

چالش‌ها و مسائلی نیز وجود دارند که برای حل آن‌ها به توسعه راه‌حل‌های بهتری نیاز است و نمی‌توان از رویکردهای سنتی در حل چنین مسایلی استفاده کرد[۹]. الگوریتم‌های فرا ابتکاری می‌توانند در حل این گونه مسائل کاربردی باشند و با رویکردهای مختلف به بهینه‌سازی مسائل غیرخطی بپردازند و عملکرد بهتری نسبت به «روش‌های تکراری (Iterative Methods) و اکتشافی ساده حریصانه Simple Greedy Heuristicsداشته باشند[۱۰].

همچنین، انواع مختلفی از مسائل وجود دارند که حل آن‌ها با استفاده از یک الگوریتم بهینه‌سازی ساده در رسیدن به بهبود سراسری غیرعملی است. برای مثال، ممکن است در یک مسئله بهینه‌سازی به دلیل وجود متغیرهای تصادفی در تابع هدف پیچیدگی هایی وجود داشته و امکان حل مسئله با استفاده از برنامه‌ریزی تصادفی (Stochastic Programming) نباشد[۱۱]. به علاوه، در بسیاری از مسائل بهینه‌سازی با توابع چندهدفه با استفاده از متغیرهای غیرخطی و مسائل هوش مصنوعی و یادگیری ماشین با مجموعه داده‌های بزرگ، یافتن پاسخ بهینه بسیار دشوار است. در چنین مسائلی، الگوریتم های فراابتکاری نقش مهمی در حل مسائل ایفا می‌کنند و برتری چشم‌گیری نسبت به سایر روش‌ها دارند[۱۲].

۲- ساختار و پیکربندی روش ها

در این پژوهش یک روش تشخیص ناهنجاری شبکه با استفاده از پروکسیFlow x پیشنهاد شده است که قابلیت اندازه‌گیری جریان‌های ارتباطی در سطح دانه‌بندی ریز را به منظور بهبود دقت تشخیص ناهنجاری دارد. پروکسی سریعFlow x می‌تواند هدرهای بیرونی پیچیده بسته‌های IP را تحلیل و پردازش آماری را به ازای هر سرویس با سرعت‌های فوق‌العاده بالا (۱۰۰ گیگابیت بر ثانیه) انجام دهد، که می‌تواند اطلاعات ترافیک کلان را به درستی به رفتارهای جریان منفرد تجزیه کند. فرض این است که اگر ترافیک به درستی تجزیه شود، ناهنجاری‌ها را به سرعت و با دقت از یک تحلیل ساده مقدار همبستگی تشخیص داده شود. الگوی سری زمانی ترافیک تمایل دارد به صورت دوره‌ای نوسان داشته و در حالی که به طور یکنواخت افزایش می‌یابد، مگر اینکه یک عامل خارجی مانند خرابی در شبکه امنیتی رخ دهد. بنابراین، روش تشخیص ناهنجاری با اعمال روش تحلیل مقدار همبستگی سبک بر روی جریان‌های ارتباطی تجزیه شده در این مقاله پیشنهادو ارایه شده است[۲۵].

در تحلیل شبکه‌ها، روش‌هایی برای تحلیل چندرسانه‌ای در لایه کاربرد[۸]مانند دسترسی به وب و برای تحلیل رابطه بین انتشارات بر اساس نظریه گراف پیشنهاد شده است. ترافیک مورد بررسی در این مقاله بیشتر مربوط به جریان‌های لایه‌های پایین‌تر است که توسط شماره پورت‌ها در لایه انتقال و آدرس‌های IP در لایه تعریف می‌شوند. روش‌های اندازه‌گیری ترافیک را می‌توان به دو دسته طبقه‌بندی کرد: اندازه‌گیری مستقیم بسته‌ها و رویکرد مبتنی بر اندازه‌گیری جریان که اطلاعات فراداده بسته‌های نمونه‌برداری شده را در فواصل زمانی منظم به دست می‌آورد[۹]. یک مثال معمول از دسته اول، بازرسی عمیق بسته (DPI) است [۱۰]که داده‌هایی با فرمتcap p را به عنوان داده‌های بزرگ جمع‌آوری کرده و یک رویکرد یادگیری ماشین در تحلیل داده‌های به دست آمده توسط DPI پیشنهاد شده است[۱۱]. با این حال، این رویکرد به دلیل حجم عظیم ترافیک در شبکه‌های IP گسترده، ناکارآمد است[۱۲].

در مقابل، رویکرد مبتنی بر اندازه‌گیری جریان در اندازه‌گیری کارآمد ترافیک پیشنهاد شده است . اگرچه تعاریف مختلفی در جریان وجود دارد، جریان‌ها با استفاده از پنج شناسه شناسایی می‌شوند[۱۳] که عبارتند از آدرس IP مبدأ، آدرس IP مقصد، شماره پورت مبدأ، شماره پورت مقصد و نوع پروتکلNet flow وIPFIX تعداد ظهور بسته‌ها را می‌شمارند، در حالی کهFlow s تعداد مشخصی بایت از ابتدای یک بسته را استخراج می‌کند[۱۴]. هر روش داده‌های جمع‌آوری شده را به یک جمع‌آورنده جریان ارسال می‌کند. اخیراً، روش‌های کارآمد مبتنی بر ساختارهای داده احتمالی پیشنهاد شده‌اند[۲۲]، مانند رادار جریان با استفاده از فیلتر بلوم، MV-sketch با استفاده از ساختارcount-min sketch ، وFlow Hashکه جریان‌های فیل (elephant flows)را شناسایی کرده و بر مشاهدات آن‌ها تمرکز می‌کند[۱۵]. با مشاهده جریان‌های ارتباطی با استفاده از این روش‌ها، اپراتورهای شبکه می‌توانند به درستی خرابی‌های سرویس را ارزیابی کرده یا مهندسی ترافیک را در شبکه‌های خود اعمال کنند[۱۶].

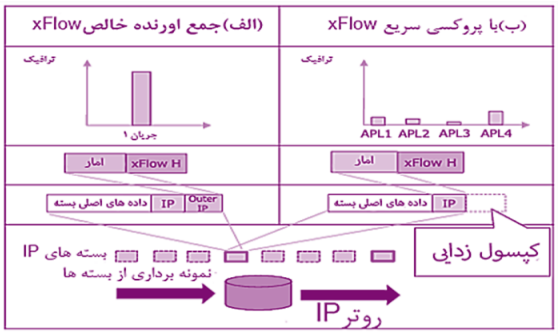
رویکردهای مبتنی بر پیش‌بینی که داده‌های سری زمانی را با استفاده از تحلیل خود همبستگی مانند ARIMAمدل‌سازی می‌کنند[۱۸] و با مقایسه مقادیر پیش‌بینی شده از مدل با مقادیر مشاهده شده، ناهنجاری‌ها را تشخیص می‌دهند، برای تشخیص ناهنجاری پیشنهاد شده‌اند[۱۹]. علاوه بر این، رویکردهای مبتنی بر یادگیری ماشین با استفاده از حافظه طولانی کوتاه‌مدت (LSTM) و شبکه عصبی کانولوشنی (CNN) برای پیش‌بینی پیشنهاد شده‌اند[۲۰]. این روش‌ها فرض می‌کنند که رفتار داده‌های سری زمانی پیچیده است و به طور نامنظم نوسان می‌کند، که با فرض ما مبنی بر دوره‌ای بودن شکل جریان ارتباطی متفاوت است[۲۱].

یک رویکرد ساده برای تشخیص ناهنجاری برای داده‌های سری زمانی که شامل پیش‌بینی مدل نمی‌شود[۲۴]، تحلیل بدون نظارت داده‌های تک‌متغیره است[۲۲]. این روش‌ها با ایجاد یک فضای پنهان با ابعاد کم از داده‌های سری زمانی نرمال و مقایسه آن با مقادیر مشاهده شده، ناهنجاری‌ها را تشخیص می‌دهند[۲۳]. به عنوان مثال، SR بر اساس تحلیل سیگنال هستند.

اگرچه روش پیشنهادی که در بخش چهارم شرح داده شده است، از این جهت که زیردنباله‌ها را مقایسه می‌کند، شبیه به رویکرد مقایسه فاصله است، اما می‌تواند با استفاده از یک تحلیل ساده مقدار همبستگی، ناهنجاری‌ها را به سرعت و با دقت تشخیص دهد[۲۶]. این به دلیل مشاهده تجربی ماست که الگوی سری زمانی ترافیک تمایل دارد به صورت دوره‌ای نوسان کند[۱۷] در حالی که به طور یکنواخت افزایش می‌یابد[۲۲]، مگر اینکه یک عامل خارجی مانند خرابی رخ دهد.

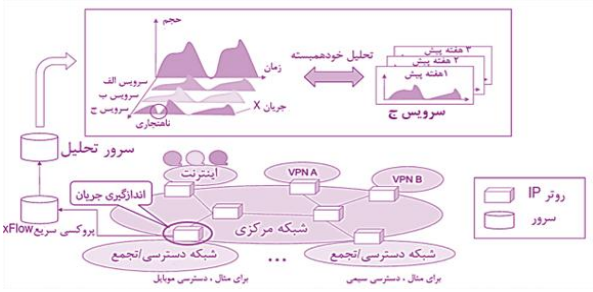
۳- روش پیشنهادی

از آنجا که ترافیک IP در شبکه‌های بزرگ به عنوان اطلاعات کلان که خدمات مختلفی بر روی ترکیب سازی شده‌اند مشاهده می‌شود، تشخیص دقیق ناهنجاری‌ها از نتایج مشاهدات به طور سنتی دشوار بوده است. با این حال، پروکسی سریعFlow x می‌تواند درون ترافیک IP را کاوش و مشاهده جریان‌ها با دانه‌بندی دلخواه را حتی در شبکه‌های مقیاس بزرگ امکان‌پذیر سازد. در شبکه‌های IP گسترده و در مقیاس بزرگ، بسته کاربر توسط هدرهای اضافی مانند هدر L2TP یا برچسب‌های SR-MPLS که توسط اپراتورهای ارتباطی اختصاص و کپسوله‌سازی شده اند. بنابراین، همانطور که در شکل یک نشان داده شده است، پروتکل‌های اندازه‌گیری جریان مانند NetFlow یا IPFIX آمار هدرهای بیرونی جمع‌آوری و از آنجا که اطلاعات هدر بیرونی شامل آدرس‌های IP دستگاه‌های داخلی شبکه اپراتور است، مشاهده رفتارهای برنامه‌های کاربردی منفرد دشوار است.



شکل ۱. اندازه‌گیری ترافیک با استفاده از پروکسی سرx Flow

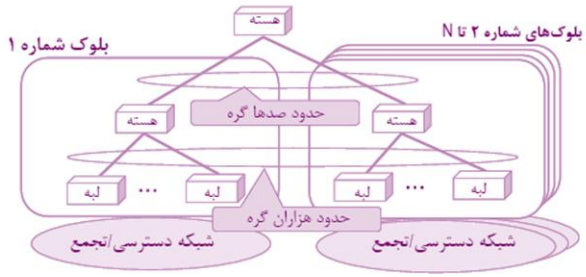
هدف این مطالعه ایجاد روشی در تشخیص ناهنجاری با استفاده از رویکرد اندازه‌گیری ترافیک تحت این فرض است که پروکسی سری Flow x می‌تواند ترافیک ارتباطی را با دانه‌بندی دلخواه مشاهده کند. علاوه بر این، از طریق ارزیابی‌ها، دستورالعمل‌هایی را به منظور دانه‌بندی مناسب مشاهده جریان در موارد استفاده خاص مشخص می‌گردد. فرض بر این است که یک شبکه IP گسترده و در مقیاس بزرگ است که توسط یک اپراتور مخابراتی ارائه می‌شود. در یک شبکه IP گسترده، شبکه‌های بی‌سیم و سیار مانند 4G، 5G و شبکه‌های سیمی با استفاده از فیبرهای نوری به عنوان شبکه‌های دسترسی برای کاربران ارائه می‌شوند. ترافیک عبوری از این شبکه‌های دسترسی از طریق روترهای لبه در مرزها به شبکه هسته جریان می‌یابد. شبکه هسته از روترهای لبه چند منظوره و روترهای هسته با ظرفیت بالا تشکیل شده است که از طریق دستگاه‌های نوری مانند مالتی‌پلکسرهای افزودن/حذف نوری قابل پیکربندی (ROADM) یا اتصالات متقاطع نوری (OXC) به یکدیگر متصل هستند.



شکل ۲. مروری بر محیط تشخیص ناهنجاری شبکه

برای هر منطقه یک بلوک تعریف شده و هر بلوک از چندین روتر لبه و یک روتر هسته تشکیل شده است. برای برقراری ارتباط ، چندین بلوک تعریف شده و یک روتر هسته سطح بالاتر بلوک‌ها را به هم متصل می‌کند. شبکه از هزاران روتر لبه و هسته تشکیل شده است. جریان‌ها توسط پروتکل Flow x فقط از روترهای هسته یا شامل روترهای لبه جمع‌آوری می‌شوند. در هر دو حالت، پروکسی سریع Flow x می‌تواند جریان‌ها را عملاً جمع‌آوری کند. از طریق شبکه هسته، کاربران می‌توانند به خدمات مختلفی مانند دسترسی به اینترنت یا اتصالات امن VPN دسترسی داشته باشند. در مدل شبکه، که جریان‌های ارتباطی در روترهای لبه با استفاده از IPFIX مشاهده می‌شوند. در این حالت، جریان‌های ارتباطی مشاهده شده همان طور که در بالا توضیح داده شد کپسوله‌سازی شده و فقط می‌توانند بر اساس موقعیت جغرافیایی طبقه‌بندی شوند، به

عنوان مثال، «جریان‌ها به روترهای IP متصل به اینترنت» یا «جریان‌ها به روترهای IP متصل به VPN » بنابراین، ابتدا هدرهای IP بیرونی جریان‌های مشاهده شده توسط IPFIX را با استفاده از پروکسی سریعxFlowحذف کرده و سپس اطلاعات جریان را در مرحله بعد به سرور تحلیل ارسال می‌کنند.



شکل ۳. مدل توپولوژی شبکه و روترها -لینک از فیبرهای نوری و گره‌های نوری مانند OXC یاROADM

در شبکه‌های IP مقیاس بزرگ، حتی اگر الگوی سری زمانی ترافیک تمایل به افزایش یکنواخت سالانه داشته باشد، تغییرات روزانه آن تمایل به دوره‌ای بودن دارد. بر این اساس، یک روش ساده تشخیص ناهنجاری طراحی شده است. روش پیشنهادی با محاسبه مقدار همبستگی بین شکل جریان هدف مورد تحلیل و شکل گذشته آن، وقوع ناهنجاری را تشخیص می‌دهد. اگر ناهنجاری رخ ندهد، مقدار همبستگی بالا است؛ در غیر این صورت ناهنجاری رخ داده شده، مقدار همبستگی پایین و همبستگی بین شکل‌ها کم است.ابتدا، داده‌های تحلیل برای جریان هدف به عنوان دنباله X به شرح زیر تهیه شده است.

(۱)

$$X = (x_1, x_2, \dots, x_n) \in R^n$$

هر عنصر xi در دنباله X نشان‌دهنده حجم ترافیک در واحد زمان است. به عنوان مثال، اگر یک نقطه داده در هر ساعت مشاهده شود و تحلیل برای ۱ روز انجام شود، nبرابر با ۲۴ تنظیم می‌شود. سپس دنباله Y را تولید می‌کند که T هفته قبل از تاریخ هدف X است.

(۲)

$$Y = (y_1^T, y_2^T, \dots, y_n^T) \in R^n, T = 1,2, \dots T_m$$

میانگین از مشاهدات متعدد را برای سرکوب تأثیر تکینگی‌های مشاهدات قبلی محاسبه می‌کند.

(۳)

$$\overline{Y} = (\overline{y}_1, \overline{y}_2, \dots, \overline{y_n}) \in R^n$$

(۴)

$$\overline{Yl} = \frac{1}{T_m} \sum_{k=1}^{T_m} y_1^k$$

از آنجا که ابعاد دنباله‌های X و $\overline{Y}$ یکسان است، مقدار همبستگی $\rho_{X,\overline{Y}}$ را می‌توان با استفاده از فرمول زیر محاسبه کرده است.

(۵)

$$\rho_{X,\overline{Y}} = \frac{\frac{1}{n}\sum_{t=1}^{n}(x_t-\overline{x})(y_t-\overline{y})}{\sigma x.\sigma y}$$

که در آن $\overline{X}$ و $\overline{Y}$ میانگین‌های X و $\overline{Y}$ هستند و σx و σy انحراف معیارهای آنها هستند $\rho_{X,\overline{Y}}$.یک مقدار استاندارد شده است که وقتی دو دنباله همبسته باشند به 1+ نزدیک است و وقتی همبسته نباشند به صفر نزدیک است. اگر $\rho_{X,\overline{Y}}$ به زیر یک مقدار آستانه از پیش تعیین شده رخ دهد تشخیص می‌دهد که یک ناهنجاری رخ داده است. اگرچه روش تشخیص ناهنجاری پیشنهادی ما به دنباله‌های X و $\overline{Y}$ نیاز دارد، اما با استفاده از مکانیزم پنجره لغزان می‌توان آن را برای تشخیص ناهنجاری شبه‌بلادرنگ نیز به کار برد. همان طور که نشان داده شده است، دنباله‌های X(tr) و $\overline{Y}^{(tr)}$ با استفاده از معادلات فوق بر اساس آخرین زمان مشاهده ترافیک tr ایجاد می‌شوند و سپس $\overline{Y}^{(tr)}$, ρX(tr) محاسبه می‌شود.

سپس، دنباله‌های X(tr + Δt) و $\overline{Y}$ (tr + Δt) در زمان tr + Δt پس از گذشت زمان مشاهده Δt ایجاد می‌شوند و مقادیر همبستگی $\overline{Y}$ (tr+Δt), ρX(tr+Δt) محاسبه می‌گردند. نحوه ارزیابی مقدار آستانه برای تعیین ناهنجاری را نه تنها به عنوان یک مقدار ثابت، بلکه به عنوان یک مقدار در حال تغییر پویا، شرح می‌دهیم. آستانه پویا Th با معادله زیر داده می‌شود.

(۶)

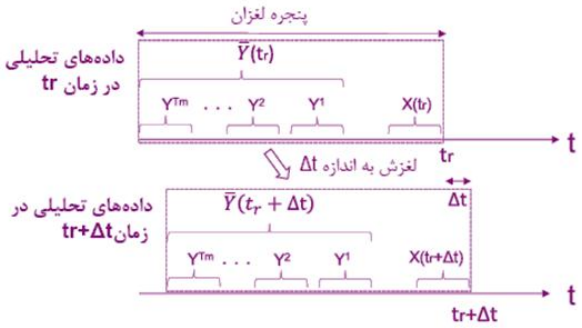
$$[Th = (1-\alpha.SR).\rho^{mean}$$

که در آن α یک ضریب مقیاس است وρ mean_میانگین مقادیر همبستگی بین دوره‌های نرمال است.فرض کنید SR نشان‌دهنده نرخ نمونه‌برداری به دست آمده توسط پروکسی سریعx Flowباشد: اگر Foنرخ جریان مشاهده شده و Fe نرخ جریان رویداد یافته باشد، که در آن یک رویداد خارجی مانند خرابی در حال وقوع است، آنگاه SR با معادله زیر تعریف می‌شود:

(۷)

$$SR = F_e/F_o$$

به عنوان مثال، وقتیSR = 1 ، نرخ جریان مشاهده شده برابر با نرخ جریان وقوع رویداد خارجی است، که نشان می‌دهد جریان برای کاربران مهم به طور فشرده با استفاده از پروکسی سریعx Flow نظارت می‌شود. برعکس، با کاهش مقدارSR ، حالتی را نشان می‌دهد که در آن چندین جریان از توده‌ها به طور کارآمد نظارت می‌شوند. وقتی SR به یک نزدیک است، کوچکتر می‌شود و وقتی به صفر نزدیک است، افزایش می‌یابد.

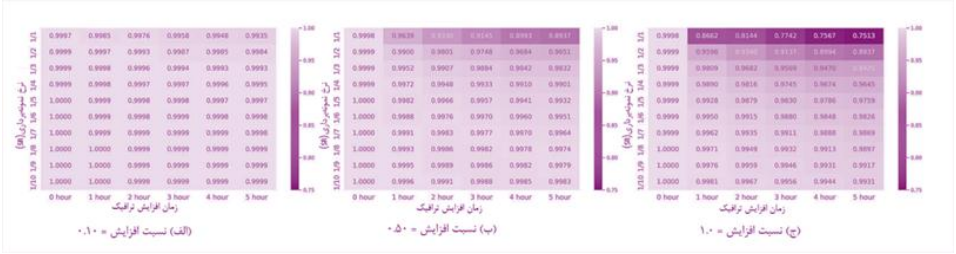


شکل ٤. تشخیص ناهنجاری شبه‌بلادرنگ با استفاده از پنجره‌های لغزان,X(t), Y(t) .

٤ . ارزیابی مکانیزم پیشنهادی

روش پیشنهادی را با شبیه‌سازی‌های کامپیوتری ارزیابی تا مشخص شود که ناهنجاری‌ها را حتی در محیطی که بسته‌ها کپسوله‌سازی شده‌اند، تشخیص دهد. علاوه بر این، کاربرد روش پیشنهادی برای دو سناریوی نوسان ترافیک غیرعادی مورد تحلیل قرار گرفته است. در روش اول کاهش ترافیک به دلیل خرابی سرویس در اینترنت است. دومی افزایش ترافیک به دلیل حملات امنیتی مصرف‌کننده پهنای باند مانند حملات DDoSاست. داده‌های سری زمانی با ترکیب سازی ۱۰ جریان ارتباطی مختلف با نرخ ترافیک تقریباً یکسان تولید شدند.

شکل ۶. مقادیر همبستگی تغییر نرخ نمونه‌برداری (SR) در رویداد خرابی. مناطق تیره‌تر در نقشه حرارتی نشان‌دهنده کاهش قابل توجه در مقادیر همبستگی



شکل ۷. مقادیر همبستگی هنگام تغییر نرخ نمونه‌برداری (SR) در رویداد افزایش ترافیک. مناطق تیره‌تر در نقشه حرارتی نشان‌دهنده کاهش قابل توجه در مقادیر همبستگی

با افزایش مقدارSR ، مقدار همبستگی کاهش می‌یابد. افزایش مقدار SR بیان کننده آن است که جریان خراب به طور فشرده‌تری نظارت می‌شود، که شناسایی عددی رویدادهای خارجی مانند خرابی سرویس را آسان‌تر می‌کند. با این حال، حتی اگر SR به اندازه ۱/۱ بالا تنظیم نشود، کاهش مقدار همبستگی را می‌توان به صورت بصری در محدوده ۳/۱ تا ۴/۱ تأیید کرد. علاوه بر این، همبستگی با افزایش زمان خرابی کاهش یافت، حتی زمانی که مقدار SR به اندازه ۱۰/۱ پایین بود. به عبارت دیگر، اگرچه تشخیص خرابی‌ها در صورت

تنظیم SR با مقدار بالا آسان است، اما بسته به مقدار آستانه همبستگی، ناهنجاری‌ها حتی با SR کوچکتر نیز قابل تشخیص هستند. (heat map)نشان می‌دهد که مقادیر همبستگی به طور قابل توجهی کاهش یافته است. علاوه بر این، شکل‌های ۶نشان می‌دهند که مقادیر تصادفی به عنوان مولفه‌های نویز به ترتیب با نرخ‌های ۱٪، ۵٪ و ۳۰٪ اضافه شده‌اند. این فرض می‌کند که شکل جریان ارتباطی دوره‌ای است اما به صورت دوره‌ای نوسان می‌کند و نوسانات کوچک و نامنظم هستند.

با افزایش مقدارSR ، مقدار همبستگی کاهش می‌یابد. افزایش مقدار SR به این معنی است که جریان خراب شده به طور فشرده‌تری نظارت می‌شود، که شناسایی عددی رویدادهای خارجی مانند خرابی سرویس را آسان‌تر می‌کند. با این حال، حتی اگر SR به اندازه ۱/۱ بالا تنظیم نشود، کاهش مقدار همبستگی را می‌توان به صورت بصری در محدوده ۳/۱ تا ۴/۱ تأیید کرد. علاوه بر این، همبستگی با افزایش زمان خرابی کاهش یافت، حتی زمانی که مقدار SR به اندازه ۱۰/۱ پایین بود. به عبارت دیگر، اگرچه تشخیص خرابی‌ها در صورت تنظیم SR با مقدار بالا آسان است، اما بسته به مقدار آستانه همبستگی، ناهنجاری‌ها حتی با SR کوچکتر نیز قابل تشخیص هستند. این همچنین نشان می‌دهد که نظارت فشرده بر یک سرویس واحد ضروری نیست و چندین سرویس را می‌توان به طور کارآمد نظارت کرد.جداول زیر دقت(accuracy) ، صحت (precision)، بازیابی (recall) و ویژگی (specificity) را برای هر شرط هنگام تغییر مقدار آستانه برای قضاوت در مورد تشخیص ناهنجاری ارائه می‌دهند. هر معیار با استفاده از مثبت واقعی(TP) ، منفی واقعی(TN) ، مثبت کاذب (FP) و منفی کاذب (FN) به شرح زیر تعریف شد.

جدول ۱. تحلیل تشخیص ناهنجاری بر اساس شاخص‌های دقت با آستانه متوسط

	نسبت نویز	صحت	دقت	بازیابی	ویژگی
خرابی	٪۱	٪۱۰۰	٪۱۰۰	٪۹۹	٪۱۰۰
خرابی	٪۱۰	٪۹۰	٪۸۳	٪۱۰۰	٪۸۰
خرابی	٪۳۰	٪۷۹	٪۷۰	٪۹۸	٪۵۸
افزایش ترافیک	٪۱۰	٪۹۱	٪۱۰۰	٪۱	٪۹۶
افزایش ترافیک	٪۵۰	٪۱۰۰	٪۱۰۰	٪۱۰۰	٪۱۰۰
افزایش ترافیک	٪۱۰۰	٪۱۰۰	٪۱۰۰	٪۱۰۰	٪۱۰۰

جدول ۲ نتایج را برای تنظیمات آستانه نسبتاً سست و متوسط نشان می‌دهد. خرابی‌های با نویز کم و افزایش ترافیک با تغییرات بزرگ در حالی که در مورد دوم با نوسان کم ترافیک، به جز در مناطقی با SR بالا، بسیاری از منفی‌های کاذب رخ می‌دهد که منجر به بازیابی کوچک می‌شود.

جدول ۲. تحلیل تشخیص ناهنجاری بر اساس شاخص‌های دقت با آستانه حساس

	نسبت نویز	صحت	دقت	بازیابی	ویژگی
خرابی	٪۱	٪۱۰۰	٪۱۰۰	٪۹۹	٪۱۰۰
خرابی	٪۱۰	٪۵۰	٪۵۰	٪۸۷	٪۸۰
خرابی	٪۳۰	٪۵۰	٪۵۰	٪۹۸	٪۳۸
افزایش ترافیک	٪۱۰	٪۵۸	٪۱۰۰	٪۶۴	٪۸۵
افزایش ترافیک	٪۵۰	٪۹۵	٪۱۰۰	٪۹۰	٪۱۰۰
افزایش ترافیک	٪۱۰۰	٪۱۰۰	٪۱۰۰	٪۱۰۰	٪۱۰۰

جدول ۳ نتایج را برای آستانه‌های سختگیرانه و حساس فهرست می‌کند. اگرچه دقت موارد با تغییر کم ترافیک (۷۱٪) بالاتر از جدول ۲ (۵۸٪) است، اما دقت برای موارد با افزایش ترافیک بالاتر (IR = 50% یا ۱۰۰٪) و نویز = ۱٪، که مناطقی با دقت بالا در جدول ۲ هستند، کاهش یافته است. علاوه بر این، ویژگی زمانی که نویز زیاد است (۱۰٪–۳۰٪) نمی‌تواند افزایش یابد؛ به عبارت دیگر، قضاوت‌های مثبت کاذب را نمی‌توان سرکوب کرد.

جدول ۳. تحلیل تشخیص ناهنجاری بر اساس شاخص‌های دقت با آستانه پویاα .

	نسبت نویز	صحت	دقت	بازیابی	ویژگی
خرابی	٪۱	٪۱۰۰	٪۱۰۰	٪۹۹	٪۸۷
خرابی	٪۱۰	٪۶۵	٪۵۰	٪۸۷	٪۸۰
خرابی	٪۳۰	٪۶۸	٪۵۰	٪۹۸	٪۴۴
افزایش ترافیک	٪۱۰	٪۷۸	٪۱۰۰	٪۶۸	٪۶۸
افزایش ترافیک	٪۵۰	٪۹۵	٪۱۰۰	٪۹۳	٪۱۰۰
افزایش ترافیک	٪۱۰۰	٪۱۰۰	٪۱۰۰	٪۱۰۰	٪۱۰۰

مهمترین نتیجه در جدول ۴ این است که بدون پیاده‌سازی پروکسی سریع xFlow ، به دلیل وضوح پایین مشاهدات، هیچ تغییر واضحی با استفاده از هیچ روش تحلیلی قابل تشخیص نیست. نتایج همچنین نشان می‌دهد که پروکسی سریع xFlow ممکن است برای SBD نیز قابل استفاده باشد در حالی که کاربرد کمی برای شباهت کسینوسی یا الگوریتم‌های مبتنی بر FFT دارد.

جدول ٤. طبقه‌بندی اندازه‌گیری ترافیک و تحلیل ترافیک سری زمانی. دامنه

طبقه بندی	اندازه گیری	روش های موجود	جنبه های فنی و مشارکت کلیدی	روش پیشنهادی
ترافیک	مستقیم	[۹]	اطلاعات دقیق از طریق اندازه گیری مستقیم بسته ها حجم عظیم داده های ترافیک	–
ترافیک	جریان	[۱]و[۲]و[۱۱]	فراداده ها– بار پردازشی کم و مقایس پذیری بالا کاربرد پذیری پایین در محیط کپسوله	–
ترافیک	جریان	[۱۲]و[۱۳]و[۱۴]	فراداده ها– بار پردازشی کم و مقایس پذیری بالا اندازه گیری از فناوری کلاسیک کاربرد پذیری پایین در محیط کپسوله	–
ترافیک	جریان	[۶]	فراداده ها– بار پردازشی کم و مقایس پذیری بالا اندازه گیری از فناوری کلاسیک (شبکه حامل در مقیاس بالا)	✓
تحلیل سری زمانی	پیش بینی مدل	[۱۹]و[۲۰]و[۲۱]و[۲۲]	پیش بینی تغییرات پیچیده سری زمانی فراداده ها– بار پردازشی و مقایس پذیری بالا اندازه گیری از فناوری پیچیده کاربرد پذیری بالادر محیط کپسوله	✓
تحلیل سری زمانی	بدون پیش بینی مدل	[۲۳]و[۲۴]و[۲۵]و[۲۶] [۲۷]و[۲۸]و[۲۹]	فراداده ها– بار پردازشی کم و مقایس پذیری بالا اندازه گیری از فناوری کلاسیک کاربرد پذیری پایین در محیط کپسوله تحلیل شباهت ها از طریق خود همبستگی ساده و سریع بدون پیش بینی	✓

۵-نتیجه گیری:

در این مطالعه، یک روش تشخیص ناهنجاری مبتنی بر جریان‌های ترافیک سری زمانی پیشنهاد شده است. ابتدا، جریان‌های ترافیک با استفاده از سیستم پیاده‌سازی شده به نام Fast Proxy سنتز می‌شوند که می‌تواند جریان‌های ترافیک را به جریان‌های منفرد با دانه‌بندی بسیار دقیق تجزیه کند و ناهنجاری‌ها را در جریان‌های تجزیه شده بر اساس یک تحلیل همبستگی ساده و پیکربندی آستانه پویا تشخیص دهد. روش پیشنهادی، ناهنجاری‌های ناشی از خرابی سرویس را با دقت تقریباً ۱۰۰٪ تشخیص می‌دهد و حتی در موارد تشخیص دشوارتر، مانند نوسانات کوچک ترافیک یا شرایط پر سر و صدا، به دقتی حدود ۸۰٪ تا ۹۰٪ دست می‌یابد. بر اساس رمزگذاری تصویر دیجیتال و یک سیستم نرم‌افزاری یکپارچه و ماژولار را طراحی و پیاده‌سازی می‌کند. این سیستم با موفقیت فرآیند پیچیده را به پنج ماژول اصلی تجزیه می‌کند. رمزگذاری صدا، رمزگذاری تصویر، تأیید حمله، بازیابی تصویر و مقایسه نتایج، که به طور قابل توجهی عملکرد و قابلیت نگهداری سیستم را بهبود می‌بخشد. هسته سیستم یک طرح رمزگذاری را اتخاذ می‌کند و تبدیل فوریه کسری را ترکیب می‌کند و به طور موثر امنیت و قابلیت ضد حمله پنهان‌سازی اطلاعات را از طریق رمزگذاری دوگانه افزایش می‌دهد. در عین حال، یک سیستم تأیید و ارزیابی شامل چندین روش حمله، همراه با شاخص‌های ارزیابی کیفیت صدای عینی، ایجاد شده است تا به تجزیه و تحلیل کمی علمی از استحکام الگوریتم دست یابد. رابط کاربری گرافیکی توسعه‌یافته، کل فرآیند را از رمزگذاری، رمزگذاری، حمله تا بازیابی به طور کامل نشان می‌دهد و به طور شهودی اثربخشی و امکان‌سنجی راه حل را تأیید می‌کند. نتایج تجربی نشان می‌دهد که طرح پیشنهادی دارای امنیت بالا و استحکام قوی است و یک راه حل موثر برای پنهان‌سازی اطلاعات ایمن و قابل اعتماد ارائه می‌دهد.

مراجع:

[1] V. Dankan Gowda, A. PolaJ. R. Hershey, Z. Chen, J. Le Roux, and S. Watanabe, “Deep clustering: discriminative embeddings for segmentation andseparation,” in International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2022
DOI: https://doi.org/10.4018/979-8-3373-0330-7.ch008

[2] Z. Wang, J. Le Roux, and J. R. Hershey, “Multi-channel Deep Clustering: Discriminative spectral and spatial embeddings for speaker-independent speech separation,” in International Conference
on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2023.

[3] Akhtar, M.S., Ekbal, A., Cambria, E.: How intense are you? predicting intensities of emotions and entiments using stacked ensemble [application notes]. IEEE Computational Intelligence Magazine 15(1), 64–75 (2020)

[4] M. Alajeely, R. Doss, and A. Ahmad, “Routing Protocols in Opportunistic Networks – A Survey,” *IETE Tech. Rev.*, vol. 35, no. 4, pp. 369–387, 2018.
DOI: https://doi.org/10.1080/02564602.2017.1304834

[5] K. Ahmad, M. Fathima, M. S. Hossen, J. Ahamed, and K. A. Bin Ahmad, “Opportunistic Networks: An Empirical Research of Routing Protocols and Mobility Models,” *SN Comput. Sci.*, vol. 4, no. 5, p. 652, 2023.
DOI: https://doi.org/10.1007/s42979-023-02054-y

[6] Alhussan, A., M. Talaat, F., El-kenawy, E.S., Abdelhamid, A., Ibrahim, A., Khafaga, D., Alnaggar, M.: Facial expression recognition model depending on optimized support vector machine. Computers, Materials and Continua 76, 499–515 (06 2023).
https://doi.org/10.32604/cmc.2023.039368

[7] R. Dalal, M. Khari, J. P. Anzola, and V. Garcia-Diaz, “Proliferation of Opportunistic Routing: A Systematic Review,” *IEEE Access*, vol. 10, pp. 5855–5883, 2022.
DOI: https://doi.org/10.1109/ACCESS.2021.3136927

[8] Li, H., Wang, N., Yang, X., Wang, X., Gao, X.: Towards semi-supervised deep facial expression recognition with an adaptive confidence margin. 2022 IEEE/CVFConference on Computer Vision and Pattern Recognition (CVPR) pp. 4156–4165 (2022), https://api.semanticscholar.org/CorpusID:247618790

[9] Li, S., Deng, W.: Reliable crowdsourcing and deep locality-preserving learning for unconstrained facial expression recognition. IEEE Transactions on Image Processing 28(1), 356–370 (2019). https://doi.org/10.1109/TIP.2018.2868382

[10] Liu, F.: Artificial intelligence in emotion quantification : A prospective verview. CAAI Artificial Intelligence Research 3, 9150040 (2024). https://doi.org/10.26599/AIR.2024.9150040, https://www.sciopen.com/article/10.
26599/AIR.2024.9150040

[11] S. Esmaeili and J. Ghasemi, "A location-aware covert communication protocol in inter-environmental communication applications," *Alexandria Eng. J.*, vol. 123, pp. 592–609, 2025.
DOI: https://doi.org/10.1016/j.aej.2025.03.087

[12] Liu, F., Wang, H.Y., Shen, S.Y., Jia, X., Hu, J.Y., Zhang, J.H., Wang, X.Y., Lei,Y., Zhou, A.M., Qi, J.Y., Li, Z.B.: Opo-fcm: A computational affection based occpad-ocean federation cognitive modeling approach. IEEE Transactions on Computational Social Systems 10(4), 1813–1825 (2023). https://doi.org/10.1109/
TCSS.2022.3199119

[13] E. H. Houssein, M. R. Saad, Y. Djenouri, G. Hu, A. A. Ali, and H. Shaban, "Metaheuristic algorithms and their applications in wireless sensor networks: review, open issues, and challenges," *Cluster Comput.*, vol. 27, no. 10, pp. 13643–13673, 2024.
DOI: https://doi.org/10.1007/s10586-024-04619-9

[14] D. Bahrepour, N. Evaznia, and T. Khodabakhshi, "A New Resource Allocation Method Based on PSO in Cloud Computing," *Int. J. Web Res.*, vol. 7, no. 2, pp. 13–21, 2024.
DOI: https://doi.org/10.22133/ijwr.2024.457539.1216

[15] Liu, H., Cai, H., Lin, Q., Li, X., Xiao, H.: Adaptive multilayer perceptual attention network for facial expression recognition. IEEE Transactions on Circuits and Systems for Video Technology 32(9), 6253–6266 (2022)

[16] N. Evaznia, R. Ebrahimi, and D. Bahrepour, "An Energy-Aware Approach to Virtual Machine Consolidation Using Classification and the Dragonfly Algorithm in Cloud Data Centers," *J. Inf. Syst. Telecommun.*, vol. 12, no. 48, pp. 280–290, 2025.
DOI: https://doi.org/10.61186/jist.48021.12.48.280

[17] Ngwe, J.L., Lim, K.M., Lee, C.P., Ong, T.S., Alqahtani, A.: Patt-lite: Lightweight patch and attention mobilenet for challenging facial expression recognition. IEEE Access 12, 79327–79341 (2024). https://doi.org/10.1109/ACCESS.2024.3407108

[18] S. Chaurasia and K. Kumar, "EEMOR: Energy Eflicient Metaheuristic Opportunistic Routing Protocol for WSNs.," Adhoc Sens. Wirel. Networks, vol. 55, 2023.
DOI: https://doi.org/10.32908/ahswn.v55.9265

[19] M. Sharifi Sani, S. Iranmanesh, H. Salarian, F. Tubbal, and R. Raad, "Optimizing Energy Efficiency in Opportunistic Networks: A Heuristic Approach to Adaptive Cluster-Based Routing Protocol," *Information*, vol. 15, no. 5, p. 283, 2024.
DOI: https://doi.org/10.3390/info15050283

[20] Y. Zing and N. Zhao, "Routing revolution: strategic applications of meta-heuristic AI in wireless sensor networks—a comprehensive survey," *Multimed. Tools Appl.*, vol. 84, no. 35, pp. 44605–44646, 2025.
DOI: https://doi.org/10.1007/s11042-025-20843-w

[21] S. Chaurasia, K. Kumar, and A. K. Kamboj, "EHRP-WSN: Energy-Efficient Hyperheuristic Routing Protocol for Wireless Sensor Networks," *AEU - Int. J. Electron. Commun.*, vol. 202, p. 156044, 2025.
DOI: https://doi.org/10.1016/j.aeue.2025.156044

[22] J. M. Belman-Flores, D. A. Rodríguez-Valderrama, S. Ledesma, J. J. García-Pabón, D. Hernández, and D. M. Pardo-Cely, "A Review on Applications of Fuzzy Logic Control for Refrigeration Systems," *Appl. Sci.*, vol. 12, no. 3, p. 1302, 2022.
DOI: https://doi.org/10.3390/app12031302

[23] Qian, B., Chen, H., Xu, Y., Wen, Y., Li, H., Xie, Y., Feng, D.D., Kim, J., Bi, L.,Xu, X., He, X., Sheng, B.: Deep contour attention learning for scleral deformation from oct images. The

Visual Computer pp. 1–16 (2024)
[24] She, J., Hu, Y., Shi, H., Wang, J., Shen, Q., Mei, T.: Dive into ambiguity: Latent distribution mining and pairwise uncertainty estimation for facial expression recognition. In: 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). pp. 6244–6253 (2021). https://doi.org/10.1109/CVPR46437.2021.00618
[25] Amirzdeh, M., Hosseini Moradi, S. A., & Ghobadi, N. (2023). Real Time Detection of Multi-Rotor Unmanned Aerial Vehicle Using YOLOv5 Optimized Algorithm. *Journal of Advanced Defense Science & Technology*, *14*(1), 11-22.
[26] M. F. Khan, E. A. Felemban, S. Qaisar, and S. Ali, "Performance Analysis on Packet Delivery Ratio and End-to-End Delay of Different Network Topologies in Wireless Sensor Networks (WSNs)," in *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, IEEE, pp. 324–329, 2013.
DOI: https://doi.org/10.1109/MSN.2013.74