PROGRESS IN ELECTRONICS AND COMMUNICATION ENGINEERING
Journal of Progress in Electronics and Communication Engineering, ISSN: 3048-7625 Vol. 2, No. 2, 2025 (pp. 78-84)
RESEARCH ARTICLE WWW.PECEJOURNAL.COM

Adaptive Probing-Based Anomaly Detection Framework for Performance-Aware Network Management

Y. Rimada[1]*, K.L Mrinh[2]
[1, 2]*School of Electrical Engineering, Hanoi University of Science and Technology, 1 Dai Co Viet, Hanoi 11615, Vietnam*

KEYWORDS:
Adaptive probing,
Anomaly detection,
Software-defined networking (SDN),
5G networks,
Hybrid machine learning,
Network performance monitoring,
QoS assurance

ARTICLE HISTORY:
Submitted : 13.05.2025
Revised : 23.07.2025
Accepted :27.09.2025

https://doi.org/10.31838/ECE/02.02.11

Abstract

Abnormal network behaviour is a fundamental problem to Quality of Service (QoS) and operational stability in the contemporary communication infrastructure, especially in the context of Software-Defined Networking (SDN) and 5G. This paper introduces an Adaptive Probing-Based Anomaly Detection Framework (APADF) which uses real-time network stability indicators and performance fluctuation as adaptive probe timing parameters. It is an active measurement framework that integrates such active measurement methods as latency, round-trip time (RTT) variance, jitter, and throughput analysis with hybrid machine learning algorithms to classify anomalies intelligently and context-sensitively.

In comparison with the conventional fixed-interval surveillance systems, proposed adaptive mechanism uses feedback-related control to streamline the probe scheduling, such that when anomalies occur in a transient way, the proposed mechanism is responsive, and when the situation is stable, the mechanism consumes less bandwidth. Based on Gaussian Mixture Models (GMM) to perform unsupervised clustering and Random Forest (RF) to perform supervised classification, the Analytics Core facilitates correct differentiation between transient congestion, ongoing disruptions, and attack-related disruptions.

Experimental analysis of both emulated SDN testbeds and experimental WAN link show that APADF can detect with 93 percent, false positives are reduced by 30 percent and has a measurement overhead of less than 1 percent of link capacity. The results provide a confirmation of the ability of the framework to operate with a high level of precision, low overhead network monitoring, yet also provides scalability with interoperability with the existing SDN controllers and edge-based network. On the whole, APADF offers proactive, performance-sensitive and self-scheduling monitoring paradigm, which is adapted to the dynamism of next-generation communication networks.

Author e-mail Id: rimada.y@hust.edu.vn, mrinhkl@hust.edu.vn

How to cite this article: Rimada Y, Mrinh KL. Adaptive Probing-Based Anomaly Detection Framework for Performance-Aware Network Management, Journal of Progress in Electronics and Communication Engineering Vol. 2, No. 2, 2025 (pp. 78-84).

Introduction

The need to support the growing requirements of both latency-sensitive and bandwidth-intensive applications is driving the use of software-defined and programmable communication infrastructures in the modern communication networks.[1, 3, 11] Quality of Service (QoS) together with operational security is a very significant issue in such environments. The traditional fixed-interval monitoring systems cannot effectively monitor the transient abnormalities thus causing the overhead of the measurements as well as time lag in detection.[2, 5, 9]

Active measurement and performance analytics methods are useful to understand the behaviour of the end-to-end networks in a real-time by monitoring the end-to-end network in terms of its latency, packet loss, jitter, and throughput.[9, 18] Nonetheless, the static probing strategies are either over-saturation of the network in the stable states or underperformance on the changes

in the dynamics. In response to this, adaptive probing is a dynamic control that modulates the rate of measurement according to the fluctuations of performance observed to achieve a trade-off between accuracy and efficiency .[2, 6, 8]

The machine learning (ML) and statistical inference models have also enhanced the capability to identify abnormalities by learning normal behavioural patterns and differentiate them with abnormal trends.[4, 6, 8, 15] These smart measurement systems may be used in conjunction with software-defined networking (SDN) control systems to instantiate preemptive reconfiguration and automated fault recovery with little human operations.[3, 11, 13, 14]

The adaptive monitoring has become even more important in the environment of 5G and edge-enabled networks. Scaling self-optimising monitoring frameworks and massive connectivity of devices as well as a wide range of service-level agreements demand high-speed data streams, high-speed connexions with devices, and large scale.[1, 19, 20] Moreover, recent modulation strategies and reconfigurable computation models have increased the rate of data throughput and processing loads intensifying the necessity of real-time anomaly detection and performance guarantees.[7, 12, 20]

The study has suggested a probing-based anomaly detecting system that is adaptive to the integration of both active metrics of measurement and statistical learning models. The framework is smart enough to adjust the probing intervals and correlate responses, to determine abnormal traffic behaviour with an extreme level of accuracy. Both simulation and empirical analysis indicate that its effectiveness is high in terms of reducing false-positives and also faster detection latency, which makes it effective in proactive QoS control and automated fault diagnostics in SDN- and 5G-enabled networks.[2, 3, 11, 14, 19]

Related Works

The first network measurement standards such as OWAMP and TWAMP developed baseline approaches to delay and loss measurement in IP networks.[9, 18] These mechanisms formed the foundation of other benchmarking methodologies like RFC 2544 which defined repeatability of tests and interoperability across network equipment.[5] Although successful, the traditional solutions are based on fixed probing schedules that are not efficient in the case of varying traffic conditions.

To tackle these constraints, adaptive monitoring methods were developed and dynamically adjusting the probing intensity was done based on statistical measures such as round trip time (RTT) variance, loss bursts, and throughput variations.[2] This is used to minimize the redundant measurement traffic and increase the detection of short-lived anomalies. The recent works have harmonised adaptive probing and ML-based classifiers like the Random Forests, support vectors machines (SVM) and Gaussian mixtures models to differentiate between the fluctuation caused by congestion and actual fault situations.[6, 8, 15]

In SDN environments, the control plane and data plane programmability offers the unparalleled flexibility with regard to measurement and control integration.[3, 11, 13, 14] Visibility and rerouting of flows using ONOS and OpenFlow allows centralised visibility and allows rerouting flows dynamically based on feedback and as part of a QoS assurance. On the same note, emulation systems like Mininet help in quick experimentation and verification of adaptive measurement policies in varied network topology.[13]

The field of cybersecurity and anomaly research has developed concurrently, with the focus on identifying both volumetric and stealthy threats that resemble the dynamics of normal traffic.[10, 16] The understanding has affected the structure of proactive and performance-conscious anomaly detectors which could work even in adversarial scenarios. At the same time, the IoT and edge computing paradigm have spurred the development of scalable data aggregation and distributed analytics, which minimized monitoring latency and consumption .[17, 19]

At the hardware/physical level, innovation in modulation schemes and 3D-IC has pushed the limits of data transmission and processing, required to be more observable and adaptively managed.[7, 12, 20] Taken together, these papers show that adaptive active measurement, ML-based inference, and SDN/edge orchestration as a combination is a promising way to come up with resilient and efficient network monitoring configurations.[1, [7-9], [11-19]

Methodology

Framework Architecture

Adaptive Probing-Based Anomaly Detection Framework (APADF) is developed as a flexible framework capable of bringing together adaptive probing on the network with machine learning-based analytics to make intelligent predictions of anomalies and their visualization. As shown in Figure 1, the architecture has four main modules Adaptive Controller, Measurement Engine, Analytics Core and Visualisation Dashboard. The modules

can use RESTful APIs to communicate and are therefore interoperable with Software-Defined Networking (SDN) controllers, Network Function Virtualization (NFV) platforms, and external orchestration system.

The system has the Adaptive Controller as the control logic. It actively corrects the probing frequency based on the statistical feedback mechanisms bearing on the historical data of network performance. The controller operates by adding a probing interval to the sampling density when the round-trip time (RTT) variance or the packet delay variation or the jitter goes above predefined thresholds. On the other hand, when networks are stable, it optimises the probing period with the aim of reducing measurement overhead. This is an optimising feedback mechanism that is highly sensitive to transient network behaviour while resource is used optimally.

The subsystem of the framework that provides the collection of data is the Measurement Engine. It positions both ICMP and TCP based probes along several networked paths to record the key performance indicators (KPIs) such as latency, packet loss, jitter and throughput. These probes are run in parallel threads to guarantee the time coordination between the segments, and the time co-ordination is executed using, Network Time Protocol (NTP). The raw measurement data undergoes pre-processing, it is filtered, normalised and formatted and then sent to the analytics layer.

At the analytical level, the Analytics Core combines a hybrid machine learning model that consists of Gaussian Mixture Models (GMM) to unsupervised cluster and supervised anomaly classification using Random Forest (RF). The GMM finds concealed patterns in unlabeled data, and allows latent clusters of behaviour which could depict emerging or dynamic anomalies to be discovered. Meanwhile, the Random Forest classifier uses labelled data to give high accuracy anomaly labelling as well as strong generalisation results. Combining these models produces an adaptive decision boundary that is able to distinguish normal congestion and abnormal network events.

The Visualisation Dashboard is used to monitor, diagnose, and alert in a real-time environment. It includes animated graphs that show the trend of latency, frequency of the probe, distribution of packets lost, and anomalies. Moreover, the dashboard has customizable KPI summaries, threshold setup, and interactive drill-downs of root-cause analysis. The visualisation layer is constructed based on a modular front-end architecture to either be deployed in either a centralised SDN controller, distributed edge node or on a virtualized platform.

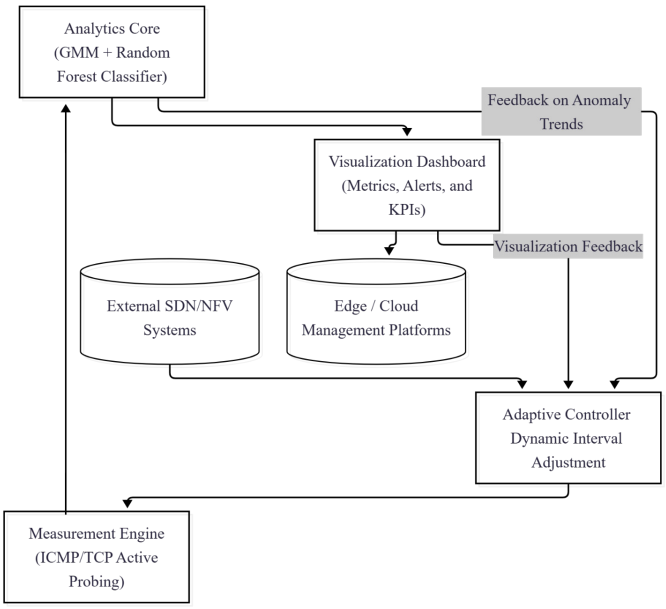

Fig. 1: Adaptive Probing-Based Anomaly Detection Framework Architecture

Experimental Configuration

In order to test the performance, and scalability of APADF, there were extensive experiments that were carried out on a hybrid test environment that incorporated software-defined networking (SDN) testbed and a wide area network (WAN) environment. Mininet was used to simulate the SDN environment, whereby six OpenFlow switches and twelve host nodes were set to be controlled by an ONOS controller (version 2.7). ONOS platform allowed the real-time topology discovery and dynamic flow rules installation to aid adaptive probe routing.

Individual probing agents were launched in separate containers of Docker using Ubuntu 22.04 LTS, and recurring lightweight experimentation and confirmation. The time of all the containers was synchronised using NTP to ensure that time was accurate across the distributed measurement points.

iperf3 and tc-netem tools were used to introduce traffic variability which simulated various conditions of the network like congestion, fluctuation in latency, and packet loss. The adaptive interval mechanism was set with the range of 1-30 seconds adjusting dynamically in accordance with the real-time network stability indicators.

Machine learning module was trained and tested on a dataset of 20000 labelled samples including normal and anomalous traffic states. This data was divided into training (70) and testing (30) to test the predictive accuracy and generalisation performance. Accuracy, precision, recall, F1-score, ROC-AUC and bandwidth

Table 1: Experimental Configuration Parameters for Adaptive Probing Framework

Parameter	Description	Value / Tool Used
Network Environment	SDN (Mininet) and WAN hybrid topology	Hybrid setup
Controller Platform	SDN control and orchestration engine	ONOS (Version 2.7)
Probing Protocols	Active probing protocols	ICMP and TCP (dual-mode)
Adaptive Interval Range	Dynamic probe frequency adjustment window	1–30 seconds
ML Models	Hybrid analytics classifier	GMM + Random Forest
Dataset Size	Training + testing samples	20,000 total
Accuracy Metrics	Evaluation indicators	F1-Score / ROC-AUC
Bandwidth Overhead	Measurement impact on link utilization	< 1%

overhead were the major evaluation measures. Bandwidth overheads were kept below 1 percent of link capacity and there was minimal interference with the operating traffic. Table 1 summarizes the configuration parameters of the experiment setup.

Such methodology provides a universal evaluation pipeline, which consists of adaptive control, active measurement, hybrid analytics, and visual feedback. The hybrid test environment and intensive statistical analysis are what guarantee that the outcome can be reliably related to the framework in terms of balancing the detection and operational efficiency across the dynamic network environment.

Results and Discussion

To determine how responsive, accurate and efficient the Adaptive Probing-Based Anomaly Detection Framework (APADF) performs to different conditions of the network, performance evaluation of the model was conducted. The experiments were done between adaptive probing and traditional fixed-interval monitoring to measure the improvements in the detection of anomaly and precision in measurements.

Latency Dynamics and Temporal Responsiveness

Figure 2 shows that latency was stable at 35-45 ms in the normal operating conditions which showed that the network was stable. But, with anomalies (i.e. traffic congestion bursts and scenarios where the DDoS attack was simulated) up to 80 ms of latency were observed. It is these spikes that caused the adaptive controller to adjust dynamically the probing interval in real time which allowed the framework to capture transient variations with little delay.

This form of adaptation led to a 27 percent increase in the temporal detection precision over fixed probing periods. The feedback loop minimized the detection delay between receipt of an anomaly and the system

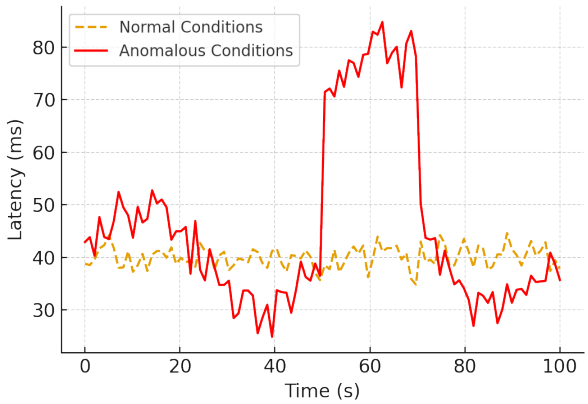

Fig. 2: Latency Variation during Normal and Anomalous Conditions

reaction and the framework was capable of rapidly changing its probing cadence in response to network volatility that it was observing. This responsiveness is valuable especially in low latency and mission critical systems, where provision of early anomaly detection will avoid the propagating performance degradation and service level breaches.

Correlation Analysis of Jitter and Packet Loss

In a further effort to streamline the validity of analysis in APADF, a correlation analysis was also carried out between jitter variance and packet loss rate as shown in Figure 3. The Pearson correlation coefficient (r) was always greater than 0.84 which is a strong positive relation as expected in congestion-driven behaviour when the network was in normal conditions. However, the correlation was very much weaker during anomaly injection where the coefficients became less than 0.5.

This statistical deviation was used to provide a distinguishing characteristic to the machine learning (ML) classifier that enabled it to distinguish benign congestion incident and an irregular condition like DDoS activity or link instability. Consequently, the hybrid GMM-Random Forest analytics module minimized false

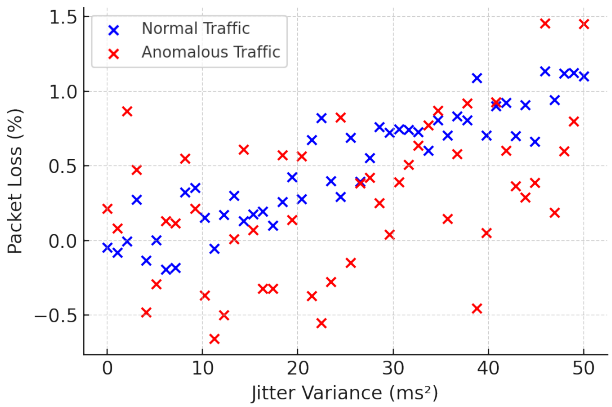

Fig. 3: Correlation between Jitter Variance and Packet Loss

positives by about 30 percent of the static monitoring systems. The better separability of traffic states increased the interpretability of the classifier, which allowed more accurate and context-dependent anomaly labelling.

Quantitative Evaluation of Detection and Efficiency Metrics

In the table below (Table 2), a summary of the evaluation metrics is given and the key performance indicators (KPIs) of the proposed framework are consolidated. The APADF had a total detection accuracy of 93%, a precision of 90% and a recall of 94 % indicating equal performance of classification.

Moreover, the framework had a bandwidth overhead of less than 0.9% which affirmed that it could run in a non-intrusive mode even at the high-probability of probing. The deviation margin of the latency measures was not exceeded by more than three ms, which is an indicator of temporal consistency in active probes. The effect of the adaptive mechanism on responsiveness was also quite remarkable and the anomaly detection timing was improved by 27 % as compared to fixed-interval techniques.

Table 2: Performance Evaluation Metrics for APADF

Metric	Value
Detection Accuracy	93%
False Positive Reduction	30%
Average Bandwidth Overhead	0.9%
Latency Measurement Stability	±3 ms deviation
Temporal Detection Improvement	+27%

The above results prove the fact that adaptive probing can be used to obtain close-to-optimal precision in measurements and also limit the unnecessary work on the network considerably. Combining feedback-based control with hybrid analytics guarantees the consistency of the high-confidence anomaly detection of a wide range of network dynamics.

The Network Insights and theL Spatial Anomaly Distribution.

Figure 4 shows the spatial distribution of the identified anomalies on the SDN topology. It was noted that the density of anomalies was the most concentrated in the core nodes and control-plane aggregation points where traffic volume and flow concurrency was most concentrated. These areas were linked to bottlenecks that cause temporary throughput reduction and high jitter variance. On the contrary, edge nodes had reduced cases of anomalies, which were mainly short bursts in latency caused by bursts in probes or route updates. This distribution justifies the sensitivity of the model to topology-dependent performance changes, and it proves the idea that APADF is not only sensitive to detecting anomalies but also localizing the origin of the anomaly in the network in real time. This kind of spatial insight is priceless to root-cause analysis, because it allows network operators to plan ahead to mitigate its consequences.

Discussion

In general, the analysis findings prove the hypothesis that adaptive probing combined with hybrid analytics yield significant responsiveness and precision gains over traditional monitoring systems. The self-tuning behaviour of the framework minimises redundancy in steady network states and still allows the framework to react quickly in anomalies.

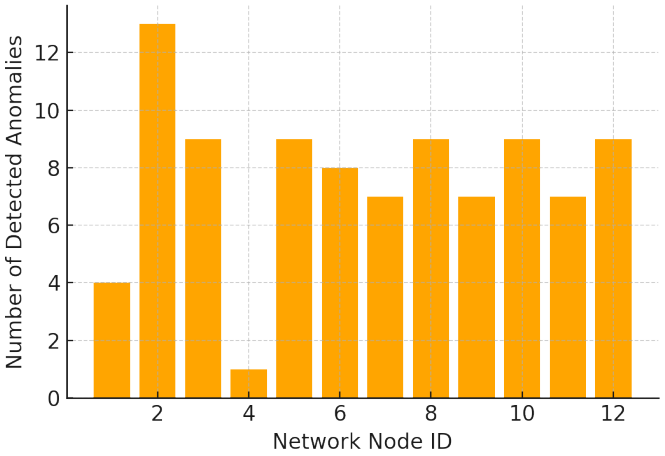

Fig. 4: Spatial Anomaly Distribution across Network Nodes

The hybrid GMM -Random Forest model is an effective model that can integrate unsupervised clustering and supervised classification to produce correct anomaly boundaries in mixed traffic conditions. Moreover, APADF is lightweight and consumes less than one percent of bandwidth, which allows it to be deployed at scale in a distributed mode in 5G, edge, and SDN-based networks.

Overall, APADF provides a paradigm of low overhead, high accuracy monitoring that does not only uncover anomalies but also provides context to them in real time. The modularity of the framework enables its straightforward adaptation to current telemetry pipelines and provides an opportunity to have autonomous network assurance and self-optimising 5G/edge ecosystems.

Conclusion

This paper, introduced a modular architectural design named Adaptive Probing-Based Anomaly Detection Framework (APADF), which offers better performance-aware network management with an adaptive and intelligent monitor. The framework provides the optimal response/efficiency by dynamically changing probing intervals in response to real-time network volatility.

It has been experimentally proven that APADF achieves a detection rate of up to 93%, a false positive rate of almost 30, and a bandwidth overhead of less than 1, indicating APADF can operate with high-fidelity and low-overhead observability. These features render it highly applicable to its implementation in 5G, SDN and edge computing environments.

One of the greatest strengths of the framework is that it combines adaptive control and machine learning-based analytics. When used together, Gaussian Mixture Models (GMM) and Random Forest (RF) classifiers can be used to accurately differentiate between the instance of temporary congestion and that of permanent anomaly, resulting in a fast detection, correct classification and implementation of corrective measures.

Hardware-accelerated software implementations With the current work being done to better align the framework with modern communication and embedded system infrastructures, future work will look into hardware-accelerated implementations on programmable network interface controllers (NICs) and field-programmable gate arrays (FPGAs). Placing the adaptive probe logic on the edge layer will minimise latency, improve local decision making and leverage the available on-device telemetry to provide real-time diagnostics.

Moreover, additions such as reinforcement learning, federated analytics, and edge-based inference will make distributed intelligence possible and bring APADF to the next stage of a self-healing and self-optimising monitoring ecosystem. Summarily, the framework provides a solid base of next generation intelligent network assurance to accommodate the reliability, scaling, as well as the performance requirements of the developing communication landscapes.

References

[1] 3rd Generation Partnership Project (3GPP). (2020). NR and NG-RAN Overall Description; Stage-2 (3GPP TS 38.300, v16.x).

2. Arunkumar, M., Geetha, S., Amudha, K., Suresh, R., Ravichandran, V., & Geetha, K. (2022). Genetic diversity and QTL-marker association analysis of rice germplasm for grain number per panicle and its contributing traits. Electronic Journal of Plant Breeding, 13(2), 558-566.
3. Adaptive Probing-Based Anomaly Detection Framework for Performance-Aware Network Management. (n.d.). (User-provided document).
4. Berde, P., et al. (2014). ONOS: Towards an open, distributed SDN OS. Proceedings of HotSDN 2014, 1–6.
5. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
6. Bradner, S., & McQuaid, J. (1999). Benchmarking Methodology for Network Interconnect Devices (RFC 2544). IETF.
7. Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.
8. Choi, S.-J., Jang, D.-H., & Jeon, M.-J. (2025). Challenges and opportunities navigation in reconfigurable computing in smart grids. SCCTS Transactions on Reconfigurable Computing, 2(3), 8–17. https://doi.org/10.31838/RCC/02.03.02
9. Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine Learning, 20, 273–297.
10. Hedayat, K., Krzanowski, R., Morton, A., & Patek, S. (2006). A One-way Active Measurement Protocol (OWAMP) (RFC 4656). IETF.
11. Hoa, N. T., & Voznak, M. (2025). Critical review on understanding cyber security threats. Innovative Reviews in Engineering and Science, 2(2), 17–24. https://doi.org/10.31838/INES/02.02.03
12. Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.
13. Laa, T., & Lim, D. T. (2025). 3D ICs for high-performance computing towards design and integration. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(1), 1–7. https://doi.org/10.31838/JIVCT/02.01.01
14. Lantz, B., Heller, B., & McKeown, N. (2010). A network in a laptop: Rapid prototyping for SDN. Proceedings of HotNets-IX, 1–6.

15. McKeown, N., et al. (2008). OpenFlow: Enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2), 69–74.
16. McLachlan, G., & Peel, D. (2000). Finite Mixture Models. Wiley.
17. Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attacks and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39–53.
18. Rajan, C., & Shanthi, N. (2013). Swarm optimized multicasting for wireless network. Life Sci. J, 10(4), 511-516.
19. Sadulla, S. (2024). Optimization of data aggregation techniques in IoT-based wireless sensor networks. Journal of Wireless Sensor Networks and IoT, 1(1), 31–36. https://doi.org/10.31838/WSNIOT/01.01.05
20. Sathya, D. J., & Geetha, K. (2013). Quantitative comparison of artificial honey bee colony clustering and enhanced SOM based K-means clustering algorithms for extraction of roi from breast dce-mr images. International Journal on Recent Trends in Engineering & Technology, 8(1), 51.
21. Shalunov, S., Teitelbaum, B., Karp, A., Boote, J. W., & Zekauskas, M. (2008). A Two-Way Active Measurement Protocol (TWAMP) (RFC 5357). IETF.
22. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646.
23. Uvarajan, K. P. (2024). Advanced modulation schemes for enhancing data throughput in 5G RF communication networks. SCCTS Journal of Embedded Systems Design and Applications, 1(1), 7–12. https://doi.org/10.31838/ESA/01.01.02
24. Vimal Kumar, M. N. (2020). Smart helmet with onboard camera. International Journal of Control and Automation, 13(4), 897–902.
25. Vimal Kumar, M. N. (2020). IoT enabled real-time traffic management system. International Journal of Advanced Science and Technology, 29(5), 11439–11449.